Mitigating Jamming Attacks Using Energy Harvesting

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

***Abstract*—The use of energy harvesting as a counter-jamming measure is investigated on the premise that part of the harmful interference can be harvested to increase the transmit power. We formulate the strategic interaction between a pair of legitimate nodes and a malicious jammer as a zero-sum game. Our analysis demonstrates that the legitimate nodes are able to neutralize the jammer. However, this policy is not necessarily a Nash equilibrium and hence is sub-optimal. Instead, harvesting the jamming interference can lead to relative gains of up to 95%, on average, in terms of Shannon capacity, when the jamming interference is high.**

***Index Terms*—Energy harvesting, jamming, game theory**

I. Introduction

In recent years, the simultaneous wireless information and power transfer has gained momentum in the realm of energy harvesting (EH) technologies. In this contribution, we focus on systems employing a time-splitting EH approach [1]–[4], i.e., during a first phase the receiver collects energy from RF microwave radiation and in a second phase it uses the harvested energy for data transfer.

An interesting application of such EH approaches arises for wireless systems under jamming attacks. In the past, two main counter-jamming approaches have been commonly considered: direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS), [5], [6]. More recently, the use of multiple antennas has been exploited in [7] against both jamming and eavesdropping. In the first two approaches, the impact of power constrained jammers can be limited by increasing the spectral resources because the optimal jamming strategy is to spread the jamming power over the entire bandwidth; whereas the former requires an increased number of antennas. In the present work, we alternatively explore the possibility of mitigating jamming attacks by using EH *without increasing the spectral or the spatial resources*. So far, there has only been a limited number of contributions in this area [8]–[11].

In [8], the jamming interference is harvested and exploited in a two-way channel assuming that the jammer's policy is fixed (i.e., the jammer is not strategic). Furthermore, in [9] a cooperative relay wiretap channel is studied, in which the helping nodes harvest energy from the legitimate link and then generate interference to the eavesdropper. On the other hand, in [11], it is shown that EH can be exploited to mitigate jamming attacks in wireless secret key generation (SKG) systems and that it is possible to neutralize the jammer, i.e., to fully compensate its impact on the SKG rate. Building on this idea, the objective of the present work is to investigate whether EH at the legitimate transmitter can be an efficient measure against jamming attacks. We investigate the strategic interaction between a pair of legitimate nodes and a jammer employing as utility function the Shannon capacity.

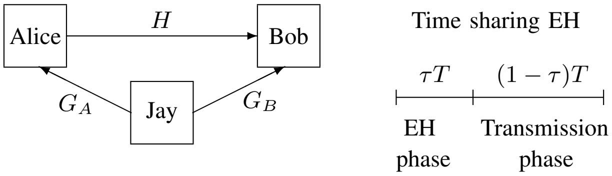

Fig. 1. System model and time sharing scheme at Alice's side.

The main contributions of this paper can be summarized as follows. First, we demonstrate that the jamming attack can be prevented entirely by adjusting the EH duration, i.e., the jammer can be neutralized (or forced to remain silent). This is only possible when the quality of the channel in the harvesting link is higher than in the jamming link. Nevertheless, neutralizing the jammer imposes too stringent restrictions on the EH duration and on the legitimate transmit power and hence is not optimal.

Second, we formulate a zero-sum game between the legitimate users and the jammer and derive the Nash equilibrium (NE) analytically. At the NE, both players transmit at full power, while, the optimal EH duration depends on the system parameters. Interestingly, we show that the NE always outperforms neutralizing the jammer. At the NE, the jamming interference is not fully cancelled but rather exploited, particularly efficient in the high jamming interference regime.

This work represents a proof of concept of the potential use of EH against jamming attacks, relying on widely used system model assumptions [1]–[3], [5], [6], [10], [11]. Demonstration of the proposed EH policy in a real testbed is left as future work, in which the effect of imperfect channel estimation, type I and II jamming detection errors, implementation aspects of EH, etc., will also be considered.

II. System model

The system model, depicted in Fig. 1, comprises three nodes: a legitimate transmitter, Alice, its intended receiver, Bob, and a malicious jammer, Jay. The channel coefficients in the links Alice-Bob, Jay-Alice and Jay-Bob are denoted by H, G_A and G_B, respectively and model fading; they are assumed to remain constant during each EH and transmission

The authors are with ETIS, UMR 8051, Université Paris Seine, Université Cergy-Pontoise, ENSEA, CNRS, France; emails: {gada.rezgui, belmega, arsenia.chorti}@ensea.fr.

cycle and to change independently from one cycle to the next. We assume that full channel state information is available at all nodes.

When Alice sends a message X_A to Bob, Jay can jam the transmission. Bob's observation Y_B can be expressed as:

$$Y_B \quad = \quad HX_A + G_B X_J + Z_B, \tag{1}$$

where the message $X_A \sim \mathcal{N}(0,p)$ is drawn from a Gaussian codebook under a short-term power constraint $0 \leq p \leq P$. Finally, $Z_B \sim \mathcal{N}(0, N_B)$ models the effect of the additive white Gaussian noise (AWGN) in the Alice-Bob link. We consider that Jay transmits Gaussian jamming signals $X_J \sim \mathcal{N}(0,\gamma)$ and $0 \leq \gamma \leq \Gamma$ represents the jamming power.

This paper studies whether EH can be exploited to harvest the jamming interference and boost the transmit power. We assume a time sharing scheme with two phases: the first phase of duration τT, where T is the symbol period, is dedicated to EH. The second phase of duration $(1-\tau)T$ is dedicated to information transmission.

Alice's observation during the EH phase is then given by:

$$Y_A \quad = \quad G_A X_J + Z_A, \tag{2}$$

where $Z_A \sim \mathcal{N}(0, N_A)$ models the effect of AWGN noise in the link Jay-Alice. As commonly assumed [2], the harvested energy is proportional to the energy of the received signal:

$$E = \tau T \zeta \mathbb{E}\left[|Y_A|^2\right] = \tau T \zeta \left(\gamma |G_A|^2 + N_A\right), \tag{3}$$

where $\zeta \in [0,1]$ is the harvesting efficiency parameter. The average power harvested during the EH phase is used in the information transmission phase and is given as follows:

$$p^{EH} \quad = \quad \frac{\tau}{1-\tau}\zeta\left(\gamma|G_A|^2 + N_A\right). \tag{4}$$

The multiplicative term $\frac{1}{1-\tau}$ in the above expression stems from keeping the energy constant during each transmission phase of duration $(1-\tau)T$ [11]. The initially available transmit power (aside from the harvested one) is also enhanced to $\frac{p}{1-\tau}$ for the same reason. Under the above assumptions and using standard time sharing arguments [12], the Shannon capacity of the Alice-Bob link is given by

$$C^{EH}(p,\tau,\gamma) = \frac{(1-\tau)}{2}\log\left(1 + \frac{\left(\frac{p}{1-\tau} + p^{EH}\right)|H|^2}{\gamma|G_B|^2 + N_B}\right). \tag{5}$$

Note that the multiplicative term $(1-\tau)$ in front of the logarithm represents the reduction of the Shannon capacity due to time sharing.

III. Jammer Neutralization

In this Section, we first investigate whether it is possible to neutralize the jammer. We note that C^{EH} is increasing with the transmit power p for fixed τ and γ. On the other hand, C^{EH} is not necessarily decreasing with the jamming power: since the interference is harvested and p^{EH} increases with γ, the Shannon capacity may even increase with the interfering power γ for specific system parameters. Although this may seem counter-intuitive, consider the case in which the interfering link is very poor $|G_B|^2 << 1$ (e.g., Jay is very far from Bob). In this case, the interference at Bob is negligible: $\gamma|G_B|^2 + N_B \simeq N_B$ and, hence, C^{EH} increases with γ due to p^{EH}. We prove this result rigorously by investigating the first-order derivatives of C^{EH}.

Proposition 1: For fixed p and τ, if $\frac{|G_A|^2}{N_A} > \frac{|G_B|^2}{N_B}$, then $C^{EH}(p,\tau,\gamma)$ is monotonically increasing w.r.t. γ if $p \leq p_{th}(\tau) \triangleq \tau K$, with $K \triangleq \left(\frac{|G_A|^2 N_B}{|G_B|^2} - N_A\right)\zeta$, and it is monotonically decreasing w.r.t. γ if $p > p_{th}(\tau)$. This implies:

$$\arg\max_{\gamma\in[0,\Gamma]} C^{EH}(p,\tau,\gamma) \quad = \quad 0, \text{ if } p \leq p_{th}(\tau), \tag{6}$$

$$\arg\max_{\gamma\in[0,\Gamma]} C^{EH}(p,\tau,\gamma) \quad = \quad \Gamma, \text{ if } p > p_{th}(\tau). \tag{7}$$

Otherwise, $C^{EH}(p,\tau,\gamma)$ is always monotonically decreasing w.r.t. γ for any fixed p and τ and

$$\arg\max_{\gamma\in[0,\Gamma]} C^{EH}(p,\tau,\gamma) \quad = \quad \Gamma. \tag{8}$$

Intuitively, if the quality of the harvesting link is higher than that of the jamming link $\frac{|G_A|^2}{N_A} > \frac{|G_B|^2}{N_B}$, then the legitimate users can neutralize the jammer by tuning the transmit power p and the EH policy τ such that $p \leq p_{th}(\tau)$. This highlights the existence of a power threshold $p_{th}(\tau)$ below which, harvesting the jamming interference in the first phase overcomes the harmful jamming in the second phase. The optimal strategy (p,τ) that neutralizes the jammer (NJ) is given below.

Theorem 1: If $\frac{|G_A|^2}{N_A} > \frac{|G_B|^2}{N_B}$, the strategy that maximizes the capacity while neutralizing the jammer (p^{NJ},τ^{NJ}) is given as follows:

a) If $p_{th}^{-1}(P) > 1$, then $(p^{NJ},\tau^{NJ}) = (p_{th}(\hat{\tau}),\hat{\tau})$, where $p_{th}^{-1}(p) = \frac{p}{K}$ is the inverse function of $p_{th}(\tau)$.

b) Otherwise, the optimal strategy is

$$\begin{aligned}
(p^{NJ},\tau^{NJ}) \quad &= \quad \underset{(p,\tau)\in\{(p_1,\tau_1),(p_2,\tau_2)\}}{\arg\max} \quad C^{EH}(p,\tau,0),\\
(p_1,\tau_1) \quad &= \quad (\min\{p_{th}(\hat{\tau}),P\}, \min\{\hat{\tau}, p_{th}^{-1}(P)\}),\\
(p_2,\tau_2) \quad &= \quad (P, \max\{\tilde{\tau}, p_{th}^{-1}(P)\}),
\end{aligned}$$

where $\hat{\tau} \in (0,1)$ and $\tilde{\tau} \in (0,1)$ are the unique solutions of the equations

$$\frac{\partial C^{EH}(p_{th}(\tau),\tau,0)}{\partial\tau} = 0 \text{ and } \frac{\partial C^{EH}(P,\tau,0)}{\partial\tau} = 0$$

respectively, which can be easily computed numerically.[1]

Fig. 2 illustrates the Shannon capacity obtained while neutralizing the jammer, $C^{EH}(p^{NJ},\tau^{NJ},0)$, as a function of the signal to interference power ratio (SIR) defined as $SIR = P/\Gamma$ in the range $P/\Gamma = -30$ dB to $P/\Gamma = 10$ dB, for various settings w.r.t. the channels gains for $N_A = -10$ dBm, $N_B = -7$ dBm, $\Gamma = 10$ dBm, $\zeta = 0.8$. These parameters were chosen to showcase the different regimes in terms of the optimal strategies at the NJ and NE states. Nevertheless, all our remarks and observations are general and remain valid irrespective of the specific choice of the system parameters.

[1] Finding explicit expressions for $\hat{\tau}$ and $\tilde{\tau}$ is non trivial and involves solving nonlinear equations containing both logarithmic and fractional terms. Instead, we can exploit numerical methods based on iterative one-dimensional search (e.g., `fzero` in MATLAB®) or methods relying on trust region or Levenberg-Marquardt techniques (e.g., `fsolve` in MATLAB®).

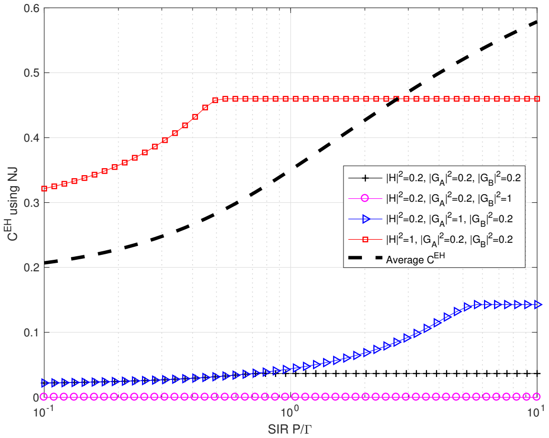

Fig. 2. Shannon capacity while neutralizing the jammer as a function of SIR. The jammer cannot be neutralized if the harvesting link is poor. Transmitting at full power P is not always optimal.

The capacity $C^{EH}(p^{NJ}, \tau^{NJ}, 0)$ is zero for $|H|^2 = 0.2$, $|G_A|^2 = 0.2$, $|G_B|^2 = 1$ since the minimum condition on the harvesting link quality is not met and the jammer cannot be neutralized. In the other settings, we can identify two regimes depending on whether $p_{th}^{-1}(P) \leq 1$ or not. When the SIR is low, the system is in case b) of Theorem 1 and increasing P increases the feasible set of the optimization problem and, hence, the optimal value of the capacity. At higher SIR, the system shifts to case a), in which the optimal solution that neutralizes the jammer no longer depends on P. The dashed black curve depicts the average $C^{EH}(p^{NJ}, \tau^{NJ}, 0)$ over 10,000 random realizations of the channel gains drawn from a standard Gaussian distribution.

We remark that to neutralize the jammer a non-zero EH duration is required, i.e, $\tau^{NJ} > 0$, during which little energy can actually be harvested (as the jammer is silent). Also, the transmit power may be required to be below the maximum available power. In light of this, we next investigate the optimal strategies of both parties in this competitive interaction.

IV. Optimal Strategies: Game Theoretic Analysis

In this Section, we study the adversarial interaction between the legitimate users and the jammer using a non-cooperative game [13]. More specifically, we formulate a two-player zero-sum game defined as the triplet:
$\mathcal{G} = \{\{L, J\}, \{A_L, A_J\}, C^{EH}(a_L, a_J)\}$, where L and J denote the opposing players; $A_L = [0, P] \times [0, 1]$ and $A_J = [0, \Gamma]$ denote the possible actions the two players can take; and $C^{EH}(a_L, a_J)$ is both the utility of L and the cost of J. The strategy of legitimate users is denoted by $a_L = (p, \tau)$ and that of the jammer by $a_J = \gamma$.

A natural solution of the game is the NE, denoted by (a_L^{NE}, a_J^{NE}), which is stable to unilateral deviations:

$$\begin{aligned} C^{EH}(a_L^{NE}, a_J^{NE}) &\geq C^{EH}(a_L, a_J^{NE}), \quad \forall a_L \neq a_L^{NE}, \\ C^{EH}(a_L^{NE}, a_J^{NE}) &\leq C^{EH}(a_L^{NE}, a_J), \quad \forall a_J \neq a_J^{NE}. \end{aligned}$$

Neither the legitimate player nor the jammer have any interest in deviating from the NE state knowing that their opponent is playing the NE strategy.

Proposition 2: The NJ state, $(p^{NJ}, \tau^{NJ}, 0)$ in Theorem 1, is not a NE of the game $\mathcal{G}$.

Proof: If $p_{th}^{-1}(P) > 1$ then $(p^{NJ}, \tau^{NJ}) = (p_{th}(\hat{\tau}), \hat{\tau})$, from Theorem 1. This cannot be a NE, because it implies that $p_{th}(\hat{\tau}) < P$, and since C^{EH} is increasing in p then player L should transmit at maximum power at the NE: $p^{NE} = P$. Otherwise, we have two cases: $(p^{NJ}, \tau^{NJ}) = (P, \max\{\tilde{\tau}, p_{th}^{-1}(P)\})$ and $(p^{NJ}, \tau^{NJ}) = (P, p_{th}^{-1}(P))$. Neither can be NE: since the jammer is silent ($\gamma^{NJ} = 0$) and only the noise N_A is harvested, the legitimate user will deviate from $\tau^{NJ} > 0$ to $\tau = 0$. EH operates as a threat to neutralize the jammer, which results in an inefficient time sharing policy.

The game's NE is given in the following theorem.

Theorem 2: The NE of the game $\mathcal{G}$ is $(p^{NE}, \tau^{NE}, \gamma^{NE}) = (P, \tau^{NE}, \Gamma)$, where $\tau^{NE} \in \{0, \tau^*\}$ with $\tau^* \in (0, 1)$ the unique solution of

$$\frac{\partial C^{EH}(P, \tau, \Gamma)}{\partial \tau} = 0 \tag{9}$$

(which can be easily computed numerically), depending on the system parameters. Moreover, the NE always outperforms the NJ state.

Proof: The transmit power is maximum $p^{NE} = P$ since C^{EH} is increasing in the transmit power p. Then, we prove by *reductio ad absurdum* that at the NE we have: $p_{th}(\tau^{NE}) \leq p^{NE}$, implying that $\gamma^{NE} = \Gamma$ from Proposition 1. Finding τ^{NE} reduces to solving the optimization problem:

$$\tau^{NE} = \arg \max_{\tau \in [0,1]} \; C^{EH}(P, \tau, \Gamma). \tag{10}$$

Based on the first and second order derivatives, $C^{EH}(P, \tau, \Gamma)$ is concave and either decreases ($\tau^{NE} = 0$) or it has a unique critical point ($\tau^{NE} = \tau^*$), depending on the parameters. To prove that the NE always outperforms the NJ state, we use two ingredients. From Proposition 1, whenever $p = p_{th}(\tau)$, the Shannon capacity is constant w.r.t. γ and, hence, $C^{EH}(p^{NJ}, \tau^{NJ}, 0) = C^{EH}(p^{NJ}, \tau^{NJ}, \Gamma)$. From the NE definition and knowing that $p^{NE} = P$ and $\gamma^{NE} = \Gamma$:

$$(P, \tau^{NE}) = \arg \max_{p, \tau} \; C^{EH}(p, \tau, \Gamma). \tag{11}$$

These two facts yield that the NE outperforms the NJ state: $C^{EH}(p^{NJ}, \tau^{NJ}, 0) \leq C^{EH}(P, \tau^{NE}, \Gamma)$.

In Fig. 3, we compare the capacity at the NE, $C^{EH}(P, \tau^{NE}, \Gamma)$, with the capacity when neutralizing the jammer, $C^{EH}(p^{NJ}, \tau^{NJ}, 0)$, normalized to the former by illustrating

$$F^{NJ} \triangleq \frac{C^{EH}(P, \tau^{NE}, \Gamma) - C^{EH}(p^{NJ}, \tau^{NJ}, 0)}{C^{EH}(P, \tau^{NE}, \Gamma)}. \tag{12}$$

The simulation setting is identical to Fig. 2. We remark that the NE always outperforms the NJ policy, which is consistent to our analysis. The intuition is that, when neutralizing the jammer, Alice does not necessarily transmit at maximum power P and has to spend a minimum proportion of time $\tau^{NJ} > 0$ for EH, as a threat to force the jammer to remain

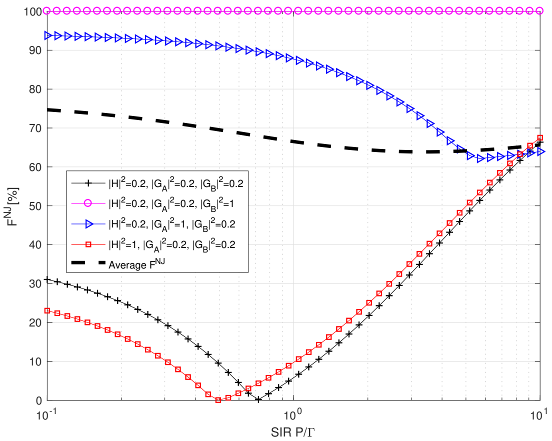

Fig. 3. NE vs. NJ efficiency: F^{NJ} in (12) as a function of SIR. The NE always outperforms the NJ state. At low SIR, exploiting the dominant jamming interference is more beneficial than silencing the jammer. At high SIR, neutralizing the jammer via EH is inefficient.

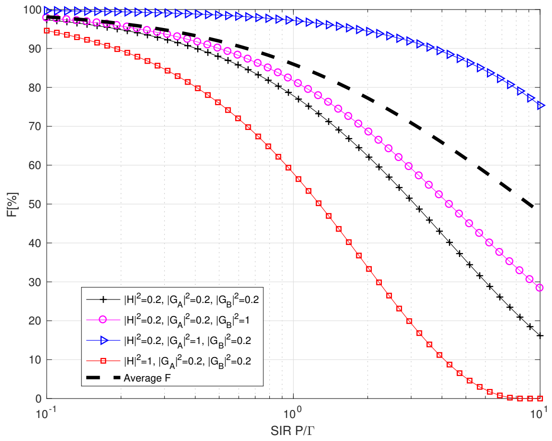

Fig. 4. EH efficiency: F in (13) as a function of SIR. EH is particularly beneficial at low SIR when the dominant jamming interference can be exploited. At high SIR, the interference becomes negligible and EH is less useful.

silent, even though no energy can actually be harvested during this time. Only in two of the four specific channel settings, the capacity at the NJ state equals the NE capacity and only at specific SIR values (the 0% minimum points). Surprisingly, using EH to neutralize the jammer is not beneficial in most cases. Instead, the legitimate users should harvest the jamming interference and use it for information transmission. The 100% relative gain curve corresponds to the case in which the jammer cannot be neutralized because of the poor quality of the harvesting link. The dashed black curve represents the average efficiency of the NE w.r.t. the NJ state and shows a relative gain between $64\% - 75\%$.

In the same setting, in Fig. 4 we evaluate the efficiency of EH as a measure against a strategic jammer and compare the capacity at the NE, $C^{EH}(P, \tau^{NE}, \Gamma)$, with $C^{EH}(P, 0, \Gamma)$, the capacity in absence of EH capability normalized to the former, by analyzing

$$F \triangleq \frac{C^{EH}(P, \tau^{NE}, \Gamma) - C^{EH}(P, 0, \Gamma)}{C^{EH}(P, \tau^{NE}, \Gamma)}. \tag{13}$$

At low SIR, the relative EH gain in terms of capacity is very high, approaching 100% when the gain of the harvesting link is high. The jamming interference is dominant and exploiting it for useful communication is very beneficial. At high SIR, the gain from EH decreases progressively towards zero since the jamming interference that can be harvested becomes negligible. The potential of using EH as an anti-jamming measure is demonstrated by the substantial relative gains in terms of Shannon capacity that can on average reach 95% in the low SIR regime.

V. Conclusion

In this paper, we showed that EH can be exploited to efficiently mitigate jamming attacks. We proved that a jammer can be completely neutralized by appropriately tuning the transmit power and the EH duration. However, this restricts the transmit power of the legitimate user and requires a minimum harvesting duration, during which little energy can actually be harvested (as the jammer is forced to remain silent). Therefore, neutralizing the jammer is not necessarily optimal. Employing a zero-sum game formulation, we showed that at the NE both players should transmit at full power and the optimal EH duration depends on the system parameters. Our simulation results show that EH can offer substantial gains in terms of capacity. At low SIR, the average gains can reach 95%, showcasing the high potential of EH as an efficient counter-jamming measure.

References

[1] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: architecture design and rate-energy tradeoff," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4754–4767, 2013.

[2] Y. Gu and S. Aissa, "RF-based energy harvesting in decode-and-forward relaying systems: ergodic and outage capacities," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6425–6434, Nov. 2015.

[3] R. Rajesh and 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.

[4] M.-L. Ku, W. Li, Y. Chen, and K. J. R. Liu, "Advances in energy harvesting communications: past, present, and future challenges," *IEEE Commun. Surveys Tuts.*, pp. 1384–1412, 2nd quarter 2016.

[5] 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.*, pp. 1167–1176, Apr. 2012.

[6] L. Xiao, T. Chen, L. Jinliang, and D. Huaiyu, "Anti-jamming transmission Stackelberg game with observation errors," *IEEE Commun. Lett.*, pp. 949–952, 2015.

[7] K. Wang, L. Yuan, T. Miyazaki, Y. Chen, and Y. Zhang, "Jamming and eavesdropping defense in green cyber-physical transportation systems using Stackelberg game," *IEEE Trans Ind. Informat.*, May 2018.

[8] Z. Fang, T. Song, and T. Li, "Energy harvesting for two way OFDM communications under hostile jamming," *IEEE Signal Process. Let.*, vol. 22, pp. 413–416, Apr. 2015.

[9] H. Xing, K.-K. Wong, Z. Chu, and A. Nallanathan, "To harvest and jam: a paradigm of self-sustaining friendly jammers for secure AF relaying," *IEEE Trans. Signal Process.*, vol. 63, no. 24, pp. 6616–6631, Dec. 2015.

[10] E. V. Belmega and A. Chorti, "Energy harvesting in secret key generation systems under jamming attacks," *IEEE Int. Conf. Commun. (ICC)*, pp. 1–6, May 2017.

[11] ——, "Protecting secret key generation systems against jamming: energy harvesting and channel hopping approaches," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2611–2626, 2017.

[12] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2012.

[13] D. Fudenberg and J. Tirole, *Game Theory*. MA: MIT Press, 1991.