Wireless-Powered Friendly Jammer for Physical Layer Security

(Invited Paper)

Wanchun Liu, Xiangyun Zhou, Salman Durrani
Research School of Engineering, The Australian National University, Canberra, Australia.
Emails: {wanchun.liu, xiangyun.zhou, salman.durrani}@anu.edu.au

***Abstract*—Exploring a cooperative node as a friendly jammer is an effective means of providing secure communication between a source-destination pair in the presence of an eavesdropper. In this work, we consider the use of a wireless-powered friendly jammer. Without relying on external energy supply, the friendly jammer is powered by the source node via wireless power transfer. We apply a simple time-switching protocol where the power transfer and jammer-assisted secure transmission occur in different time blocks. By investigating the long-term behavior of the communication protocol, we derive a closed-form expression of the throughput. We further optimize the jamming power and the rate parameters for maximizing the throughput subject to a secrecy outage probability constraint.**

I. Introduction

Due to the high computational complexity of upper-layer cryptosystems in dynamic wireless networks, techniques for securing wireless communication at the physical layer has attracted significant interest in the past decade [1–3]. In particular, cooperative jamming [4] has been demonstrated to be an effective means to provide secure wireless communications [5–8]. However, this is often realized at the expense of the additional power consumption of the friendly jamming nodes.

For the convenience of deployment with mobility requirement and other constraints, the jamming nodes may not have connection to power lines. Thus, similarly to other battery-powered communication nodes not relying on the power lines, a jammer's lifetime is constrained by the energy stored in its battery. The authors in [9] considered the deployment of an energy harvesting friendly jammer which promises to greatly enhance the lifetime of the jammer, so as to increase the security of a communication link. However, conventional energy harvesting methods rely on ambient energy sources which are uncontrollable. In addition, the energy harvesting devices may have large dimension requirements or high implementation complexity and cost.

In this paper, motivated by the emerging research on radio-frequency (RF) powered communication nodes with simple RF energy conversion circuit [10], [11], we consider the deployment of a friendly jammer which is wireless-powered by the source node in a controlled manner and used for protecting the secure communication between the source-destination pair in the presence of an eavesdropper. Our contributions are as follows:

The work of X. Zhou was supported by the Australian Research Council's Discovery Project funding scheme (project number DP150103905).

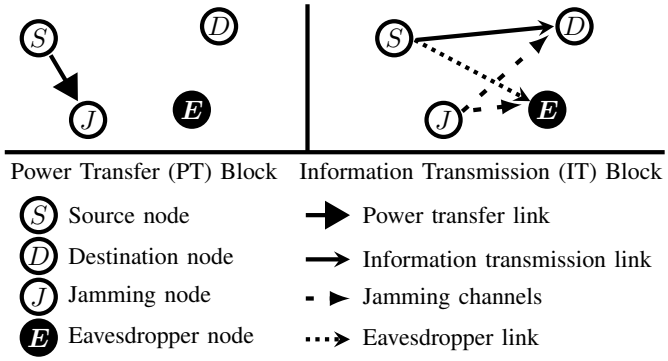

Fig. 1 System model with illustration of the power transfer and information transmission blocks.

- We design a communication protocol that provides secure transmission by using a friendly jammer which is wireless-powered by the source node. This protocol simply switches between power transfer (PT) and information transmission (IT) in different time blocks depending on both the energy level at the jammer and the channel between the source and the destination.
- We study the long-term behavior of the proposed protocol. Depending of the system parameters, the communication process has two kinds of long-term behavior: energy accumulation and energy balanced. We derive a closed-form expression of the achievable throughput of the proposed protocol with fixed-rate transmission.
- We focus on the energy balanced case and study the optimal protocol design. In particular, we optimize the jamming power and the rate parameters of secure communication to achieve the maximum throughput while satisfying a constraint on secrecy outage probability. We see that the optimal throughput reaches a finite upper bound even if the source transmit power increases towards infinity.

II. System Model

We consider a communication scenario where a source (S) communicates with a destination node (D) in the presence of a passive eavesdropper (E) with the help of a friendly jammer (J). We assume that all nodes are equipped with a single antenna. All the channel links are composed of large-scale path loss with exponent m and small-scale Rayleigh

fading. These fading channel gains are modeled as quasi-static frequency non-selection parameters, which means that they are constant over the block time of T seconds, and independent and identically distributed (i.i.d.) between blocks. The channel state information (CSI) of the links from source and jammer to the destination are assumed to be known at both ends, but the CSI of the eavesdropping link is only known to the eavesdropper itself. The distances and the fading channel gains of the links $i \to j$, are denoted as d_{ij} and h_{ij}, $i, j, \in \{S, D, J, E\}$, respectively. In addition, the noise power at the eavesdropper is assumed to be zero as a worst-case scenario.

The jammer is assumed to be an energy-constrained node with no power of its own but equipped with a simple RF energy harvesting circuit, which is use to harvest energy from the RF signal from the source. We assume that the harvested energy is stored in the jammer's battery with infinite capacity.

The proposed friendly jammer assisted secure communication protocol, which will be described in detail later in Sec. II-B, consists of two kinds of blocks in general: (i) power transfer (PT) block and (ii) information transmission (IT) block shown in Fig. 1. The signal models in PT and IT blocks are given below:

A. Signal Model

1) PT: During a PT block, the source sends an RF signal, x_{SJ} (its variance is normalized to one), with power $\mathcal{P}_s$. Thus, the jammer receives

$$y_J = \frac{1}{\sqrt{d_{SJ}^m}} \sqrt{\mathcal{P}_s} h_{SJ} x_{SJ} + n_J, \tag{1}$$

where n_J is the additive white Gaussian noise (AWGN) at the jammer. Then, y_J is converted to a direct current signal and the energy stored in the battery. From (1), by ignoring the noise power, the harvested energy is given by [12]

$$\rho_J(h_{SJ}) = \eta \left| \frac{1}{\sqrt{d_{SJ}^m}} \sqrt{\mathcal{P}_s} h_{SJ} \right|^2 T, \tag{2}$$

where η is the energy conversion efficiency of RF-DC conversion operation for energy storage at the jammer. Because h_{SJ} is i.i.d. across all blocks with complex Gaussian distribution with normalized variance, we have $\mathbb{E}\left\{|h_{SJ}|^2\right\} = 1$. Therefore, the average harvested energy ρ_J is given by

$$\rho_J = \mathbb{E}\left\{\rho_J(h_{SJ})\right\} = \mathbb{E}\left\{\eta \frac{1}{d_{SJ}^m} \mathcal{P}_s \left|h_{SJ}\right|^2 T\right\} = \frac{\eta \mathcal{P}_s T}{d_{SJ}^m}. \tag{3}$$

2) IT: During an IT block, the source transmits the information-carrying signal x_{SD} (its variance is normalized to one) with power $\mathcal{P}_s$. At the same time, the jammer sends a noise-like signal x_{JD} (its variance is normalized to one) with power $\mathcal{P}_J$, affecting both the destination and the eavesdropper. Thus, the received signal at the destination, y_D, is given by

$$y_D = \frac{1}{\sqrt{d_{SD}^m}} \sqrt{\mathcal{P}_s} h_{SD} x_{SD} + \frac{1}{\sqrt{d_{JD}^m}} \sqrt{\mathcal{P}_J} h_{JD} x_{JD} + n_d, \tag{4}$$

where n_d is the AWGN at the destination with variance σ_d^2.

Similarly, the received signal at the eavesdropper, y_E, is given by

$$y_E = \frac{1}{\sqrt{d_{SE}^m}} \sqrt{\mathcal{P}_s} h_{SE} x_{SD} + \frac{1}{\sqrt{d_{JE}^m}} \sqrt{\mathcal{P}_J} h_{JE} x_{JD} + n_e, \tag{5}$$

where n_e is the AWGN at the eavesdropper which we have assumed to be zero as a worst-case scenario.

From (4), the SINR at the destination is

$$\gamma_d = \frac{\frac{\mathcal{P}_s}{d_{SD}^m} |h_{SD}|^2}{\sigma_d^2 + \frac{\mathcal{P}_J}{d_{JD}^m} |h_{JD}|^2}, \tag{6}$$

and the capacity of $S \to D$ link is given as

$$C_d = \log_2 (1 + \gamma_d). \tag{7}$$

Since $|h_{SD}|^2$ and $|h_{JD}|^2$ follow i.i.d. exponential distribution, γ_d has the cumulative distribution function (cdf) as

$$F_{\gamma_d}(x) = 1 - \frac{e^{-\frac{x}{\rho_d}}}{1 + \varphi x}, \tag{8}$$

where

$$\varphi = \frac{\mathcal{P}_J}{\mathcal{P}_s} \frac{d_{SD}^m}{d_{JD}^m}. \tag{9}$$

For convenience, we define the SNR at the destination (without jamming noise) as

$$\rho_d \triangleq \frac{\mathcal{P}_s}{d_{SD}^m \sigma_d^2}. \tag{10}$$

From (5), the SINR at the eavesdropper is

$$\gamma_e = \frac{1}{\phi} \frac{|h_{SE}|^2}{|h_{JE}|^2}, \tag{11}$$

where

$$\phi = \frac{\mathcal{P}_J}{\mathcal{P}_s} \frac{d_{SE}^m}{d_{JE}^m}. \tag{12}$$

Hence, the capacity of $S \to E$ link is given as

$$C_e = \log_2 (1 + \gamma_e). \tag{13}$$

From [13], the probability density function (pdf) of γ_e is given by

$$f_{\gamma_e}(x) = \phi \left(\frac{1}{\phi x + 1} \right)^2. \tag{14}$$

B. Secure Communication Protocol

Now we describe the proposed secure communication protocol. We first explain the secure encoding scheme in each IT block. Then, we describe how the protocol determines when to transfer power and when to transmit information.

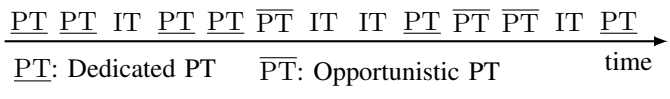

Fig. 2 Illustration of the proposed protocol.

1) Secure Encoding Scheme: In IT blocks, we consider fixed-rate transmission of secret information from the source to the destination, using Wyner's wiretap code [14]. The wiretap code has two rate parameters: rate of codeword transmission and rate of secret information, denoted by R_t and R_s, respectively. The positive rate difference, $R_t - R_s$, is the cost to provide secrecy against the eavesdropper. Since we consider quasi-static fading channel, we use outage based measures: connection outage probability and secrecy outage probability, which are defined, respectively, as

$$p_{\rm co} = \Pr\left\{R_t > C_d\right\}, \tag{15}$$

$$p_{\rm so} = \Pr\left\{R_t - R_s < C_e\right\}. \tag{16}$$

Given the values of the rate parameters, R_t and R_s, the connection outage probability is a measure of the fading channel quality of the $S \to D$ link, while the secrecy outage probability is a measure of the secrecy level.

2) PT-IT Scheme: The jammer power $\mathcal{P}_J$ is determined offline and kept constant in all IT blocks. The proposed communication protocol determines whether to be in an IT block (as opposed to a PT block) according to the following two conditions: (i) At the beginning of the block, the jammer has enough energy, $\mathcal{P}_J T$, to support jamming with power $\mathcal{P}_J$ over a block of T seconds, and (ii) the link $S \to D$ does not suffer connection outage, which means it can support the codeword transmission rate R_t.

If both conditions are satisfied, the block is chosen to be an IT block for transmitting the confidential information. If at least one condition is not satisfied, the block is chosen to be a PT block for wirelessly charging the jammer. Specifically, if the first condition is not satisfied, then the PT block is referred to as a *dedicated PT block*, which means the jammer is short of energy for jamming and wireless power transfer is absolutely necessary. If the first condition is satisfied but the second condition is not, then the PT block is referred to as an *opportunistic PT block*. This is the situation where the communication link $S \to D$ does not support the transmission rate R_t, hence an opportunity for PT occurs in this block (because IT should not happen) in spite of the fact that the jammer has already meet the energy requirement for jamming. A illustration of the proposed protocol is given in Fig. 2.

III. Problem Formulation

A. Performance Metrics

We measure the long-term performance of our proposed protocol using the throughput of transmission (i.e., the average number of bits of confidential information received at the destination per unit time), subject to a given secrecy constraint against eavesdropping. Specifically, we describe the secrecy constraint as a threshold on the secrecy outage probability, i.e.,

$$p_{\rm so} \le \varepsilon, \tag{17}$$

where ε is the threshold. Under such a secrecy constraint, we compute the throughput as [13], [15]

$$\pi = p_{\rm tx} R_s, \tag{18}$$

where $p_{\rm tx}$ is the probability of the communication process being in IT blocks, i.e., the percentage of time for secure communication.

From the secure encoding scheme we adopted and the secrecy outage probability in (16), when increasing R_s in order to improve the throughput in (18), the constraint of secrecy outage probability in (17) may be violated. From the PT-IT scheme we proposed, the probability of being an IT block, $p_{\rm tx}$, is related to (i) the jamming power $\mathcal{P}_J$ and (ii) the connection outage probability of the link $S \to D$, $p_{\rm co}$. Thus, in order to calculate π in (18), we have to find an explicit expression for $p_{\rm tx}$, which is given in the following subsection.

B. Long-term Behavior and Information Transmit Probability

Focusing on the long-term behavior of the communication process determined by our proposed protocol, it is easy to figure out that the behavior of the communication process falls in one of the following two cases:

- *Energy Accumulation*: In this case, on average, the energy harvested at the jammer during opportunistic PT blocks is higher than the energy required during an IT block. Thus, in the long term, the energy steadily accumulates at the jammer and there is no need for dedicated PT blocks (the harvested energy by opportunistic PT blocks fully meets the energy consumption requirement at the jammer).
- *Energy Balanced*: In this case, on average, the energy harvested at the jammer during opportunistic PT blocks is not larger than the energy required during an IT block. Thus, in the long term, dedicated PT blocks are sometimes required to make sure that the energy harvested from both dedicated and opportunistic PT blocks equals the energy required for jamming in IT blocks on average.

We determine the conditions under which the communication process falls in either of the two cases in Lemma 1 below.

Lemma 1. The communication process with the proposed communication protocol leads to energy accumulation if

$$\frac{p_{\rm co}}{1 - p_{\rm co}} > \frac{\mathcal{P}_J T}{\rho_J} \tag{19}$$

is satisfied. Otherwise, the communication process is energy balanced.

Proof. The complete proof can be found in Appendix A in [16] and is omitted here due to space constraints. ■

Different communication behaviors lead to different results for $p_{\rm tx}$. Nevertheless, we are able to obtain a general expression for $p_{\rm tx}$ as presented in Theorem 1 below.

Theorem 1. The information transmission probability for the proposed secure communication protocol is given by

$$p_{\rm tx} = \frac{1}{1+\max\left\{\frac{\mathcal{P}_J T}{\rho_J}, \frac{p_{\rm co}}{1-p_{\rm co}}\right\}}. \tag{20}$$

Proof. Due to space limitations, a sketch of the proof is given: We first model the communication process in both energy accumulation and energy balanced cases as Markov chains and show the ergodicity of the process. This then allows us to derive the stationary probability of a block being used for IT. The detailed proof can be found Appendix B in [16]. ■

Substituting (20) into (18), we have the expression of throughput

$$\pi = \frac{R_s}{1+\max\left\{\frac{\mathcal{P}_J T}{\rho_J}, \frac{p_{\rm co}}{1-p_{\rm co}}\right\}}. \tag{21}$$

From (7), (8) and (15), we get an expression of $p_{\rm co}$ as

$$p_{\rm co} = 1 - \frac{e^{-\frac{2^{R_t}-1}{\rho_d}}}{1+\frac{\mathcal{P}_J}{\mathcal{P}_s}\frac{d_{SD}^m}{d_{JD}^m}\left(2^{R_t}-1\right)}. \tag{22}$$

Substituting (22) into (21), we obtain the achievable throughput of the proposed protocol. In the next section, we will derive the throughput under the secrecy outage constraint.

IV. Optimization for Energy Balanced Design

In the last section, we see that there are two different long-term behaviors of the communication process. In the rest of the paper, we focus on the energy balanced case and study the optimal offline design of the secure communication protocol. The design parameters to optimize are the jamming power $\mathcal{P}_J$, the codeword rate R_t and the secret information rate R_s. The study on the energy accumulation case can be found in [16].

A. Optimization Problem and Solution

We consider the optimal secure communication design as follows:

$$\begin{aligned} &\max_{\mathcal{P}_J, R_t, R_s} \quad \pi \\ &\text{s.t. } p_{\rm so} \le \varepsilon,\ p_{\rm co}/(1-p_{\rm co}) \le \mathcal{P}_J T/\rho_J,\ \mathcal{P}_J \ge 0,\ R_t \ge R_s \ge 0, \end{aligned} \tag{23}$$

where the first constraint is on the secrecy level and the second constraint is the condition for the energy balanced case. This design aims to maximize the throughput with the constraint on the secrecy outage probability.

From (13), (14), (16) and (17), the constraint of secrecy outage probability in (23) can be rewritten as

$$p_{\rm so} = \mathbb{P}\left\{R_t - R_s < \log_2\left(1+\gamma_e\right)\right\} \le \varepsilon. \tag{24}$$

By substituting (14) into (24), and after some simplification, we have

$$\mathcal{P}_J \ge \mathcal{P}_s \frac{d_{JE}^m}{d_{SE}^m}\frac{\left(\varepsilon^{-1}-1\right)}{2^{R_t-R_s}-1}. \tag{25}$$

From (15), the energy balanced constraint in (23) can be further simplified as

$$\left(1+\frac{\mathcal{P}_J}{\mathcal{P}_s}\frac{d_{SD}^m}{d_{JD}^m}\left(2^{R_t}-1\right)\right)e^{\frac{2^{R_t}-1}{\rho_d}} - 1 \le \frac{\mathcal{P}_J T}{\rho_J}. \tag{26}$$

From the expression of throughput in (21), it is easy to verify that both of (25) and (26) are active constraints, i.e., by adjusting the parameters, the throughput can always be further improved if any of the two constraints is loose. Therefore, the equalities hold in (25) and (26). Now, we have obtained the optimal jamming power from (25),

$$\mathcal{P}_J^\star = \mathcal{P}_s \frac{d_{JE}^m}{d_{SE}^m}\frac{\left(\varepsilon^{-1}-1\right)}{2^{R_t-R_s}-1}, \tag{27}$$

and by taking (26) and (27) into (23), the optimization problem can be rewritten as

$$\max_{R_t, R_s \ge 0} \quad \frac{R_s}{1+\frac{k_1}{2^{R_t-R_s}-1}}, \quad \text{s.t. (26) holds with equality,} \tag{28}$$

where $k_1 = \frac{d_{SJ}^m}{\eta}\frac{d_{JE}^m}{d_{SE}^m}\left(\varepsilon^{-1}-1\right)$, and $\mathcal{P}_J$ in the constraint is substituted by (27).

From the constraint in (28), after some manipulations, R_s can be expressed as a function of R_t, thus, the optimization problem above can be further simplified as a one-dimensional problem w.r.t. R_t. Calculating the derivative of the target function in (28) w.r.t. R_t, after some simplifications, the optimal codeword rate $R_t^\star$ is the root of following equation which can be easily solved by a linear search:

$$\zeta'\left(\frac{1+\frac{k_1}{\zeta}}{\ln 2\left(1+\zeta\right)} - \frac{k_1\left(R_t - \log_2\left(1+\zeta\right)\right)}{\zeta^2}\right) = 1, \tag{29}$$

where

$$\zeta = \frac{k_1 - k_2 e^{\frac{2^{R_t}-1}{\rho_d}}\left(2^{R_t}-1\right)}{e^{\frac{2^{R_t}-1}{\rho_d}}-1}, \quad k_2 = \frac{d_{JE}^m}{d_{SE}^m}\frac{d_{SD}^m}{d_{JD}^m}\left(\varepsilon^{-1}-1\right), \tag{30}$$

$$\zeta' = \frac{\ln 2\ e^{\frac{2^{R_t}-1}{\rho_d}}}{\left(e^{\frac{2^{R_t}-1}{\rho_d}}-1\right)^2}\left(k_2\ 2^{R_t}\left(1+\frac{1}{\rho_d}-e^{\frac{2^{R_t}-1}{\rho_d}}\right) - \frac{k_1+k_2}{\rho_d}\right),$$

and the optimal secret information rate, $R_s^\star = R_t^\star - \log_2\left(1+\zeta^\star\right)$, where $\zeta^\star$ is calculated by taking $R_t^\star$ into (30).

B. High SNR Regime

Depending on the power budget of the source node, it may be allowed to increase the source transmit power $\mathcal{P}_s$ in order to improve the system performance. It is not immediately clear whether increasing $\mathcal{P}_s$ leads to better performance as it affects the quality of signal reception at both the destination and eavesdropper, as well as the power transfer to the jammer. To obtain some insights, we consider the high SNR regime. Note that we have defined SNR at the destination (without the effect of jamming noise) as ρ_d in (10).

Corollary 1. When the SNR at the destination is sufficiently high, the asymptotically optimal rate parameters and an upper bound on throughput are given by

$$\tilde{R}_t^\star = \log_2\left(1+\frac{k_1}{k_2}\right), \tag{31a}$$

$$\tilde{\pi}^\star = \frac{\tilde{R}_s^\star}{1+\frac{k_1}{2^{\tilde{R}_t^\star-\tilde{R}_s^\star}-1}}, \tag{31b}$$

where k_2 is defined in (30), and the asymptotically optimal secrecy rate $\tilde{R}_s^\star$ is obtained by solving the following equation

$$2^{2\left(\tilde{R}_t^\star-R_s\right)}+\left(k_1-\ln 2\ k_1R_s-2\right)2^{\left(\tilde{R}_t^\star-R_s\right)}-k_1=0. \tag{32}$$

Proof. The result is obtained in a straightforward manner by letting $\rho_d \to \infty$ or equivalently $\mathcal{P}_s \to \infty$. ■

The upper bound on throughput implies that one cannot effectively improve the throughput by further increasing $\mathcal{P}_s$ when the SNR at the destination is already high. It is then interesting to see how fast the throughput converges to the upper bound as $\mathcal{P}_s$ increases.

V. Numerical Results

In this section, we present numerical results to demonstrate the performance of the proposed secure communication protocol. We set the path loss exponent as $m = 3$ and the length of time block as $T = 1$ ms. We set the energy conversion efficiency as $\eta = 0.5$ [12]. We assume that the source, jammer, destination and eavesdropper are placed along a horizontal line, and the distances are given by $d_{SJ} = 25$ m, $d_{SE} = 40$ m, $d_{SD} = 50$ m, $d_{JE} = 15$ m, $d_{JD} = 25$ m, in line with [4]. We set $\sigma_d^2 = -100$ dBm. We do not specify the bandwidth of communication, hence the rate parameters are expressed in units of bit per channel use (bpcu).

Fig. 3 shows that the optimal throughput in the energy balanced design obtained in the previous section grows with the source transmit power, but quickly reaches the upper bound given in Corollary 1. Specifically, the upper bound is reached at source transmit power of 10 dBm or less. Also we see that a more stringent requirement (a lower threshold) on the secrecy outage probability decreases the achievable throughput as we expected.

VI. Conclusions

In this paper, we investigated secure communication with the help from a wireless-powered jammer. We proposed a simple communication protocol and analyzed its long-term behavior. Furthermore, we derived the achievable throughput with fixed-rate transmission. For the design under energy balanced behavior, we further optimized the jamming power and the rate parameters to achieve the maximum throughput subject to a secrecy outage probability constraint. Our analytical and simulation results show that as the source transmit power increases, the throughput quickly reaches an upper bound.

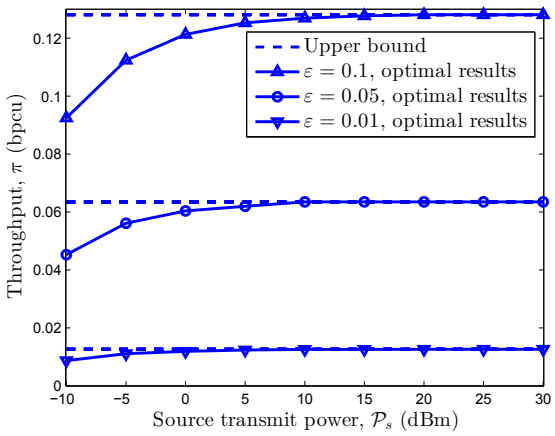

Fig. 3 Optimal throughput vs. source transmit power in the energy balanced design.

References

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

[2] A. Mukherjee, S. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[3] X. Zhou, L. Song, and Z. Zhang, *Physical Layer Security in Wireless Communications*. CRC Press, 2013.

[4] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[5] O. Simeone and P. Popovski, "Secure communications via cooperating base stations," *IEEE Commun. Lett.*, vol. 12, no. 3, pp. 188–190, Mar. 2008.

[6] I. Krikidis, J. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[7] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Apr. 2011.

[8] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[9] A. Mukherjee and J. Huang, "Deploying multi-antenna energy-harvesting cooperative jammers in the MIMO wiretap channel," in *Proc. IEEE ICASSP*, Nov. 2012, pp. 1886–1890.

[10] K. Huang and X. Zhou, "Cutting the last wires for mobile communications by microwave power transfer," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 86–93, Jun. 2015.

[11] S. Bi, C. K. Ho, and R. Zhang, "Wireless powered communication: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 117–125, Apr. 2015.

[12] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989–2001, May 2013.

[13] X. Zhang, X. Zhou, and M. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.

[14] X. Tang, R. Liu, P. Spasojevic, and H. Poor, "On the throughput of secure hybrid-ARQ protocols for gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1591, Apr. 2009.

[15] X. Zhou, M. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[16] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure Communication with a Wireless-Powered Friendly Jammer," *to appear in IEEE Trans. Wireless Commun.*, 2015. [Online]. Available: http://arxiv.org/pdf/1412.0349v2.pdf