Secure Communication With a Wireless-Powered Friendly Jammer

Wanchun Liu, *Student Member, IEEE*, Xiangyun Zhou, *Member, IEEE*, Salman Durrani, *Senior Member, IEEE*, and Petar Popovski, *Senior Member, IEEE*

***Abstract*—In this paper, we propose using a wireless-powered friendly jammer to enable secure communication between a source node and destination node, in the presence of an eavesdropper. We consider a two-phase communication protocol with fixed-rate transmission. In the first phase, wireless power transfer is conducted from the source to the jammer. In the second phase, the source transmits the information-bearing signal under the protection of a jamming signal sent by the jammer using the harvested energy in the first phase. We analytically characterize the long-term behavior of the proposed protocol and derive a closed-form expression for the throughput. We further optimize the rate parameters for maximizing the throughput subject to a secrecy outage probability constraint. Our analytical results show that the throughput performance differs significantly between the single-antenna jammer case and the multiantenna jammer case. For instance, as the source transmit power increases, the throughput quickly reaches an upper bound with single-antenna jammer, while the throughput grows unbounded with multiantenna jammer. Our numerical results also validate the derived analytical results.**

***Index Terms*—Physical layer security, friendly jammer, cooperative jamming, wireless power transfer, throughput.**

I. Introduction

A. Background and Motivation

PHYSICAL layer security has been recently proposed as a complement to cryptography method to provide secure wireless communications [1], [2]. It is a very different paradigm where secrecy is achieved by exploiting the physical layer properties of the wireless communication system, especially interference and fading. Several important physical layer security techniques have been investigated in the past decade (see a survey article [3] and the references therein). Inspired by cooperative communication without secrecy constraints, user cooperation is a promising strategy for improving secrecy performance. There are mainly two kinds of cooperation: cooperative relaying and cooperative jamming. As for cooperative relaying, the well-known decode-and-forward and amplify-and-forward schemes were discussed in [4]–[6] with secrecy considerations. Following the idea of artificial noise in [7], cooperative jamming was investigated as an effective method to enhance secrecy [8]–[16]. In this scheme, a friendly jammer transmits a jamming signal to interfere with the eavesdropper's signal reception at the same time when the source transmits the message signal. In [8]–[10], the authors focused on the design of a single-antenna jammer. In [11] and [12], multiple single-antenna jammers were considered to generate distributed cooperative jamming signals. In [13], the authors studied multi-antenna jammer (called relay in [13]) in secure wireless networks. Motivated by this work, the authors in [14]–[16] considered multi-antenna jammers in MIMO (multiple-input and multiple-output) networks.

In many wireless network applications, communication nodes may not have connection to power lines due to mobility or other constraints. Thus, their lifetime is usually constrained by energy stored in the battery. In order to prolong the lifetime of energy-constrained wireless nodes, energy harvesting has been proposed as a very promising approach [17], [18]. Conventional energy harvesting methods rely on various renewable energy sources in the environment, such as solar, vibration, thermoelectric and wind, thus are usually uncontrollable. For a wireless communication environment, harvesting energy from radio-frequency (RF) signals has recently attracted a great deal of attention [19]–[21]. A new energy harvesting solution called wireless power transfer is adopted in recent research on energy-constrained wireless networks [22]–[27]. Generally speaking, the key idea is that a wireless node could capture RF signal sent by a source node and convert it into direct current to charge its battery, then use it for signal processing or transmission. In [22]–[24], the authors considered the scenario that the destination simultaneously receives wireless information and harvests wireless power transfered by the source. Motivated by these works, the authors in [25]–[27] studied how the wireless nodes can make use of the harvested energy from wireless power transfer to enable communications. The wireless power transfer process can be fully controlled, and hence, can be used in wireless networks with critical quality-of-service constrained applications, such as secure wireless communications. In [28], [29], the authors considered secure communications with one information receiver and one (or several) wireless energy-harvesting eavesdropper(s). In [30], the authors studied the coexistence of three destination types in a network: an information receiver, a receiver for harvesting wireless energy and an eavesdropper. In [31], the authors considered the wireless

Manuscript received November 30, 2014; revised April 15, 2015 and July 7, 2015; accepted August 24, 2015. Date of publication August 28, 2015; date of current version January 7, 2016. This work was supported by the Australian Research Council's Discovery Project Funding Scheme (Project number DP150103905). The associate editor coordinating the review of this paper and approving it for publication was Dr. Kai Zeng.

W. Liu, X. Zhou, and S. Durrani are with the Research School of Engineering, the Australian National University, Canberra, ACT 2601, Australia (e-mail: wanchun.liu@anu.edu.au; xiangyun.zhou@anu.edu.au; salman.durrani@anu.edu.au).

P. Popovski is with the Department of Electronic Systems, Aalborg University, Aalborg 9220, Denmark (e-mail: petarp@es.aau.dk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2015.2474378

communication network with eavesdroppers and two types of legal receivers which can receive information and harvest wireless energy at the same time: desired receiver and idle receiver, while the idle receivers are treated as potential eavesdroppers. All these works on secure communication did not explicitly study how the harvested energy at the receiver is used.

B. Our Work and Contribution

This paper considers a scenario that the network designer wants to establish secure communication between a pair of source-destination devices with minimal cost. To this end, a simple passive device is deployed nearby as a helper. Such a device does not have connection to power line and is only activated during secure communication. The requirements of simplicity and low cost bring important challenges: the helping device should have low complexity in its design and operation, with a low-cost energy harvesting method to enable its operation when needed. Consequently, the helping device should ideally have very little workload of online computation and minimal coordination or information exchange with the source-destination pair.

To solve the above-mentioned secure communication design problem, we propose to use a wireless-powered friendly jammer as the helping device, where the jammer harvests energy via wireless power transfer from the source node. The energy harvesting circuit (consisting of diode(s) and a passive low-pass filter [19], [23]) is very simple and cost effective. More importantly, such a design allows us to control the energy harvesting process for the jammer, which is very different from the conventional energy harvesting methods that rely on uncontrollable energy sources external to the communication network. We use a simple time-switching protocol [22], [25], [32], where power transfer (PT) and information transmission (IT) are separated in time. In this regard, the time allocation between PT and IT must be carefully designed in order to achieve the best possible throughput performance. We solve this problem by optimizing the jamming power, which indirectly gives the best time allocation for achieving the maximum throughput while satisfying a given secrecy constraint. We further optimize the rate parameters of secure communication. All design parameters are optimized offline with only statistical knowledge of the wireless channels.

The main contributions of this work are summarized below:

- The novelty of the work lies in the design of a communication protocol that provides secure communication using an energy-constrained jamming node wirelessly powered by the source node. The protocol sets a target jamming power and switches between IT and PT depending on whether the available energy at the jammer meets the target power or not.
- We study the long-term behavior of the proposed communication protocol and derive a closed-form expression of the probability of IT. Based on this, we obtain the achievable throughput of the protocol with fixed-rate transmission.
- We optimize the rate parameters to achieve the maximum throughput while satisfying a constraint on the secrecy outage probability. Further design insights are obtained by considering the high SNR regime and the large number of antennas regime. We show that when the jammer has a single antenna, increasing the source transmit power quickly makes the throughput converge to an upper bound. However, when the jammer has multiple antennas, increasing the source transmit power or the number of jammer antennas improves the throughput significantly.

Our work is different from the following most related studies: In [33], the authors considered a MISO secure communication scenario, without the help of an individual jammer. Different from [33], we consider using wireless-powered jammer to help the secure communication. Therefore, in our analysis, we study the cooperation of jammer and source and design the protocol to balance the time spent on PT and IT, in order to achieve the maximum throughput of the secure communication. In [32], the authors considered using a wireless-powered relay to help the point-to-point communication. Different from [32], we consider a secure communication scenario. In our analysis, we optimize the jamming power and rate parameters for secure communication, which was not considered in [32]. In [34], the authors designed jamming signal of energy harvesting jammer to help the secure communication based on the knowledge of the uncontrollable energy harvesting process. Different from [34], we consider using wireless-powered jammer where the wireless power transfer process is totally controllable. In our work, we jointly design the wireless power transfer process and the communication process. Therefore, the design approach is fundamentally different between [34] and our work.

The remainder of this paper is organized as follows. Section II presents the system model. Section III proposes the secure communication protocol. Section IV analyzes the protocol and derives the achievable throughput. Section V formulates an optimization problem for secrecy performance, and gives the optimal design. Section VI presents numerical results. Finally, conclusions are given in Section VII.

II. System Model

We consider a communication scenario where a source node (S) communicates with a destination node (D) in the presence of a passive eavesdropper (E) with the help of a friendly jammer (J), as illustrated in Fig. 1. We assume that the jammer has N_J antennas ($N_J \geq 1$), while all the other nodes are equipped with a single antenna only. Also we assume that the eavesdropper is just another communication node in the same network which should not have access to the information transmitted from the source to the destination. Therefore, the locations of all nodes are public knowledge.

A. Jammer Model

In this work, the jammer is assumed to be an energy constrained node with no power of its own and having a rechargeable battery with infinite capacity [24], [32], [35]. In order to make use of the jammer, the source node wirelessly charges the jammer via wireless power transfer. Once the jammer harvests

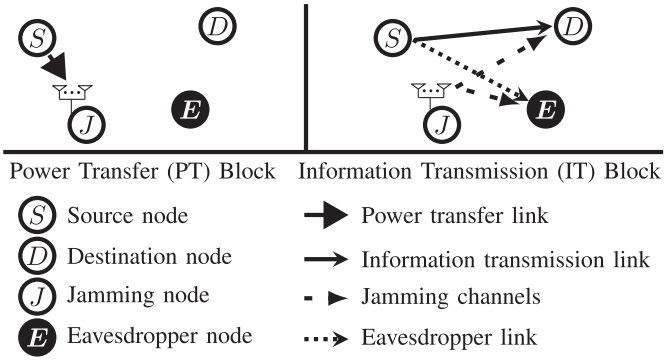


Fig. 1. System model with illustration of the power transfer and information transmission phases.

sufficient energy, it can be used for transmitting friendly jamming signals to enhance the security of the communication between the source and the destination. We assume that the jammer's energy consumption is dominated by the jamming signal transmission, while the other energy consumption, e.g., due to the signal processing, is relatively insignificant and hence ignored for simplicity [23], [26].

B. Channel Assumptions

We assume that all the channel links are composed of large-scale path loss with exponent m and statistically independent small-scale Rayleigh fading. We denote the inter-node distance of links $S \to J$, $S \to D$, $J \to D$, $S \to E$ and $J \to E$ by d_{SJ}, d_{SD}, d_{JD}, d_{SE} and d_{JE}, respectively. The fading channel gains of the links $S \to J$, $S \to D$, $S \to E$, $J \to E$ and $J \to D$ are denoted by $\boldsymbol{h}_{SJ}$, h_{SD}, h_{SE}, $\boldsymbol{h}_{JE}$, $\boldsymbol{h}_{JD}$, respectively. These fading channel gains are modeled as quasi-static frequency non-selective parameters, which means that they are constant over the block time of T seconds and independent and identically distributed between blocks. Consequently, each element of these complex fading channel coefficients are circular symmetric complex Gaussian random variables with zero mean and unit variance. In this paper, we make the following assumptions on channel state information (CSI) and noise power:

- The CSI (h_{SD} and $\boldsymbol{h}_{JD}$) is assumed to be perfectly available at both the transmitter and receiver sides. This allows benchmark system performance to be determined.
- The CSI of the eavesdropper is only known to itself.
- Noise power at the eavesdropper is zero in line with [36], which corresponds to the worst case scenario.

C. Transmission Phases

The secure communication with wireless-powered jammer takes places in two phases: (i) power transfer (PT) phase and (ii) information transmission (IT) phase, as shown in Fig. 1. During the PT phase, the source transfers power to the jammer by sending a radio signal with power $\mathcal{P}_s$. The jammer receives the radio signal, converts it to a direct current signal and stores the energy in its battery. During the IT phase, the jammer sends jamming signal to the eavesdropper with power $\mathcal{P}_J$ by using the stored energy in the battery. At the same time, the source transmits the information signal to the destination with power $\mathcal{P}_s$ under the protection of the jamming signal. We define the *information transmission probability* as the probability of the communication process being in the IT phase and denote it by p_{tx}.

D. Secure Encoding and Performance Metrics

We consider confidential transmission between the source and the destination, using Wyner's wiretap code [37]. Specifically, there are two rate parameters of the wiretap code, namely the rate of codeword transmission, denoted by R_t, and the rate of secret information, denoted by R_s. The positive rate difference $R_t - R_s$ is the cost to provide secrecy against the eavesdropper. A M-length wiretap code is constructed by generating 2^{MR_t} codewords $x^M(w, v)$ of the length M, where $w = 1, 2, \ldots, 2^{MR_s}$ and $v = 1, 2, \ldots, 2^{M(R_t - R_s)}$. For each message index w, the value of v is selected randomly with uniform probability from $\left\{1, 2, \ldots, 2^{M(R_t - R_s)}\right\}$, and the constructed codeword to be transmitted is $x^M(w, v)$. Clearly, reliable transmission from the source to the destination cannot be achieved when $R_t > C_d$, where C_d denotes the channel capacity of $S \to D$ link. This event is defined as connection outage event. From [37], perfect secrecy cannot be achieved when $R_t - R_s < C_e$, where C_e denotes the fading channel capacity of $S \to E$ link. This event is defined as secrecy outage event. In this work, we consider fixed rate transmission, which means R_t and R_s are fixed and chosen offline following [38], [39].

Since we consider quasi-static fading channel, we use outage based measures as considered in [38], [39]. Specifically, the connection outage probability and secrecy outage probability are defined, respectively, as

$$p_{co} = \mathbb{P}\{R_t > C_d\}, \tag{1}$$

$$p_{so} = \mathbb{P}\{R_t - R_s < C_e\}, \tag{2}$$

where $\mathbb{P}\{\nu\}$ denotes the probability for success of event ν. Note that the connection outage probability is a measure of the fading channel quality of the $S \to D$ link. Since the current CSI is available at the legitimate nodes, the source can always suspend transmission when connection outage occurs. This is easy to realize by one-bit feedback from the destination. Therefore, in this work, connection outage leads to suspension of IT but not decoding error at the destination.

Our figure of merit is the throughput, π, which is the average number of bits of confidential information received at the destination per unit time [33], [39], and is given by

$$\pi = p_{tx} R_s. \tag{3}$$

As we will see in Section IV, the information transmission probability p_{tx} contains the connection outage probability p_{co}.

It is important to note that a trade-off exists between throughput achieved at the destination and secrecy against the eavesdropper (measured by the secrecy outage probability). For example, increasing R_s would increase π in (3), but also increase p_{so} in (2). This trade-off will be investigated later in Section V in this paper.

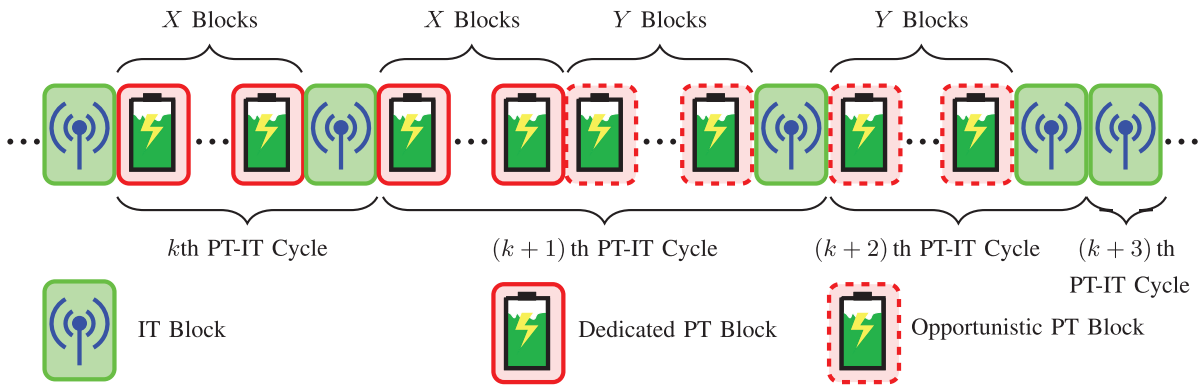


Fig. 2. Illustration of four types of PT-IT cycles.

III. Proposed Secure Communication Protocol

In this section, we propose a simple fixed-power and fixed-rate secure communication protocol, which employs a wireless-powered jammer. Note that more sophisticated power and rate adaptation strategies at the source are possible but outside the scope of this paper.

A. Transmission Protocol

We consider the communication in blocks of T seconds, each block being either a PT or an IT block. Intuitively, IT should happen when the jammer has sufficient energy for jamming and the $S \to D$ link is in a good condition to ensure successful information reception at the destination. We define the two conditions for a block to be used for IT as follows:

- At the beginning of the block, the jammer has enough energy, $\mathcal{P}_J T$, to support jamming with power $\mathcal{P}_J$ over an information transmission block of T seconds, and
- the link $S \to D$ does not suffer connection outage, which means it can support the codeword transmission rate R_t from the source to the destination.

Note that both conditions are checked at the start of each block using the knowledge of the actual amount of energy in the jammer's battery and the instantaneous CSI of $S \to D$ link, and both conditions must be satisfied simultaneously for the block to be an IT block. If the first condition is not satisfied, then the block is used for PT and we refer to it as a *dedicated PT block*. If the first condition is satisfied while the second condition is not, then the block is still used for PT but we refer it as an *opportunistic PT block*. Note that $\mathcal{P}_J$ is a design parameter in the proposed protocol.

For an accurate description of the transmission process, we define a PT-IT cycle as a sequence of blocks which either consists of a single IT block or a sequence of PT blocks followed by an IT block. Let discrete random variables X and Y ($X, Y = 0, 1, 2, \ldots$) denote the number of dedicated and opportunistic PT blocks in a PT-IT cycle, respectively. In our proposed protocol, the following four types of PT-IT cycles are possible:

1) $X > 0,\ Y = 0$, i.e., PT-IT cycle contains X dedicated PT blocks followed by an IT block. This is illustrated as the kth PT-IT cycle in Fig. 2.
2) $X > 0,\ Y > 0$, i.e., PT-IT cycle contains X dedicated PT blocks and Y opportunistic PT blocks followed by an IT block. This is illustrated as the $(k+1)$ th PT-IT cycle in Fig. 2.
3) $X = 0,\ Y > 0$, i.e., PT-IT cycle contains Y opportunistic PT blocks followed by an IT block. This is illustrated as the $(k+2)$ th PT-IT cycle in Fig. 2.
4) $X = 0,\ Y = 0$, i.e., PT-IT cycle contains one IT block only. This is illustrated as the $(k+3)$ th PT-IT cycle in Fig. 2.

B. Long-Term Behavior

We are interested in the long-term behavior (rather than that during the transition stage) of the communication process determined by our proposed protocol. After a sufficiently long time, 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, after a long time has passed, the energy steadily accumulates at the jammer and there is no need for dedicated PT blocks (the harvested energy by opportunistic PT blocks fully meet the energy consumption requirement at the jammer). Consequently, only PT-IT cycles with $X = 0$ can occur.
- *Energy Balanced*: In this case, on average, the energy harvested at the jammer during opportunistic PT blocks is lower than the energy required during an IT block. Thus, after a long time has passed, 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. Consequently, all four types of PT-IT cycles can occur.

Remarks: Although we have assumed infinite battery capacity for simplicity in the analysis, it is important to discuss the effect on finite battery capacity. In fact, our analytical result is valid for finite battery capacity as long as the battery capacity

in much higher than the required jamming energy $\mathcal{P}_J T$.[1] To be specific:

i) When the communication process is in the energy accumulation case, the harvested energy steadily accumulates at the jammer, thus, the energy level will always reach the maximum battery capacity after a sufficient long time and stay near the maximum capacity for the remaining time period. This means that the energy level in the battery is always much larger than the required jamming energy level. Thus, having a finite battery capacity has hardly any effect on the communication process, as compared with infinite capacity.

ii) When the communication process is in the energy balanced case, on average, the harvested energy equals the required (consumed) jamming energy. Therefore, the energy level mostly stays between zero and the required jamming energy level, $\mathcal{P}_J T$. This also means that the energy level in the battery can hardly approach the maximum battery capacity. Thus, having a finite battery capacity has almost no effect on the communication process, compared with infinite capacity.

Therefore, although our analysis is based on the assumption of infinite battery capacity, the analytical results still hold with practical finite battery capacity.

In the next section, the mathematical model for the proposed protocol is presented. The boundary condition between the energy accumulation and energy balanced cases is derived. In Section VI, we will also verify the long-term behavior through simulations.

IV. Protocol Analysis

In this section, we analyze the proposed secure communication protocol and derive the achievable throughput for the proposed secure communication protocol.

A. Signal Model

In a PT block, the source sends radio signal x_{SJ} with power $\mathcal{P}_s$. Thus, received signal at the jammer, $\boldsymbol{y}_J$ is given by

$$\boldsymbol{y}_J = \frac{1}{\sqrt{d_{SJ}^m}}\sqrt{\mathcal{P}_s}\boldsymbol{h}_{SJ}x_{SJ} + \boldsymbol{n}_J, \tag{4}$$

where x_{SJ} is the normalized signal from the source in an PT block, and $\boldsymbol{n}_J$ is the additive white Gaussian noise (AWGN) at the jammer. From equation (4), by ignoring the noise power, the harvested energy is given by [22]

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

where η is the energy conversion efficiency of RF-DC conversion operation for energy storage at the jammer. Because the elements of $\boldsymbol{h}_{SJ}$ are independent identically distributed complex Gaussian random variable with normalized variance, we have $\mathbb{E}\left\{|\boldsymbol{h}_{SJ}|^2\right\} = N_J$. Therefore, the average harvested energy ρ_J is given by

$$\rho_J = \mathbb{E}\left\{\rho_J(\boldsymbol{h}_{SJ})\right\} = \mathbb{E}\left\{\eta\frac{1}{d_{SJ}^m}\mathcal{P}_s\left|\boldsymbol{h}_{SJ}\right|^2 T\right\} = \frac{\eta N_J \mathcal{P}_s T}{d_{SJ}^m}. \tag{5}$$

During an IT block, the source transmits information-carrying signal with the protection from the jammer. The jammer applies different signaling methods depending on its number of antennas. When $N_J = 1$, the jammer sends a noise-like signal x_{JD} with power $\mathcal{P}_J$, affecting both the destination and the eavesdropper. When $N_J > 1$, by using the artificial interference generation method in [36], the jammer generates an $N_J \times (N_J - 1)$ matrix $\boldsymbol{W}$ which is an orthonormal basis of the null space of $\boldsymbol{h}_{JD}$, and also an vector $\boldsymbol{v}$ with $N_J - 1$ independent identically distributed complex Gaussian random elements with normalized variance.[2] Then the jammer sends $\boldsymbol{Wv}$ as jamming signal. Thus, the received signal at the destination, y_D, is given by

$$y_D = \begin{cases} \dfrac{\sqrt{\mathcal{P}_s}}{\sqrt{d_{SD}^m}}h_{SD}x_{SD} + \dfrac{\sqrt{\mathcal{P}_J}}{\sqrt{d_{JD}^m}}h_{JD}x_{JD} + n_d, & N_J = 1, \\ \dfrac{\sqrt{\mathcal{P}_s}}{\sqrt{d_{SD}^m}}h_{SD}x_{SD} + n_d, & N_J > 1, \end{cases} \tag{6}$$

where x_{SD} is the normalized information signal from the source in an IT block and n_d is the AWGN at the destination with variance σ_d^2. Note that for $N_J > 1$, the received signal is free of jamming, because the jamming signal is transmitted into the null space of $\boldsymbol{h}_{JD}$.

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

$$y_E = \begin{cases} \dfrac{\sqrt{\mathcal{P}_s}}{\sqrt{d_{SE}^m}}h_{SE}x_{SD} + \dfrac{\sqrt{\mathcal{P}_J}}{\sqrt{d_{JE}^m}}h_{JE}x_{JD} + n_e, & N_J = 1, \\ \dfrac{\sqrt{\mathcal{P}_s}}{\sqrt{d_{SE}^m}}h_{SE}x_{SD} + \dfrac{\sqrt{\mathcal{P}_J}}{\sqrt{d_{JE}^m}}\boldsymbol{h}_{JE}\dfrac{\boldsymbol{Wv}}{\sqrt{N_J - 1}} + n_e, & N_J > 1, \end{cases} \tag{7}$$

where n_e is the AWGN at the eavesdropper which we have assumed to be 0 as a worst-case scenario.

From (6), the SINR at the destination is

$$\gamma_d = \begin{cases} \dfrac{\frac{\mathcal{P}_s}{d_{SD}^m}|h_{SD}|^2}{\sigma_d^2 + \dfrac{\mathcal{P}_J}{d_{JD}^m}|h_{JD}|^2}, & N_J = 1 \\ \dfrac{\mathcal{P}_s|h_{SD}|^2}{d_{SD}^m\sigma_d^2}, & N_J > 1 \end{cases} \tag{8}$$

[1] From [40], for typical energy storage, including super-capacitor or chemical battery, the capacity easily reaches several Joules, or even several thousand Joules. While in our work, from the simulation results to be presented later, the optimal value of required jamming energy is only several micro Joules. Therefore, it is reasonable to say that the battery capacity in practice is much larger than the required jamming energy.

[2] With the assumption of zero additive noise at the eavesdropper, the null-space artificial jamming scheme works when the number of jamming antennas in larger than the number of eavesdropper antennas, as discussed in [36]. This condition is satisfied in this work when $N_J > 1$.

Hence the capacity of $S \to D$ link is given as $C_d = \log_2(1+\gamma_d)$.

Since $|h_{SD}|$ and $|h_{JD}|$ are Rayleigh distributed, $|h_{SD}|^2$ and $|h_{JD}|^2$ are exponential distributed and γ_d has the cumulative distribution function (cdf) as

$$F_{\gamma_d}(x) = \begin{cases} 1 - \dfrac{e^{-\frac{x}{\rho_d}}}{1+\varphi x}, & N_J = 1, \\ 1 - e^{-\frac{x}{\rho_d}}, & N_J > 1, \end{cases} \tag{9}$$

where

$$\varphi = \frac{\mathcal{P}_J}{\mathcal{P}_s}\frac{d_{SD}^m}{d_{JD}^m}. \tag{10}$$

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

$$\rho_d \triangleq \frac{\mathcal{P}_s}{d_{SD}^m \sigma_d^2}. \tag{11}$$

From (7), the SINR at the eavesdropper is

$$\gamma_e = \begin{cases} \dfrac{1}{\phi}\dfrac{|h_{SE}|^2}{|h_{JE}|^2}, & N_J = 1, \\ \dfrac{1}{\phi}\dfrac{|h_{SE}|^2}{\frac{\|\boldsymbol{h}_{JE}\mathbf{W}\|^2}{N_J-1}}, & N_J > 1, \end{cases} \tag{12}$$

where

$$\phi = \frac{\mathcal{P}_J}{\mathcal{P}_s}\frac{d_{SE}^m}{d_{JE}^m}. \tag{13}$$

Hence, the capacity of $S \to E$ link is given as $C_e = \log_2(1+\gamma_e)$. Using the fact that h_{SE}, h_{JE} and the entries of $\boldsymbol{h}_{JE}\mathbf{W}$ are independent and identically distributed (i.i.d.) complex Gaussian variables, from [33], γ_e has the probability density function (pdf) as

$$f_{\gamma_e}(x) = \begin{cases} \phi\left(\dfrac{1}{\phi x+1}\right)^2, & N_J = 1, \\ \phi\left(\dfrac{N_J-1}{\phi x+N_J-1}\right)^{N_J}, & N_J > 1. \end{cases} \tag{14}$$

Using the pdf of γ_e in (14), the secrecy outage probability defined in (2) can be evaluated.

B. Information Transmission Probability

Focusing on the long-term behavior, we analyze the proposed secure communication protocol and derive the information transmission probability p_{tx}, which in turn gives the throughput in (3). Note that p_{tx} is the probability of an arbitrary block being used for IT. As discussed in the last section, the communication process falls in either energy accumulation or energy balanced case. Thus, p_{tx} will have different values for the two different cases. First we mathematically characterize the condition of being in either case in the lemma below.

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

$$\frac{p_{co}}{1-p_{co}} > \frac{\mathcal{P}_J T}{\rho_J} \tag{15}$$

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

Proof: See Appendix A. ■

Using Lemma 1, we can find the general expression for p_{tx} as presented in Theorem 1 below.

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

$$p_{tx} = \frac{1}{1+\max\left\{\frac{\mathcal{P}_J T}{\rho_J}, \frac{p_{co}}{1-p_{co}}\right\}}, \tag{16}$$

where

$$p_{co} = \begin{cases} 1 - \dfrac{e^{-\frac{2^{R_t}-1}{\rho_d}}}{1+\frac{\mathcal{P}_J}{\mathcal{P}_s}\frac{d_{SD}^m}{d_{JD}^m}\left(2^{R_t}-1\right)}, & N_J = 1, \\ 1 - e^{-\frac{2^{R_t}-1}{\rho_d}}, & N_J > 1. \end{cases} \tag{17}$$

Proof: 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 either directly or by using time averaging. The detailed proof can be found in Appendix B. ■

By substituting (16) in (3), we obtain the achievable throughput of the proposed protocol.

V. Optimal Design for Throughput

In the last section, we derived the achievable throughput with given design parameters. Specifically the jamming power $\mathcal{P}_J$ is a design parameter of the protocol. A different value of $\mathcal{P}_J$ results in a different impact on the eavesdropper's SINR, hence leads to different secrecy outage probability defined in (2). Also the rate parameters of the wiretap code, R_t and R_s, affect the secrecy outage probability. Hence, it is interesting to see how one can optimally design these parameters to maximize the throughput while keeping the secrecy outage probability below a prescribed threshold. In this section, we present such an optimal fixed-rate design of the proposed secure communication protocol. The optimization is done offline, hence does not increase the complexity of the proposed protocol.

A. Problem Formulation

We consider the optimal secure communication design as follows:

$$\begin{aligned} &\max_{\mathcal{P}_J, R_t, R_s} \quad \pi \\ &\text{s.t.} \quad p_{so} \le \varepsilon, \mathcal{P}_J \ge 0, R_t \ge R_s \ge 0, \end{aligned} \tag{18}$$

where ε is the secrecy outage probability constraint. This design aims to maximize the throughput with the constraint on the secrecy outage probability.

From (2), the secrecy outage probability should meet the requirement that

$$p_{so} = \mathbb{P}\left\{R_t - R_s < \log_2(1+\gamma_e)\right\} \le \varepsilon. \tag{19}$$

By substituting (14) into (19), and after some manipulations, the jamming power $\mathcal{P}_J$ should satisfy the condition

$$\mathcal{P}_J \ge \hat{\mathcal{P}}_J \triangleq \begin{cases} \mathcal{P}_s \dfrac{d_{JE}^m}{d_{SE}^m} \dfrac{\left(\varepsilon^{-1}-1\right)}{2^{R_t-R_s}-1}, & N_J = 1, \\ \mathcal{P}_s \dfrac{d_{JE}^m}{d_{SE}^m} \dfrac{(N_J-1)\left(\varepsilon^{-\frac{1}{N_J-1}}-1\right)}{2^{R_t-R_s}-1}, & N_J > 1. \end{cases} \tag{20}$$

From (16), we can see that π decreases with $\mathcal{P}_J$. Thus, the maximum π is obtained when

$$\mathcal{P}_J^\star = \hat{\mathcal{P}}_J. \tag{21}$$

The jammer harvests energy from the source in each PT block. The dynamically harvested and accumulated energy at the jammer must exceed $\mathcal{P}_J^\star T$, before it can be used to send jamming signal with power $\mathcal{P}_J^\star$.

Substituting (21) and (16), into (3), the throughput with optimal jamming power $\mathcal{P}_J^\star$ satisfying the secrecy outage constraint of $p_{so} \le \varepsilon$, is given by (22), shown at the bottom of the page.

Note that the terms (a) and (b) in (22) are the terms $\frac{\mathcal{P}_J T}{\rho_J}$ and $\frac{p_{co}}{1-p_{co}}$ in Lemma 1, respectively. Thus, if we choose (R_t, R_s) to make $(a) < (b)$, the communication process leads to energy accumulation; while if (R_t, R_s) make $(a) \ge (b)$, the communication process is energy balanced. For analytical convenience, we define three 2-dimension rate regions:

$$\mathcal{D}_1 \triangleq \{(R_t, R_s)\,|(a) < (b),\, R_t \ge R_s \ge 0\}, \tag{23}$$

$$\hat{\mathcal{D}} \triangleq \{(R_t, R_s)\,|(a) = (b),\, R_t \ge R_s \ge 0\}, \tag{24}$$

$$\mathcal{D}_2 \triangleq \{(R_t, R_s)\,|(a) > (b),\, R_t \ge R_s \ge 0\}, \tag{25}$$

where rate region $\hat{\mathcal{D}}$ denotes the boundary between regions $\mathcal{D}_1$ and $\mathcal{D}_2$. From the discussion above, if $(R_t, R_s) \in \mathcal{D}_1$, the communication process leads to energy accumulation, while if $(R_t, R_s) \in \mathcal{D}_2 \cup \hat{\mathcal{D}}$, it is energy balanced.

Using (22), the optimization problem in (18) can be rewritten as

$$\begin{aligned} &\max_{R_t, R_s} \ \pi\left(\mathcal{P}_J^\star\right) \\ &\text{s.t. } R_t \ge R_s \ge 0. \end{aligned} \tag{26}$$

The optimization problem in (26) can be solved with global optimal solution. The solution for $N_J = 1$ and $N_J > 1$ are presented in the next two subsections.

B. Optimal Rate Parameters with Single-Antenna Jammer

Proposition 1: When $N_J = 1$, the optimal R_t and R_s can be obtained by using the following facts:
IF $\left(R_t^\star, R_s^\star\right) \in \mathcal{D}_1$, i.e., the case of energy accumulation, $R_s^\star$ is the unique root of equation (monotonic increasing on the left side):

$$k_2\left(2^{R_s} + \frac{2^{R_s}-1}{\xi}\right)\left(R_s \ln 2 - 1 + \frac{R_s \ln 2}{\xi}\right) = 1, \tag{27}$$

and $R_t^\star$ is given by

$$R_t^\star = R_s^\star + \log_2\left(1+\xi^\star\right), \tag{28}$$

where

$$\xi = \frac{1}{2}\left(-\frac{k_2\left(2^{R_s}-1\right)}{1+k_2 2^{R_s}} + \left(\left(\frac{k_2\left(2^{R_s}-1\right)}{1+k_2 2^{R_s}}\right)^2 + \frac{4\rho_d k_2\left(1-\frac{1}{2^{R_s}}\right)}{1+k_2 2^{R_s}}\right)^{\frac{1}{2}}\right), \tag{29}$$

and $\xi^\star$ is obtained by taking $R_s^\star$ into (29).
ELSE, $\left(R_t^\star, R_s^\star\right) \in \hat{\mathcal{D}}$, i.e., the energy balanced case, and $R_t^\star$ is the root of following equation which can be easily solved by a linear search:

$$\zeta'\left(\frac{1+\frac{k_1}{\zeta}}{\ln 2\,(1+\zeta)} - \frac{k_1\left(R_t - \log_2(1+\zeta)\right)}{\zeta^2}\right) = 1, \tag{30}$$

$$\pi\left(\mathcal{P}_J^\star\right) = \begin{cases} \dfrac{R_s}{1+\max\left\{\underbrace{\dfrac{d_{SJ}^m}{\eta}\dfrac{d_{JE}^m}{d_{SE}^m}\dfrac{\left(\varepsilon^{-1}-1\right)}{2^{R_t-R_s}-1}}_{(a)}, \underbrace{e^{\frac{\left(2^{R_t}-1\right)}{\rho_d}\left(1+\frac{d_{JE}^m}{d_{SE}^m}\frac{d_{SD}^m}{d_{JD}^m}\frac{\left(\varepsilon^{-1}-1\right)}{2^{R_t-R_s}-1}\left(2^{R_t}-1\right)\right)}-1}_{(b)}\right\}}, & N_J = 1, \\ \dfrac{R_s}{1+\max\left\{\underbrace{\dfrac{d_{SJ}^m}{N_J\eta}\dfrac{d_{JE}^m}{d_{SE}^m}\dfrac{(N_J-1)\left(\varepsilon^{-\frac{1}{N_J-1}}-1\right)}{2^{R_t-R_s}-1}}_{(a)}, \underbrace{e^{\frac{2^{R_t}-1}{\rho_d}}-1}_{(b)}\right\}}, & N_J > 1. \end{cases} \tag{22}$$

where

$$\zeta = \frac{k_1 - k_2 e^{\frac{2^{R_t}-1}{\rho_d}}\left(2^{R_t}-1\right)}{e^{\frac{2^{R_t}-1}{\rho_d}}-1}, \tag{31}$$

$$\zeta' = \frac{\ln 2\, e^{\frac{2^{R_t}-1}{\rho_d}}}{\left(e^{\frac{2^{R_t}-1}{\rho_d}}-1\right)^2}\left(k_2\, 2^{R_t}\left(1+\frac{1}{\rho_d}-e^{\frac{2^{R_t}-1}{\rho_d}}\right)-\frac{k_1+k_2}{\rho_d}\right), \tag{32}$$

$$k_1 = \frac{d_{SJ}^m}{\eta}\frac{d_{JE}^m}{d_{SE}^m}\left(\varepsilon^{-1}-1\right), \tag{33}$$

$$k_2 = \frac{d_{JE}^m}{d_{SE}^m}\frac{d_{SD}^m}{d_{JD}^m}\left(\varepsilon^{-1}-1\right), \tag{34}$$

and $R_s^\star = R_t^\star - \log_2(1+\zeta^\star)$, where $\zeta^\star$ is calculated by taking $R_t^\star$ into (31).

Proof: See Appendix C. ■

Note that the optimal (R_t, R_s) never falls in region $\mathcal{D}_2$. This is because the throughput in $\mathcal{D}_2$ increases towards the boundary of $\mathcal{D}_1$ and $\mathcal{D}_2$, that is $\hat{\mathcal{D}}$. The detailed explanation is given in Appendix C.

Proposition 1 can then be used to obtain the optimal values of R_t and R_s as follows. We firstly assume the optimal results are in the region $\mathcal{D}_1$, thus, R_s and R_t can be obtained by equation (27) and (28). Then, we check whether the results are really in $\mathcal{D}_1$. If they are, we have obtained the optimal results. If not, we solve equation (30) to obtain the optimal R_t and R_s.

1) High SNR Regime: We want know whether we can largely improve throughput by increasing the transmit power at the source, $\mathcal{P}_s$, thus, 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 (11).

Corollary 1: When $N_J = 1$ and the SNR at the destination is sufficiently high, the asymptotically optimal rate parameters and an upper bound of throughput are given by

$$\tilde{R}_s^\star = \frac{1+\mathrm{W}_0\left(\frac{1}{ek_2}\right)}{\ln 2}, \tag{35a}$$

$$\tilde{R}_t^\star = \tilde{R}_s^\star + \log_2\left(1+\tilde{\xi}^\star\right), \tag{35b}$$

$$\tilde{\pi}^\star = \frac{\mathrm{W}_0\left(\frac{1}{ek_2}\right)}{\ln 2}, \tag{35c}$$

where k_2 is defined in (34),

$$\tilde{\xi}^\star = \left(\frac{\rho_d k_2\left(1-\frac{1}{2^{\tilde{R}_s^\star}}\right)}{1+k_2 2^{\tilde{R}_s^\star}}\right)^{\frac{1}{2}}, \tag{36}$$

and $\mathrm{W}_0(\cdot)$ is the principle branch of the Lambert W function [41].

Proof: See Appendix D. ■

Remarks:

i) The upper bound of throughput implies that one cannot effectively improve the throughput by further increasing $\mathcal{P}_s$ when the SNR at the destination is already high.

ii) It can be checked that when $\mathcal{P}_s$ is sufficiently high, the optimized communication process leads to energy accumulation. Intuitively, this implies that when the available harvested energy is very large, the jammer should store a significant portion of the harvested energy in the battery rather than fully using it, because too much jamming noise can have adverse impact on SINR at the destination in this single-antenna jammer scenario. This behavior will also be verified in Section VI, Fig. 4.

C. Optimal Rate Parameters with Multiple-Antenna Jammer

Proposition 2: When $N_J > 1$, the optimal R_s and R_t are in region $\hat{\mathcal{D}}$ which also means that the optimal communication process is in the energy balanced case, and the optimal values are given by

$$R_t^\star = \log_2 z^\star,$$
$$R_s^\star = \log_2 \frac{z^\star}{1+\frac{M}{e^{\frac{z^\star-1}{\rho_d}}-1}}, \tag{37}$$

where $z^\star$ is calculated as the unique solution of

$$\frac{\rho_d}{z} - \ln z + \ln\left(1+\frac{M}{e^{\frac{z-1}{\rho_d}}-1}\right) + \frac{M e^{\frac{z-1}{\rho_d}}}{\left(e^{\frac{z-1}{\rho_d}}-1\right)^2 + M\left(e^{\frac{z-1}{\rho_d}}-1\right)} = 0, \tag{38}$$

and

$$M = \frac{d_{SJ}^m}{N_J \eta}\frac{d_{JE}^m}{d_{SE}^m}(N_J-1)\left(\varepsilon^{-\frac{1}{N_J-1}}-1\right). \tag{39}$$

Proof: See Appendix E. ■

We can see that the left side of (38) is a monotonic decreasing function of z. Thus, z can be easily obtained by using numerical methods.

1) High SNR Regime: Similar to the single-antenna jammer case, we are interested in whether increasing the source transmission power $\mathcal{P}_s$, is an effective way of improving throughput. Hence the high SNR regime is considered:

Corollary 2: When $N_J > 1$ and the SNR at the destination is sufficiently high, the asymptotically optimal rate parameters and an upper bound of throughput are given by

$$\tilde{R}_t^\star = \log_2(2\rho_d) - \log_2\left(\mathrm{W}_0(2\rho_d)\right), \tag{40a}$$

$$\tilde{R}_s^\star = \frac{2\mathrm{W}_0(2\rho_d)}{\ln 2} - \log_2(M\rho_d), \tag{40b}$$

$$\tilde{\pi}^\star = \tilde{R}_s^\star, \tag{40c}$$

where $z^\star = \frac{2\rho_d}{\mathrm{W}_0(2\rho_d)}$ and M is defined in (39).

Proof: See Appendix F. ■

Remarks:

1) The throughput will always increase with increasing transmit power $\mathcal{P}_s$ (because ρ_d increases as $\mathcal{P}_s$ increases).

This is in contrast to the single-antenna jammer case, because the multi-antenna jamming method only interferes the $S \to E$ link.

ii) From Proposition 2 and Corollary 2, when $\mathcal{P}_s$ is sufficiently large, the optimized communication process is still energy balanced, which is different from the single-antenna jammer scenario. Intuitively, storing extra energy is not a good choice, because we can always use the accumulated energy to jam at the eavesdropper without affecting the destination, which in turn improves the throughput.

2) Large N_J Regime: We also want to know that whether we can largely improve the throughput by increasing the number of antennas at the jammer.

Corollary 3: In large N_J scenario, the asymptotically optimal rate parameters and an upper bound of throughput are given by

$$\tilde{R}_t^\star = \frac{\mathrm{W}_0(\rho_d)}{\ln 2}, \tag{41a}$$

$$\tilde{R}_s^\star = \log_2 \frac{e^{\mathrm{W}_0(\rho_d)}}{1 + \frac{M}{e^{\frac{\mathrm{W}_0(\rho_d)-1}{\rho_d}} - 1}}, \tag{41b}$$

$$\tilde{\pi}^\star = \frac{\mathrm{W}_0(\rho_d)}{\ln 2\, e^{\frac{1}{\mathrm{W}_0(\rho_d)} - \frac{1}{\rho_d}}}, \tag{41c}$$

where M is defined in (39).

Proof: See Appendix F. ■

Remark: Corollary 3 gives an asymptotic upper bound on throughput for this protocol, thus, π does not increase towards infinity with N_J. Intuitively, the throughput cannot always increase with N_J, because it is bounded by the $S \to D$ channel capacity which is independent with N_J.

VI. 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 $T = 1$ millisecond. We set the energy conversion efficiency as $\eta = 0.5$ [22], [23], [25]. Note that the practical designs of rectifier for RF-DC conversion achieve the value of η between 0.1 and 0.85 [19]. Such a range makes wireless energy harvesting technology meaningful. A rectifier design with $\eta < 0.1$ is unlikely to be used in practice. 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 [13]. Unless otherwise stated, we set $\sigma_d^2 = -100$ dBm, and the secrecy outage probability requirement $\varepsilon = 0.01$. We do not specify the bandwidth of communication, hence the rate parameters are expressed in units of bit per channel use (bpcu).

To give some ideas about the energy harvesting process at the jammer under this setting: When $N_J = 1$ and $\mathcal{P}_s = 30$ dBm, the average power that can be harvested (after RF-DC conversion) is -15 dBm, thus, the overall energy harvesting efficiency (i.e., the ratio between the harvested power at the jammer and the transmit power at the source) is $(-15\text{ dBm})/(30\text{ dBm}) \approx 3 \times 10^{-5}$. Note that, although the average harvested power at the jammer is relatively small, a small jamming power is sufficient to achieve good secure communication performance. For instance, the optimal jamming power under this setting is only -13 dBm based on the analytical results in Section V. In order to transmit the jamming signal at the optimal power of -13 dBm with the average harvested power of -15 dBm, roughly 61% of time is used for charging and 39% of time is used for secure communication with jamming.

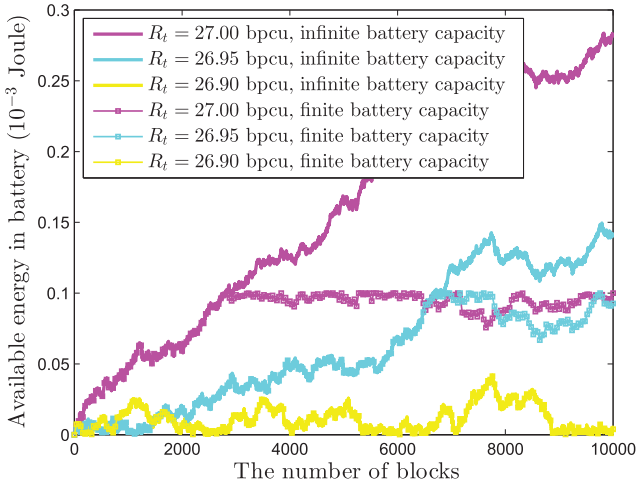


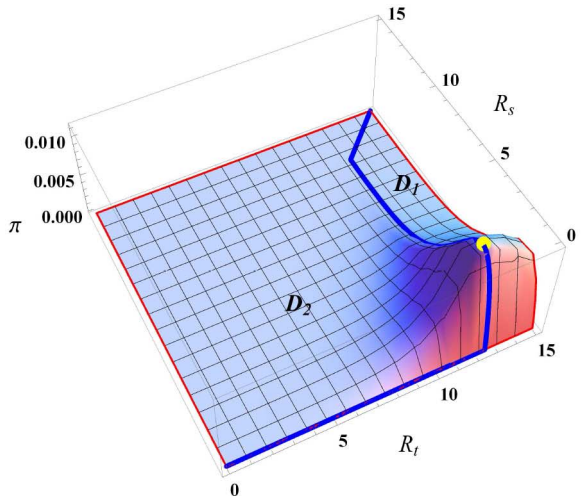
Fig. 3. Available energy in battery during the communication process.

A. Energy Accumulation and Energy Balanced Cases

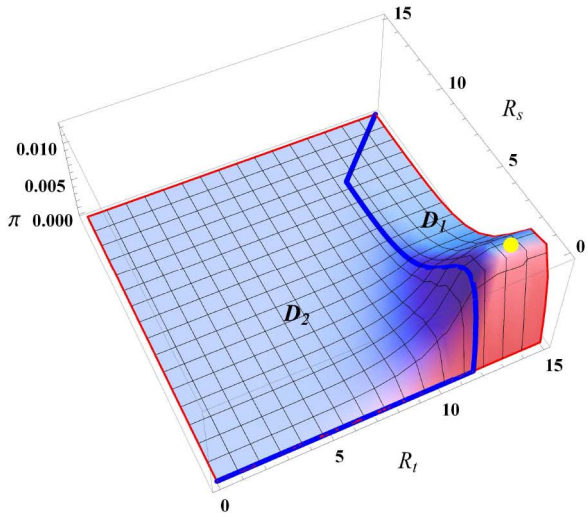
Fig. 3 shows the simulation results on the available energy in the battery in the communication process. The jammer has 8 antennas ($N_J = 8$) and the target jamming power is $\mathcal{P}_J = 0$ dBm. The source transmit power is $\mathcal{P}_s = 30$ dBm. Thus, the energy consumption in one IT block at the jammer, $\mathcal{P}_J T$, is 10^{-6} Joule, and the average harvested energy in one PT block, ρ_J, is 2.56×10^{-7} Joule. From Lemma 1 and (17), when $\frac{p_{co}}{1-p_{co}} > \frac{\mathcal{P}_J T}{\rho_J}$ which means $R_t > 26.92$ bpcu, the communication process leads to energy accumulation, while if $R_t \leq 26.92$ bpcu, it is the energy balanced.

First, we focus on the curves with infinite battery capacity. We can see that when $R_t = 26.9$ bpcu, the available energy goes up and down, but does not have the trend of energy accumulation. Thus, the communication process is energy balanced. When $R_t = 26.95$ and 27 bpcu, the available energy grows up, and the communication process leads to energy accumulation. Therefore, the condition given in Lemma 1 is verified.

In Fig. 3, we also plot a set of simulation results with finite battery capacity as $E_{\max} = 0.1 \times 10^{-3}$ Joule. As we can see, for the energy accumulative cases, i.e., $R_t = 26.95$ and 27.00 bpcu, the energy level stays near the battery capacity (0.1×10^{-3} Joule) after experienced a sufficient long time, which is much higher than the required jamming energy level $\mathcal{P}_J T = 10^{-6}$ Joule. Therefore, in practice, having a finite battery capacity has hardly any effect on the communication process, as compared with infinite capacity.



(a) $N_J = 1$, $\mathcal{P}_s = 0$ dBm



(b) $N_J = 1$, $\mathcal{P}_s = 30$ dBm

Fig. 4. Optimal rate parameters for $N_J = 1$.

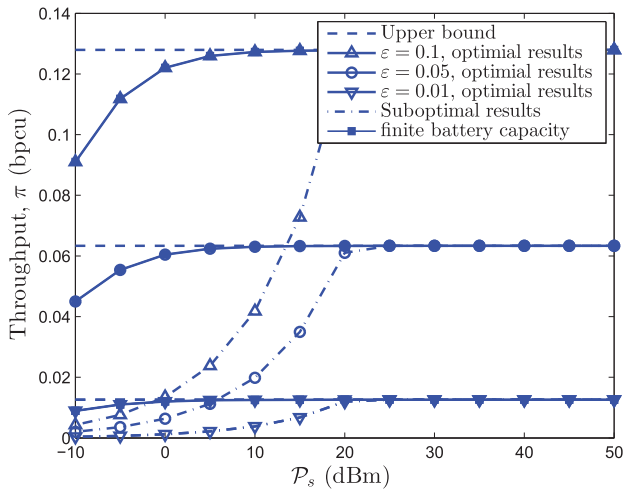
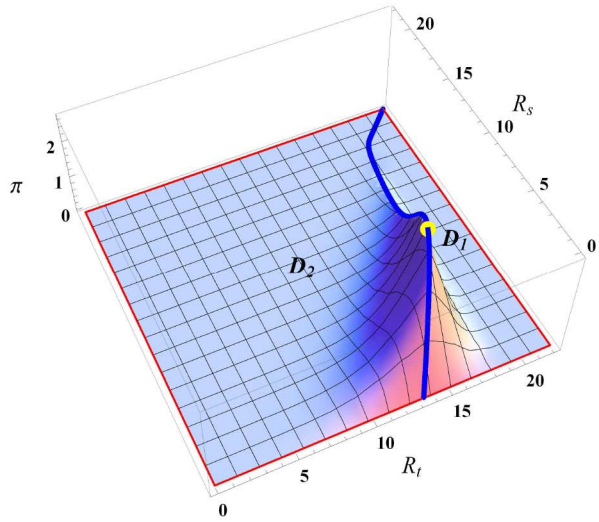
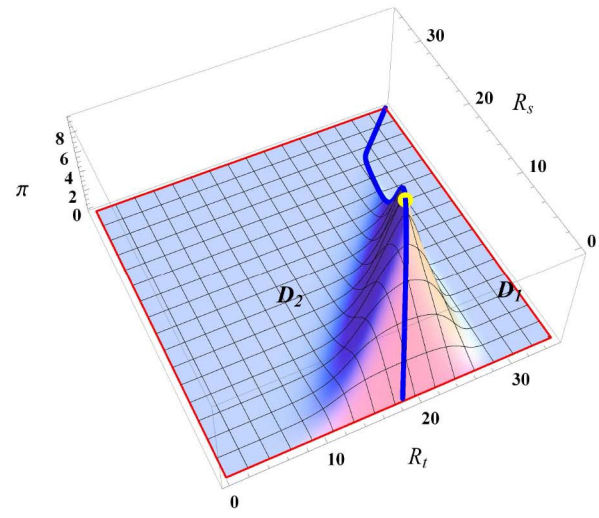


Fig. 5. Throughput versus source transmit power $\mathcal{P}_s$ for $N_J = 1$.



(a) $N_J = 8$, $\mathcal{P}_s = 0$ dBm



(b) $N_J = 8$, $\mathcal{P}_s = 30$ dBm

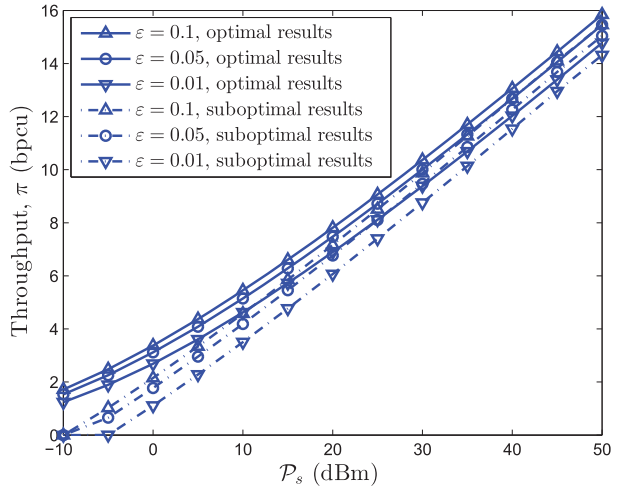
Fig. 6. Optimal rate parameters for $N_J = 8$.

B. Rate Regions with Single-Antenna Jammer

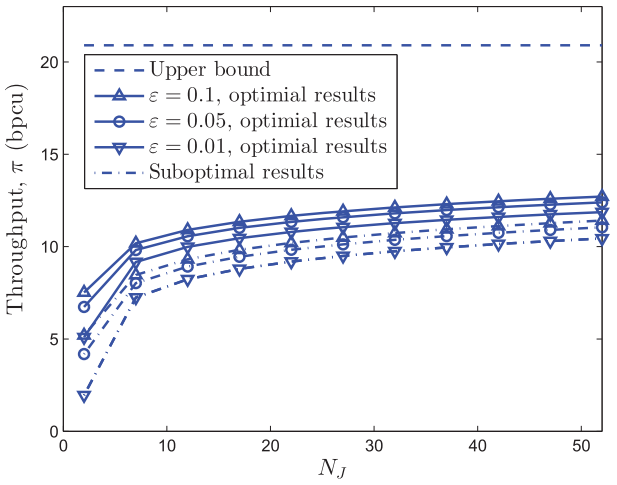
Fig. 4 plots the throughput in (22) with different R_t and R_s in the single-antenna jammer scenario. In Fig. 4(a), we set $\mathcal{P}_s = 0$ dBm. The optimal rate parameters $\left(R_t^\star, R_s^\star\right)$ are obtained in the region $\hat{\mathcal{D}}$, which is the boundary of $\mathcal{D}_1$ and $\mathcal{D}_2$. This implies that the optimized communication process is energy balanced. In Fig. 4(b), we increase $\mathcal{P}_s$ to 30 dBm. The optimal rate parameters $\left(R_t^\star, R_s^\star\right)$ are obtained in the region $\mathcal{D}_1$. This implies that the optimized communication process leads to energy accumulation. This observation agrees with the remarks after Corollary 1 regarding the optimal operating point when the SNR at the destination is sufficiently large.

C. Throughput Performance with Single-Antenna Jammer

Fig. 5 plots the throughput with optimal designs given by Proposition 1. We also include the suboptimal performance which is achieved by using the asymptotically optimal rate parameters in Corollary 1, as well as the upper bound on throughput in Corollary 1.



(a) Throughput vs. source transmit power $\mathcal{P}_s$ for $N_J = 8$.



(b) Throughput vs. number of antennas at the jammer, $N_J \geq 2$.

Fig. 7. Throughput for $N_J > 1$.

First, we focus on the curves with infinite battery capacity. We can see that when $\mathcal{P}_s = 5$ dBm, the optimal throughput almost reaches the upper bound. Also we can see that when $\mathcal{P}_s < 20$ dBm, the suboptimal performance has a large gap with the optimal one, while when $\mathcal{P}_s > 20$ dBm, the suboptimal performance is very close to the optimal one.

In Fig. 5, we also plot a set of simulation results with finite battery capacity as $E_{\max} = 0.1 \times 10^{-3}$ Joule. It is easy to see that our analytical results for infinite battery capacity fit very well with the simulation results for finite battery capacity. Therefore, a practical finite battery capacity have negligible effect on the performance of the protocol, and our analysis are valid in the practical scenario.

D. Rate Regions with Multiple-Antenna Jammer

Fig. 6 plots the throughput in (22) with different R_t and R_s in the multiple-antenna jammer scenario. In Fig. 6(a) and Fig. 6(b), we set $\mathcal{P}_s = 0$ dBm and 30 dBm, respectively. The optimal rate parameters $\left(R_t^\star, R_s^\star\right)$ are both obtained in the region $\hat{\mathcal{D}}$. This implies that the optimized communication process is energy balanced, which agrees with the remarks after Corollary 2.

E. Throughput Performance with Multiple-Antenna Jammer

Fig. 7(a) plots the optimal throughput from Proposition 2. We also present the suboptimal performance which is achieved by the asymptotically optimal rate parameters obtained in Corollary 2. We can see that the throughput increases with $\mathcal{P}_s$ unbounded. Also we can see that the suboptimal performance is reasonably good when $\mathcal{P}_s > 20$ dBm.

Fig. 7(b) plots the throughput achieved with the optimal design given in Proposition 2 for different N_J. The source transmit power is $\mathcal{P}_s = 30$ dBm. We also include the suboptimal performance achieved by the asymptotically optimal rate parameters in the large N_J regime (Corollary 3) as well as the upper bound on throughput in Corollary 3.

We can see that with the increment of N_J, although theoretically the throughput is upper bounded as $N_J \to \infty$, the available throughput within practical range of N_J is far from the upper bound. Hence, increasing N_J is still an efficient way to improve the throughput with practical antenna size. Also we can see that the suboptimal performance is acceptable but the gap from the optimal throughput performance is still noticeable.

VII. Conclusion

In this paper, we investigated secure communication with the help from a wireless-powered jammer. We proposed a simple communication protocol and derived its achievable throughput with fixed-rate transmission. We further optimized the rate parameters to achieve the best throughput subject to a secrecy outage probability constraints. As energy harvesting and wireless power transfer become emerging solutions for energy constrained networks, this work has demonstrated how to make use of an energy constrained friendly jammer to enable secure communication without relying on an external energy supply. For future work, the protocol can be extended to include more sophisticated adaptive transmission schemes, such as variable power transmission with an average power constraint at the source. Also these schemes can be generalized to multiple antennas at all nodes as well but with a certain constraint on the receiver noise level or the number of transmit/receive antennas at the jammer/eavesdropper (as needed in all physical layer security work). We will explore these relevant problems in our further work. Also our design idea can be borrowed and apply other EH method, such as solar, vibration, thermoelectric, wind and even hybrid energy harvesting with several energy sources. However, apart from secure communication performance and EH efficiency, dimension requirements, implementation complexity, costs should be considered. Also our design idea can be borrowed and applied with other EH methods, such as solar, vibration, thermoelectric, wind, and even hybrid energy harvesting with several energy sources. However, apart from communication performance and EH efficiency, dimension requirements, implementation complexity and costs should also be taken into account in the design.

APPENDIX A
PROOF OF LEMMA 1

In one PT-IT cycle, once the available energy is higher than $\mathcal{P}_J T$, there will be Y opportunistic PT blocks. The probability of the discrete random variable Y being k is the probability that the successive k blocks, suffer from connection outage of the $S \to D$ link, and the $(k+1)$th block does not have the $S \to D$ outage. Due to the i.i.d. channel gains in different blocks, Y follows a geometric distribution and the probability mass function (pmf) is given by

$$\mathbb{P}\{Y=k\} = p_{co}^{k}\left(1-p_{co}\right), k=0,1,\ldots. \tag{A.1}$$

The mean value of Y is given by

$$\mathbb{E}\{Y\} = \sum_{k=0}^{\infty} k\mathbb{P}\{Y=k\} = \sum_{k=0}^{\infty} k p_{co}^{k}\left(1-p_{co}\right) = \frac{p_{co}}{1-p_{co}}. \tag{A.2}$$

As we have defined ρ_J as the average harvested energy by one PT block, the average harvested energy by Y opportunistic PT blocks in one PT-IT cycle is given by

$$\mathcal{E}_Y = \mathbb{E}\{Y\}\rho_J = \frac{p_{co}}{1-p_{co}}\rho_J. \tag{A.3}$$

If the average harvested energy by opportunistic PT blocks in a PT-IT cycle is higher than the required energy, $\mathcal{P}_J T$, for jamming in one IT block, the communication process leads to energy accumulation. Otherwise, we need dedicated PT blocks in some PT-IT cycles, and the communication process is energy balanced. Thus, we have the condition in Lemma 1.

APPENDIX B
PROOF OF THEOREM 1

We derive information transmission probability p_{tx} in the following two cases.

Energy Accumulation Case: In this case, there are no dedicated PT blocks. We use a simple Markov chain with two states, IT and opportunistic PT, to model the communication process. When the fading channel of $S \to D$ link suffers connection outage, the block is in the opportunistic PT state, otherwise it is in the IT state. This Markov chain is ergodic since the fading channel of $S \to D$ link is i.i.d. between blocks. The information transmission probability is simply the probability that the $S \to D$ link does not suffer connection outage, hence we have

$$p_{tx} = 1 - p_{co} = \frac{1}{1+\frac{p_{co}}{1-p_{co}}}. \tag{B.1}$$

Energy Balanced Case: In this case, the available energy at the jammer becomes directly relevant to whether a block is used for IT or PT. Following the recent works, such as [27], we model the energy state at the beginning/end of each time block as a Markov chain in order to obtain the information transmission probability. Since the energy state is continuous, we adopt Harris chain which can be treated as a Markov chain on a general state space (continuous state Markov chain).

It is easy to show that this Harris chain is recurrent and aperiodic, because any current energy state can be revisited in some future block, and one cannot find any two energy states that the transition from one to the other is periodic. Therefore, the Harris chain is ergodic [42], and there exists a unique stationary measure (stationary distribution), which means that the stationary distribution of available energy at the beginning/end of each block exists. Thus, the stationary probability of a block being used for IT (p_{tx}) or PT exists.

Instead of deriving the stationary distribution of energy states, we use time averaging which makes use of the ergodic property, to calculate the information transmission probability p_{tx} which is given by

$$p_{tx} = \lim_{\mathcal{N}_{total}\to\infty} \frac{\mathcal{N}_{IT}}{\mathcal{N}_{PT}+\mathcal{N}_{IT}} = \lim_{\mathcal{N}_{total}\to\infty} \frac{1}{1+\mathcal{N}_{PT}/\mathcal{N}_{IT}}, \tag{B.2}$$

where $\mathcal{N}_{IT}$ and $\mathcal{N}_{PT}$ denotes the number of IT and PT blocks in the communication process, $\mathcal{N}_{total} \triangleq \mathcal{N}_{PT}+\mathcal{N}_{IT}$. By using the principle of conservation of energy (i.e., all the harvested energy in PT blocks are used for jamming in IT blocks) and the law of large numbers, we have

$$\lim_{\mathcal{N}_{total}\to\infty} \frac{\mathcal{N}_{PT}\,\rho_J}{\mathcal{N}_{IT}\,\mathcal{P}_J T} = 1, \tag{B.3}$$

where ρ_J is the average harvested energy in one PT block defined in (5) and $\mathcal{P}_J T$ is the energy used for jamming in one IT block. By taking (B.3) into (B.2) the information transmission probability is given by

$$p_{tx} = \frac{1}{1+\frac{\mathcal{P}_J T}{\rho_J}}. \tag{B.4}$$

General Expression: Based on Lemma 1, (B.1) and (B.4), we can easily obtain the general expression for p_{tx} as

$$p_{tx} = \frac{1}{1+\max\left\{\frac{\mathcal{P}_J T}{\rho_J}, \frac{p_{co}}{1-p_{co}}\right\}}. \tag{B.5}$$

From (1), we have,

$$p_{co} = \mathbb{P}\left\{\log_2(1+\gamma_d) < R_t\right\} = \mathbb{P}\left\{\gamma_d < 2^{R_t}-1\right\} = F_{\gamma_d}\left(2^{R_t}-1\right). \tag{B.6}$$

By taking (9) into (B.6), we obtain the expression of p_{co} in (17).

APPENDIX C
PROOF OF PROPOSITION 1

Case I: If optimal $(R_t, R_s) \in \mathcal{D}_1$, the optimization problem can be rewritten as

$$\max_{(R_t,R_s)\in\mathcal{D}_1} \quad \pi = \frac{R_s}{e^{\frac{\left(2^{R_t}-1\right)}{\rho_d}}\left(1+\frac{k_2\left(2^{R_t}-1\right)}{2^{R_t-R_s}-1}\right)}. \tag{C.1}$$

The optimal (R_t, R_s) should satisfies $\frac{\partial \pi}{\partial \varsigma} = 0$ and $\frac{\partial \pi}{\partial R_s} = 0$, where $\varsigma \triangleq 2^{R_t}$.

Since ς only appears in the denominator of (C.1), by taking the partial derivative of (C.1) about ς,

$$\frac{\partial \pi}{\partial \varsigma} = 0 \Leftrightarrow \frac{\partial\left(e^{\frac{(\varsigma-1)}{\rho_d}}\left(1+\frac{k_2(\varsigma-1)}{\frac{\varsigma}{2^{R_s}}-1}\right)\right)}{\partial \varsigma} = 0, \tag{C.2}$$

which can be further expanded and simplified as

$$e^{\frac{\varsigma}{\rho_d}}\left(\frac{1}{\rho_d}\left(1+\frac{k_2\left(\varsigma-1\right)}{\frac{\varsigma}{2^{R_s}}-1}\right)-\frac{k_2\left(1-\frac{1}{2^{R_s}}\right)}{\left(\frac{\varsigma}{2^{R_s}}-1\right)^2}\right)=0. \quad \text{(C.3)}$$

Because $e^{\frac{\varsigma}{\rho_d}}>0$, (C.3) is equivalent to

$$\left(\frac{\varsigma}{2^{R_s}}-1\right)\left(\frac{\varsigma}{2^{R_s}}-1+k_2 2^{R_s}\left(\frac{\varsigma}{2^{R_s}}-1\right)+k_2 2^{R_s}\left(1-\frac{1}{2^{R_s}}\right)\right) - \rho_d k_2\left(1-\frac{1}{2^{R_s}}\right)=0. \quad \text{(C.4)}$$

By using $\xi \triangleq \frac{\varsigma}{2^{R_s}}-1$, (C.4) can be further simplified as

$$\xi^2+\frac{k_2 2^{R_s}\left(1-\frac{1}{2^{R_s}}\right)}{1+k_2 2^{R_s}}\xi-\frac{\rho_d k_2\left(1-\frac{1}{2^{R_s}}\right)}{1+k_2 2^{R_s}}=0, \quad \text{(C.5)}$$

which has a single positive root as (since $\xi>0$)

$$\xi=\frac{1}{2}\left(-\frac{k_2\left(2^{R_s}-1\right)}{1+k_2 2^{R_s}} + \left(\left(\frac{k_2\left(2^{R_s}-1\right)}{1+k_2 2^{R_s}}\right)^2+\frac{4\rho_d k_2\left(1-\frac{1}{2^{R_s}}\right)}{1+k_2 2^{R_s}}\right)^{\frac{1}{2}}\right). \quad \text{(C.6)}$$

Also we have

$$\frac{\partial\,\pi}{\partial\,R_s}=\frac{\left(1+\frac{k_2\left(2^{R_t}-1\right)}{2^{R_t-R_s}-1}\right)-R_s\left(\frac{\ln 2\; k_2\; 2^{R_t-R_s}\left(2^{R_t}-1\right)}{\left(2^{R_t-R_s}-1\right)^2}\right)}{e^{\frac{2\left(2^{R_t}-1\right)}{\rho_d}}\left(1+\frac{k_2\left(2^{R_t}-1\right)}{2^{R_t-R_s}-1}\right)^2}=0. \quad \text{(C.7)}$$

Since the denominator of the middle term of (C.7) is greater than zero, (C.7) reduces to

$$k_2\left(2^{R_s}+\frac{2^{R_s}-1}{\xi}\right)\left(\ln 2\; R_s-1+\frac{\ln 2\; R_s}{\xi}\right)=1, \quad \text{(C.8)}$$

where k_2 is defined in (34).

Taking (C.6) into (C.8), optimal R_s, $R_s^\star$ can be obtained easily by linear search, since the left side of (C.8) is monotonically increasing with R_s which can be easily proved. The optimal R_t can be calculated as

$$R_t^\star=R_s^\star+\log_2\left(1+\xi^\star\right), \quad \text{(C.9)}$$

where $\xi^\star$ can be obtained by taking $R_s^\star$ into (C.6).

Case II: If optimal $(R_t,\,R_s)\in\hat{\mathcal{D}}\cup\mathcal{D}_2$, (22) can be rewritten as

$$\pi=\frac{R_s}{1+\frac{k_1}{2^{R_t-R_s}-1}}. \quad \text{(C.10)}$$

Because π in (C.10) increases with R_t, optimal R_t and R_s should be found at the boundary of $\mathcal{D}_1$ and $\mathcal{D}_2$, that is $\hat{\mathcal{D}}$. Letting $(a)=(b)$, we have

$$1+\frac{k_1}{2^{R_t-R_s}-1}=e^{\frac{2^{R_t}-1}{\rho_d}}+\frac{k_2\,e^{\frac{2^{R_t}-1}{\rho_d}}\left(2^{R_t}-1\right)}{2^{R_t-R_s}-1}, \quad \text{(C.11)}$$

which can be further simplified as

$$2^{R_s}=\frac{2^{R_t}}{1+\zeta}, \quad \text{(C.12)}$$

where

$$\zeta=\frac{k_1-k_2\,e^{\frac{2^{R_t}-1}{\rho_d}}\left(2^{R_t}-1\right)}{e^{\frac{2^{R_t}-1}{\rho_d}}-1}>0. \quad \text{(C.13)}$$

Thus, from (C.12) we have

$$R_s=R_t-\log_2\left(1+\zeta\right). \quad \text{(C.14)}$$

By taking (C.14) into (C.10), we have

$$\pi=\frac{R_t-\log_2\left(1+\zeta\right)}{1+\frac{k_1}{\zeta}}. \quad \text{(C.15)}$$

By taking the derivative of π about R_t in (C.15), optimal R_t should satisfy

$$\frac{\left(1-\frac{1}{\ln 2}\frac{\zeta'}{1+\zeta}\right)\left(1+\frac{k_1}{\zeta}\right)-\left(R_t-\log_2\left(1+\zeta\right)\right)\left(-\frac{k_1}{\zeta^2}\right)\zeta'}{\left(1+\frac{k_1}{\zeta}\right)^2}=0, \quad \text{(C.16)}$$

where

$$\zeta'\triangleq\frac{\mathrm{d}\zeta}{\mathrm{d}R_t}=\frac{\ln 2\; e^{\frac{2^{R_t}-1}{\rho_d}}}{\left(e^{\frac{2^{R_t}-1}{\rho_d}}-1\right)^2}\left(k_2\,2^{R_t}\left(1+\frac{1}{\rho_d}-e^{\frac{2^{R_t}-1}{\rho_d}}\right)-\frac{k_1+k_2}{\rho_d}\right). \quad \text{(C.17)}$$

And (C.16) can be further simplified as

$$\zeta'\left(\frac{1+\frac{k_1}{\zeta}}{\ln 2\left(1+\zeta\right)}-\frac{k_1\left(R_t-\log_2\left(1+\zeta\right)\right)}{\zeta^2}\right)=1. \quad \text{(C.18)}$$

Thus, $R_t^\star$ can be calculated as the solution of (C.18), and from (C.14)

$$R_s^\star=R_t^\star-\log_2\left(1+\zeta^\star\right), \quad \text{(C.19)}$$

where $\zeta^\star$ is calculated by taking $R_t^\star$ into (C.13).

Note that, if the optimal (R_t, R_s) for problem (C.1) is obtained in region $\mathcal{D}_1$, they are the optimal rate parameters for problem (26). This is because, firstly, the above discussion and derivations show that the optimal rate parameters can only be obtained in region $\mathcal{D}_1$ and $\hat{\mathcal{D}}$. Secondly, by using the continuity of the function of throughput (22), if the optimal (R_t, R_s) for problem (C.1) are obtained in region $\mathcal{D}_1$, the maximal throughput in region $\mathcal{D}_1$ (i.e., the maximal value of the object function of (C.1) in $\mathcal{D}_1$), is larger than its boundary $\hat{\mathcal{D}}$. Thus, the optimal rate parameters are obtained and fall in region $\mathcal{D}_1$.

APPENDIX D
PROOF OF COROLLARY 1

We consider the asymptotically high SNR regime, i.e., $\rho_d \to \infty$ or equivalently $\mathcal{P}_s \to \infty$.

When $\rho_d \to \infty$, we firstly assume $\left(R_t^\star, R_s^\star\right)$ is obtained in the region $\mathcal{D}_1$. The value of R_s that satisfies (27) cannot go to infinity regardless of the value of ξ. Thus, we have $\xi \to \infty$ as $\rho_d \to \infty$, and (27) can be rewritten as

$$k_2 2^{R_s} (\ln 2 R_s - 1) = 1, \tag{D.1}$$

where k_2 is defined in (34). From (D.1) optimal R_s for the case $\rho_d \to \infty$ can be calculated as

$$R_s^\star = \frac{1 + \mathrm{W}_0\left(\frac{1}{k_2 2^{\frac{1}{\ln 2}}}\right)}{\ln 2} = \frac{1 + \mathrm{W}_0\left(\frac{1}{ek_2}\right)}{\ln 2}. \tag{D.2}$$

From (29), we know that $\xi = \mathcal{O}\left(\rho_d^{\frac{1}{2}}\right) = \mathcal{O}\left(\mathcal{P}_s^{\frac{1}{2}}\right)$, and because $\xi = \frac{2^{R_t}}{2^{R_s}} - 1$, we have $2^{R_t} = \mathcal{O}\left(\mathcal{P}_s^{\frac{1}{2}}\right)$. It can be easily verified that the assumption that optimal $(R_t, R_s) \in \mathcal{D}_1$ is correct. From Proposition 1 and (22), optimal (R_t, R_s) and π is obtained.

APPENDIX E
PROOF OF PROPOSITION 2

Because (a) in (22) decreases with R_t, while (b) increases with R_t, optimal R_t can be obtained when the two parts become equal with each other, i.e., optimal $(R_t, R_s) \in \hat{\mathcal{D}}$. Thus, optimization problem (26) can be rewritten as

$$\max_{R_t, R_s} \frac{R_s}{1 + \max\left\{\frac{d_{SJ}^m}{N_J \eta}\frac{d_{JE}^m}{d_{SE}^m}\frac{(N_J-1)\left(\varepsilon^{-\frac{1}{N_J-1}}-1\right)}{2^{R_t-R_s}-1}, e^{\frac{2^{R_t}-1}{\rho_d}} - 1\right\}}$$

$$\text{s.t. } \frac{d_{SJ}^m}{N_J \eta}\frac{d_{JE}^m}{d_{SE}^m}\frac{(N_J-1)\left(\varepsilon^{-\frac{1}{N_J-1}}-1\right)}{2^{R_t-R_s}-1} = e^{\frac{2^{R_t}-1}{\rho_d}} - 1, R_t \geq R_s \geq 0. \tag{E.1}$$

By solving the equality constraint, we have

$$2^{R_s} = \frac{2^{R_t}}{1 + \frac{M}{e^{\frac{2^{R_t}-1}{\rho_d}} - 1}}, \tag{E.2}$$

where M is defined in (39). Certainly, $R_t \geq R_s$ is satisfied in (E.2). By taking (E.2) into (E.1), the optimization problem can be rewritten as

$$\max_{R_t \geq 0} \frac{\log_2\left(\frac{2^{R_t}}{1+\frac{M}{e^{\frac{2^{R_t}-1}{\rho_d}}-1}}\right)}{e^{\frac{2^{R_t}-1}{\rho_d}}}. \tag{E.3}$$

Now we use z to denote 2^{R_t}, thus $R_t = \log_2 z$. By taking the derivative of objective function about z in (E.3), and then setting it equal to 0, optimal z, $z^\star$ can be calculated as the solution of (38) which is monotone decreasing function with z on the left side.

APPENDIX F
PROOF OF COROLLARIES 2 AND 3

When $\rho_d \to \infty$, (38) approximates as $2\frac{\rho_d}{z} - \ln z = 0$. Thus, we have $z^\star = \frac{2\rho_d}{\mathrm{W}_0(2\rho_d)}$. From (22) and Proposition 2, Corollary 2 can be easily obtained. When $N_J \to \infty$, from (39), we have $M = \frac{d_{SJ}^m}{N_J \eta}\frac{d_{JE}^m}{d_{SE}^m}(N_J - 1)\left(\varepsilon^{-\frac{1}{N_J-1}} - 1\right) \to 0$. Therefore, (38) approximates to $\frac{\rho_d}{z} - \ln z = 0$. Thus, we have the expression of optimal z in $N_J \to \infty$ regime as $z^\star = e^{\mathrm{W}_0(\rho_d)}$. From (22) and Proposition 2, Corollary 3 can be easily obtained.

REFERENCES

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

[2] X. Zhou, L. Song, and Z. Zhang, *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, 2013.

[3] 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.

[4] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, Apr. 2009, pp. 2613–2616.

[5] V. Aggarwal, L. Sankar, A. Calderbank, and H. Poor, "Secrecy capacity of a class of orthogonal relay eavesdropper channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, Jul. 2009, Art. no: 494696.

[6] J. Li, A. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[7] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[8] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

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

[10] 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.

[11] 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.

[12] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

[13] 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.

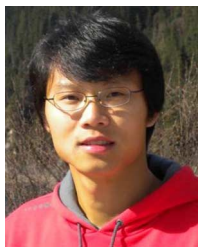
[14] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[15] S. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013–5022, Oct. 2011.

[16] J. Yang, I.-M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840–2852, Jun. 2013.

[17] L. Varshney, "Transporting information and energy simultaneously," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2008, pp. 1612–1616.
[18] P. Grover and A. Sahai, "Shannon meets Tesla: Wireless information and power transfer," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2010, pp. 2363–2367.
[19] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 757–789, Second Quart. 2015.
[20] K. Huang and X. Zhou, "Cutting last wires for mobile communication by microwave power transfer," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 86–93, Jun. 2015.
[21] 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.
[22] 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.
[23] 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, Nov. 2013.
[24] L. Liu, R. Zhang, and K.-C. Chua, "Wireless information transfer with opportunistic energy harvesting," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 288–300, Jan. 2013.
[25] H. Ju and R. Zhang, "Throughput maximization in wireless powered communication networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 1, pp. 418–428, Jan. 2014.
[26] A. Nasir, X. Zhou, S. Durrani, and R. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622–3636, Jul. 2013.
[27] S. Lee, R. Zhang, and K. Huang, "Opportunistic wireless energy harvesting in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 9, pp. 4788–4799, Sep. 2013.
[28] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2014, pp. 5402–5407.
[29] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Trans. Signal Process.*, vol. 62, no. 7, pp. 1850–1863, Apr. 2014.
[30] R. Feng, Q. Li, Q. Zhang, and J. Qin, "Robust secure transmission in MISO simultaneous wireless information and power transfer system," *IEEE Trans. Veh. Technol.*, vol. 64, no. 1, pp. 400–405, May 2014.
[31] D. Ng, E. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.
[32] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Wireless-powered relays in cooperative communications: Time-switching relaying protocols and throughput analysis," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1607–1622, May 2015.
[33] 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.
[34] A. Mukherjee and J. Huang, "Deploying multi-antenna energy-harvesting cooperative jammers in the MIMO wiretap channel," in *Proc. IEEE Conf. Rec. 46 Asilomar Signals Syst. Comput.*, Nov. 2012, pp. 1886–1890.
[35] J. Yang and S. Ulukus, "Optimal packet scheduling in a multiple access channel with energy harvesting transmitters," *J. Commun. Netw.*, vol. 14, no. 2, pp. 140–150, Apr. 2012.
[36] X. Zhou and M. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.
[37] A. D. Wyner, "The wire-tap channel," *Bell Syst. Techn. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[38] 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.
[39] 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.
[40] S. Sudevalayam and P. Kulkarni, "Energy harvesting sensor nodes: Survey and implications," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 3, pp. 443–461, Third Quart. 2011.
[41] R. Corless, G. Gonnet, D. Hare, D. Jeffrey, and D. Knuth, "On the Lambert W function," *Adv. Comput. Math.*, vol. 5, no. 1, pp. 329–359, 1996.
[42] R. Durrett, *Probability: Theory and Examples*. Cambridge, U.K.: Cambridge Univ. Press, 2010.

Wanchun Liu (S'13) received the B.S. and M.S.E. degrees in electronics and information engineering from Beihang University, Beijing, China. She is currently pursuing the Ph.D. degree at the Research School of Engineering, Australian National University, Canberra, ACT, Australia. Her research interests include wireless communications and includes the application of wireless communication networks powered by energy harvesting.



Xiangyun Zhou (M'11) received the B.E. degree (Hons.) in electronics and telecommunications engineering and the Ph.D. degree in telecommunications engineering from the Australian National University, Canberra, ACT, in 2007 and 2010, respectively. From 2010 to 2011, he worked as a Postdoctoral Fellow with the UNIK—University Graduate Center, University of Oslo, Oslo, Norway. He joined the Australian National University in 2011 and currently works as a Senior Lecturer. His research interests include communication theory and wireless networks. He currently serves on the Editorial Board of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATION and the IEEE COMMUNICATION LETTERS. He also served as a Guest Editor for the *IEEE Communication Magazine*'s feature topic on wireless physical layer security in 2015 and *EURASIP Journal on Wireless Communications and Networking*'s special issue on energy harvesting wireless communications in 2014. He was a Co-Chair of the ICC workshop on wireless physical layer security at ICC'14 and ICC'15. He was the Chair of the ACT Chapter of the IEEE Communications Society and Signal Processing Society from 2013 to 2014. He was a recipient of the Best Paper Award at ICC'11.

Salman Durrani (S'00–M'05–SM'10) received the B.Sc. (first class Hons.) degree in electrical engineering from the University of Engineering and Technology, Lahore, Pakistan, and the Ph.D. degree in electrical engineering from the University of Queensland, Brisbane, QLD, Australia, in 2000 and 2004, respectively. Since 2005, he has been with Australian National University, Canberra, ACT, Australia, where he is currently a Senior Lecturer with the Research School of Engineering, College of Engineering and Computer Science. He has coauthored more than 95 publications to date in refereed international journals and conferences. His research interests include wireless communications and signal processing, including synchronization in communication systems, wireless energy harvesting systems, outage and connectivity of finite area networks and signal processing on the unit sphere. He currently serves as an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS and as the Chair of the ACT Chapter of the IEEE Signal Processing and Communications Societies. He is a Member of Engineers Australia and a Senior Fellow of The Higher Education Academy, U.K.

Petar Popovski (S'97–A'98–M'04–SM'10) received the Dipl. -Ing. degree in electrical engineering and the Magister Ing. degree in communication engineering from the Sts. Cyril and Methodius University, Skopje, Macedonia, and the Ph.D. degree from Aalborg University,Aalborg, Denmark, in 1997, 2000, and 2004, respectively. He is currently a Professor with Aalborg University, where he leads a research group on machine-to-machine communications. He has authored more than 200 journals, conference proceedings and books, and more than 30 patents and patent applications. His research interests include wireless communication and networking, information theory and protocol design. In the past, he served as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE JSAC COGNITIVE RADIO SERIES and Senior Editor for the IEEE COMMUNICATIONS LETTERS. He is currently an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS. From 2012 to 2014, he served as the Chair of the IEEE ComSoc Emerging Technology Committee on Smart Grid Communications. He is a Steering Committee Member for the IEEE INTERNET OF THINGS JOURNAL, as well as Steering Committee Member of IEEE SmartGridComm. In 2015, he was the recipient of the Consolidator Grant from the European Research Council.