Improving Secrecy Performance of a Wirelessly Powered network

Zhuo Chen, Zhiguo Ding, *Member, IEEE* , Xuchu Dai

Abstract

This paper considers the secrecy communication of a wirelessly powered network, where an energy constrained legitimate transmitter (Alice) sends message to a legitimate receiver (Bob) with the energy harvested from a dedicated power beacon (PB), while an eavesdropper (Eve) intends to intercept the information. A simple time-switching protocol with a time-switching ratio α is used to supply power for the energy constrained legitimate transmitter. To improve the physical layer security, we firstly propose a protocol that combines maximum ratio transmission (MRT) with zero-forcing (ZF) jamming for the case where Eve is passive in the network, so that Alice only has access to the channel state information (CSI) of Bob. Then we propose a protocol that uses a ZF transmitting strategy to minimize the signal-to-noise ratio (SNR) at Eve for the case where Eve is active in the network, so that Alice only has access to the partial CSI of Eve. Closed-form expressions and simple approximations of the connection outage probability and secrecy outage probability are derived for both protocols. Furthermore, the secrecy throughput as well as the diversity orders achieved by our proposed protocols are characterized and the optimal time-switching ratio α and power allocation coefficient β for secrecy throughput maximization are derived in the high SNR regime. Finally, numerical results validate the effectiveness of the proposed schemes.

Zhuo Chen and Xuchu Dai are with Key Lab of Wireless-Optical Commun., Chinese Acad. of Sciences, Sch. Info Science & Tech., Univ. Science & Tech. China, Hefei, Anhui, 230027, P.R.China(e-mail:cz1992@mail.ustc.edu.cn, daixc@ustc.edu.cn).

Zhiguo Ding is with the School of Computer and Communications, Lancaster University, LA1 4YW, UK(e-mail:z.ding@lancaster.ac.uk).

I. INTRODUCTION

With the current growing demand for energy in modern wireless networks, energy harvesting techniques that scavenge energy from ambient environment such as wind and solar, have attracted a lot of attention as important ways of prolonging the lifetime of energy-constrained wireless networks [1]. However, harvesting energy from solar, wind or other natural energy depends heavily on location and weather conditions, and so fails to generate stable energy output. It follows that such techniques may not be suitable for powering wireless devices with strict quality of service requirements [2]. An alternative solution, generally referred to as wireless energy transfer (WET), which exploits the radio frequency (RF) signals as a means for energy transportation, has been proposed. RF signals are widely used, which means that WET can provide stable energy supplies for mobile devices. The area of wireless powered communication (WPC) design and optimization is always a hot topic in the field of WET [3], because it considers the transfer and usage of energy synthetically. Multi-antenna techniques are one method adopted to improve the performance of WET over fading channels, and works by exploiting spatial degrees of freedom [4]. The application of advanced smart antenna technologies to WPC, including multiple-input multiple-output and relaying techniques, are also investigated for their use in significantly improving the energy efficiency and also the spectral efficiency of WET [5]. In [6], an energy-constrained relay is considered for use in enhancing the information transmission rate of an energy-constrained source in a wireless-powered cooperative communication network. In [7], the tradeoff between wireless energy and information transfer when adjusting the transfer duration with a total duration constraint is considered. As a result, two wireless energy and information transfer tradeoff schemes, which work by maximizing an upper bound and an approximate lower bound of the average information transmission rate, are proposed. In [8], an optimal time allocation scheme is proposed for a wireless communication network with a full-duplex hybrid energy and information access point and a set of wireless users with energy harvesting capabilities.

Nevertheless, due to the open nature of wireless medium, RF signals are shared by multiple nodes, which constitute potential eavesdroppers. Hence, information leakage is also a critical

problem to be addressed in a wireless powered communication network (WPCN). As shown in [3], which considers the effects of having limited power supply in WPCNs, modifying physical layer security is a better method of realizing wireless security when compared to conventional cryptographic approaches. The basic idea of physical layer security technology is to exploit the physical characteristics of wireless channels in order to provide secure transmission without relying on traditional encryption mechanisms [9]. It has been shown that a positive secrecy rate can be achieved for the scenario where the source, destination and eavesdropper are equipped with a single antenna, and the source-eavesdropper channel is a degraded version of the main source-destination channel [9], [10]. When the source-destination channel condition is inferior to the source-eavesdropper channel condition, using multiple antennas can help to improve the secrecy rates. In [11]–[14], the secrecy capacity of the multiple-input multiple-output (MIMO) wiretap channel, where each node is equipped with multiple antennas, has been investigated in the presence of one or more eavesdroppers. Also, an artificial jamming scheme introduced in [15], which injects artificial-noise (AN) into the wireless communication system, has been recognized as an active approach for improving the physical layer security. In [16], [17], artificial-noise is applied to the multiple-input single-output (MISO) networks to enhance secrecy transmission, and in [18], it is considered for use in the downlink secure transmission of a multi-cell massive MIMO system with matched-filter precoding.

Recently, the application of physical layer security technology to WPCNs has gained lots of attention. In [19], the optimal beamforming design and power allocation scheme for MISO systems in the presence of one or more eavesdroppers are presented, while in [20], the beamforming design for maximizing the achievable secrecy rate in MIMO networks that are subject to a total power constraint and an energy harvesting constraint is studied. In [21], the authors consider resource allocation for cognitive networks, and in [22], the power allocation for secure OFDMA systems with wireless information and power transfer is investigated. The above works consider a hybrid network architecture, where the information source acts simultaneously as the source of energy. However, just as shown in [23], [24], it is generally infeasible to power larger devices with the energy harvested from hybrid networks. Therefore, a novel network

architecture is proposed, where a dedicated station called power beacon (PB) is incorporated into a WPCN to supply power for the energy-constrained device.

The performance of a secure WPCN with a dedicated power beacon (PB) is analyzed in [2] and its robust resource allocation is presented in [25]. However, in the area of secure communications in WPCNs with dedicated PBs, artificial jamming has not been considered for use in improving the secrecy performance of the whole system. Motivated by this, we consider the secrecy communication of a wirelessly powered network consisting of one power beacon (PB), one legitimate transmitter (Alice) and one legitimate receiver (Bob) in the presence of a single eavesdropper (Eve). Artificial jamming is designed for the network. To be more specific, we firstly propose a protocol that combines maximum ratio transmission (MRT) with zero-forcing (ZF) jamming for the case where Eve is passive in the network,so that Alice only has access to the channel state information (CSI) of Bob. Then we propose a protocol that uses a ZF transmitting strategy to minimize the signal-to-noise ratio (SNR) at Eve for the case where Eve is active in the network, so that Alice has access to the partial CSI of Eve. Closed-form expressions and simple approximations of the connection outage probability and secrecy outage probability are derived for both protocols. Furthermore, the secrecy throughput as well as the diversity orders achieved by our proposed protocols are characterized. Finally, the optimal time-switching ratio α and power allocation coefficient β for secrecy throughput maximization are derived in the high SNR regime.

The remainder of the paper is organized as follows. Section II describes the system model and presents the transmission protocols, while Section III-A provides an analytical study comparing their connection outage probability, secrecy outage probability, diversity order and secrecy throughput. In Section III-B, the optimal resource allocation (i.e. the values of α and β which maximize secrecy throughput) is discussed for the high SNR regime. Section IV presents the numerical results to validate our theoretic results and the secrecy performance of the proposed protocols. Finally, Section V concludes the paper and gives a brief summary of the key findings.

II. System Model

We consider the secrecy communication of a wirelessly powered network consisting of one power beacon (PB), one legitimate transmitter (Alice) and one legitimate receiver (Bob) in the presence of one eavesdropper (Eve). The legitimate transmitter Alice is equipped with N antennas, while all the other nodes in the considered system are equipped with a single antenna. It is also assumed that the channels experience Rayleigh fading, remain constant over the transmission block time T, and vary independently and identically from one block to the other.

Alice is not self-powered and needs to harvest energy from the signals sent by the PB. In this paper, we adopt the time-sharing protocol proposed in [26], wherein the entire transmission slot with time duration T is divided into two orthogonal phases. The first phase is for power transfer and has time duration αT (where $\alpha \in (0,1)$ is the time switching ratio) and the second is for information transmission and has time duration $(1-\alpha)T$. During the first phase, the PB sends the energy signal x_e to Alice. The received signal at Alice can be expressed as

$$\mathbf{y}_s = \sqrt{\frac{P}{d_1^{\tau}}}\mathbf{h}_{PS}x_e + \mathbf{n}_s,$$

where P is the transmit power of the PB, d_1 is the distance between the PB and Alice, τ is the path loss exponent, x_e is the energy signal with unit power and $\mathbf{n}_s$ is an N-dimensional additive white Gaussian noise (AWGN) vector with $\mathcal{E}\left\{\mathbf{n}_s\mathbf{n}_s^H\right\} = N_0\mathbf{I}$. The $N \times 1$ vector $\mathbf{h}_{PS}$ denotes the channel between the PB and Alice and its elements are independent and identically distributed (i.i.d.) complex Gaussian variables with zero mean and unit variance. At the end of the first phase, the energy Alice has harvested can be expressed as

$$E = \frac{\eta\alpha T P\|\mathbf{h}_{PS}\|^2}{d_1^{\tau}},$$

where η $(0 < \eta < 1)$ denotes the energy conversion efficiency. As in [26], we assume that the energy harvested during the first phase is stored in a supercapacitor and then fully consumed by Alice to send signals in the second phase. So during the second phase, the transmit power of Alice can be expressed as

$$P_S = \frac{E}{(1-\alpha)T} = \frac{\mathcal{K}Py_1}{d_1^{\tau}},$$

where $y_1 = \|\mathbf{h}_{PS}\|^2$ and $\mathcal{K} = \frac{\eta\alpha}{1-\alpha}$.

Now, let us consider the information transmission phase. With the aim of guaranteeing security, we propose two protocols. The first is for the case where Eve is passive in the network, while the second is for the case where Eve is active.

A. Eve is Passive

When Eve is passive in the network, Alice only has access to the CSI of Bob. To utilize the CSI of the main channel, we combine maximum ratio transmission (MRT) with zero-forcing (ZF) jamming. To be more specific, let the $1 \times N$ vector $\mathbf{h}_{SD}$ denote the channel from Alice to Bob whose elements are i.i.d. complex Gaussian variables with zero mean and unit variance, and order the elements of $\mathbf{h}_{SD}$ as $h_1 \geq h_2 \geq \cdots h_N$. Then Alice selects the K ($K \geq 2$) best antennas corresponding to the channels $h_1, h_2, \cdots h_K$ to perform both MRT and ZF jamming at the same time. Let us define $\widehat{\mathbf{h}}_{SD} = [h_1 h_2 \cdots h_K]$ as the $1 \times K$ vector corresponding to the K best channels form Alice to Bob. Then Alice uses these antennas to transmit

$$\widehat{x}_s = \sqrt{\beta P_S}\frac{\widehat{\mathbf{h}}_{SD}^H}{\left\|\widehat{\mathbf{h}}_{SD}\right\|}x_s + \sqrt{(1-\beta)P_S}\mathbf{w}_J x_J,$$

where β denotes the proportion of Alice's power allocated to maximum ratio information transmission, x_s is the information signal with unit power, $\mathbf{w}_J$ is the $K \times 1$ ZF beamforming vector which satisfies $\|\mathbf{w}_J\| = 1$ and $\widehat{\mathbf{h}}_{SD}\mathbf{w}_J = 0$ and x_J is the jamming signal with unit power. Hence, the received signal at Bob can be written as

$$y_D = \sqrt{\frac{\beta P_S}{d_2^\tau}}\|\widehat{\mathbf{h}}_{SD}\|x_s + n_D,$$

where d_2 is the distance between Alice and Bob and n_D denotes the AWGN with zero mean and variance N_0. Similarly, the signal received at Eve can be expressed as

$$y_E = \sqrt{\frac{\beta P_S}{d_3^\tau}}\mathbf{h}_{SE}\frac{\widehat{\mathbf{h}}_{SD}^H}{\|\widehat{\mathbf{h}}_{SD}\|}x_s + \sqrt{\frac{(1-\beta)P_S}{d_3^\tau}}\mathbf{h}_{SE}\mathbf{w}_J x_J + n_E,$$

where d_3 is the distance between Alice and Eve, the $1 \times K$ vector $\mathbf{h}_{SE}$ denotes the channel from Alice's transmitting antennas to Eve whose elements are i.i.d. complex Gaussian variables with zero mean and unit variance, n_E denotes the AWGN with zero mean and variance N_0.

Let us define $y_2 = \left\|\widehat{\mathbf{h}}_{SD}\right\|^2$, $y_3 = \left|\mathbf{h}_{SE}\frac{\widehat{\mathbf{h}}_{SD}^H}{\left\|\widehat{\mathbf{h}}_{SD}\right\|}\right|^2$, and $y_4 = |\mathbf{h}_{SE}\mathbf{w}_J|^2$. Then, the instantaneous SNR at Bob and Eve can be expressed as

$$\gamma_D = \frac{\beta\mathcal{K}Py_1y_2}{d_1^\tau d_2^\tau N_0}, \tag{1}$$

and

$$\gamma_E = \frac{\beta\mathcal{K}Py_1y_3}{(1-\beta)\mathcal{K}Py_1y_4 + d_1^\tau d_3^\tau N_0}, \tag{2}$$

respectively.

B. Eve is Active

When Eve is active in the network, Alice has access to the partial CSI of Eve. To utilize the CSI of the wiretap channel, we use a ZF transmitting strategy to minimize the SNR at Eve. Initially, Alice selects K ($K \geq 2$) antennas randomly, to participate in transmission. Let the $1 \times K$ vectors $\mathbf{g}_{SE}$ and $\mathbf{g}_{SD}$ denote the channels from Alice's transmitting antennas to Eve and Bob respectively, where the elements of the channels are i.i.d. complex Gaussian variables with zero mean and unit variance. In this paper, we assume that Alice only has partial eavesdropper CSI, which can be modeled as

$$\mathbf{g}_{SE} = \widehat{\mathbf{g}}_{SE} + \Delta_E,$$

where $\widehat{\mathbf{g}}_{SE}$ is Alice's estimation of the wiretap channel and Δ_E is the estimation error, which is an K-dimensional AWGN vector with $\mathcal{E}\left\{\Delta_E\Delta_E^H\right\} = N_E\mathbf{I}$.

Then Alice uses the K antennas to transmit

$$\acute{x}_s = \sqrt{\beta P_S}\mathbf{w}_s x_s + \sqrt{(1-\beta)P_S}\mathbf{w}_e x_J,$$

where $\mathbf{w}_s$ is the $K \times 1$ beamforming vector satisfying $\|\mathbf{w}_s\| = 1$ and $\widehat{\mathbf{g}}_{SE}\mathbf{w}_s = 0$, and $\mathbf{w}_e$ is the $K \times 1$ beamforming vector satisfying $\|\mathbf{w}_e\| = 1$ and $\mathbf{g}_{SD}\mathbf{w}_e = 0$. Then the received signals at Bob and Eve can be written as

$$\widehat{y}_D = \sqrt{\frac{\beta P_S}{d_2^\tau}}\mathbf{g}_{SD}\mathbf{w}_s x_s + n_D,$$

and

$$\widehat{y}_E = \sqrt{\frac{\beta P_S}{d_3^\tau}}\Delta_E \mathbf{w}_s x_s + \sqrt{\frac{(1-\beta)P_S}{d_3^\tau}}\mathbf{g}_{SE}\mathbf{w}_e x_J + n_E,$$

respectively.

Let us define $z_2 = |\mathbf{g}_{SD}\mathbf{w}_s|^2$, $z_3 = |\mathbf{g}_{SE}\mathbf{w}_e|^2$ and $z_4 = |\Delta_E \mathbf{w}_s|^2$. Then, the instantaneous SNR at Bob and Eve can be expressed as

$$\widehat{\gamma}_D = \frac{\beta \mathcal{K} P y_1 z_2}{d_1^\tau d_2^\tau N_0}, \tag{3}$$

and

$$\widehat{\gamma}_E = \frac{\beta \mathcal{K} P y_1 z_4}{(1-\beta)\mathcal{K} P y_1 z_3 + d_1^\tau d_3^\tau N_0}, \tag{4}$$

respectively.

C. Secrecy Throughput

In this paper, we study the secrecy performance of our proposed protocols by considering the outage based secrecy metrics. Let us denote the confidential message rate as R_s and the rate of the transmitted codeword as R_t. When the capacity of the main channel from Alice to Bob is below R_t, Bob can not decode the received message correctly. Thus we define the probability of this event as connection outage probability. On the other hand, when the capacity of the wiretap channel from Alice to Eve is above the rate $R_e \triangleq R_t - R_s$, we cannot guarantee perfect security, so Eve may be able to intercept the message. The probability of such an event occuring is defined as secrecy outage probability. With a given connection outage probability σ and secrecy outage probability ϵ the secrecy throughput can be defined as

$$\mathcal{C} \triangleq (1-\sigma)R_s,$$

which is suitable for evaluating the secrecy performance of systems with stringent delay constraints [27].

III. Secrecy Performance Analysis and Optimization

In this section, we start by giving the exact closed-form expressions of the connection outage probability and the secrecy outage probability of our proposed protocols. We then investigate the secrecy throughput of the system. At last, we give the diversity orders of our proposed protocols in the high SNR regime and derive the optimal time switching ratio α and power allocating coefficient β for a given connection outage probability σ and secrecy outage probability ϵ.

A. Secrecy Throughput Analysis

1) When Eve is Passive: As shown in Section II-C and Section II-A, when Eve is passive, the connection outage probability can be defined as

$$P_{co}^{MRT} = \mathbf{Pr}\left((1-\alpha)\log_2(1+\gamma_D) < R_t\right). \tag{5}$$

Let us define $G = \frac{\beta\mathcal{K}P}{d_1^\tau d_2^\tau N_0}$ and $\gamma' = \frac{2^{\left(\frac{R_t}{1-\alpha}\right)}-1}{G}$. Then the connection outage probability is given by:

Theorem 1. *P_{co}^{MRT} can be expressed as*

$$P_{co}^{MRT} = 1 - \binom{N}{K}\left[\sum_{k=0}^{N-1}\frac{2\gamma'^{(K+k)/2}}{k!(K-1)!}\mathbf{K}_{(K-k)}(2\sqrt{\gamma'}) + \sum_{l=1}^{N-K}(-1)^{(K+l-1)}\binom{N-K}{l}\left(\frac{K}{l}\right)^{(K-1)}\right. \tag{6}$$
$$\left.\left(\sum_{k=0}^{N-1}\frac{2\gamma'^{(k+1)/2}\left(\frac{K}{l+K}\right)^{(1-k)/2}}{k!}\mathbf{K}_{(1-k)}\left(2\sqrt{\frac{l+K}{K}\gamma'}\right) - \sum_{m=0}^{K-2}\frac{\left(\frac{-l}{K}\right)^m}{m!}\sum_{k=0}^{N-1}\frac{2\gamma'^{(m+k+1)/2}}{k!}\mathbf{K}_{(m-k+1)}(2\sqrt{\gamma'})\right)\right],$$

where $\mathbf{K}_n(x)$ is the n-th order, second kind, modified Bessel function [28].

Proof. See Appendix. □

Similarly, when Eve is passive, the secrecy outage probability can be defined as

$$P_{so}^{MRT} = \mathbf{Pr}\left((1-\alpha)\log_2(1+\gamma_E) > R_e\right). \tag{7}$$

Let us define $\gamma_e = 2^{\left(\frac{R_e}{1-\alpha}\right)} - 1$, $e_1 = \frac{d_1^\tau d_3^\tau \gamma_e N_0}{\mathcal{K}P\beta}$ and $e_2 = \frac{(1-\beta)\gamma_e}{\beta}$. Then the secrecy outage probability is given by:

Theorem 2. *P_{so}^{MRT} can be expressed as*

$$P_{so}^{MRT} = \frac{1}{(1+e_2)}\sum_{k=0}^{N-1}\frac{2e_1^{(k+1)/2}}{k!}\mathbf{K}_{(1-k)}\left(2\sqrt{e_1}\right). \tag{8}$$

Proof. See Appendix. □

Now let us consider the maximal secrecy throughput $\mathcal{C}^{MRT} = (1-\sigma)(R_t - R_e)$ under the outage constraints $P_{co}^{MRT} \leq \sigma$ and $P_{so}^{MRT} \leq \epsilon$. Since P_{co}^{MRT} is a monotonic increasing function of R_t, and P_{so}^{MRT} is a monotonic decreasing function of R_e, the outage constraints can be degraded to $P_{co}^{MRT} = \sigma$ and $P_{so}^{MRT} = \epsilon$. Unfortunately, the expressions in Theorem 1 and Theorem 2 are too complex to get a closed-form analysis result for $\mathcal{C}^{MRT}$. However, by employing the bisection search, numeral results for the maximal R_t and minimal R_e can be obtained, and the maximal secrecy throughput can be calculated as $\mathcal{C}^{MRT} = (1-\sigma)(R_t - R_e)$.

In the following, we study the secrecy performance in the high SNR regime. When $P/N_0 \to \infty$, P_{co}^{MRT} and P_{so}^{MRT} can be approximated using the following corollary.

Corollary 3. *When $P/N_0 \to \infty$,*

$$P_{co}^{MRT} \approx M\gamma'^{N} \ln \gamma',$$

where

$$M = \binom{N}{K}\left[\sum_{k=0}^{N-1}\frac{(-1)^{(K-k)}}{k!(K-1)!(N-K)!(N-k)!} + \sum_{l=1}^{N-K}(-1)^{(K+l)}\binom{N-K}{l}\left(\frac{K}{l}\right)^{(K-1)}\right. \\ \left.\left(\sum_{k=0}^{N-1}\frac{(-1)^k\left(\frac{K+l}{K}\right)^{N-1}}{k!(N-k)!(N-1)!} - \sum_{m=0}^{K-2}\frac{\left(\frac{-l}{K}\right)^m}{m!}\sum_{k=0}^{N-1}\frac{(-1)^{(m-k)}}{k!(N-m-1)!(N-k)!}\right)\right], \tag{9}$$

and

$$P_{so}^{MRT} \approx \frac{1}{1+e_2}.$$

Proof. See Appendix. □

Recall the expression of diversity order that is defined as [29]:

$$d \triangleq -\lim_{\rho\to\infty}\frac{\log[P_e(\rho)]}{\log(\rho)}, \tag{10}$$

where P_e is the maximum likelihood (ML) probability of detection error. The outage probability will be studied by following similar steps to [29], since the ML error probability can be tightly bounded by the outage probability at high SNR. Based on Corollary 4 we can then find the diversity order of the system when Eve is passive.

Corollary 4. *The diversity order of the system when Eve is passive can be expressed as*

$$d^{MRT} = N. \tag{11}$$

Proof. See Appendix. □

Note that our proposed protocol achieves a full diversity gain when Eve is passive.

2) When Eve is Active: Similarly, when Eve is active, the connection outage probability can be defined as

$$P_{co}^{ZF} = \mathbf{Pr}\left((1-\alpha)\log_2(1+\widehat{\gamma}_D) < R_t\right).$$

The connection outage probability is then given by:

Theorem 5. *P_{co}^{ZF} can be expressed as*

$$P_{co}^{ZF} = 1 - \sum_{k=0}^{N-1} \frac{2\gamma'^{(k+1)/2}}{k!}\mathbf{K}_{(1-k)}\left(2\sqrt{\gamma'}\right). \tag{12}$$

Proof. See Appendix. □

Furthermore, when Eve is active, the secrecy outage probability can be defined as

$$P_{so}^{ZF} = \mathbf{Pr}\left((1-\alpha)\log_2(1+\widehat{\gamma}_E) > R_e\right). \tag{13}$$

Then the secrecy outage probability is given by:

Theorem 6. *P_{so}^{ZF} can be expressed as*

$$P_{so}^{ZF} = \frac{1}{(1+e_2/N_E)} \sum_{k=0}^{N-1} \frac{2\left(\frac{e_1}{N_E}\right)^{(k+1)/2}}{k!}\mathbf{K}_{(1-k)}\left(2\sqrt{\frac{e_1}{N_E}}\right). \tag{14}$$

Proof. See Appendix. □

In the high SNR regime, when $P/N_0 \to \infty$, P_{co}^{ZF} and P_{so}^{ZF} can be approximated using the following corollary.

Corollary 7. *When $P/N_0 \to \infty$*

$$P_{co}^{ZF} \approx \frac{\gamma'}{N-1},$$

and

$$P_{so}^{ZF} \approx \frac{1}{1+e_2/N_E}.$$

Proof. See Appendix. □

By applying Corollary 8 we can then find the diversity order of the system when Eve is active.

Corollary 8. *The diversity order of the system when Eve is active can be expressed as*

$$d^{ZF} = 1.$$

Proof. See Appendix. □

B. Optimizing α and β for Secrecy Throughput Maximization in high SNR regimes

1) When Eve is Passive: Now let us consider the maximal secrecy throughput $\mathcal{C}^{MRT} = (1-\sigma)(R_t - R_e)$ when Eve is passive. We define $M\sigma'^N \ln \sigma' = \sigma$, then from Corollary 3 and the outage constraints $P_{co}^{MRT} = \sigma$ and $P_{so}^{MRT} = \epsilon$, we have that $\mathcal{C}^{MRT}$ can be approximated as

$$\mathcal{C}^{MRT} \approx (1-\sigma)(R_t^{MRT} - R_e^{MRT}),$$

in the high SNR regime, where

$$R_t^{MRT} = (1-\alpha)\log_2\left(1 + \frac{\beta\mathcal{K}P\sigma'}{N_0 d_1^\tau d_2^\tau}\right),$$

and

$$R_e^{MRT} = (1-\alpha)\log_2\left(2 + \frac{\beta-\epsilon}{\epsilon(1-\beta)}\right).$$

Therefore, the optimal time and power allocating coefficients (α^*, β^*) can be approximated as the solution of the following optimization problem:

$$\mathbf{OP}1: \quad \max_{(\alpha,\beta)} \quad (1-\sigma)(1-\alpha)\left(\log_2\left(1 + \frac{\beta\mathcal{K}P\sigma'}{N_0 d_1^\tau d_2^\tau}\right) - \log_2\left(2 + \frac{\beta-\epsilon}{\epsilon(1-\beta)}\right)\right)$$
$$\text{s.t.} \quad 0 \le \alpha, \beta \le 1.$$

Theorem 9. *In the high SNR regime, under the outage constraints $P_{co}^{MRT} \leq \sigma$ and $P_{so}^{MRT} \leq \epsilon$, the optimal time and power allocating coefficients (α^*, β^*) can be approximated as*

$$\beta^* \approx \begin{cases} \frac{1}{2} & \text{if } \epsilon = \frac{1}{2} \\ \frac{\epsilon - \sqrt{\epsilon - \epsilon^2}}{2\epsilon - 1} & \text{otherwise} \end{cases}$$

and

$$\alpha^* \approx \frac{1}{1 + \mathbf{W}(e^{V \ln 2})}, \tag{15}$$

where $\mathbf{W}(x) = f^{-1}(xe^x)$ is the the Lambert W function and

$$V = \log_2 \left(\frac{\beta \eta P \sigma'}{N_0 d_1^\tau d_2^\tau} \right) - \frac{1}{\ln 2} - \log_2 \left(2 + \frac{\beta - \epsilon}{\epsilon(1 - \beta)} \right).$$

Proof. See Appendix. □

2) When Eve is Active: Similarly, let us consider the maximal secrecy throughput $\mathcal{C}^{ZF} = (1 - \sigma)(R_t - R_e)$ when Eve is active. Firstly, we define $\widehat{\sigma} = (N - 1)\sigma$ and $\widehat{\epsilon} = \epsilon / \left(N_E + (1 - N_E)\epsilon\right)$. Then, given Corollary 7 and the outage constraints $P_{co}^{ZF} = \sigma$ and $P_{so}^{ZF} = \epsilon$, $\mathcal{C}^{ZF}$ can be approximated in the high SNR regime as

$$\mathcal{C}^{ZF} \approx (1 - \sigma)(R_t^{ZF} - R_e^{ZF}),$$

where

$$R_t^{ZF} = (1 - \alpha) \log_2 \left(1 + \frac{\beta \mathcal{K} P \widehat{\sigma}}{N_0 d_1^\tau d_2^\tau} \right),$$

and

$$R_e^{ZF} = (1 - \alpha) \log_2 \left(2 + \frac{\beta - \widehat{\epsilon}}{\widehat{\epsilon}(1 - \beta)} \right).$$

Then, by Theorem 9, it follows that the optimal time and power allocating coefficients (α', β') can be approximated as

$$\beta' \approx \begin{cases} \frac{1}{2} & \text{if } \widehat{\epsilon} = \frac{1}{2} \\ \frac{\widehat{\epsilon} - \sqrt{\widehat{\epsilon} - \widehat{\epsilon}^2}}{2\widehat{\epsilon} - 1} & \text{otherwise} \end{cases}$$

and

$$\alpha' \approx \frac{1}{1 + \mathbf{W}(e^{V' \ln 2})}, \tag{16}$$

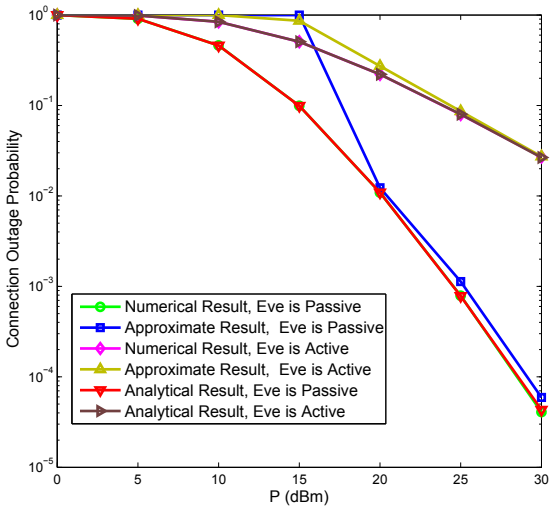

Fig. 1. Connection Outage Probability

where $\mathbf{W}(x) = f^{-1}(xe^x)$ is the the Lambert W function and

$$V' = \log_2\left(\frac{\beta\eta P\widehat{\sigma}}{N_0 d_1^{\tau} d_2^{\tau}}\right) - \frac{1}{\ln 2} - \log_2\left(2 + \frac{\beta - \widehat{\epsilon}}{\widehat{\epsilon}(1-\beta)}\right).$$

IV. Numerical Result

In this section, we present the numerical results to validate our analytical conclusions. Unless otherwise stated, we set the path loss exponent as $\tau = 2.5$, the distance between the power beacon and Alice as $d_1 = 10$m, the distance between Alice and Eve as $d_3 = 10$m, the noise power as $N_0 = -80$dBm and the energy conversion efficiency as $\eta = 0.3$. In the following, some representative simulation results are given to provide deeper insight into the proposed secrecy transmission protocols.

In Fig. 1, we show the connection outage probability for the two protocols. In this figure, we assume that $d_2 = 10$m (the distance between Alice and Bob), $N = 3$, $K = 2$, $\alpha = 0.8$, $\beta = 0.3$ and $R_t = 3$ Bits/s/Hz. From this figure, we can see that the analytical result coincides with numerical simulation perfectly and the approximation deviates a little more when compared with them in the high SNR regime. The approximation and numerical simulation curves get closer when the transmitting power P increases, and the connection outage probability of the

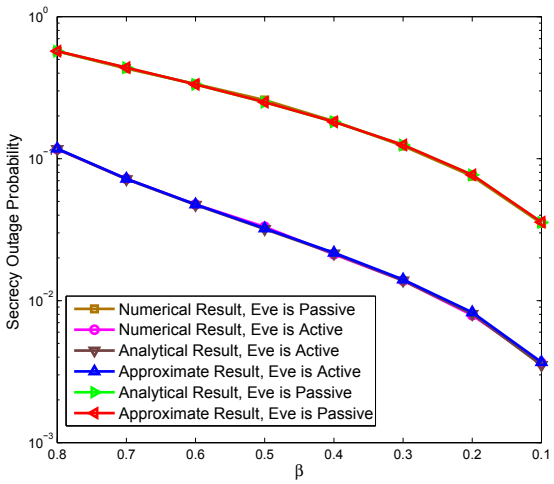

Fig. 2. Secrecy Outage Probability

protocol we proposed for when Eve is passive outperforms that of the protocol proposed for when Eve is active. From Section III, we know that the protocol proposed for when Eve is passive achieves full diversity order while that proposed for when Eve is active only achieves a unit diversity order, and that is also confirmed by this figure.

In Fig. 2, we show how the secrecy outage probabilities vary when we use different power allocation coefficients β for each of the two protocols. In this figure, we assume that $N = 3$, $K = 2$, $\alpha = 0.5$, $R_e = 1$ Bits/s/Hz, $P = 10$dBm and $N_E = 0.1$. From this figure, we can see that the analytical result and approximate result coincide with the numerical simulation perfectly. Moreover, the secrecy outage probability of the protocol that we propose when Eve is active outperforms that of the protocol proposed when Eve is passive. When β decreases, the proportion of Alice's power allocated to jamming increases and the secrecy outage probability decreases quickly. This validates the effectiveness of the ZF jamming used in this paper.

In Fig. 3, to evaluate the suboptimal choice of (α, β) proposed in Theorem 9, the suboptimal secrecy throughput with Theorem 9 is compared with the optimal secrecy throughput. We assume that $d_2 = 10$m, $\sigma = 0.0001$, $\epsilon = 0.01$ and $K = 2$ and that the optimal secrecy throughput $(\alpha, \beta) \in [0 : 0.01 : 1] \times [0 : 0.01 : 1]$ can be found via exhaustive search. From this figure, we can see that the suboptimal result found using Theorem 9 approaches the optimal result perfectly

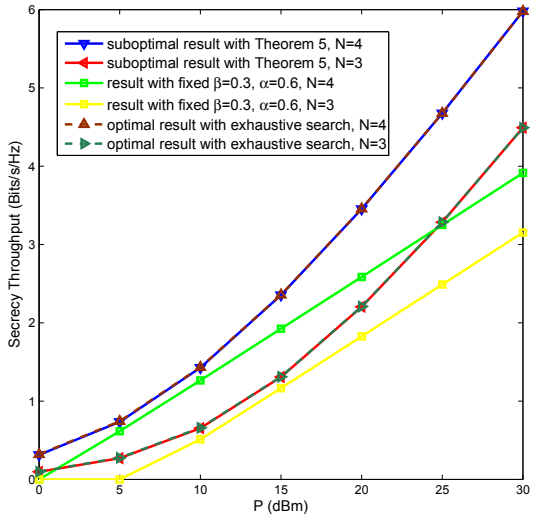

Fig. 3. Optimal secrecy throughput

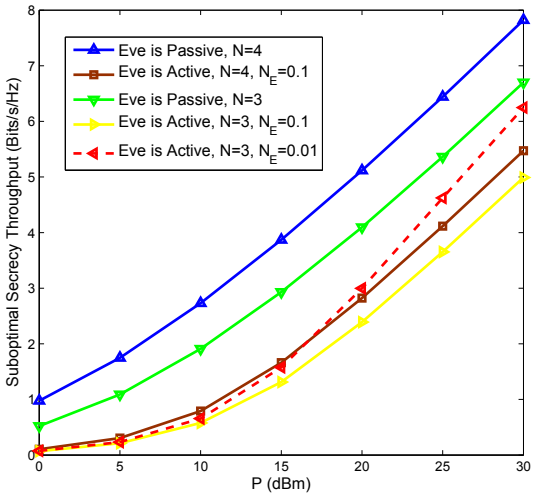

Fig. 4. Secrecy throughput of the two protocols

and outperforms the result with fixed (α, β), which validates the theorem's effectiveness.

In Fig. 4, we compare the secrecy throughput of the two protocols. In this figure, we assume that $d_2 = 10$m, $\sigma = 0.01$, $\epsilon = 0.01$ and $K = 2$, and that the allocation coefficients (α, β) of the two protocols are found using the suboptimal schemes in (15) and (16), respectively. From

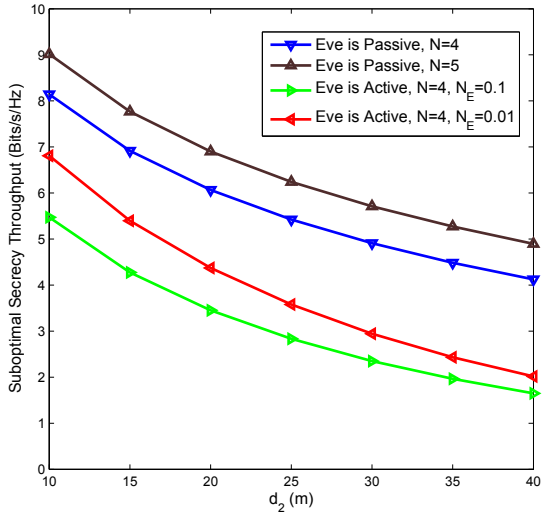

Fig. 5. Secrecy throughput of the two protocols vs distance

this figure, we can see that the secrecy throughput of the protocol that we propose when Eve is passive outperforms that of the protocol proposed when Eve is active. Increasing N improves the secrecy throughput of both protocols, and the secrecy throughput decreases with N_E when Eve is active.

Fig. 5 shows the secrecy throughput of the two protocols versus d_2 (the distance between Alice and Bob) when $P = 30$dBm, $\sigma = 0.01$, $\epsilon = 0.01$ and $K = 4$. From this figure, we can see that the protocol that we propose when Eve is passive always outperforms the protocol proposed when Eve is active. Furthermore, both protocols can be seen to achieve a positive secrecy throughput even when d_2 (the distance between Alice and Bob) is larger than d_3 (the distance between Alice and Eve), demonstrating their efficacy. Finally, increasing N can combat the loss of secrecy throughput caused by increasing the distance, d_2. However, the effect of N_E is small when d_2 is large.

V. Conclusions

In this paper on the enhancement of physical layer security we began by proposing a protocol that combines maximum ratio transmission (MRT) with zero-forcing (ZF) jamming for the case

where an eavesdropper, Eve, is passive in the network. We then proposed a protocol that uses a ZF transmitting strategy to minimize the signal-to-noise ratio (SNR) at Eve for the case where Eve is active in the network. For both protocols, closed-form expressions as well as simple approximations of the connection outage probability and secrecy outage probability are presented, from which the secrecy throughput as well as the diversity orders achieved by our proposed protocols are derived. Finally, the optimal time-switching ratio α and power allocation coefficient β for secrecy throughput maximization are derived in the high SNR regime. Numerical results show that with these values for α and β, the secrecy throughput approaches the optimal result perfectly and outperforms the schemes in which α and β are fixed. The two protocols both achieve positive secrecy throughput even when d_2 (the distance between Alice and Bob) is larger than d_3 (the distance between Alice and Eve) and this validates the effectiveness of the two protocols.

APPENDIX

Proof of Theorem 1 : Using (1) and (5), we may express P_{co}^{MRT} as

$$\begin{aligned} P_{co}^{MRT} &= \mathbf{Pr}\left((1-\alpha)\log_2\left(1+\frac{\beta\mathcal{K}Py_1y_2}{d_1^\tau d_2^\tau N_0}\right)<R_t\right) \\ &= \mathbf{Pr}\left(y_1y_2<\gamma'\right), \end{aligned}$$

where $\gamma' = \left(2^{\left(\frac{R_t}{1-\alpha}\right)}-1\right) d_1^\tau d_2^\tau N_0/(\beta\mathcal{K}P)$, and the probability density function (pdf) of y_1 follows a chi-squared distribution with 2N degrees of freedom given by [30]:

$$f_{y_1}(x) = \frac{x^{N-1}e^{-x}}{(N-1)!}. \tag{17}$$

As such, the connection outage probability can be written as

$$P_{co}^{MRT} = \underset{y_2}{\mathcal{E}}\left\{\int_0^{\gamma'/y_2}\frac{x^{N-1}e^{-x}}{(N-1)!}dx\right\}.$$

With the help of Eq. (3.351.1) [28], we obtain

$$\begin{aligned} P_{co}^{MRT} &= 1-\underset{y_2}{\mathcal{E}}\left\{e^{-\gamma'/y_2}\sum_{k=0}^{N-1}\frac{1}{k!}\left(\frac{\gamma'}{y_2}\right)^k\right\} \\ &= 1-H, \end{aligned}$$

where $H = \underset{y_2}{\mathcal{E}}\left\{e^{-\gamma'/y_2}\sum_{k=0}^{N-1}\frac{1}{k!}\left(\frac{\gamma'}{y_2}\right)^k\right\}$. Furthermore, as in [31], we know that the pdf of y_2 can be expressed as

$$f_{y_2}(x) = \binom{N}{K}\left[\frac{x^{K-1}e^{-x}}{(K-1)!} + \sum_{l=1}^{N-K}(-1)^{K+l-1}\binom{N-K}{l}\left(\frac{K}{l}\right)^{K-1} e^{-x}\left(e^{-(lx/K)} - \sum_{m=0}^{K-2}\frac{1}{m!}\left(\frac{-lx}{K}\right)^m\right)\right].$$

Then H can be expressed as

$$H = \binom{N}{K}\int_0^{+\infty}\sum_{k=0}^{N-1}\frac{\gamma'^k}{k!(K-1)!}e^{-(\gamma'/x+x)}x^{K-1-k} + \sum_{l=1}^{N-K}(-1)^{K+l-1}\binom{N-K}{l}\left(\frac{K}{l}\right)^{K-1}$$
$$\left(\sum_{k=0}^{N-1}\frac{\gamma'^k}{k!}e^{-(\frac{l+K}{K}x+\frac{\gamma'}{x})}x^{-k} - \sum_{m=0}^{K-2}\frac{1}{m!}\left(\frac{-l}{K}\right)^m\sum_{k=0}^{N-1}\frac{\gamma'^k}{k!}e^{-(x+\frac{\gamma'}{x})}x^{m-k}\right)dx.$$

Finally, by invoking Eq. (3.471.9) [28], we obtain

$$H = \binom{N}{K}\left[\sum_{k=0}^{N-1}\frac{2\gamma'^{(K+k)/2}}{k!(K-1)!}\mathbf{K}_{(K-k)}(2\sqrt{\gamma'}) + \sum_{l=1}^{N-K}(-1)^{(K+l-1)}\binom{N-K}{l}\left(\frac{K}{l}\right)^{(K-1)}\right.$$
$$\left.\left(\sum_{k=0}^{N-1}\frac{2\gamma'^{(k+1)/2}\left(\frac{K}{l+K}\right)^{(1-k)/2}}{k!}\mathbf{K}_{(1-k)}\left(2\sqrt{\tfrac{l+K}{K}\gamma'}\right) - \sum_{m=0}^{K-2}\frac{\left(\frac{-l}{K}\right)^m}{m!}\sum_{k=0}^{N-1}\frac{2\gamma'^{(m+k+1)/2}}{k!}\mathbf{K}_{(m-k+1)}(2\sqrt{\gamma'})\right)\right],$$

and the theorem is proved. ■

Proof of Theorem 2 : Using (2) and (7), P_{so}^{MRT} can be expressed as

$$\begin{aligned}
P_{so}^{MRT} &= \mathbf{Pr}\left((1-\alpha)\log_2\left(1+\frac{\beta\mathcal{K}Py_1y_3}{(1-\beta)\mathcal{K}Py_1y_4 + d_1^\tau d_3^\tau N_0}\right) > R_e\right)\\
&= \mathbf{Pr}\left(\frac{\beta\mathcal{K}Py_1y_3}{(1-\beta)\mathcal{K}Py_1y_4 + d_1^\tau d_3^\tau N_0} > \gamma_e\right)\\
&= \mathbf{Pr}\left(\beta\mathcal{K}Py_3 > \frac{d_1^\tau d_3^\tau N_0\gamma_e}{y_1} + (1-\beta)\mathcal{K}Py_4\gamma_e\right)\\
&= \mathbf{Pr}\left(y_1 > \frac{d_1^\tau d_3^\tau N_0\gamma_e}{\mathcal{K}P(\beta y_3 - (1-\beta)y_4\gamma_e)} \quad \&\& \quad y_3 > \frac{\beta}{1-\beta}\gamma_e y_4\right),
\end{aligned}$$

where $\gamma_e = 2^{\left(\frac{R_e}{1-\alpha}\right)} - 1$. Furthermore, recall that $y_3 = \left|\mathbf{h}_{SE}\frac{\widehat{\mathbf{h}}_{SD}^H}{\|\widehat{\mathbf{h}}_{SD}\|}\right|^2$ and $y_4 = |\mathbf{h}_{SE}\mathbf{w}_J|^2$. Since $\frac{\widehat{\mathbf{h}}_{SD}^H}{\|\widehat{\mathbf{h}}_{SD}\|}$ and $\mathbf{w}_J$ are orthonormal vectors, it follows that y_3 and y_4 follow an exponential distribution with unit power and are independent of each other. The pdf of y_1 has been shown in (17), and so the secrecy outage probability can be written as

$$P_{so}^{MRT} = \int_0^{+\infty}\int_{e_2y_4}^{+\infty}\int_{\frac{e_1}{y_3-e_2y_4}}^{+\infty}\frac{y_1^{N-1}e^{-y_1}}{(N-1)!}e^{-y_3}e^{-y_4}dy_1dy_3dy_4,$$

where $e_1 = \frac{d_1^\tau d_3^\tau \gamma_e N_0}{\mathcal{K} P \beta}$ and $e_2 = \frac{(1-\beta)\gamma_e}{\beta}$. With the help of Eq. (3.351.2) [28] , we obtain

$$P_{so}^{MRT} = \int_0^{+\infty} \int_{e_2 y_4}^{+\infty} \sum_{k=0}^{N-1} \frac{e_1^k e^{-\frac{e_1}{y_3 - e_2 y_4}}}{k!(y_3 - e_2 y_4)^k} e^{-y_3} e^{-y_4} dy_3 dy_4.$$

Let us define $t = y_3 - e_2 y_4$, then P_{so}^{MRT} can be expressed as

$$\begin{aligned} P_{so}^{MRT} &= \int_0^{+\infty} \int_0^{+\infty} \sum_{k=0}^{N-1} \frac{e_1^k e^{-\frac{e_1}{t}}}{k! t^k} e^{-(t+e_2 y_4)} e^{-y_4} dt dy_4 \\ &= \int_0^{+\infty} e^{-(e_2+1)y_4} \int_0^{+\infty} \sum_{k=0}^{N-1} \frac{e_1^k}{k!} t^{-k} e^{-(e_1/t+t)} dt dy_4. \end{aligned}$$

Finally, by invoking Eq. (3.471.9) [28], we obtain

$$\begin{aligned} P_{so}^{MRT} &= \int_0^{+\infty} e^{-(e_2+1)y_4} \sum_{k=0}^{N-1} \frac{2 e_1^{(k+1)/2}}{k!} \mathbf{K}_{(1-k)}(2\sqrt{e_1}) dy_4 \\ &= \frac{1}{1+e_2} \sum_{k=0}^{N-1} \frac{2 e_1^{(k+1)/2}}{k!} \mathbf{K}_{(1-k)}(2\sqrt{e_1}), \end{aligned}$$

and the theorem is proved. ■

Proof of Corollary 3 : In the high SNR regime, when $P/N_0 \to \infty$, we know that $\gamma' \to 0$ and $e_1 \to 0$. Utilizing Theorems 1 and 2, the expressions of the connection outage probability P_{co}^{MRT} and the secrecy outage probability P_{so}^{MRT} may be given as:

$$P_{co}^{MRT} = 1 - \binom{N}{K} \left[\sum_{k=0}^{N-1} \frac{2\gamma'^{(K+k)/2}}{k!(K-1)!} \mathbf{K}_{(K-k)}(2\sqrt{\gamma'}) + \sum_{l=1}^{N-K} (-1)^{(K+l-1)} \binom{N-K}{l} \left(\frac{K}{l}\right)^{(K-1)} \right.$$
$$\left. \left(\sum_{k=0}^{N-1} \frac{2\gamma'^{(k+1)/2} \left(\frac{K}{l+K}\right)^{(1-k)/2}}{k!} \mathbf{K}_{(1-k)} \left(2\sqrt{\tfrac{l+K}{K}\gamma'} \right) - \sum_{m=0}^{K-2} \frac{\left(\frac{-l}{K}\right)^m}{m!} \sum_{k=0}^{N-1} \frac{2\gamma'^{(m+k+1)/2}}{k!} \mathbf{K}_{(m-k+1)}(2\sqrt{\gamma'}) \right) \right]$$

and

$$P_{so}^{MRT} = \frac{1}{1+e_2} \sum_{k=0}^{N-1} \frac{2 e_1^{(k+1)/2}}{k!} \mathbf{K}_{(1-k)}(2\sqrt{e_1}).$$

After expanding the Bessel function by Eq. (8.446) [28] and omitting the high order items of γ' and e_1, we obtain

$$P_{co}^{MRT} \approx M \gamma'^N \ln \gamma',$$

where

$$M = \binom{N}{K} \left[\sum_{k=0}^{N-1} \frac{(-1)^{(K-k)}}{k!(K-1)!(N-K)!(N-k)!} + \sum_{l=1}^{N-K} (-1)^{(K+l)} \binom{N-K}{l} \left(\frac{K}{l}\right)^{(K-1)} \right.$$

$$\left(\sum_{k=0}^{N-1}\frac{(-1)^k\left(\frac{K+l}{K}\right)^{N-1}}{k!(N-k)!(N-1)!}-\sum_{m=0}^{K-2}\frac{\left(\frac{-l}{K}\right)^m}{m!}\sum_{k=0}^{N-1}\frac{(-1)^{(m-k)}}{k!(N-m-1)!(N-k)!}\right)\Bigg],$$

and

$$P_{so}^{MRT}\approx\frac{1}{1+e_2}.$$

This proves the corollary. ■

Proof of Corollary 4 : We begin by defining the outage probability as

$$P_{out}^{MRT}\triangleq\mathbf{Pr}\left((1-\alpha)\left(\log_2\left(1+\gamma_D\right)-\log_2\left(1+\gamma_E\right)\right)<R_s\right).$$

In the high SNR regime, we have $\rho = P/N_0 \to \infty$ as $\gamma_D \to \infty$, and so $\log_2(1+\gamma_D) - \log_2(1+\gamma_E) \to \log_2(1+\gamma_D)$. Therefore, in the high SNR regime, $P_{out}^{MRT} \approx \mathbf{Pr}\left((1-\alpha)\log_2(1+\gamma_D)<R_s\right)$. Finally, using Corollary 3 and the fact that $\lim_{x\to\infty}\frac{\log x}{x}=0$, we know that $d^{MRT}\triangleq-\lim_{\rho\to\infty}\frac{\log[P_{out}^{MRT}(\rho)]}{\log(\rho)}=N$, which proves the corollary. ■

Proof of Theorem 9 : From section III-A1, we know that in the high SNR regime, under the outage constraints $P_{co}^{MRT}\le\sigma$ and $P_{so}^{MRT}\le\epsilon$, the optimal time and power allocating coefficients (α^*,β^*) can be approximated as the solution of the following optimization problem:

$$\mathbf{OP}1: \quad \max_{(\alpha,\beta)} \quad (1-\sigma)(1-\alpha)\left(\log_2\left(1+\frac{\beta\mathcal{K}P\sigma'}{N_0d_1^\tau d_2^\tau}\right)-\log_2\left(2+\frac{\beta-\epsilon}{\epsilon(1-\beta)}\right)\right) \quad (18)$$
$$\text{s.t.} \qquad 0\le\alpha,\beta\le1.$$

Since $(1-\sigma)$ is not determined by (α,β), the optimization problem can be reconstructed as

$$\mathbf{OP}2: \quad \max_{(\alpha,\beta)} \quad R_s^{MRT}$$
$$\text{s.t.} \qquad 0\le\alpha,\beta\le1,$$

where $R_s^{MRT}=(1-\alpha)\left(\log_2\left(1+\frac{\beta\mathcal{K}P\sigma'}{N_0d_1^\tau d_2^\tau}\right)-\log_2\left(2+\frac{\beta-\epsilon}{\epsilon(1-\beta)}\right)\right)$. In the following, we show that R_s^{MRT} is a concave function of (α,β) in the high SNR regime.

From the expression for R_s^{MRT} we have

$$\frac{\partial R_s^{MRT}}{\partial\alpha}=\frac{\frac{\eta\beta\rho\sigma'}{d_1^\tau d_2^\tau}}{\left(1+\frac{\beta\mathcal{K}\rho\sigma'}{d_1^\tau d_2^\tau}\right)(1-\alpha)\ln2}-\log_2\left(1+\frac{\beta\mathcal{K}\rho\sigma'}{d_1^\tau d_2^\tau}\right)+\log_2\left(2+\frac{\beta-\epsilon}{\epsilon(1-\beta)}\right) \quad (19)$$

and

$$\frac{\partial R_s^{MRT}}{\partial \beta} = \frac{(1-\alpha)\left(\frac{\mathcal{K}\rho\sigma'}{d_1^\tau d_2^\tau}\right)}{\left(1+\frac{\beta\mathcal{K}\rho\sigma'}{d_1^\tau d_2^\tau}\right)\ln 2} - \frac{(1-\alpha)(1-\epsilon)}{\ln 2[2\epsilon(1-\beta)^2+(1-\beta)(\beta-\epsilon)]},$$

where $\rho = P/N_0$. We then derive the second-order derivatives of R_s^{MRT}:

$$\frac{\partial^2 R_s^{MRT}}{\partial^2 \alpha} = \frac{\eta\beta\rho\sigma'}{d_1^\tau d_2^\tau \ln 2}\left[\frac{-\frac{\eta\beta\rho\sigma'}{d_1^\tau d_2^\tau}}{\left(1+\frac{\beta\mathcal{K}\rho\sigma'}{d_1^\tau d_2^\tau}\right)^2(1-\alpha)^3}\right],$$

and it is easy to see that $\frac{\partial^2 R_s^{MRT}}{\partial^2 \alpha} \leq 0$ in all cases. We also have

$$\frac{\partial^2 R_s^{MRT}}{\partial^2 \beta} = \frac{-(1-\alpha)\left(\frac{\mathcal{K}\rho\sigma'}{d_1^\tau d_2^\tau}\right)^2}{\left(1+\frac{\beta\mathcal{K}\rho\sigma'}{d_1^\tau d_2^\tau}\right)^2\ln 2} + \frac{(1-\alpha)(1-\epsilon)[1-2\beta+\epsilon(4\beta-3)]}{\ln 2[2\epsilon(1-\beta)^2+(1-\beta)(\beta-\epsilon)]^2}.$$

In the high SNR regime, when $\rho \to \infty$, $1+\frac{\beta\mathcal{K}\rho\sigma'}{d_1^\tau d_2^\tau} \to \frac{\beta\mathcal{K}\rho\sigma'}{d_1^\tau d_2^\tau}$. So $\frac{\partial^2 R_s^{MRT}}{\partial^2 \beta}$ can be approximated as

$$\begin{aligned}\frac{\partial^2 R_s^{MRT}}{\partial^2 \beta} &\approx \frac{-(1-\alpha)}{\beta^2 \ln 2} + \frac{(1-\alpha)(1-\epsilon)(1-2\beta+4\beta\epsilon-3\epsilon)}{\ln 2(1-\beta)^2(\beta+\epsilon-2\beta\epsilon)^2} \\ &= \frac{-(1-\alpha)}{\ln 2}(A-B),\end{aligned}$$

where

$$A = \frac{1}{\beta^2} \quad \text{and} \quad B = \frac{(1-\epsilon)(1-2\beta+4\beta\epsilon-3\epsilon)}{(1-\beta)^2(\beta+\epsilon-2\beta\epsilon)^2}.$$

Now we prove that $A-B$ is always greater than zero. B can be expressed as

$$B = \frac{C}{(1-\beta)^2 D},$$

where

$$\begin{aligned}C &= (1-\epsilon)(1-2\beta+4\beta\epsilon-3\epsilon) \\ &= (3-4\beta)\epsilon^2+(6\beta-4)\epsilon-2\beta+1\end{aligned} \tag{20}$$

and

$$\begin{aligned}D &= (\beta+\epsilon-2\beta\epsilon)^2 \\ &= \epsilon^2+\beta^2+2\beta\epsilon-4\beta\epsilon^2-4\beta^2\epsilon+4\epsilon^2\beta^2.\end{aligned}$$

Equation 20 implies that $C = (1-\epsilon)[(1-2\beta)+\epsilon(4\beta-3)]$. We now consider three cases depending on the value of β. First, let $\frac{1}{2} < \beta < \frac{3}{4}$. Then we have $1-2\beta < 0$ and $\epsilon(4\beta-3) < 0$, so that $C < 0$ and $A-B > 0$. Next consider the case where $\beta > \frac{3}{4}$. Then $(2\beta-1)/\epsilon-(4\beta-3) > (2\beta-1)-(4\beta-3) = 2-2\beta > 0$ and $C = -(1-\epsilon)\epsilon[(2\beta-1)/\epsilon-(4\beta-3)] < 0$, from which it also follows that $A-B > 0$.

Finally, we consider the case where $\beta < \frac{1}{2}$ and we cannot tell whether $C < 0$ or $C > 0$. When $C < 0$, $B < 0$ and it is straightforward to see that $A-B > 0$. On the other hand, when $C > 0$, we have $(1-2\beta)+\epsilon(4\beta-3) > 0$, and thus $\epsilon < \frac{2\beta-1}{4\beta-3}$. It follows that

$$\frac{\partial C}{\partial \epsilon} = -[(1-2\beta)+\epsilon(4\beta-3)] + (1-\epsilon)(4\beta-3) < 0$$

and

$$\frac{\partial D}{\partial \epsilon} = 2(1-2\beta)(\beta+\epsilon-2\beta\epsilon) > 0.$$

This means that the maximum value of C and minimum value of D, and thus the maximum value for B, occur when $\epsilon = 0$. Now we only need to prove that when $\beta < \frac{1}{2}$ and $\epsilon = 0$, $A-B > 0$. In this case, $A-B$ can be expressed as

$$\begin{aligned} A-B &= \frac{1}{\beta^2} - \frac{1-2\beta}{(1-\beta)^2\beta^2} \\ &= \frac{\beta^2}{\beta^2(1-\beta)^2} \\ &> 0, \end{aligned}$$

proving that $A-B$ is always greater than zero and that, therefore, $\frac{\partial^2 R_s^{MRT}}{\partial^2 \beta} \leq 0$ in the high SNR regime.

In the high SNR regime, when $1+\frac{\beta\mathcal{K}\rho\sigma'}{d_1^T d_2^T} \to \frac{\beta\mathcal{K}\rho\sigma'}{d_1^T d_2^T}$, we know the following:

$$\begin{aligned} [1] \quad \frac{\partial R_s^{MRT}}{\partial \beta} &= \frac{(1-\alpha)\left(\frac{\mathcal{K}\rho\sigma'}{d_1^T d_2^T}\right)}{\left(1+\frac{\beta\mathcal{K}\rho\sigma'}{d_1^T d_2^T}\right)\ln 2} - \frac{(1-\alpha)(1-\epsilon)}{\ln 2[2\epsilon(1-\beta)^2+(1-\beta)(\beta-\epsilon)]} \\ &\approx \frac{(1-\alpha)}{\ln 2}\left(\frac{1}{\beta} - \frac{(1-\epsilon)}{(1-\beta)(\epsilon+\beta-2\epsilon\beta)}\right) \end{aligned} \tag{21}$$

$$[2] \quad \frac{\partial^2 R_s^{MRT}}{\partial\beta\partial\alpha} \approx \frac{1}{\ln 2}\left(\frac{-1}{\beta}+\frac{(1-\epsilon)}{(1-\beta)(\epsilon+\beta-2\epsilon\beta)}\right)$$

$$[3] \quad \frac{\partial^2 R_s^{MRT}}{\partial^2\alpha} = \frac{\eta\beta\rho\sigma'}{d_1^\tau d_2^\tau \ln 2}\left[\frac{-\frac{\eta\beta\rho\sigma'}{d_1^\tau d_2^\tau}}{\left(1+\frac{\beta\mathcal{K}\rho\sigma'}{d_1^\tau d_2^\tau}\right)^2(1-\alpha)^3}\right] \approx \frac{-1}{\alpha^2(1-\alpha)\ln 2}$$

$$[4] \quad \frac{\partial^2 R_s^{MRT}}{\partial^2\beta} = \frac{-(1-\alpha)\left(\frac{\mathcal{K}\rho\sigma'}{d_1^\tau d_2^\tau}\right)^2}{\left(1+\frac{\beta\mathcal{K}\rho\sigma'}{d_1^\tau d_2^\tau}\right)^2\ln 2}+\frac{(1-\alpha)(1-\epsilon)[1-2\beta+\epsilon(4\beta-3)]}{\ln 2[2\epsilon(1-\beta)^2+(1-\beta)(\beta-\epsilon)]^2} \approx \frac{-(1-\alpha)}{\ln 2}\left(\frac{1}{\beta^2}-\frac{(1-\epsilon)(1-2\beta+4\beta\epsilon-3\epsilon)}{(1-\beta)^2(\beta+\epsilon-2\beta\epsilon)^2}\right).$$

Then we have

$$\begin{aligned}
&\frac{\partial^2 R_s^{MRT}}{\partial^2\alpha}\frac{\partial^2 R_s^{MRT}}{\partial^2\beta}-\left(\frac{\partial^2 R_s^{MRT}}{\partial\beta\partial\alpha}\right)^2 \\
&=\left(\frac{1}{\ln 2}\right)^2\left[\left(\frac{1}{\alpha^2\beta^2}-\frac{(1-\epsilon)(1-2\beta+4\beta\epsilon-3\epsilon)}{\alpha^2(1-\beta)^2(\beta+\epsilon-2\beta\epsilon)^2}\right)-\left(\frac{-1}{\beta}+\frac{(1-\epsilon)}{(1-\beta)(\epsilon+\beta-2\epsilon\beta)}\right)^2\right] \\
&>\left(\frac{1}{\ln 2}\right)^2\left[\left(\frac{1}{\beta^2}-\frac{(1-\epsilon)(1-2\beta+4\beta\epsilon-3\epsilon)}{(1-\beta)^2(\beta+\epsilon-2\beta\epsilon)^2}\right)-\left(\frac{-1}{\beta}+\frac{(1-\epsilon)}{(1-\beta)(\epsilon+\beta-2\epsilon\beta)}\right)^2\right] \\
&=\left(\frac{1}{\ln 2}\right)^2\frac{(1-\epsilon)}{(1-\beta)(\epsilon+\beta-2\epsilon\beta)}\left(\frac{-(1-2\beta+4\beta\epsilon-3\epsilon)}{(1-\beta)(\epsilon+\beta-2\epsilon\beta)}-\frac{(1-\epsilon)}{(1-\beta)(\epsilon+\beta-2\epsilon\beta)}+\frac{2}{\beta}\right) \\
&=\left(\frac{1}{\ln 2}\right)^2\frac{(1-\epsilon)}{(1-\beta)^2(\epsilon+\beta-2\epsilon\beta)^2}O,
\end{aligned}$$

where

$$\begin{aligned}
O &= -(1-2\beta+4\beta\epsilon-3\epsilon)-(1-\epsilon)+\frac{2}{\beta}(1-\beta)(\epsilon+\beta-2\epsilon\beta) \qquad (22)\\
&= \frac{2\epsilon(1-\beta)}{\beta} \\
&> 0.
\end{aligned}$$

From which it follows that $\frac{\partial^2 R_s^{MRT}}{\partial^2\alpha}\frac{\partial^2 R_s^{MRT}}{\partial^2\beta}-\left(\frac{\partial^2 R_s^{MRT}}{\partial\beta\partial\alpha}\right)^2 > 0$ always holds in the high SNR regime.

Therefore we have proved that the optimization problem in (18) is a concave problem, and its optimal solution (α^*, β^*) can be calculated as $\frac{\partial R_s^{MRT}}{\partial \alpha} = 0$ and $\frac{\partial R_s^{MRT}}{\partial \beta} = 0$ in the high SNR regime. Finally, from (19) and (21), we have

$$\beta^* = \begin{cases} \frac{1}{2} & \text{if } \epsilon = \frac{1}{2} \\ \frac{\epsilon - \sqrt{\epsilon - \epsilon^2}}{2\epsilon - 1} & \text{otherwise} \end{cases}$$

and

$$\alpha^* = \frac{1}{1 + \mathbf{W}(e^{V \ln 2})},$$

where $\mathbf{W}(x) = f^{-1}(xe^x)$ is the the Lambert W function and

$$V = \log_2 \left(\frac{\beta \eta P \sigma'}{N_0 d_1^\tau d_2^\tau} \right) - \frac{1}{\ln 2} - \log_2 \left(2 + \frac{\beta - \epsilon}{\epsilon(1-\beta)} \right).$$

This completes the proof. ■

Proof of Theorem 5 : From Equations (3) and (12), we know that P_{co}^{ZF} can be expressed as

$$\begin{aligned} P_{co}^{ZF} &= \mathbf{Pr}\left((1-\alpha) \log_2 \left(1 + \frac{\beta \mathcal{K} P y_1 z_2}{d_1^\tau d_2^\tau N_0} \right) < R_t \right) \\ &= \mathbf{Pr}\left(y_1 z_2 < \gamma' \right), \end{aligned}$$

where $\gamma' = \left(2^{\left(\frac{R_t}{1-\alpha} \right)} - 1 \right) d_1^\tau d_2^\tau N_0 / (\beta \mathcal{K} P)$, and the pdf of z_2 is an exponential distribution with unit power. Then, by following the same steps as in the proof of Theorem 1, we obtain

$$P_{co}^{ZF} = 1 - \sum_{k=0}^{N-1} \frac{2 \gamma'^{(k+1)/2}}{k!} \mathbf{K}_{(1-k)} \left(2\sqrt{\gamma'} \right),$$

which completes the proof of the theorem. ■

Proof of Theorem 6 : From Equations (4) and (13), we know that P_{so}^{ZF} can be expressed as

$$P_{so}^{ZF} = \mathbf{Pr}\left((1-\alpha) \log_2 \left(1 + \frac{\beta \mathcal{K} P y_1 z_4}{(1-\beta) \mathcal{K} P y_1 z_3 + d_1^\tau d_3^\tau N_0} \right) > R_e \right).$$

where $\gamma_e = 2^{\left(\frac{R_e}{1-\alpha} \right)} - 1$ and the pdf of z_3 is an exponential distribution with unit power. The pdf of z_4 is an exponential distribution with power N_E. Using the same method as in the proof of Theorem 2, we may then express P_{so}^{ZF} as

$$P_{so}^{ZF} = \frac{1}{(1 + e_2/N_E)} \sum_{k=0}^{N-1} \frac{2 \left(\frac{e_1}{N_E} \right)^{(k+1)/2}}{k!} \mathbf{K}_{(1-k)} \left(2\sqrt{\frac{e_1}{N_E}} \right),$$

and the theorem is proved. ■

Proof of Corollary 7 : In the high SNR regime, when $P/N_0 \to \infty$, we know that $\gamma' \to 0$ and $e_1 \to 0$. By Theorems 5 and 6, the expressions of the connection outage probability P_{co}^{ZF} and the secrecy outage probability P_{so}^{ZF} are given by:

$$P_{co}^{ZF} = 1 - \sum_{k=0}^{N-1} \frac{2\gamma'^{(k+1)/2}}{k!} \mathbf{K}_{(1-k)} \left(2\sqrt{\gamma'}\right).$$

and

$$P_{so}^{ZF} = \frac{1}{(1+e_2/N_E)} \sum_{k=0}^{N-1} \frac{2\left(\frac{e_1}{N_E}\right)^{(k+1)/2}}{k!} \mathbf{K}_{(1-k)} \left(2\sqrt{\frac{e_1}{N_E}}\right).$$

After expanding the Bessel function by Eq. (8.446) [28] and omitting the high order items of γ' and e_1, we can obtain

$$P_{co}^{ZF} \approx \frac{\gamma'}{N-1} \tag{23}$$

and

$$P_{so}^{ZF} \approx \frac{1}{1+e_2/N_E}, \tag{24}$$

which proves the corollary. ■

Proof of Corollary 8 : We define the outage probability as

$$P_{out}^{ZF} \triangleq \mathbf{Pr}\left((1-\alpha)\left(\log_2\left(1+\widehat{\gamma}_D\right) - \log_2\left(1+\widehat{\gamma}_E\right)\right) < R_s\right). \tag{25}$$

Then, with the help of corollary 7 and following the same steps as in the proof of Corollary 4, we have $d^{ZF} \triangleq -\lim_{\rho\to\infty} \frac{\log[P_{out}^{ZF}(\rho)]}{\log(\rho)} = 1$, and the corollary is proved. ■

REFERENCES

[1] 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, 2013.

[2] X. Jiang, C. Zhong, X. Chen, T. Q. Duong, T. A. Tsiftsis, and Z. Zhang, "Secrecy performance of wirelessly powered wiretap channels," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3858–3871, 2016.

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

[4] X. Chen, Z. Zhang, H.-H. Chen, and H. Zhang, "Enhancing wireless information and power transfer by exploiting multi-antenna techniques," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 133–141, 2015.

[5] Z. Ding, C. Zhong, D. W. K. Ng, M. Peng, H. A. Suraweera, R. Schober, and H. V. Poor, "Application of smart antenna technologies in simultaneous wireless information and power transfer," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 86–93, 2015.

[6] H. Chen, Y. Li, J. L. Rebelatto, B. F. Uchôa-Filho, and B. Vucetic, "Harvest-then-cooperate: Wireless-powered cooperative communications," *IEEE Trans. Signal Process.*, vol. 63, no. 7, pp. 1700–1711, 2015.

[7] X. Chen, C. Yuen, and Z. Zhang, "Wireless energy and information transfer tradeoff for limited-feedback multiantenna systems with energy beamforming," *IEEE Trans Veh. Technol.*, vol. 63, no. 1, pp. 407–412, 2014.

[8] X. Kang, C. K. Ho, and S. Sun, "Full-duplex wireless-powered communication network with energy causality," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5539–5551, 2015.

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

[10] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory.*, vol. 54, no. 10, pp. 4687–4698, 2008.

[11] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory.*, vol. 57, no. 8, pp. 4961–4972, 2011.

[12] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory.*, vol. 55, no. 6, pp. 2547–2553, 2009.

[13] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory.*, vol. 56, no. 7, pp. 3088–3104, 2010.

[14] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennasłpart II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory.*, vol. 56, no. 11, pp. 5515–5532, 2010.

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

[16] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE. J. Sel. Areas Commun*, vol. 31, no. 9, pp. 1728–1740, 2013.

[17] X. Zhang, X. Zhou, and M. R. 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, 2013.

[18] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, 2014.

[19] H. Zhang, C. Li, Y. Huang, and L. Yang, "Secure beamforming for SWIPT in multiuser MISO broadcast channel with confidential messages," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1347–1350, 2015.

[20] Q. Shi, W. Xu, J. Wu, E. Song, and Y. Wang, "Secure beamforming for MIMO broadcasting with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2841–2853, 2015.

[21] D. W. K. Ng, E. S. Lo, and R. Schober, "Multiobjective resource allocation for secure communication in cognitive radio networks with wireless information and power transfer," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, pp. 3166–3184, 2016.

[22] X. Huang, Q. Li, Q. Zhang, and J. Qin, "Power allocation for secure OFDMA systems with wireless information and power transfer," *IET Electron. Lett.*, vol. 50, no. 3, pp. 229–230, 2014.

[23] 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, 2015.

[24] K. Huang and V. K. Lau, "Enabling wireless power transfer in cellular networks: architecture, modeling and deployment," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 902–912, 2014.

[25] Y. Wu, X. Chen, C. Yuen, and C. Zhong, "Robust resource allocation for secrecy wireless powered communication networks," *IEEE Commun. Lett.*

[26] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622–3636, 2013.

[27] C. Wang and H.-M. Wang, "Opportunistic jamming for enhancing security: Stochastic geometry modeling and analysis," 2016.

[28] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 6th ed. Academic Press, 2000.

[29] L. Zheng and D. N. C. Tse, "Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels," *IEEE Trans. Inf. Theory.*, vol. 49, no. 5, pp. 1073–1096, 2003.

[30] M. K. Simon and M.-S. Alouini, *Digital communication over fading channels*. John Wiley & Sons, 2005.

[31] M.-S. Alouini and M. K. Simon, "An MGF-based performance analysis of generalized selection combining over rayleigh fading channels," *IEEE Trans. Commun.*, vol. 48, no. 3, pp. 401–415, 2000.