Security Enhancement of Wireless Networks with Wireless-Powered Full-Duplex Relay and Friendly Jammer Nodes

Zahra Mobini†, Mohammadali Mohammadi†, and Chintha Tellambura†
†Faculty of Engineering, Shahrekord University, Iran (e-mail: z.mobini, m.a.mohammadi@eng.sku.ac.ir)
†Department of Electrical and Computer Engineering, University of Alberta, Canada (e-mail: chintha@ece.ualberta.ca)

***Abstract*—In this paper we propose an energy harvesting-based cooperative jamming and full-duplex relaying scheme to enhance the secrecy rate for wireless communication between a source node and a destination node, in the presence of an eavesdropper. To characterize the performance, we develop a mathematical analysis framework for instantaneous and average secrecy rates. We consider the practical interference limited scenario, and derive exact closed-form expressions for the cumulative distribution function of the signal-to-noise-plus-interference ratio (SNIR) at the destination and eavesdropper nodes. Accordingly, the asymptotic average secrecy rates are derived. We show that the proposed protocol improves the average secrecy rate of a wireless cooperative network substantially. However, the instantaneous secrecy rate performance gain is highly depend on the duration of energy harvesting, the amount of self-interference and the corresponding channels and positions of the nodes in the system.**

I. Introduction

A. Motivation and Background

Wireless networks are susceptible to listening by any unintended receiver within a communication range, known as eavesdropper, which can overhear and probably decode the transmitted information [1] due to the broadcast nature of the wireless channels. Secret key encryption techniques have long been regarded as a common way to prevent eavesdropping and enhance security. However, encryption is implemented at higher network layers and may lead to increased system complexity and costs. Due to this reason, physical-layer security has emerged as a promising secure communication technique by exploiting the wireless physical-layer properties [1], [2]. One well-known performance criterion in physical-layer security is the secrecy rate defined as the rate difference between the transmission rate of the legitimate channel and that of the wiretap channel, i.e., the channel between the transmission node and the eavesdropper. If the secrecy rate falls below zero, the transmission becomes insecure, and the eavesdropper can intercept confidential information [2]. To alleviate this problem, enhancing the secrecy rate by taking advantage of user cooperation has been proposed.

There are two secure user cooperation modes: cooperative relaying and cooperative jamming where in the former the legitimate channel is strengthened by a relay node and in the latter the wiretap channel rate is degraded by a jammer node [2]. On the other hand half-duplex (HD) constraint of the cooperative relaying leads to a loss of spectral efficiency while recent multimedia centric wireless applications have created a high demand for bandwidth. An attractive solution to improve the spectral efficiency is to allow full-duplex (FD) operation at the relay which allows simultaneous transmission and reception of signals using the same frequency [3]–[7]. The authors in [2], [8] have addressed secure communications of one source-destination pair with the help of multiple HD relays in the presence of one or more eavesdroppers. In [9], [10], it was shown that by introducing cooperative transmission into secrecy communication systems the outage probability approaching zero can be achieved. The authors in [11] analyzed and compared the ergodic secrecy rate performance of the cooperative jamming and cooperative relaying, in the low and high signal-to-noise ratio regimes and for different eavesdropper positions. In [6], [7], secure wireless communications between a source and a destination aided by a FD relay, in the presence of an eavesdropper utilizing cooperative relaying and cooperative jamming are explored.

The aforementioned publications demonstrate that the achievable secrecy rate can be improved by user cooperation, either via relaying or via cooperative jamming. However, they have not jointly considered the following challenges: 1) HD constraint of the cooperative relaying and 2) extra power consumption of relay and jammer considering the life-time issue, which is one of the major challenges for contemporary wireless networks such as sensor and ad-hoc networks. Their wireless nodes are power-limited by batteries and may not be connected to the power grid due to mobility or other constraints. A potential solution is harvesting ambient power or wireless power transfer [12], [13].

B. Problem Statement and Key Contributions

Motivated by these challenges, we develop a novel secure wireless communication scheme that efficiently deals with the presence of an eavesdropper while taking advantage of FD cooperative relaying, cooperative jamming and energy harvesting. We employ the time-splitting (TS) architecture for energy harvesting [14]. Hence, the cooperation round consists of two phases: energy harvesting phase and information transmission phase. Specifically, for a transmission block time T, $0 \leq \alpha \leq 1$ fraction of the block time is dedicated to energy harvesting and the remaining time, $(1-\alpha)T$, is used for

information transmission. We then investigate instantaneous and average secrecy rates, which are two fundamental secrecy performance criteria in the active eavesdropping scenario [2], [15]. Note that an active eavesdropping scenario where the channel state information (CSI) of the eavesdropping channel is available at the source and relay nodes is of practical interest in many classes of applications that the users play dual roles as legitimate receivers for some signals and eavesdroppers for others [2], [15]. For example, the potential application scenarios include multicast, multi-unicast and unicast systems.

The main contributions of this paper are as follows:

- We propose a FD-relaying protocol that provides secure communication using a jamming node. Both relay and jammer nodes are wirelessly powered by the source node. We also study the output signal-to-noise-plus-interference ratio (SNIR) at the destination and eavesdropper nodes.
- We derive analytical expressions for the instantaneous and average secrecy rates. To gain more design insights and to provide mathematical framework, we consider a practical interference limited scenario and derive a closed-form expression for the cumulative distribution function (cdf) of the SNIR at the destination and eavesdropper nodes. Accordingly, the asymptotic average secrecy rate is calculated. With simulation results, we validate our analysis and show that the proposed protocol significantly improves the secrecy rate of the wireless cooperative network.

Notation: We assume $(\cdot)^\dagger$ and $\Pr(\cdot)$ denote the conjugate transpose operator and probability respectively; $f_X(\cdot)$ and $F_X(\cdot)$ denote the probability density function (pdf) and cdf of the random variable (RV) X, respectively; $\mathcal{CN}(\mu,\sigma^2)$ denotes a circularly symmetric complex Gaussian RV x with mean μ and variance σ^2; $K_\nu(\cdot)$ is the νth order modified Bessel function of the second kind [16, Eq. (8.432)]; $\mathsf{E_i}(x)$ is the exponential integral function [17, Eq. (5.1.4)] and $G_{pq}^{mn}\left(z \mid \begin{smallmatrix} a_1 \cdots a_p \\ b_1 \cdots b_q \end{smallmatrix}\right)$ denotes the Meijer G-function [16, Eq. (9.301)].

II. System Model And Transmission Protocol

We consider a communication scenario where a source node S communicates with a destination node D in the presence of an eavesdropper E with the help of a trusted relay R and a friendly jammer J. The trusted relay node and the jammer node are energy constrained nodes and have the rechargeable batteries with infinite capacity. In order to make use of the relay and the jammer, the source node wirelessly charges them via wireless power transfer. Once the relay and the jammer harvest sufficient energy they can be used for information transmission and for transmitting friendly jamming signals to enhance the security of the communication, respectively. The source is assumed to be located far away from the destination and eavesdropper, such that there is no direct link from the source to the destination or eavesdropper. We assume that the relay applies the decode-and-forward (DF) protocol. The channel coefficients for $S-R$, $S-J$, $R-D$, $R-J$, $R-E$, $J-R$, $J-E$, and $J-D$ are denoted as h_{SR}, h_{SJ}, h_{RD}, h_{RJ}, h_{RE}, h_{JR}, h_{JE} and h_{JD}, respectively. We assume that all channels experience block Rayleigh fading and remain constant over one block but varies independently and identically from one block to another. Thus, all channel gains are independent and identically distributed (i.i.d) exponential random variables with unit mean. d_{SR}, d_{SJ}, d_{RD}, d_{RJ}, d_{RE}, d_{JR}, d_{JE}, and d_{JD} are the distances between the pairs $S-R$, $S-J$, $R-D$, $R-J$, $R-E$, $J-R$, $J-E$, and $J-D$, respectively.

A. Transmission Protocol

We assume that source, destination, eavesdropper and jammer nodes are subject to a HD constraint, while the relay station operates in a FD mode. The simultaneous transmission and reception at the relay in FD mode causes self-interference (SI) from the transmit antenna to the receive antenna which cannot be cancelled completely [18]. Nevertheless, many effective SI cancellation techniques have been proposed to date [5], [18]. Hence, we assume that an imperfect interference cancellation scheme is used at the relay. We model the residual SI channel h_{RR} as $h_{RR} \sim \mathcal{CN}(0,\sigma_{RR}^2)$, which is a common assumption in the literature [3], [5].

The secure protocol with wireless-powered relay and jammer takes places in two phases. Particularly, during the energy harvesting phase of duration αT, the source transfers power to the relay and jammer by sending a radio signal with power p_S. The relay and jammer apply the harvest-use architecture [14] and hence, they receive the radio signal, convert it to a direct current signal and store the energy. The received signal at the relay and jammer can be expressed as

$$r_e[n] = \sqrt{\frac{p_S}{d_{SR}^m}} h_{SR} x_e[n] + n_R[n], \tag{1a}$$

$$y_J[n] = \sqrt{\frac{p_S}{d_{SJ}^m}} h_{SJ} x_e[n] + n_J[n], \tag{1b}$$

where x_e is the energy symbol with unit energy, $\mathtt{E}\left\{x_e[n]x_e^\dagger[n]\right\} = 1$ and m is the path loss exponent. n denotes the symbol index; $n_R[n] \sim \mathcal{CN}(0,\sigma_R^2)$ and $n_J[n] \sim \mathcal{CN}(0,\sigma_J^2)$ denote the noise at R and J, respectively. Therefore, using (1a) and (1b), the harvested energy at R and J in each unit slot are given by $p_R = \frac{\kappa}{d_{SR}^m} p_S |h_{SR}|^2$ and $p_J = \frac{\kappa}{d_{SJ}^m} p_S |h_{SJ}|^2$, respectively, where $\kappa = \frac{\eta\alpha}{(1-\alpha)}$ and η, $0 \le \eta \le 1$ is RF-to-DC energy conversion efficiency.

During the information transmission phase with the remaining time $(1-\alpha)T$, the source transmits $x_S[n]$ to the FD relay R, while R simultaneously receives $r[n]$ and forwards $x_R[n]$ with power p_R to the destination using the harvested energy in the first transmission phase. At the same time, eavesdropper overhears the information signal $x_R[n]$ while the jammer sends jamming signal to the eavesdropper with power p_J to compromise eavesdropper. More specifically, the jammer sends an artificial noise signal x_J, affecting the relay, destination and eavesdropper. The received signal at R can be expressed as

$$r[n] = \sqrt{\frac{p_S}{d_{SR}^m}} h_{SR} x_S[n] + h_{RR} x_R[n] + \sqrt{\frac{p_J}{d_{JR}^m}} h_{JR} x_J[n] + n_R[n], \tag{2}$$

where $x_S[n]$, $x_R[n]$ and $x_J[n]$ are respectively satisfying, $\mathtt{E}\left\{x_S[n]x_S^\dagger[n]\right\} = 1$, $\mathtt{E}\left\{x_R[n]x_R^\dagger[n]\right\} = p_R$ and $\mathtt{E}\left\{x_J[n]x_J^\dagger[n]\right\} = 1$. Since R adopts the DF protocol, upon receiving the signal, it first decodes x_S and then forwards the signal to D. The relay transmit signal is given by [18]

$$x_R[n] = \sqrt{p_R}x_S[n-\tau], \tag{3}$$

where τ accounts for the time delay caused by relay processing. Finally, the received signal at D and E are expressed as

$$y_D[n] = \sqrt{\frac{1}{d_{RD}^m}}h_{RD}x_R[n] + \sqrt{\frac{p_J}{d_{JD}^m}}h_{JD}x_J[n] + n_D[n], \tag{4}$$

$$y_E[n] = \sqrt{\frac{1}{d_{RE}^m}}h_{RE}x_R[n] + \sqrt{\frac{p_J}{d_{JE}^m}}h_{JE}x_J[n] + n_E[n], \tag{5}$$

where $n_D[n] \sim \mathcal{CN}(0, \sigma_D^2)$ and $n_E[n] \sim \mathcal{CN}(0, \sigma_E^2)$ are the noise at the D and E respectively.

Accordingly, the received SNIR at the D, γ_D, is given by

$$\gamma_D = \min\left(\frac{c_1|h_{SR}|^2}{c_2|h_{SR}|^2|h_{RR}|^2+c_3|h_{SJ}|^2|h_{JR}|^2+1}, \frac{c_4|h_{SR}|^2|h_{RD}|^2}{c_5|h_{SJ}|^2|h_{JD}|^2+1}\right), \tag{6}$$

where $c_1 = \frac{\rho_1}{d_{SR}^m}$, $c_2 = \frac{\kappa\rho_1}{d_{SR}^m}$ $c_3 = \frac{\kappa\rho_1}{d_{SJ}^m d_{JR}^m}$, $c_4 = \frac{\kappa\rho_2}{d_{SR}^m d_{RD}^m}$ and $c_5 = \frac{\kappa\rho_2}{d_{SJ}^m d_{JD}^m}$, $\rho_1 = \frac{p_S}{\sigma_R^2}$ and $\rho_2 = \frac{p_S}{\sigma_D^2}$. The overheard SNIR for the eavesdropper can be expressed by

$$\gamma_E = \frac{b_1|h_{SR}|^2|h_{RE}|^2}{b_2|h_{SJ}|^2|h_{JE}|^2+1}, \tag{7}$$

where $b_1 = \frac{\kappa\rho_3}{d_{SR}^m d_{RE}^m}$, $b_2 = \frac{\kappa\rho_3}{d_{SJ}^m d_{JE}^m}$ and $\rho_3 = \frac{p_S}{\sigma_E^2}$.

III. Performance Analysis

In this work, we consider active eavesdropping scenario wherein the CSI of the eavesdropping channel is available at the source and relay nodes. A fundamental secrecy performance criterion for such a scenario is instantaneous secrecy rate defined as [15]

$$R_0 = \lfloor R_t - R_e \rfloor^+, \tag{8}$$

where $\lfloor x \rfloor^+ = \max(x, 0)$, R_t and R_e are the instantaneous rates for data transmission and eavesdropping respectively. Therefore, the source can transmit confidential messages to the destination at a rate R_0 to guarantee perfect secrecy. Another relevant criterion could be average secrecy rate.

With definition (8), the R_0 of the proposed protocol can be written as

$$R_0 = (1-\alpha)\lfloor \log(1+\gamma_D) - \log(1+\gamma_E) \rfloor^+. \tag{9}$$

Now, we derive the average secrecy rate, the average of R_0 over γ_D and γ_E, which is given by

$$\bar{R}_0 = \int_0^\infty \int_0^\infty R_0 f_{\gamma_D}(x_1) f_{\gamma_E}(x_2) dx_1 dx_2. \tag{10}$$

The average secrecy rate in (10) can be reexpressed as [19]

$$\bar{R}_0 = \frac{1-\alpha}{\ln 2}\int_0^\infty \frac{F_{\gamma_E}(x_2)}{1+x_2}(1 - F_{\gamma_D}(x_2))dx_2. \tag{11}$$

To calculate the average secrecy rate, $\bar{R}_0$, based on (11), we proceed to derive the cdf of the SNIR at the destination, $F_{\gamma_D}(\cdot)$, and cdf of the SNIR at eavesdropper, $F_{\gamma_E}(\cdot)$. Let us denote $X_0 = |h_{SR}|^2$, $X_1 = |h_{RR}|^2$, $X_2 = |h_{JR}|^2$, $Y_0 = |h_{SJ}|^2$, $Y_1 = |h_{RD}|^2$, and $Y_2 = |h_{JD}|^2$. Accordingly, the cdf of γ_D in (6) can be expressed as

$$\begin{aligned} F_{\gamma_D}(z) &= \\ &\Pr\left(\min\left(\underbrace{\frac{c_1X_0}{c_2X_0X_1 + c_3Y_0X_2 + 1}}_{\gamma_1}, \underbrace{\frac{c_4X_0Y_1}{c_5Y_0Y_2+1}}_{\gamma_2}\right) < z\right) \\ &= 1 - \Pr(\min(\gamma_1, \gamma_2) > z) \\ &= 1 - \Pr(\gamma_1 > z, \gamma_2 > z). \end{aligned} \tag{12}$$

From (12), there exists two common RVs X_0 and Y_0 which leads to a statistical dependence related to the terms γ_1 and γ_2. Herein, we first apply the conditional statistics by fixing X_0 and Y_0. We then average over these RVs. With this aim, the cdf of γ_D can be expressed as

$$\begin{aligned} F_{\gamma_D}(z) = 1 - \int_0^\infty \int_0^\infty &\left(1 - F_{\gamma_1|X_0,Y_0}(z)\right) \times \\ &\left(1 - F_{\gamma_2|X_0,Y_0}(z)\right) f_{X_0}(x) f_{Y_0}(y) dx dy. \end{aligned} \tag{13}$$

In addition, it is easy to show that

$$F_{\gamma_1|X_0,Y_0}(z) = e^{\frac{z-c_1X_0}{zc_3Y_0}} + \frac{e^{\frac{-c_1}{c_2z}+\frac{1}{c_2X_0}} - e^{\frac{-1}{c_3Y_0}\left(\frac{c_1X_0}{z}-1\right)}}{1 - \frac{c_3Y_0}{c_2X_0}}, \tag{14}$$

and

$$F_{\gamma_2|X_0,Y_0}(z) = 1 - \frac{e^{\frac{-z}{c_4X_0}}}{1 + \frac{c_5Y_0}{c_4X_0}z}. \tag{15}$$

Substituting (14) and (15) into (13) and using the pdfs $f_{X_0}(x_0) = e^{-x_0}u(x_0)$ and $f_{Y_0}(y_0) = e^{-y_0}u(y_0)$, the cdf of γ_D can be written as

$$\begin{aligned} F_{\gamma_D}(z) = 1 - \int_0^\infty \int_0^\infty &\frac{e^{\frac{-z}{c_4x}}}{1 + \frac{c_5y}{c_4x}z}\left[1 - e^{\frac{z-c_1x}{zc_3y}} - \right. \\ &\left. \frac{e^{\frac{-c_1}{c_2z}+\frac{1}{c_2x}} - e^{\frac{-1}{c_3y}\left(\frac{c_1x}{z}-1\right)}}{1 - \frac{c_3y}{c_2x}}\right] e^{-(x+y)} dx dy. \end{aligned} \tag{16}$$

We now derive the cdf of the SNIR at eavesdropper, $F_{\gamma_E}(\cdot)$. Let us denote $V = |h_{SR}|^2|h_{RE}|^2$ and $W = |h_{SJ}|^2|h_{JE}|^2$. Hence, γ_E in (7) can be written as

$$\gamma_E = \frac{b_1V}{b_2W+1}. \tag{17}$$

Accordingly, the cdf of γ_E can be expressed as

$$\begin{aligned} F_{\gamma_E}(z) &= \int_0^\infty \Pr\left(b_1V < z(b_2W+1)\right) \\ &= \int_0^\infty F_V\left(z\frac{b_2w+1}{b_1}\right) f_W(w) dw. \end{aligned} \tag{18}$$

$$F_{\tilde{\gamma}_D}(z) = 1 - \frac{c_3 c_4}{c_8(zc_5 - c_4)}\left(\frac{c_1}{c_3 z} e^{\frac{c_1}{c_3 z}} \mathsf{Ei}\left(\frac{-c_1}{c_3 z}\right) + 1\right) - c_3 c_4 \left(\frac{c_3 c_5 z + c_2 c_4}{c_8^2 (zc_5 - c_4)^2} e^{\frac{c_1}{c_3 z}} \mathsf{Ei}\left(\frac{-c_1}{c_3 z}\right) + \frac{c_9 e^{\frac{-c_6}{z}} \mathsf{Ei}(\frac{c_6}{z})}{zc_5 + \frac{c_3 c_4}{c_2}}\right)$$
$$+ \frac{z c_3 c_{10} e^{c_7} \mathsf{Ei}(-c_7)}{(1 - c_{10} z)^2 (c_2 c_{10} z + c_3)} - c_4 \left[\ln\left(\frac{(zc_5)^{\frac{\Psi_1(z)}{zc_5}}}{c_3^{\frac{\Psi_2(z)}{c_3}}}\right) - \ln\left(\frac{c_4^{\frac{\Psi_1(z)}{zc_5}}}{c_2^{\frac{\Psi_2(z)}{c_3}}}\right) + \frac{(c_8 - c_2 e^{\frac{-c_1}{c_2 z}})}{(c_4 - zc_5)c_8}\right], \quad (24)$$

In order to evaluate (18), we require the cdf of V and the pdf of W, which can be readily evaluated as [20]

$$F_V(v) = 1 - 2\sqrt{v} K_1(2\sqrt{v}), \quad (19)$$

and

$$f_W(w) = 2K_0(2\sqrt{w}), \quad (20)$$

respectively. Invoking $F_V(v)$ and $f_W(w)$, the cdf of γ_E can be expressed as

$$F_{\gamma_E}(z) = 1 - 4\int_0^\infty \sqrt{\frac{z}{b_1}(1 + b_2 w)}$$
$$K_1\left(2\sqrt{\frac{z}{b_1}(1 + b_2 w)}\right) K_0(2\sqrt{w}) dw. \quad (21)$$

Substituting (16) and (21) into (11), the average secrecy rate of the proposed protocol can be derived.

To the best of the author's knowledge, however, the dual integral in (16) and the integral in (21) do not admit the closed-form solutions for the cdfs of γ_D and γ_E, respectively. However, they can be efficiently evaluated numerically using Matlab. In the physical layer secrecy systems, on the other hand, to focus on the secrecy performance, it is common to adopt interference limited assumption wherein the noise at a receiving node is ignored. Accordingly, in the following, we consider the interference limited scenario which is of practical interest [4][1] and enables us to derive asymptotic closed-form expressions for the cdf of the SNIR at the destination, $F_{\tilde{\gamma}_D}(\cdot)$, and eavesdropper, $F_{\tilde{\gamma}_E}(\cdot)$. These expressions provide useful theoretical performance bounds for the average secrecy rate in the studied system. We will validate the interference limited assumption in Section IV.

A. Asymptotic Analysis

By applying the interference limited assumption on (6) and (7), the received SNIR at D and the overheard SNIR at the eavesdropper can be respectively written as

$$\tilde{\gamma}_D = \min\left(\frac{c_1 |h_{SR}|^2}{c_2 |h_{SR}|^2 |h_{RR}|^2 + c_3 |h_{SJ}|^2 |h_{JR}|^2}, \frac{c_4 |h_{SR}|^2 |h_{RD}|^2}{c_5 |h_{SJ}|^2 |h_{JD}|^2}\right), \quad (22)$$

and

$$\tilde{\gamma}_E = \frac{b_1 |h_{SR}|^2 |h_{RE}|^2}{b_2 |h_{SJ}|^2 |h_{JE}|^2}. \quad (23)$$

Now we characterize the asymptotic expressions for the cdf of the SNIR at the destination and eavesdropper.

[1]This assumption is also used in some of the main literatures on performance analysis of wireless cooperative transmissions [6], [12], [14] and does not affect the main conclusions drawn from the paper.

Theorem 1: The expression for asymptotic $F_{\tilde{\gamma}_D}(\cdot)$ is derived as (24) at the top of the page where $c_6 = \frac{-c_1}{c_2}$, $c_7 = \frac{c_1 c_5}{c_3 c_4}$, $c_8 = c_2 + c_3$, $c_9 = \frac{\frac{c_3}{c_2^2}}{(1 + \frac{c_3}{c_2})^2}$, $c_{10} = \frac{c_5}{c_4}$, and

$$\Psi_1(z) = \frac{c_2(1 - e^{\frac{-c_1}{c_2 z}}) + \frac{c_3}{c_{10} z}}{(c_2 + \frac{c_3}{c_{10} z})(1 - \frac{1}{c_{10} z})^2},$$

$$\Psi_2(z) = \frac{c_3(zc_5 - c_4)c_8 - (2zc_5 c_3 + zc_5 c_2 - c_3 c_4)(c_8 - c_2 e^{\frac{-c_1}{c_2 z}})}{(c_4 - zc_5)^2 c_8^2}.$$

Proof. Let us denote $X = c_1 / (c_2 X_1 + c_3 X_2 X_3)$ where $X_1 = |h_{RR}|^2$, $X_2 = |h_{JR}|^2$ and $X_3 = \frac{|h_{SJ}|^2}{|h_{SR}|^2}$, and $Y = \frac{c_4 Y_1}{c_5 Y_2 X_3}$, with $Y_1 = |h_{RD}|^2$ and $Y_2 = |h_{JD}|^2$. Accordingly, the cdf of $\tilde{\gamma}_D$ in (22) becomes

$$F_{\tilde{\gamma}_D}(z) = \Pr(\min(X, Y) < z),$$
$$= 1 - \Pr(X > z, Y > z). \quad (25)$$

Conditioned on X_3, the RVs X and Y are independent and hence we have

$$\Pr(X > z, Y > z) \quad (26)$$
$$= \int_0^\infty \left(1 - F_{X|X_3}(z)\right)\left(1 - F_{Y|X_3}(z)\right) f_{X_3}(x) dx.$$

We now look at the first item in the integral, which can be expressed as

$$1 - F_{X|X_3}(z) = 1 - \Pr\left(\frac{c_1}{c_2 X_1 + c_3 X_2 X_3} < z\right)$$
$$= \int_0^{\frac{c_1}{c_3 X_3 z}} F_{X_1}\left(\frac{c_1 - c_3 x X_3 z}{c_2 z}\right) f_{X_2}(x) dx. \quad (27)$$

Recall that X_1 and X_2 are exponential random variables with mean 1, thus (27) can be derived as

$$1 - F_{X|X_3}(z) = \frac{c_2 - c_2 e^{\frac{-c_1}{c_2 z}} + (e^{\frac{-c_1}{c_3 X_3 z}} - 1) c_3 X_3}{c_2 - c_3 X_3}. \quad (28)$$

The second item in the integral (26) can be written similarly as

$$1 - F_{Y|X_3}(z) = 1 - \Pr\left(Y_1 < \frac{z c_5 X_3}{c_4} Y_2\right) = \frac{c_4}{z c_5 X_3 + c_4}. \quad (29)$$

The pdf of RV X_3 can be readily evaluated as

$$f_{X_3}(x) = \frac{1}{(x+1)^2}. \quad (30)$$

Then, substituting (28), (29) and (30) into (25), we have

$$F_{\tilde{\gamma}_D}(z) = 1 - c_4 \int_0^\infty \frac{c_2 - c_2 e^{\frac{-c_1}{c_2 z}} + (e^{\frac{-c_1}{c_3 x z}} - 1) c_3 x}{(c_2 - c_3 x)(z c_5 x + c_4)(x+1)^2} dx \quad (31)$$

Now, after some simple algebraic manipulations and using the integral identities [21, Eq. (2.3.4)], [16, Eq. (3.353.3) and Eq. (3.352.4)], we yield the desired result in (24). ■

Theorem 2: The asymptotic cdf of $\tilde{\gamma}_E$ can be expressed by

$$F_{\tilde{\gamma}_E}(z) = 1 - G_{2,2}^{2,2}\left(\frac{b_2 z}{b_1}\middle|\begin{matrix}0,0\\1,0\end{matrix}\right). \tag{32}$$

Proof. The proof has been omitted due to space limitation. ■ Substituting (24) and (32) into (11), the asymptotic average secrecy rate can be readily evaluated.

IV. NUMERICAL RESULTS

These are presented to validate our analytical expressions, demonstrate the performance of the proposed secure transmission protocol, denoted by FDJ, and investigate the impact of key system parameters on its performance. We set the path loss exponent and energy conversion efficiency as $m = 3$ and $\eta = 0.5$.

Also, for comparison purposes, performance of secure HD-relaying protocol, denoted by HDJ, is provided. Here is a brief description of the HDJ protocol, which will be compared against FDJ. The system model is the same as that of the FDJ protocol, except for the HD relay. Specifically, during the first phase of duration αT, the source transfers power to the relay and jammer and the remaining block time, $(1-\alpha)T$ is used for secure information transmission, such that half of that, $(1-\alpha)T/2$, is used for the source to relay information transmission and the remaining half, $(1-\alpha)T/2$, is used for the relay to destination information transmission. At the same time, the jammer transmits intentional interference to degrade the relay-eavesdropper link. The harvested energy at the relay and jammer can be written as $p_R = \frac{\kappa'}{d_{SR}^m} p_S |h_{SR}|^2$ and $p_J = \frac{\kappa'}{d_{SJ}^m} p_S |h_{SJ}|^2$, respectively, where $\kappa' \triangleq \frac{2\eta\alpha}{(1-\alpha)}$. Thus, by replacing κ with κ' in (6) and (7) and omitting the terms containing the SI and the jammer interference in the first-hop SNIR expression at destination in (6), the SNIR at the destination and eavesdropper of the HDJ protocol can be obtained. Here, we study the secrecy rate performance of HDJ protocol through numerical analysis. The corresponding analytical analysis is omitted due to space limitation.

Fig. 1 shows the influence of the time-split parameter α on the instantaneous secrecy rate for a single time frame and channel realizations. We assume that S, R, J, E and D are located at $(0,0)$, $(20,10)$, $(20,-10)$, $(40,0)$ and $(50,0)$, respectively. There are two groups of curves: setting-1 (solid line) and setting-2 (dashed line) curves. Setting-1 and setting-2 refer to the following settings: 1) $h_{SR} = -0.12 - 0.88i$, $h_{SJ} = -0.30 + 1.21i$, $h_{RE} = 0.11 - 0.012i$, $h_{RD} = 0.90 + 0.003i$, $h_{RR} = -0.09 + 0.21i$, $h_{JR} = -1.08 - 0.27i$, $h_{JE} = 1.20 - 0.94i$ and $h_{JD} = 0.51 + 0.34i$. 2) $h_{SR} = 0.50 - 0.79i$, $h_{SJ} = 0.43 - 0.67i$, $h_{RE} = -0.45 + 0.068i$, $h_{RD} = -0.80 - 0.75i$, $h_{RR} = 0.013 - 0.36i$, $h_{JR} = -0.30 + 0.67i$, $h_{JE} = 0.67 - 0.09i$ and $h_{JD} = -0.16 + 0.087i$, respectively. The following conclusions are drawn from Fig. 1.

1) There is an interesting trade-off between α and the instantaneous secrecy rate for FDJ and HDJ transmission protocols. More specifically, first, as α increases, the secrecy rate increases but later, it starts decreasing as α increases from the optimal value. The intuitive reason is that, generally speaking, a longer energy harvesting time α increases the harvested energy at the relay and jammer nodes and consequently improves the secrecy rate. However, it decreases the available time for information transmission phase and vice-versa. Therefore, it is important to determine the optimum value of α to further optimize the secrecy rate performance.
2) It is clear that for setting-1, FDJ achieves a higher instantaneous secrecy rate than HDJ over the entire range of the α. However, for setting-2, we see that FDJ outperforms HDJ when $\alpha < 0.67$, and exhibits an inferior performance when $\alpha > 0.67$. This is mainly due to the effect of two extra interferences at the relay, SI interference caused by the signal leakage from the transceiver output to the input and co-channel interference due to the simultaneous relay and jammer transmissions (please see (6)) which are not present in the HDJ protocol and can reduce the instantaneous secrecy rate of the system. In addition, simulation results, not shown in the paper due to space constraints, reveal that the duration of time devoted for energy harvesting[2], the strength of the SI and the corresponding nodes channels and their relative positions in the network are the key factors determining to what extent the instantaneous secrecy rate superiority of the FDJ protocol holds.

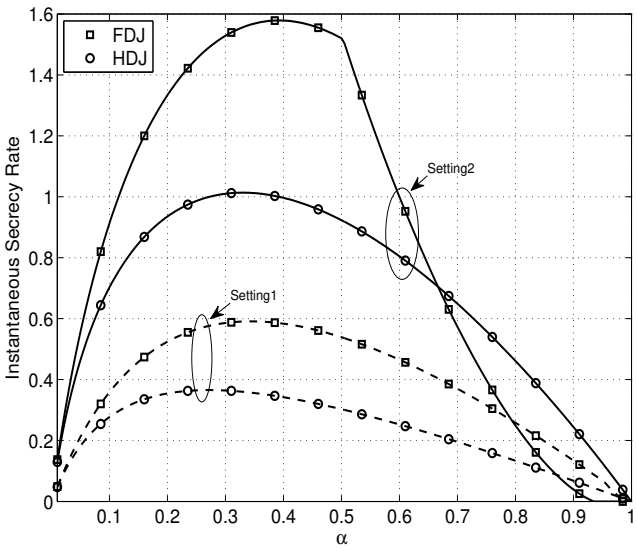

Fig. 1. Instantaneous secrecy rate of FDJ and HDJ transmission schemes as a function of α.

Fig. 2 illustrates the average secrecy rate of FDJ and HDJ transmission protocols versus source power in the wireless cooperative network with and without jammer. S, R, J, E and D are located at $(0,0)$, $(20,0)$, $(20,-10)$, $(40,0)$ and $(50,0)$, respectively. Two main observations that follow from

[2]when α is large, excessive amount of energy is collected, which is actually detrimental since it causes strong SI, which degrades the secrecy performance of FDJ.

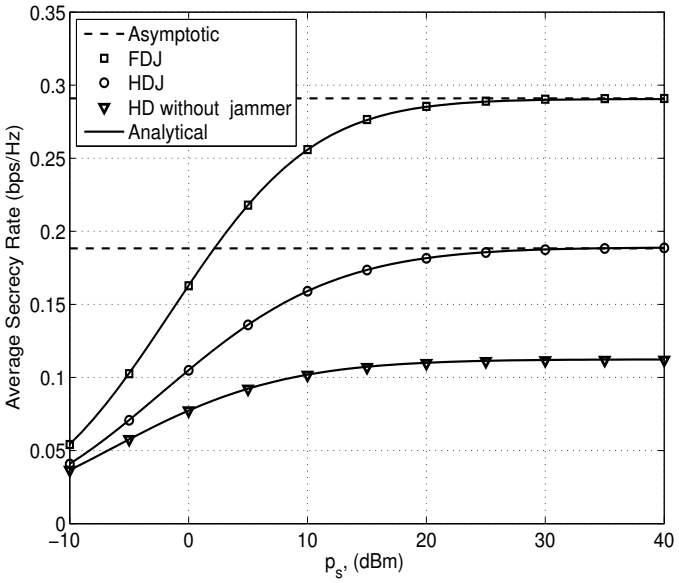

Fig. 2. Average secrecy rate of FDJ and HDJ transmission protocols versus transmission source power p_S.

this simulation are as follows. First, the average secrecy rate of the wireless powered cooperative network in the presence of eavesdropper can be significantly improved using the jammer node, *e.g.*, HDJ provides up to 70% enhancement in the average secrecy rate as compared with the conventional HD-relaying without jammer scheme. Second, as expected, the secure proposed FDJ protocol, outperforms all other schemas on all source power values. When the source node power values are high, it can increase the average secrecy rate efficiency up to 1.5 times over the HDJ protocol and up to 2.5 times over the HD-relaying without jammer scenario. Fig. 2 also shows that the analytical results derived in the paper are in exact agreement with the simulation results and the asymptotic curves tightly converge to the exact ones at the high SNR regime. These observations validate the derived analytical results and the motivation of the interference-limited assumption.

V. Conclusion

In this paper we have investigated the performance of a secure wireless-powered system utilizes FD-relaying along with cooperative jamming. We proposed a secure protocol takes places in two phases: energy harvesting phase and information transmission phase where the information signal is transmitted under the protection of a jamming signal sent by the jammer. We provided a mathematical framework for the instantaneous and average secrecy rate for the active eavesdropper scenario. We also presented asymptotic closed-form expression for the cdfs of the SNIR at the destination and eavesdropper nodes for the proposed protocol and accordingly the asymptotic average secrecy rates were calculated. We showed that by using wireless powered FD-relay and friendly jammer, the average secrecy rate can enhance up to 2.5 times than the HD-relaying transmission protocol without using jammer.

References

[1] A. Mukherjee, S. A. A. 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, Feb. 2014.

[2] 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.

[3] M. Duarte, "Full-duplex wireless: Design, implementation and characterization," Ph.D. dissertation, Dept. Elect. and Computer Eng., Rice University, Houston, TX, 2012.

[4] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless communications and networks," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1633–1636, Sept. 2014.

[5] M. Mohammadi, B. K. Chalise, H. A. Suraweera, C. Zhong, G. Zheng, and I. Krikidis, "Throughput analysis and optimization of wireless-powered multiple antenna full-duplex relay systems," *IEEE Trans. Commun.*, vol. 64, no. 4, pp. 1769–1785, Apr. 2016.

[6] S. Parsaeefard and T. Le-Ngoc, "Improving wireless secrecy rate via full-duplex relay-assisted protocols," *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 2095–2107, Oct. 2015.

[7] L. Tang, X. Gong, J. Wu, and J. Zhang, "Secure wireless communications via cooperative relaying and jamming," in *Proc. IEEE GLOBECOM Workshops (GC Wkshps)*, Houston, TX, Dec. 2011, pp. 849–853.

[8] 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, Mar. 2011.

[9] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359–368, Feb. 2012.

[10] ——, "Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting," *IEEE Trans. Wireless Commun.*, vol. 10, no. 6, pp. 1725–1729, June 2011.

[11] H. Deng, H. M. Wang, W. Guo, and W. Wang, "Secrecy transmission with a helper: To relay or to jam," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 293–307, Feb. 2015.

[12] W. Liu, X. Zhou, and a. P. P. S. Durrani, "Secure communication with a wireless-powered friendly jammer," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 401–415, Jan. 2016.

[13] G. Wang, F. Gao, R. Fan, and C. Tellambura, "Ambient backscatter communication systems: detection and performance analysis," *IEEE Trans. Commun.*, vol. 64, no. 11, pp. 4836–4846, 2016.

[14] 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.

[15] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054–6067, Nov. 2014.

[16] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th ed. Academic Press, 2007.

[17] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables.*, 9th ed. New York: Dover, 1970.

[18] T. Riihonen, S. Werner, and R. Wichman, "Mitigation of loopback self-interference in full-duplex MIMO relays," *IEEE Trans. Signal Process.*, vol. 59, no. 12, pp. 5983–5993, Dec. 2011.

[19] K. P. Peppas, N. C. Sagias, and A. Maras, "Physical layer security for multiple-antenna systems: A unified approach," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 314–328, Jan. 2016.

[20] C. Zhong, H. A. Suraweera, G. Zheng, I. Krikidis, and Z. Zhang, "Wireless information and power transfer with full duplex relaying," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3447–3461, Oct. 2014.

[21] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integral and Series, vol. 1: Elementary Functions*. Gordon and Breach, New York-London, 1992.