# Wireless-Powered Full-Duplex Relay and Friendly Jamming for Secure Cooperative Communications

Zahra Mobini, *Member, IEEE*, Mohammadali Mohammadi, *Member, IEEE,* and Chintha Tellambura, *Fellow, IEEE*

***Abstract*—Wireless energy harvesting, physical-layer security and full-duplex wireless are important, emerging fifth generation (5G) technologies. In this paper, we thus investigate a source-destination link with an energy-harvesting full-duplex relay and a jammer (to degrade the eavesdropper channel) in the presence of an eavesdropper. Thus, to exploit energy harvesting and to improve security, we propose a full-duplex jammer (FDJ) protocol and its half-duplex version (HDJ). Two cases for availability of the eavesdropper channel state information (ECSI) are considered: complete ECSI and incomplete ECSI. For both FDJ and HDJ protocols and for complete ECSI, we derive the instantaneous and average secrecy rates and compute optimal time-split for energy harvesting. To gain more insights, we consider a practical interference-limited scenario and derive closed-form cumulative distribution function (cdf) of the SINR (signal-to-interference plus noise ratio) at the destination and eavesdropper nodes. Comparatively, we show that FDJ improves instantaneous secrecy rate over HDJ. However, the degree of improvement is highly dependent on time-split for energy harvesting, amount of self-interference (SI), the channel gains and locations of the nodes. For incomplete ECSI scenario, we derive asymptotic secrecy outage and show that FDJ performs better for small-to-medium values of source powers; otherwise, HDJ yields a higher gain. Moreover, we derive asymptotic secrecy outage. We show that FDJ increases the average secrecy rate 150% over HDJ and 260% over half-duplex relaying without jammer. In terms of secrecy outage probability, FDJ performs better for the small to medium values of source powers, while HDJ achieves a higher gain at high source power values.**

## I. Introduction

Due to the explosive growth of wireless subscribers and networks, heightened concerns about climate change, and related reasons, energy and security are critical factors in the design of fifth generation (5G) wireless mobile networks. Security is especially challenging because wireless broadcast signals can be heard by both intended users and malicious eavesdroppers. To enhance security, one can exploit the properties of the wireless physical layer, especially interference rather than cryptographic techniques [1], [2]. These physical layer security techniques can significantly boost the secrecy rate of a wireless network [1], [3]. The secrecy rate is the difference between the instantaneous rate of the legitimate channel and that of the wiretap channel, i.e., the channel between the transmitter and the eavesdropper [4]. If the secrecy rate falls below zero, the eavesdropper can intercept confidential information [2], [5].

Cooperative communication techniques attack this problem either by strengthening the legitimate channel (cooperative relaying) and/or by degrading the wiretap channel rate (cooperative jamming) [2], [6]–[12]. In [2], [7], the security of a single source-destination pair is strengthened with the help of multiple relays in the presence of one or more eavesdroppers. Decode-and-forward (DF) and amplify-and-forward (AF) relaying and cooperative jamming, i.e., sending a jamming signal to interfere with the reception of eavesdropper, can significantly improve the secrecy performance. This approach results in secrecy outage reaching zero [8], [9]. Moreover, ergodic secrecy rate of cooperative jamming and relaying, in the low and high signal-to-noise ratio (SNR) regimes and for different eavesdropper positions is analyzed [10]. In contrast, [11], [12] investigates the physical layer security issues for a two-way relay system for an un-trusted relay scenario. Most existing works consider half-duplex (HD) relays only.

However, an HD relay requires two time-slots per data transfer [10], which halves the secrecy rate compared to direct transmission. Thus, this spectral loss may be recovered by full-duplex (FD) relaying, where the relay node receives and transmits simultaneously in the same frequency band [13]–[17]. However, the problem is that the receiver section of an FD node is interfered by its own transmit signals, i.e., self-interference (SI) [18]. While SI can be as high as 100 dB, many effective SI cancellation techniques have been developed [15], [18], [19] to enhance the practical viability of FD systems. Thus, the progress of SI cancellation and further hardware improvements help us to exploit FD relays along with cooperative jamming [20], [21]. For example, Parsaeefard *et al*. [20] investigates a friendly FD relay and power allocation to maximize the secrecy rate. Reference [21] examines the potential security enhancement in the presence of an eavesdropper by a cooperative multi-antenna FD relay and cooperative jamming with and without the eavesdropper's channel state information (CSI).

However, nodes in typical sensor and ad-hoc wireless networks are likely battery powered and are off the power grid due to mobility or other constraints. For example, in remote health control with the human-embedded sensors, monitoring and the disaster relief applications, nodes are not easily accessible, and charging or replacing their batteries is difficult, expensive or even risky. The limited operational lifetime of such networks may be further degraded by the energy overhead for secure communications [22]. For example, to intensify the user desired rate and/or to impose the controlled interference on the eavesdropper, the cooperative

Manuscript received Feb. 14, 2018; revised May 06, 2018; accepted Jul 17, 2018. The associate editor coordinating the review of this paper and approving it for publication was Dr. L. Lifeng. This work was presented in part at the IEEE ICC 2017 Workshops (Workshop on Full-Duplex Communications for Future Wireless Networks), Paris, France, May 2017.

Z. Mobini and M. Mohammadi are with the Faculty of Engineering, Shahrekord University, Shahrekord 115, Iran (Email: z.mobini@eng.sku.ac.ir, m.a.mohammadi@eng.sku.ac.ir).

C. Tellambura is with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB T6G 2V4 Canada (email: chintha@ece.ualberta.ca).

relay and/or the jammer must spend more energy. As such, the nodes scavenging energy from external resources such as solar, wind and especially ambient RF (radio frequency) power may help prolong the network life-time [23]–[26]. But such sources are unpredictable and uncontrollable, which renders them unsuitable for some wireless applications. Thus, energy harvesting from ambient RF signals has recently emerged as a new paradigm for certain wireless networks [27].

Motivated by these crucial factors, we develop a novel secure joint FD cooperative relaying and jamming scheme, called FDJ, that achieves impressive security performance against an eavesdropper while harvesting energy. This FDJ protocol has wide applications in general wireless ad-hoc and sensor networks, for example among several, a secure remote monitoring system where a monitor reports confidential information to the monitoring center with the aid of the wireless-powered FD relay and jammer nodes at no extra power consumption. We employ the time-splitting (TS) architecture for energy harvesting [23], [28] and investigate three different performance metrics depending on the availability of eavesdropper CSI (ECSI). With complete ECSI [29], we derive two fundamental secrecy performance criteria; namely, instantaneous and average secrecy rates. For incomplete ECSI [29], we study the secrecy outage which is the probability that the secrecy rate falls bellow a predetermined threshold necessary to support the desired secrecy rate [5], [29], [30].

Our results complement and strengthen this emerging area, but differ from recent works [20], [21], [25], [26], [31]. Specially, [20], [21], [31] considered only cooperative relaying or cooperative jamming without energy harvesting. However, our model is different because it incorporates joint cooperative FD relaying and cooperative jamming. More importantly, we also take into account energy harvesting for relay and jammer nodes to improve the security without consuming extra energy. This completely changes the problem formulation. The relay and jammer transmit powers are not fixed. In fact they are random variables which depend on the source-relay and source-jammer channels, time splitting factor and the energy conversion efficiency of the deployed energy harvester at the nodes. Moreover, to be realistic with FDJ, we consider both inter-user interference at the relay and destination nodes and SI at the FD relay. The above differences in system model and assumptions result in different signal-to-interference-plus-noise ratio (SINR) variables and related analysis approach is completely different from existing ones.

Joint relay selection and cooperative jamming is considered in [32] for improving the physical-layer secrecy of a wireless system with multiple intermediate nodes. This study allocates power among the source, HD relay and friendly jammers to maximize the secrecy rate under the total power constraint. In contrast to our work, this work does not exploit FD transmission and energy harvesting solutions to improve the spectral and power efficiency. Also, in [25], Xing *et al*. considered an HD AF relay wiretap channel with a harvest-and-jam relaying protocol and maximized the secrecy rate at the destination subject to transmit-power constraints. In [26], a wireless-powered friendly jammer is devised to enhance security of direct transmissions and the rate parameters are optimized to achieve the best throughput subject to a secrecy outage probability constraint. Both [25] and [26] consider respectively HD AF relaying transmission and direct transmission, which are different from ours. The main contributions of this paper are as follows:

- We propose the FDJ protocol, a secure FD-relaying protocol using a jamming node, whose key feature is that both relay and jammer are powered by source transmissions. As a benchmark, we also investigate the HD version of the identical system, called HDJ. At the outset, we derive the output SINR at destination and eavesdropper nodes.
- For complete ECSI scenario, we derive analytical expressions for the instantaneous and average secrecy rates for both FDJ and HDJ protocols and numerically obtain the optimal time-split devoted for energy harvesting. To gain more design insights and develop mathematical analysis, we consider the practical interference-limited scenario and derive closed-form cumulative distribution function (cdf) of the SINR at the destination and eavesdropper nodes. Accordingly, the asymptotic average secrecy rates are also derived.
- We compare FDJ and HDJ and show that FDJ improves instantaneous secrecy rate. However, the degree of improvement is highly dependent on the time-split devoted for energy harvesting, amount of SI (originated by the signal leakage from the transmitter to the receiver), the channel gains and positions of the nodes. For incomplete ECSI scenario, we derive the asymptotic secrecy outage and show that from the viewpoint of outage, FDJ performs better for the small to medium values of source powers, while HDJ yields a higher gain at high source power values.

We remark that this manuscript is the substantial extension of our previous work [33]. Specifically, this work is different from [33] in three ways. First, [33] only investigates the average secrecy rate. However, this work derives analytical expressions for the instantaneous and average secrecy rates and numerically obtain the optimal time-split devoted for energy harvesting. Moreover, for incomplete ECSI scenario, we derive the asymptotic secrecy outage probability. Second, in [33] only FDJ is studied, while in this work we analytically investigate both FDJ and HDJ transmission protocols. Third, to provide insights into the choice of one protocol with a higher secrecy rate, we include a discussion on performance comparison of the proposed protocols.

*Notation:* The unit step function $u(t) = 1$ for $t > 0$ and zero otherwise. The operators $(\cdot)^\dagger$ and $\Pr(\cdot)$ denote conjugate transpose and probability. For random variable (RV) $X$, $f_X(\cdot)$ and $F_X(\cdot)$ denote the probability density function (pdf) and cdf. A circularly symmetric complex Gaussian RV with mean $\mu$ and variance $\sigma^2$ is $\mathcal{CN}(\mu, \sigma^2)$. The gamma function $\Gamma(a)$ is given in [34, Eq. (8.310.1)]; $K_\nu(\cdot)$ is the $\nu$-th order modified Bessel function of the second kind [34, Eq. (8.432)]; $\mathsf{Ei}(x)$ is the exponential integral function [35, Eq. (5.1.2)]; $E_n(x)$ is the $E_n$-function [35, Eq. (5.1.4)]; $G_{pq}^{mn}\left(z \mid \begin{smallmatrix} a_1 \cdots a_p \\ b_1 \cdots b_q \end{smallmatrix}\right)$ denotes the Meijer G-function [34, Eq. (9.301)] and $\mathcal{W}_{\lambda,w}$ is the Whittaker function defined in [34, Eq. (9.220)].

## II. System Model and Transmission Protocols

We consider source node $S$ is communicating with a destination node $D$ in the presence of an eavesdropper $E$ with the help of a trusted relay $R$ and a friendly jammer $J$[1]. The $S$, $R$ and $J$ nodes are assumed to be located in a same cluster that is far away from the destination and eavesdropper[2]. The long distances between the source and destination/eavesdropper imply that there is a higher probability that these links suffer strong blockage and shadowing, compared to those links between the source, relay and jammer nodes and hence there is no direct link from the source to the destination or to eavesdropper [25][3]. In addition, the trusted relay node and the jammer node are energy constrained nodes and have no external power supply. The source node charges them via wireless power transfer. Once sufficient energy has been harvested, the relay and jammer are ready to perform transmitting information and friendly jamming signals to enhance the security of communication. The $S, D, J$ and $E$ are assumed to be single-antenna nodes while $R$ is equipped with two antennas. We refer to the so-called RF chain preserved condition [37] for HDJ transmission protocol. It is worth pointing out that, FD operation was first enabled using either two separate antennas, or one shared antenna to transmit and receive simultaneously. Nevertheless, different implementation alternatives for various single and multiple antenna extensions have been proposed to date. Depending on the number of receive/transmit antennas implemented at the FD terminal, four different scenarios can be considered, namely, single-input single-output, single-input multiple-output, multiple-input single-output, and multiple-input multiple-output.

We assume that the relay applies DF protocol. In contrast, with AF relays, exact distribution for the received SNR/SINR and secrecy outage or average secrecy rate are generally intractable. Then, the tight upper bound on the SNR/SINR distributions can be derived by considering DF [38]. As appropriate, we define the channel coefficient $h_{\sharp,\#}$ and distance $d_{\sharp,\#}$ between node $\sharp \in \{S, R, D, J, E\}$ and $\# \in \{S, R, D, J, E\}$. 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 power gains are independent and identically distributed (i.i.d) Exponential RVs with unit mean. For both FDJ and HDJ, we adopt the TS strategy [23], [28] for energy harvesting, hence the cooperation round consists of two phases: energy harvesting and information transmission. Specifically, for a transmission block time $T$, $0 < \alpha < 1$ fraction is dedicated to energy harvesting and the remaining time, $(1-\alpha)T$, for information transmission [15]. Detailed description of the transmission protocols are provided as follows.

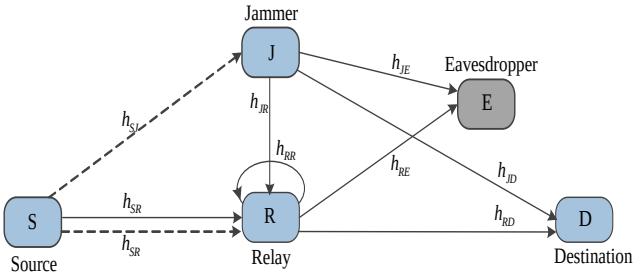


Fig. 1. An illustration of the FDJ transmission protocol. The dashed lines represent the links for the first phase (power transmission phase) with duration $\alpha T$, and the solid lines represent the links for the second phase (information transmission phase) with duration $(1-\alpha)T$.

### A. FDJ Transmission Protocol

We assume that source, destination, eavesdropper and jammer nodes are all HD, while the relay is FD (Fig. 1). To be realistic, we assume that imperfect SI cancellation at the relay. Accordingly, we model the SI channel $h_{RR}$ with Rayleigh flat fading, $h_{RR} \sim \mathcal{CN}(0, \sigma_{RR}^2)$, which is a well accepted model in the literature [15], [39]. In this model, the FD relay estimates the strong line-of-sight component of the SI channel and removes it. Therefore, the residual interference is mainly affected by the Rayleigh fading component of the SI channel and its strength is proportional to the level of suppression achieved by the adopted specific cancellation method [15].

The secure FDJ protocol employs two phases. For energy harvesting phase, relay and jammer nodes deploy the TS protocol and apply the harvest-use architecture [23], [24] where the energy harvested is stored in a supercapacitor and then fully consumed by the nodes in the information transmission phase. Particularly, during the first phase of duration $\alpha T$, the source transfers power to the relay and jammer by sending a radio signal with power $p_S$. The received signal at the relay and jammer can be respectively 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 $n = 1, 2, \ldots$ is the symbol index, $x_e[n]$ is the energy symbol with unit energy: $\mathtt{E}\{x_e[n]x_e^\dagger[n]\} = 1$, $m$ is the path loss exponent. The terms $n_R[n] \sim \mathcal{CN}(0, \sigma_R^2)$ and $n_J[n] \sim \mathcal{CN}(0, \sigma_J^2)$ denote the noise at $R$ and $J$, respectively. The relay and jammer receive the radio signal, convert it to a direct current signal and store the energy. 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 $\kappa \triangleq \frac{\eta\alpha}{(1-\alpha)}$ and $0 < \eta < 1$ is RF-to-DC energy conversion efficiency.

During the information transmission phase of time length $(1-\alpha)T$, the source transmits $x_S[n]$ to the FD relay $R$, while $R$ simultaneously receives $r[n]$ and forwards $x_R[n]$ to the destination using the harvested energy. At the same time,

[1]Although the single-relay and jammer schemes are much simpler to investigate, their performance analysis is still very challenging, and such networks have not been well studied in the literature, especially for wireless-powered nodes and joint FD relaying and jamming. Nevertheless, performance analysis of relay and jammer selection for secure wireless-powered cooperative communications is an interesting future direction worth more research.

[2]In many practical scenarios, the eavesdroppers are assumed to be distributed outside a disc centered on the transmitter, called security zone, to avoid getting exposed [36].

[3]The existence of the source-eavesdropper direct link actually can further improve eavesdropping performance [31]. Therefore, our analysis provide upper bound on the secrecy rate and lower bound on the outage probability of the network with direct source-eavesdropper link.

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

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

where $x_S[n]$ is the source information symbol with unit energy, $\mathtt{E}\left\{x_S[n]x_S^\dagger[n]\right\} = 1$, $x_R[n]$ is the transmitted relay signal satisfying $\mathtt{E}\left\{x_R[n]x_R^\dagger[n]\right\} = 1$ and $x_J[n]$ is the transmitted jamming signal satisfying $\mathtt{E}\left\{x_J[n]x_J^\dagger[n]\right\} = 1$. 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]

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

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

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

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

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 SINR at the $D$, $\gamma_D^{\mathsf{FD}}$, is given by

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

where

$$c_1 = \frac{\rho_1}{d_{SR}^m}, c_2 = \frac{\kappa\rho_1}{d_{SR}^m}, c_3 = \frac{\kappa\rho_1}{d_{SJ}^m d_{JR}^m}, c_4 = \frac{\kappa\rho_2}{d_{SR}^m d_{RD}^m}, c_5 = \frac{\kappa\rho_2}{d_{SJ}^m d_{JD}^m}, \rho_1 = \frac{p_S}{\sigma_R^2}, \rho_2 = \frac{p_S}{\sigma_D^2}. \quad (7)$$

The overheard SINR for the eavesdropper can be expressed by

$$\gamma_E^{\mathsf{FD}} = \frac{b_1|h_{SR}|^2|h_{RE}|^2}{b_2|h_{SJ}|^2|h_{JE}|^2 + 1}, \quad (8)$$

where

$$b_1 = \frac{\kappa\rho_3}{d_{SR}^m d_{RE}^m}, b_2 = \frac{\kappa\rho_3}{d_{SJ}^m d_{JE}^m}, \rho_3 = \frac{p_S}{\sigma_E^2}. \quad (9)$$

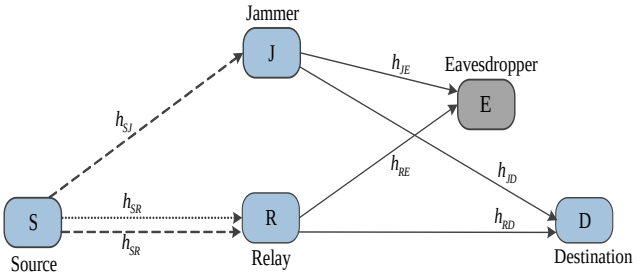


Fig. 2. An illustration of the HDJ transmission protocol. The dashed lines represent the links for the power transmission phase with duration $\alpha T$, the dotted line represents the source to relay information transmission with duration $(1-\alpha)T/2$ and the solid lines represent the relay information transmission and the jammer interference transmission with duration $(1-\alpha)T/2$.

### *B. HDJ Transmission Protocol*

Here, we derive the SINR for the HDJ secrecy relay system, against which FDJ will be compared. In the HDJ secrecy relay system, during the first phase of duration $\alpha T$, the source transfers power to the relay and jammer and the remaining time, $(1-\alpha)T$ is used for information transmission, such that half of that, $(1-\alpha)T/2$, is used for the source to relay information transmission. The remaining half, $(1-\alpha)T/2$, is used for the relay to destination information transmission while the jammer simultaneously transmits intentional interference to degrade the relay-eavesdropper link.

The received signals at the relay and jammer in the energy harvesting phase are given by (1a) and (1b) and hence the relay and jammer transmit power 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 $\kappa' \triangleq \frac{2\eta\alpha}{(1-\alpha)}$. During the information transmission phase the relay receives

$$r[n] = \sqrt{\frac{p_S}{d_{SR}^m}} h_{SR} x_S[n] + \sqrt{\frac{p_J}{d_{JR}^m}} h_{JR} x_J[n] + n_R[n]. \quad (10)$$

After the relay successfully decodes and regenerates the original signal, it forwards $x_R[n]$ to the destination while the jammer sends a jamming signal. Hence, the received signals at $D$ and $E$ are given by

$$y_D[n] = \sqrt{\frac{p_R}{d_{RD}^m}} h_{RD} x_R[n] + \sqrt{\frac{p_J}{d_{JR}^m}} h_{JD} x_J[n] + n_D[n], \quad (11)$$

and

$$y_E[n] = \sqrt{\frac{p_R}{d_{RE}^m}} h_{RE} x_R[n] + \sqrt{\frac{p_J}{d_{JE}^m}} h_{JE} x_J[n] + n_E[n]. \quad (12)$$

Accordingly, the SINR at the destination and eavesdropper are given respectively by

$$\gamma_D^{\mathsf{HD}} = \min\left(c_1|h_{SR}|^2, \frac{2c_4|h_{SR}|^2|h_{RD}|^2}{2c_5|h_{SJ}|^2|h_{JD}|^2 + 1}\right), \quad (13)$$

and

$$\gamma_E^{\mathsf{HD}} = \frac{2b_1|h_{SR}|^2|h_{RE}|^2}{2b_2|h_{SJ}|^2|h_{JE}|^2 + 1}. \quad (14)$$

We note that in the HDJ protocol, jamming signal is transmitted only in the second half of the information transmission phase to degrade the relay-eavesdropper link and it does not interfere with the first-hop transmission.

## III. Performance Analysis

In this work, we study two different scenarios for the availability of ECSI at the legitimate system. The first is the complete ECSI case, where the legitimate system knows the CSI of all the eavesdropping link. The second is the incomplete ECSI case where the CSI of the eavesdropping links is unknown. A fundamental secrecy performance criterion in the complete ECSI scenario is instantaneous secrecy rate defined as [5], [29]

$$R_0^{\mathsf{i}} = \lfloor R_t^{\mathsf{i}} - R_e^{\mathsf{i}} \rfloor^+, \tag{15}$$

where $\lfloor x \rfloor^+ = \max(x, 0)$, $\mathsf{i} \in \{\mathsf{FD}, \mathsf{HD}\}$, and $R_t^{\mathsf{i}}$ and $R_e^{\mathsf{i}}$ are the instantaneous rates for data transmission and eavesdropping respectively. Therefore, the source can transmit confidential messages to the destination at a rate $R_0^{\mathsf{i}}$ to guarantee perfect secrecy. Another relevant criterion is average secrecy rate. Note that complete ECSI scenario is of practical interest in many classes of applications where the users play dual roles as legitimate receivers for some signals and eavesdroppers for others [2], [5]. For example, the potential application scenarios include multicast, multi-unicast and unicast systems. However, with incomplete ECSI, the relay and source nodes do not know the ECSI and hence perfect secrecy rate cannot be guaranteed [5], [29]. The secrecy outage thus becomes an important performance metric, which is the probability that the secrecy rate falls bellow a predetermined threshold necessary to support the desired secrecy rate.

In this section, we first concentrate on the complete ECSI scenario and derive the FDJ and HDJ instantaneous secrecy and average secrecy rates. We provide the optimal energy harvesting time allocation strategies that maximize the instantaneous secrecy rate. Moreover, we derive the asymptotic average secrecy rate. We also consider the incomplete ECSI scenario and derive the secrecy outage probability performance for both FDJ and HDJ.

### A. Instantaneous Secrecy Rate

*1) FDJ Transmission Protocol*: With definition (15), the instantaneous secrecy rate of FDJ protocol can be given by

$$\begin{aligned} R_0^{\mathsf{FD}} &= \lfloor R_t^{\mathsf{FD}} - R_e^{\mathsf{FD}} \rfloor^+ \\ &= (1-\alpha)\lfloor \log(1+\gamma_D^{\mathsf{FD}}) - \log(1+\gamma_E^{\mathsf{FD}}) \rfloor^+. \end{aligned} \tag{16}$$

From (16), we observe the secrecy rate $R_0^{\mathsf{FD}}$ is a function of $\alpha$, the time fraction devoted for energy harvesting. Our objective is thus to determine the optimum value of $\alpha$ that maximizes the instantaneous secrecy rate of the FDJ protocol.

The optimal $\alpha_{\mathsf{FD}}^*$ can be obtained by solving the following optimization problem

$$\alpha_{\mathsf{FD}}^* = \underset{0<\alpha<1}{\arg\max}\, R_0^{\mathsf{FD}}(\alpha). \tag{17}$$

However, since both the expressions of $\gamma_D^{\mathsf{FD}}$ and $\gamma_E^{\mathsf{FD}}$ in $R_0^{\mathsf{FD}}$ consist of $\alpha$ and due to the complicated form of $R_0^{\mathsf{FD}}(\alpha)$, a closed-form solution for the optimum $\alpha_{\mathsf{FD}}^*$ appears intractable. As in [16], [28], we numerically evaluate $\alpha_{\mathsf{FD}}^*$ by using the Matlab or Mathematica.

*2) HDJ Transmission Protocol*: Similarly, for the HDJ protocol, the instantaneous secrecy rate can be computed as

$$\begin{aligned} R_0^{\mathsf{HD}} &= \lfloor R_t^{\mathsf{HD}} - R_e^{\mathsf{HD}} \rfloor^+ \\ &= \frac{(1-\alpha)}{2}\lfloor \log(1+\gamma_D^{\mathsf{HD}}) - \log(1+\gamma_E^{\mathsf{HD}}) \rfloor^+, \end{aligned} \tag{18}$$

and the optimal $\alpha_{\mathsf{HD}}^*$ could be obtained by solving the following optimization problem

$$\alpha_{\mathsf{HD}}^* = \underset{0<\alpha<1}{\arg\max}\, R_0^{\mathsf{HD}}(\alpha). \tag{19}$$

Although (19) does not admit a closed-form solution, numerical evaluation is easy and efficient.

### B. Average Secrecy Rate

Here, we derive the average secrecy rate which is a fundamentally important performance metric for characterizing the complete ECSI scenario. The average secrecy rate is the average of $R_0^{\mathsf{i}}$ over $\gamma_D^{\mathsf{i}}$ and $\gamma_E^{\mathsf{i}}$ and is given by

$$\begin{aligned} \bar{R}_0^{\mathsf{i}} &= \int_0^\infty \int_0^\infty R_0^{\mathsf{i}} f_{\gamma_D^{\mathsf{i}}}(x_1) f_{\gamma_E^{\mathsf{i}}}(x_2) dx_1 dx_2 \\ &= \int_0^\infty \left( \int_0^\infty \left[ \log\left(\frac{1+x_1}{1+x_2}\right) \right]^+ f_{\gamma_E^{\mathsf{i}}}(x_2) dx_2 \right) f_{\gamma_D^{\mathsf{i}}}(x_1) dx_1 \\ &\overset{(a)}{=} \int_0^\infty \left( \int_0^{x_1} \log\left(\frac{1+x_1}{1+x_2}\right) f_{\gamma_E^{\mathsf{i}}}(x_2) dx_2 \right) f_{\gamma_D^{\mathsf{i}}}(x_1) dx_1, \end{aligned} \tag{20}$$

where (a) follows from the definition of $R_o^{\mathsf{i}}$ and the condition $R_o^{\mathsf{i}} \geq 0$ or equivalently $\log\left(\frac{1+x_1}{1+x_2}\right) \geq 0$, which implies that $x_2 \leq x_1$. Using the similar steps as in [30], the average secrecy rate in (20) can be re-expressed as [30]

$$\bar{R}_0^{\mathsf{i}} = \frac{\ell^{\mathsf{i}}}{\ln 2} \int_0^\infty \frac{F_{\gamma_E^{\mathsf{i}}}(x_2)}{1+x_2} (1 - F_{\gamma_D^{\mathsf{i}}}(x_2)) dx_2, \tag{21}$$

where $\mathsf{i} \in \{\mathsf{FD}, \mathsf{HD}\}$, $\ell^{\mathsf{FD}} = (1-\alpha)$, and $\ell^{\mathsf{HD}} = \frac{(1-\alpha)}{2}$.

*1) FDJ Transmission Protocol*: To compute the average secrecy rate for FDJ, $\bar{R}_0^{\mathsf{FD}}$, based on (21), we proceed to derive the SINR cdf at the destination, $F_{\gamma_D^{\mathsf{FD}}}(\cdot)$, and cdf of the SINR at eavesdropper, $F_{\gamma_E^{\mathsf{FD}}}(\cdot)$. For notational convenience, we 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 $\gamma_D^{\mathsf{FD}}$ in (6) can be expressed as

$$\begin{aligned} &F_{\gamma_D^{\mathsf{FD}}}(z) = \\ &\Pr\left( \min\left( \underbrace{\frac{c_1 X_0}{c_2 X_0 X_1 + c_3 Y_0 X_2 + 1}}_{\gamma_1}, \underbrace{\frac{c_4 X_0 Y_1}{c_5 Y_0 Y_2 + 1}}_{\gamma_2} \right) < z \right), \\ &\quad = 1 - \Pr(\gamma_1 > z, \gamma_2 > z). \end{aligned} \tag{22}$$

In (22), the common RVs $X_0$ and $Y_0$ in $\gamma_1$ and $\gamma_2$ lead to statistical dependencies. Herein, we first fix $X_0$ and $Y_0$ and obtain the conditional cdf, which is then averaged over these RVs. Thus, the cdf of $\gamma_D^{\mathsf{FD}}$ can be expressed as

$$F_{\gamma_D^{\mathsf{FD}}}(z) = 1 - \int_0^\infty \int_0^\infty \big(1 - F_{\gamma_1|X_0,Y_0}(z)\big)\big(1 - F_{\gamma_2|X_0,Y_0}(z)\big) \times f_{X_0}(x) f_{Y_0}(y) dx dy. \quad (23)$$

In addition, we can readily show that

$$F_{\gamma_1|X_0,Y_0}(z) = e^{\frac{z - c_1 X_0}{z c_3 Y_0}} + \frac{e^{\frac{-c_1}{c_2 z} + \frac{1}{c_2 X_0}} - e^{\frac{-1}{c_3 Y_0}\left(\frac{c_1 X_0}{z} - 1\right)}}{1 - \frac{c_3 Y_0}{c_2 X_0}}, \quad (24)$$

and

$$F_{\gamma_2|X_0,Y_0}(z) = 1 - \frac{e^{\frac{-z}{c_4 X_0}}}{1 + \frac{c_5 Y_0}{c_4 X_0} z}. \quad (25)$$

Substituting (24) and (25) into (23) and using the pdfs $f_{X_0}(x) = e^{-x}u(x)$ and $f_{Y_0}(y) = e^{-y}u(y)$, the cdf of $\gamma_D^{\mathsf{FD}}$ can be obtained as

$$F_{\gamma_D^{\mathsf{FD}}}(z) = 1 - \int_0^\infty \int_0^\infty \frac{e^{\frac{-z}{c_4 x}}}{1 + \frac{c_5 y}{c_4 x} z} \left[1 - e^{\frac{z - c_1 x}{z c_3 y}} - \frac{e^{\frac{-c_1}{c_2 z} + \frac{1}{c_2 x}} - e^{\frac{-1}{c_3 y}\left(\frac{c_1 x}{z} - 1\right)}}{1 - \frac{c_3 y}{c_2 x}}\right] e^{-(x+y)} dx dy. \quad (26)$$

We now derive the cdf of the SINR at eavesdropper, $F_{\gamma_E^{\mathsf{FD}}}(\cdot)$. Let us denote $V = |h_{SR}|^2 |h_{RE}|^2$ and $W = |h_{SJ}|^2 |h_{JE}|^2$. Hence, $\gamma_E^{\mathsf{FD}}$ in (8) can be written as

$$\gamma_E^{\mathsf{FD}} = \frac{b_1 V}{b_2 W + 1}. \quad (27)$$

Accordingly, the cdf of $\gamma_E^{\mathsf{FD}}$ can be expressed as

$$F_{\gamma_E^{\mathsf{FD}}}(z) = \Pr\left(b_1 V < z(b_2 W + 1)\right) = \int_0^\infty F_V\left(z \frac{b_2 w + 1}{b_1}\right) f_W(w) dw. \quad (28)$$

In order to evaluate (28), we require the cdf of $V$ and the pdf of $W$, which can be readily evaluated as [16]

$$F_V(v) = 1 - 2\sqrt{v} K_1(2\sqrt{v}), \text{ and } f_W(w) = 2K_0(2\sqrt{w}), \quad (29)$$

respectively. By invoking $F_V(v)$ and $f_W(w)$ in (29) the cdf of $\gamma_E^{\mathsf{FD}}$ is obtained as

$$F_{\gamma_E^{\mathsf{FD}}}(z) = 1 - 4\int_0^\infty \sqrt{\frac{z}{b_1}(1 + b_2 w)} K_1\left(2\sqrt{\frac{z}{b_1}(1 + b_2 w)}\right) \times K_0(2\sqrt{w}) dw. \quad (30)$$

To the best of the author's knowledge, the dual integral in (26) and the integral in (30) do not admit the closed-form solutions for the cdfs of $\gamma_D^{\mathsf{FD}}$ and $\gamma_E^{\mathsf{FD}}$, respectively. To overcome this, we will subsequently discuss the interference-limited scenario and derive the closed-form expressions for the cdfs of $\gamma_D^{\mathsf{FD}}$ and $\gamma_E^{\mathsf{FD}}$. From (26), (30) and (21), the exact average secrecy rate of FDJ protocol can be derived.

*2) HDJ Transmission Protocol*: Now, in order to present the average secrecy rate of the HDJ, $\bar{R}_0^{\mathsf{HD}}$, similarly, we first evaluate the cdf of the SINR at the destination, $F_{\gamma_D^{\mathsf{HD}}}(\cdot)$, and the cdf of the SINR at eavesdropper, $F_{\gamma_E^{\mathsf{HD}}}(\cdot)$. The SINR at the destination given in (13) can be re-expressed as

$$\gamma_D^{\mathsf{HD}} = X_0 \min\left(c_1, \frac{2c_4 |h_{RD}|^2}{2c_5 W + 1}\right). \quad (31)$$

Let $T = \min\left(c_1, \frac{2c_4 |h_{RD}|^2}{2c_5 W + 1}\right)$. Using similar steps as in the [16], the cdf of $T$ conditioned on $W$ is obtained as

$$f_{T|W}(t) = \begin{cases} 1 & \text{if } t \geq c_1; \\ 1 - e^{\frac{-t}{c_4}(c_5 W + \frac{1}{2})} & \text{if } t < c_1. \end{cases} \quad (32)$$

Averaging over $W$, using the integral identity [34, Eq. (6.614.4)], we obtain

$$f_T(t) = \begin{cases} 1 & \text{if } t \geq c_1; \\ 1 - \frac{e^{\frac{-t}{2c_4} + \frac{c_4}{2c_5 t}}}{\sqrt{\frac{c_5 t}{c_4}}} \mathcal{W}_{\frac{-1}{2}, 0}\left(\frac{c_4}{c_5 t}\right) & \text{if } t < c_1. \end{cases} \quad (33)$$

Now, conditioned on $X_0 = |h_{SR}|^2$ we get

$$F_{\gamma_D^{\mathsf{HD}}}(z) = 1 - \int_0^{c_1} \frac{e^{\frac{-z}{c_4 x} - \frac{c_4 x}{2c_5 z} - x}}{\sqrt{\frac{c_5 z}{c_4 x}}} \mathcal{W}_{\frac{-1}{2}, 0}\left(\frac{c_4 x}{c_5 z}\right) dx. \quad (34)$$

Similar to the FDJ case, the cdf of the SINR at eavesdropper for HDJ protocol, $F_{\gamma_E^{\mathsf{HD}}}(\cdot)$ can be readily derived as

$$F_{\gamma_E^{\mathsf{HD}}}(z) = 1 - 4\int_0^\infty \sqrt{\frac{z}{2b_1}(1 + 2b_2 w)} \times K_1\left(2\sqrt{\frac{z}{2b_1}(1 + 2b_2 w)}\right) K_0(2\sqrt{w}) dw. \quad (35)$$

Substituting (34) and (35) into (21) yields the exact expression for $\bar{R}_0^{\mathsf{HD}}$. Again the cdfs of $\gamma_D^{\mathsf{HD}}$ and $\gamma_E^{\mathsf{HD}}$ involve an integral which generally does not admit a closed-form solution.

In the following, we consider interference-limited assumption [40] which enables us to derive asymptotic closed-form expressions for the cdf of destination and eavesdropper SINRs. They provide useful theoretical performance bounds for the average secrecy rate and outage probability. In the interference-limited scenario, the aggregate interference power from the jammer's transmission (for the relay, destination, and eavesdropper) and residual SI (for the relay) are assumed to dominate the performance, and as such the thermal noise is ignored.

### C. Asymptotic Analysis

Applying the interference-limited assumption on (6) and (13), the received SINR at $D$ for the FDJ and HDJ protocols can be respectively written as

$$\tilde{\gamma}_D^{\mathsf{FD}} = \min\left(\underbrace{\frac{c_1 |h_{SR}|^2}{c_2 |h_{SR}|^2 |h_{RR}|^2 + c_3 |h_{SJ}|^2 |h_{JR}|^2}}_{\tilde{\gamma}_3}, \underbrace{\frac{c_4 |h_{SR}|^2 |h_{RD}|^2}{c_5 |h_{SJ}|^2 |h_{JD}|^2}}_{\tilde{\gamma}_4}\right), \quad (36)$$

and

$$\tilde{\gamma}_D^{\mathsf{HD}} = \min\left(\underbrace{c_1 |h_{SR}|^2}_{\tilde{\gamma}_5}, \underbrace{\frac{c_4 |h_{SR}|^2 |h_{RD}|^2}{c_5 |h_{SJ}|^2 |h_{JD}|^2}}_{\tilde{\gamma}_4}\right). \quad (37)$$

Moreover, applying the interference-limited assumption on (8) and (14), the overheard SINR at the eavesdropper for both the protocols can be expressed as

$$\tilde{\gamma}_E = \frac{b_1|h_{SR}|^2|h_{RE}|^2}{b_2|h_{SJ}|^2|h_{JE}|^2}, \tag{38}$$

and hence $F_{\tilde{\gamma}_E^{\mathsf{FD}}}(\cdot) = F_{\tilde{\gamma}_E^{\mathsf{HD}}}(\cdot) = F_{\tilde{\gamma}_E}(\cdot)$. Now we characterize the asymptotic expressions for the cdf of the SINR at the destination and eavesdropper.

*1) FDJ Transmission Protocol*:

*Proposition 1:* The expression for asymptotic $F_{\tilde{\gamma}_D^{\mathsf{FD}}}(\cdot)$ is derived as (39) at the top of the next page where $c_i$, $i = 1, \cdots, 5$, have been defined in (7). Moreover, $c_6 = \frac{-c_1}{c_2}$, $c_7 = \frac{c_1 c_5}{c_3 c_4}$, $c_8 = c_2 + c_3$, $c_9 = \frac{\frac{c_3^3}{c_2^2}}{(1+\frac{c_3}{c_2})^2}$, $c_{10} = \frac{c_5}{c_4}$,

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

and

$$\Psi_2(z) = \frac{c_3(zc_5 - c_4)c_8 - (2zc_5c_3 + zc_5c_2 - c_3c_4)(c_8 - c_2 e^{\frac{-c_1}{c_2 z}})}{(c_4 - zc_5)^2 c_8^2}.$$

*Proof:* See Appendix A. ∎

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

$$F_{\tilde{\gamma}_E}(z) = 1 - G_{2,2}^{2,2}\left(\frac{b_2 z}{b_1}\middle| \begin{matrix} 0, 0 \\ 1, 0 \end{matrix}\right). \tag{40}$$

*Proof:* See Appendix B. ∎

Substituting (39) and (40) into (21), the asymptotic average secrecy rate for FDJ can be readily evaluated as (41) at the top of the next page.

*Corollary 3:* When jammer is located midway between the source and relay, asymptotic average secrecy rate for FDJ protocol can be approximated as

$$\bar{R}_0^{\mathsf{FD}} \approx \frac{1-\alpha}{\ln 2}\left(G_{1,1;2,2;2,2}^{1,1;2,2;2,2}\left[\begin{matrix} 0 \\ 0 \end{matrix}\middle| \begin{matrix} 0, 0 \\ 1, 0 \end{matrix}\middle| \begin{matrix} 0, 1 \\ 1, 1 \end{matrix}\middle| \frac{b_2}{b_1}\middle| \frac{c_5}{c_4}\right] - G_{1,1;2,2;1,0}^{1,1;2,2;0,1}\left[\begin{matrix} 0 \\ 0 \end{matrix}\middle| \begin{matrix} 0, 0 \\ 1, 0 \end{matrix}\middle| \begin{matrix} 0, 1 \\ 1, 1 \end{matrix}\middle| \frac{b_2}{b_1}\middle| \kappa\right]\right), \tag{41}$$

where $G^{\cdot,\cdot;\cdot,\cdot;\cdot,\cdot}_{\cdot,\cdot;\cdot,\cdot;\cdot,\cdot}[\cdot,\cdot]$ denotes the extended generalized bivariate Meijer's G function [41].

*Proof:* See Appendix C. ∎

The asymptotic result in (41) presents an average secrecy rate floor and indicates that more source transmit power does not guarantee a higher secrecy rate in FDJ protocol. This finding is validated by Fig. 4. In the FD protocol without jammer, however, the secrecy rate decreases for high transmission power regime. In particular, for this protocol, the SINR at $D$ is given by $\min\left(\frac{1}{\kappa|h_{RR}|^2}, c_4|h_{SR}|^2|h_{RD}|^2\right)$, and the SINR at $E$ is $b_1|h_{SR}|^2|h_{RE}|^2$. As we observe the first-hop SINR at $D$ is independent of $p_S$ while the SINR at $E$ improves directly proportional to the $p_S$. Thus, the average secrecy rate is severely degraded by high values of $p_S$.

Moreover, from (41) we observe that the average secrecy rate of the FDJ protocol is a function of time split, $\alpha$, and is a decreasing function of SI strength, $\sigma_{RR}^2$. In the high SNR regime, the average secrecy rate is a decreasing function of the conversion efficiency, $\eta$, of the deployed energy harvester at the relay and jammer nodes. This is intuitive because increasing $\eta$, increases the source and jammer transmission power which increases the amount of SI and inter-user interference at the relay and reduces the first-hop SINR at the destination.

*2) HDJ Transmission Protocol*: Now, let us consider the HDJ case. The cdf of $\tilde{\gamma}_D^{\mathsf{HD}}$ is presented in the following corollary.

*Corollary 4:* For the HDJ transmission, the cdf of $\tilde{\gamma}_D^{HD}$ can be approximated as

$$F_{\tilde{\gamma}_D^{\mathsf{HD}}}(z) \approx 1 + e^{\frac{-z}{c_1}} - \sum_{n=1}^{\infty} \frac{n!(c_5 z)^n(-1)^n \mathcal{G}(n)}{c_4^n}, \tag{42}$$

where

$$\mathcal{G}(n) = (-1)^n \frac{\mathsf{Ei}\left(-\frac{z}{c_1}\right)}{(n-1)!} + \frac{e^{-\frac{z}{c_1}}}{\left(\frac{z}{c_1}\right)^{n-1}} \times \sum_{k=0}^{n-2} \frac{(-1)^k \left(\frac{z}{c_1}\right)^k}{(n-1)(n-2)\cdots(n-1-k)}.$$

*Proof:* See Appendix D. ∎

It is worth to mention that the series in (42) can be truncated using few terms up to 10.

Substituting (40) and (42) into (21), the asymptotic average secrecy rate for HDJ can be approximated as

$$\bar{\tilde{R}}_0^{\mathsf{HD}} \approx \frac{k^{\mathsf{HD}}}{\ln 2} \int_0^{\infty} \frac{1 - G_{2,2}^{2,2}\left(\frac{b_2 z}{b_1}\middle| \begin{matrix} 0,0 \\ 1,0 \end{matrix}\right)}{1+z} \times \left(\sum_{n=1}^{\infty} \frac{n!(c_5 z)^n(-1)^n \mathcal{G}(n)}{c_4^n} - e^{\frac{-z}{c_1}}\right) dz. \tag{43}$$

### *D. Performance Comparison of the Proposed Protocols*

Comparison of FDJ and HDJ provides insights into the choice of one protocol with a higher secrecy rate. To this end, we have the following result:

*Remark 1:* Referring to the spectral efficiency factor of $(1-\alpha)$ for the secrecy rate of FDJ compared with $\frac{(1-\alpha)}{2}$ for the HDJ protocol, one may reasonably argue that FDJ may offer higher secrecy rates compared with HDJ. However, when $\tilde{\gamma}_D^{\mathsf{FD}} < \sqrt{\tilde{\gamma}_D^{\mathsf{HD}} \tilde{\gamma}_E}$, we have $\tilde{R}_0^{\mathsf{FD}} < \tilde{R}_0^{\mathsf{HD}}$, i.e., the secrecy rate advantage of FDJ over HDJ completely diminishes. The reasons are (a) the effect of SI caused by the signal leakage from the transceiver output to the input [42] and (b) an extra interference at the relay due to the jammer's transmission (see (36) and (37)), which reduce the instantaneous secrecy rate of FDJ, but are not present with HDJ. It is clear that *ideal* FDJ, without SI and jammer interference on the relay, doubles the secrecy rate of the HDJ scheme. However, more realistically (as per simulations), the average secrecy rate can increase by 50% over the HDJ protocol.

We next consider FDJ with interference-limited assumption and in the high-SNR regime. Although this is an ideal assumption, it leads to useful theoretical bounds for practical design. Our aim is to identify communication scenarios where FDJ

$$F_{\tilde{\gamma}_D^{\mathsf{FD}}}(z) = 1 - \frac{c_3c_4}{c_8(zc_5-c_4)}\left(\frac{c_1}{c_3z}e^{\frac{c_1}{c_3z}}\mathsf{Ei}\left(\frac{-c_1}{c_3z}\right)+1\right) - c_3c_4\left(\frac{c_3c_5z+c_2c_4}{c_8^2(zc_5-c_4)^2}e^{\frac{c_1}{c_3z}}\mathsf{Ei}\left(\frac{-c_1}{c_3z}\right)+\frac{c_9e^{\frac{-c_6}{z}}\mathsf{Ei}(\frac{c_6}{z})}{zc_5+\frac{c_3c_4}{c_2}}\right) + \frac{zc_3c_{10}e^{c_7}\mathsf{Ei}(-c_7)}{(1-c_{10}z)^2(c_2c_{10}z+c_3)} - c_4\left[\ln\left(\frac{(zc_5)^{\frac{\Psi_1(z)}{zc_5}}}{c_3^{\frac{\Psi_2(z)}{c_3}}}\right) - \ln\left(\frac{c_4^{\frac{\Psi_1(z)}{zc_5}}}{c_2^{\frac{\Psi_2(z)}{c_3}}}\right) + \frac{(c_8-c_2e^{\frac{-c_1}{c_2z}})}{(c_4-zc_5)c_8}\right], \tag{39}$$

$$\bar{\tilde{R}}_0^{\mathsf{FD}} = \frac{k^{\mathsf{FD}}}{\ln 2}\int_0^\infty\left(\frac{1-G_{2,2}^{2,2}\left(\frac{b_2z}{b_1}\middle|\begin{matrix}0,0\\1,0\end{matrix}\right)}{1+z}\left(\frac{c_3c_4}{c_8(zc_5-c_4)}\left(\frac{c_1}{c_3z}e^{\frac{c_1}{c_3z}}\mathsf{Ei}\left(\frac{-c_1}{c_3z}\right)+1\right)\right.\right. + c_3c_4\left(\frac{c_3c_5z+c_2c_4}{c_8^2(zc_5-c_4)^2}e^{\frac{c_1}{c_3z}}\mathsf{Ei}\left(\frac{-c_1}{c_3z}\right)+\frac{c_9e^{\frac{-c_6}{z}}\mathsf{Ei}(\frac{c_6}{z})}{zc_5+\frac{c_3c_4}{c_2}}\right) - \frac{zc_3c_{10}e^{c_7}\mathsf{Ei}(-c_7)}{(1-c_{10}z)^2(c_2c_{10}z+c_3)} + c_4\left[\ln\left(\frac{(zc_5)^{\frac{\Psi_1(z)}{zc_5}}}{c_3^{\frac{\Psi_2(z)}{c_3}}}\right) - \ln\left(\frac{c_4^{\frac{\Psi_1(z)}{zc_5}}}{c_2^{\frac{\Psi_2(z)}{c_3}}}\right) + \frac{(c_8-c_2e^{\frac{-c_1}{c_2z}})}{(c_4-zc_5)c_8}\right]\right)\right)dz. \tag{41}$$

exhibits poorer instantaneous secrecy rate than HDJ. These are detailed next.

*Corollary 5:* For interference-limited assumption and in the high-SNR regime, in two critical scenarios

1) $\tilde{\gamma}_4 \geq \tilde{\gamma}_5$ and $\tilde{\gamma}_3^2 < \tilde{\gamma}_5\tilde{\gamma}_E$
2) $\tilde{\gamma}_3 \leq \tilde{\gamma}_4 \leq \tilde{\gamma}_5$ and $\tilde{\gamma}_3^2 < \tilde{\gamma}_4\tilde{\gamma}_E$,

HDJ outperforms FDJ, while in other cases FDJ can provide the better performance.

*Proof:* Note that in the high-SNR regime the asymptotic instantaneous secrecy rates can be respectively approximated as [31]

$$\tilde{R}_0^{\mathsf{FD}} \approx \lfloor (1-\alpha)\log\left(\min\left(\tilde{\gamma}_3,\tilde{\gamma}_4\right)\right) - (1-\alpha)\log(\tilde{\gamma}_E)\rfloor^+, \tag{44}$$

and

$$\tilde{R}_0^{\mathsf{HD}} \approx \left\lfloor \frac{(1-\alpha)}{2}\log\left(\min\left(\tilde{\gamma}_5,\tilde{\gamma}_4\right)\right) - \frac{(1-\alpha)}{2}\log(\tilde{\gamma}_E)\right\rfloor^+, \tag{45}$$

where $\tilde{\gamma}_3 \leq \tilde{\gamma}_5$.

Let

$$\mathcal{A} = \tilde{R}_0^{\mathsf{FD}} - \tilde{R}_0^{\mathsf{HD}}. \tag{46}$$

Depending on the values of $\tilde{\gamma}_3$, $\tilde{\gamma}_4$ and $\tilde{\gamma}_5$, $\mathcal{A}$ can be simplifies to the following cases.

- If $\tilde{\gamma}_5 \leq \tilde{\gamma}_4$, (46) reduces to

$$\mathcal{A} = \frac{(1-\alpha)}{2}\log\left(\frac{\tilde{\gamma}_3^2}{\tilde{\gamma}_5\tilde{\gamma}_E}\right).$$

  Thus, if $\tilde{\gamma}_3^2 < \tilde{\gamma}_5\tilde{\gamma}_E$, $\mathcal{A} < 0$.
- If $\tilde{\gamma}_3 \leq \tilde{\gamma}_4$ and $\tilde{\gamma}_5 \geq \tilde{\gamma}_4$ (46) reduces to

$$\mathcal{A} = (1-\alpha)\log\left(\frac{\tilde{\gamma}_3^2}{\tilde{\gamma}_4\tilde{\gamma}_E}\right).$$

  Thus, if $\tilde{\gamma}_3^2 < \tilde{\gamma}_4\tilde{\gamma}_E$, $\mathcal{A} < 0$.

■

*Remark 2:* In the system under consideration with interference-limited assumption and in the high-SNR regime, when $\tilde{\gamma}_E < \tilde{\gamma}_4 \leq \tilde{\gamma}_3$, we have $\tilde{R}_0^{\mathsf{FD}} = 2\tilde{R}_0^{\mathsf{HD}}$.

*Remark 3:* Please note that the total transmitted energy of the relay and jammer nodes for FDJ and HDJ protocols are the same. However, if the system is concerned with the source transmission energy, $\tilde{\gamma_5}$ in Corollary 5 should be replaced with $2\tilde{\gamma_5}$ for fair comparison. With this change the source consumes the same amount of energy for both protocols.

Corollary 5 and Remark 2 show that FDJ is more beneficial for the communication scenarios in which the first-hop SINR of the destination is much stronger than the second-hop SINR. This is the case where for example SI strength and the inter-user interference at the relay are low. Nevertheless, in practice, SI and inter-user interference can be reduced significantly by exploiting techniques such as beamforming designs and interference coordination. Also, the appropriate choice of design parameters, such as transmission powers, energy harvesting time, and relative distance between the nodes may still guarantee the FDJ gains over secure wireless networks. The effect of design parameters on FDJ and HDJ is not always clear cut and is further discussed in Section IV.

### *E. Secrecy Outage Given Incomplete ECSI*

We now consider the incomplete ECSI scenario, where the source and relay nodes do not know the eavesdropper channel and hence transmit at a constant rate $\Re_s$ bits/sec/Hz. The transmission guarantees perfect secrecy if $R_0^{\mathsf{i}} \geq \Re_s$. On the other hand, if $R_0^{\mathsf{i}} < \Re_s$ ($R_0^{\mathsf{i}}$ in (15)) the transmission is vulnerable to eavesdropping and perfect secrecy is not guaranteed [30]. In other words, unlike the complete ECSI case, lack of ECSI may result in outage events where the instantaneous secrecy rate is below the transmission rate. Accordingly, to characterize this, we adopt the secrecy outage probability, $\mathsf{P}_{\mathsf{out}}^{\mathsf{i}}$ for $\mathsf{i} \in \{\mathsf{FD},\mathsf{HD}\}$, which can be expressed as [30]

$$\mathsf{P}_{\mathsf{out}}^{\mathsf{i}} = \Pr\{R_0^{\mathsf{i}} < \Re_s\} = \int_0^\infty F_{\gamma_D^{\mathsf{i}}}[2^{\frac{\Re_s}{k^{\mathsf{i}}}}(1+x)-1]f_{\gamma_E^{\mathsf{i}}}(x)dx. \tag{47}$$

In order to find this outage, we require the pdf of $\gamma_E^{\mathsf{i}}$ and the cdf of the RV $\gamma_D^{\mathsf{i}}$. Since we have the closed-form cdf of the SINR at the destination and eavesdropper nodes for the interference-limited scenario, we derive the asymptotic secrecy outage probability, $\tilde{\mathsf{P}}_{\mathsf{out}}^{\mathsf{i}}$,

$$\tilde{\mathsf{P}}_{\mathsf{out}}^{\mathsf{i}} = \Pr\{\tilde{R}_0^{\mathsf{i}} < \Re_s\} = \int_0^{\infty} F_{\tilde{\gamma}_D^{\mathsf{i}}}[2^{\frac{\Re_s}{k^{\mathsf{i}}}}(1+x)-1] f_{\tilde{\gamma}_E}(x)dx. \tag{48}$$

*1) FDJ Transmission Protocol*: The cdf of $\tilde{\gamma}_D^{\mathsf{FD}}$ is given in closed-form in (39). Therefore, the remaining task is to characterize the pdf of $\tilde{\gamma}_E$. From (40), taking the first order derivative of the cdf of $\tilde{\gamma}_E$ with respect to $z$, we have

$$\begin{aligned} f_{\tilde{\gamma}_E} &= -\frac{\partial G_{2,2}^{2,2}\left(\frac{b_2 z}{b_1}\middle|\begin{matrix}0,0\\1,0\end{matrix}\right)}{\partial z} \\ &= \frac{-b_2}{b_1 z} G_{3,3}^{2,3}\left(\frac{b_2 z}{b_1}\middle|\begin{matrix}-1,-1,-1\\0,-1,0\end{matrix}\right). \end{aligned} \tag{49}$$

Now, using the cdf of $\tilde{\gamma}_D^{\mathsf{FD}}$, and substituting (49) into (47) we obtain asymptotic $\tilde{\mathsf{P}}_{\mathsf{out}}^{\mathsf{FD}}$.

*2) HDJ Transmission Protocol*: Similarly, using the cdf of $\tilde{\gamma}_D^{\mathsf{HD}}$ (given in (42)), and substituting (49) into (48), the asymptotic outage probability for the HDJ transmission, $\tilde{\mathsf{P}}_{\mathsf{out}}^{\mathsf{HD}}$, can be computed.

From $\tilde{\mathsf{P}}_{\mathsf{out}}^{\mathsf{FD}}$ and $\tilde{\mathsf{P}}_{\mathsf{out}}^{\mathsf{HD}}$ we observe that the secrecy outage probability for both FDJ and HDJ protocols is independent of source power and shows an outage floor.

*Remark 4:* It is noteworthy that the derived expressions for $\tilde{\mathsf{P}}_{\mathsf{out}}^{\mathsf{FD}}$ and $\tilde{\mathsf{P}}_{\mathsf{out}}^{\mathsf{HD}}$ are not simple enough to provide immediate insight, but they are general and fast to evaluate using software packages such as Mathematica and MATLAB.

## IV. Numerical Results and Discussion

Here, numerical results are presented to validate analytical expressions, demonstrate the performance of FDJ and HDJ and investigate the impact of key system parameters on their performances. We adopt some parameters of the 3GPP LTE specifications for small cell deployments. The maximum source transmit power is set to 40 dBm. Moreover, the $S-R, S-D, J-R, J-E, J-D, E-R$, and $E-D$ link distances take values between 10 and 50 meters, which are the case for small cell. The energy conversion efficiency $\eta$ is set to the typical value of $0.5$ [15], [26].

### A. Instantaneous Secrecy Rate

Fig. 3 shows the influence of the time-split $\alpha$ on the instantaneous secrecy rate. We assume that $S$, $R$, $J$, $E$ and $D$ are located at $(0,0)$ m, $(20,10)$ m, $(20,-10)$ m, $(40,0)$ m and $(50,0)$ m, respectively. We focus on a single time frame with the following settings: *Setting-1:* $|h_{SR}|^2 = 0.78$, $|h_{SJ}|^2 = 1.55$, $|h_{RE}|^2 = 0.01$, $|h_{RD}|^2 = 0.81$, $|h_{RR}|^2 = 0.05$, $|h_{JR}|^2 = 1.07$, $|h_{JE}|^2 = 2.32$ and $|h_{JD}|^2 = 0.36$. *Setting-2:* $|h_{SR}|^2 = 0.87$, $|h_{SJ}|^2 = 0.63$, $|h_{RE}|^2 = 0.2$, $|h_{RD}|^2 = 1.2$, $|h_{RR}|^2 = 0.13$, $|h_{JR}|^2 = 0.54$, $|h_{JE}|^2 = 0.46$ and $|h_{JD}|^2 = 0.03$. *Setting-3:* $|h_{SR}|^2 = 1.53$, $|h_{SJ}|^2 = 1.03$, $|h_{RE}|^2 = 1.34$, $|h_{RD}|^2 = 0.81$, $|h_{RR}|^2 = 0.11$, $|h_{JR}|^2 = 1.69$, $|h_{JE}|^2 = 1.92$ and $|h_{JD}|^2 = 0.45$. The following conclusions are drawn from Fig. 3.

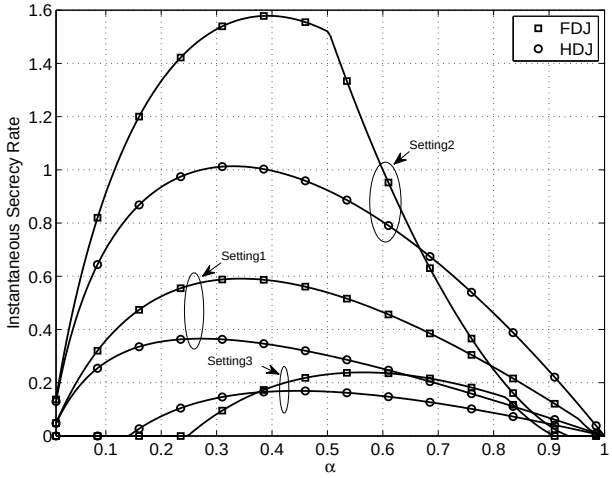


Fig. 3. Instantaneous secrecy rate of FDJ and HDJ protocols as a function of $\alpha$.

1) An interesting trade-off exists between $\alpha$ and the instantaneous secrecy rate for both protocols. More specifically, first, as $\alpha$ increases, the secrecy rate increases but it then starts decreasing as $\alpha$ increases beyond optimal value. The intuitive reason is that large time split $\alpha$ increases the harvested energy by relay and jammer and consequently improves the secrecy rate. However, it decreases the available time for information transmission phase. Therefore, it is important to optimize $\alpha$ to maximize the secrecy rate.
2) It is clear that for setting-1, FDJ achieves a higher instantaneous secrecy rate than HDJ for all $\alpha$. However, for setting-2, we see that FDJ outperforms HDJ when $\alpha < 0.67$, and exhibits an inferior performance when $\alpha > 0.67$. Also, for setting-3 HDJ outperforms FDJ when $\alpha < 0.39$, and FDJ exhibits a better performance when $\alpha > 0.39$. This result is in accordance with Section III-D shows that the strength of the SI, the value of $\alpha$ and the corresponding nodes channels and their relative positions are the key factors determining the extent to which FDJ outperforms HDJ.

### B. Average Secrecy Rate

Fig. 4 illustrates the average secrecy rate of FDJ and HDJ protocols versus source power with and without jammer for $\alpha = 0.5$. The locations of $S$, $R$, $J$, $E$ and $D$ are $(0,0)$ m, $(20,0)$ m, $(20,-10)$ m, $(40,0)$ m and $(50,0)$ m, respectively. Three main observations that follow from this simulation are as follows:

1) First, the average secrecy rate against the eavesdropper can be significantly improved using the jammer node, *e.g.*, HDJ provides up to $70\%$ enhancement compared to the HD relaying without jammer.
2) Second, as expected, FDJ outperforms all other schemes for all values of the source power. When the source node power values are high, FDJ can achieve, respectively,

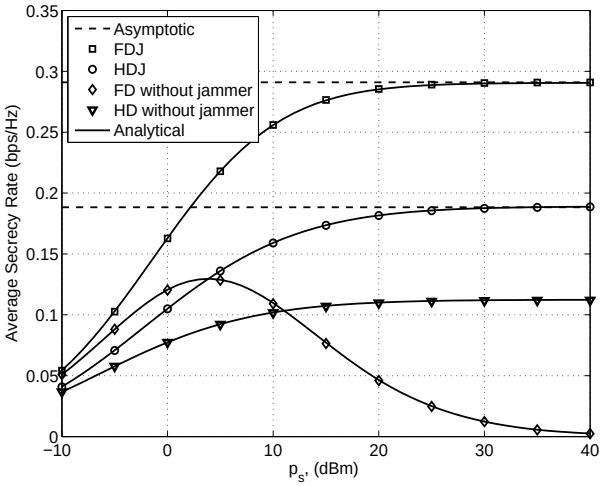


Fig. 4. Average secrecy rate of FDJ and HDJ protocols versus source power $p_S$.

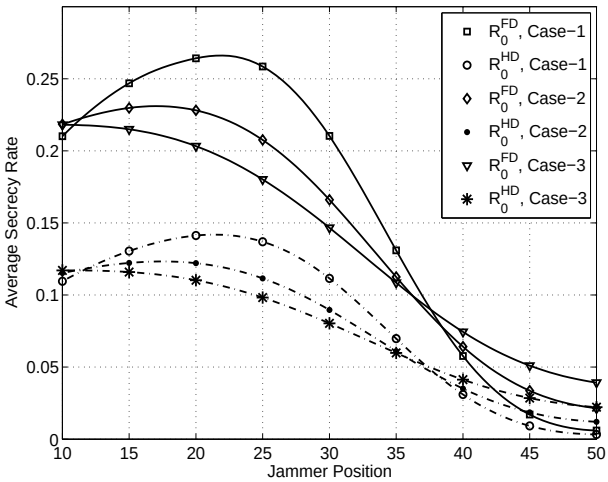


Fig. 5. Average secrecy rate of FDJ and HDJ protocols versus different positions of the jammer.

$54\%$ and $260\%$, average secrecy gains compared to FD and HD relaying schemes without the jammer.

3) Third, the average secrecy rate of FDJ, HDJ and HD relaying without jammer protocols converge to finite limits at high transmission source power which is in agreement with the analysis in previous section. More specifically, with high source transmit power, the FDJ almost achieves the average secrecy rate of $0.29$ bps/Hz, which is nearly $1.5$ times than that of HDJ and $2.6$ times than that of HD relaying without jammer. In the FD protocol without jammer, however, the secrecy rate first increases with the transmission source power $p_S$, and then decreases when $p_S$ increases beyond a certain value. The above observations reveal the existence of various design choices when performance-complexity tradeoff is considered.

Fig. 4 also shows that the analytical results tightly match simulation results and that asymptotic curves tightly converge to the exact ones at the high-SNR regime. These observations validate the derived analytical results and justify the interference-limited assumption.

Fig. 5 shows the impact of jammer position on the average secrecy rate. The $S$, $R$, $E$ and $D$ are located at $(0, 0)$ m, $(20, 0)$ m, $(30, 10)$ m, and $(50, 0)$ m, respectively. Three cases are considered where the y-coordinates of the jammer are fixed as $-5$ m, $-10$ m and $-15$ m respectively, and the x-coordinates of the jammer are within the range of $[10, 50]$ m. In particular, simulation results lead to the following conclusions.

1) As expected, as jammer gets closer to the horizontal line, both protocols achieve better average secrecy rates. Particularly, the FDJ in case-1 exhibits the best secrecy rate performance. The superior performance of the FDJ is more pronounced especially between 20 m and 30 m values of x-coordinates of the jammer.
2) As the jammer moves from the source to the destination, the average secrecy rate of all schemes increase first and then decrease. Thus, there exists an optimal point for the jamming position. However, as clearly observed, FDJ and HDJ protocols have different intersections with the horizontal axis for each case, which means that the best position of the jammer is different for the three cases with three different values of y-coordinate jammer positions. We observe that for all cases the best position for the jammer is somewhere between the source and eavesdropper. Specifically, we can see that the highest average secrecy rate of FDJ happens when the x-coordinate of the eavesdropper is 22 m in case-1, 17 m in case-2, and 10 m in case-3, respectively. Thus the best position for FDJ in case-3 is the nearest one to the source. This is due to the fact that the jammer is energy constrained and hence when the y-coordinate of the jammer increases it should get closer to the source to collect sufficient amount of energy to enable a secure communication. On the contrary, in case-1 where the jammer has the superior energy harvesting capability, it could stay closer to the eavesdropper so that the interference from the jammer to the eavesdropper is much stronger and the jammer would be more effective to improve the secrecy rate.
3) When the jammer moves close to the destination node, the average secrecy rate is substantially reduced. The reason is that as the relative distance between the jammer and the destination reduces, the jamming signal causes stronger interference on the destination, which degrades the destination's SINR.

### C. Secrecy Outage Probability

Fig. 6 compares the secrecy outage of FDJ and HDJ protocols versus source power and with different residual SI strength at the relay, $\sigma_{RR}^2$. The $S$, $R$, $J$, $E$, and $D$ are located at $(0, 0)$ m, $(20, 0)$ m, $(20, -10)$ m, $(40, -30)$ m, and $(50, 0)$ m, respectively and $\alpha = 0.5$. For high values of source transmit power, $p_S$, the secrecy outage performance of both protocols degrades. This is because the inter-user interference from jammer goes up with higher $p_S$. In addition, for the FDJ protocol when the source transmit power increases and $\alpha$ is fixed, an excessive amount of energy will be collected

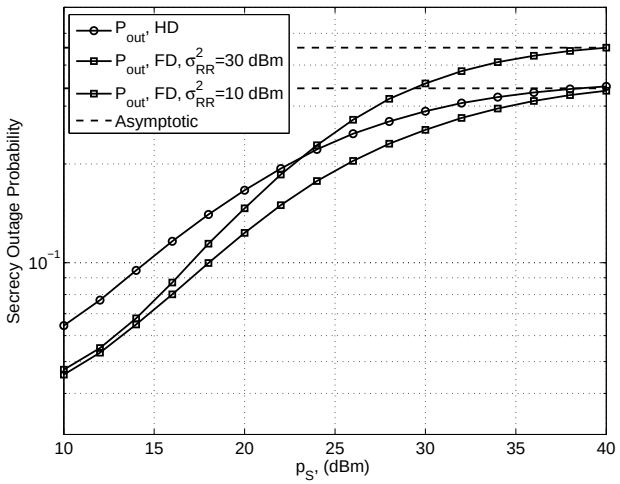


Fig. 6. Secrecy outage probability versus $p_S$ of FDJ and HDJ protocols for different residual SI strength, $\sigma^2_{RR}$.

at the relay, which is actually detrimental[4] since it causes strong SI, which degrades the secrecy outage performance of FDJ system. Clearly, the performance degradation is more prominent for higher value of $\sigma^2_{RR}$. Asymptotic results are also presented in Fig. 6. We observe that FDJ achieves lower secrecy outage probability, but its advantage over HDJ is less than 40%. This is expected because FDJ protocol suffers from SI at the relay and inter-user interference at both relay and destination nodes. However, in HDJ protocol the only interference is inter-user interference at the destination node. Therefore, when compatibility with HDJ systems is a concern, one can reasonably expect that the performance gain of FDJ relative to the HDJ is directly related to the strength of the SI and the quality of inter-user interference suppression techniques. In particular, while with low SI the FDJ outperforms the HDJ, with strong SI FDJ performs worse than HDJ.

## V. Conclusions

Energy, security and spectral efficiency are critical factors for emerging fifth generation (5G) wireless networks. Thus, wireless energy harvesting, physical-layer security and full-duplex wireless are being developed. In this context, we investigated the performance of a secure wireless-powered network with joint FD relaying and cooperative jamming. We proposed a secure FDJ protocol, also treated the HDJ protocol and analyzed their instantaneous and average secrecy rates for the complete ECSI scenario. We also presented asymptotic closed-form SINR cdf for the destination and eavesdropper nodes. Accordingly, the asymptotic average secrecy rates were also derived. These expressions provide valuable theoretical performance bounds for the average secrecy rates and secrecy outage and facilitate the design and analysis of secure wireless-powered FD relaying systems. Moreover, for the incomplete ECSI scenario, the asymptotic secrecy outages of FDJ and HDJ were studied. We showed that FDJ could substantially boost the system performance compared to the HDJ protocol for all source transmission powers. However, secrecy-rate performance gain of FDJ over HDJ is highly depend on the time-split $\alpha$, the amount of SI, and the channel gains and node locations. Finally, we found that as the jammer has the superior energy harvesting capability, it could stay closer to the eavesdropper, a highly effective strategy to improve the secrecy rate.

It would be interesting to extend these results to other practical secure wireless networks. For instance, networks under hostile jamming and eavesdropping, network with direct source-eavesdropper and source-destination links, and MIMO systems. Another potential future research direction would be to investigate the application of harvest-store-use (HSU) architecture in secure wireless-powered cooperative networks.

[4]It is worth to mention that, as it is stated in [16], the intuitive reason behind this phenomenon is that the transmission power is increased while the energy-harvesting time fraction, $\alpha$, is fixed. Clearly, by tuning $\alpha$ better performance can be achieved.

## VI. Acknowledgement

This work has been financially supported by the research deputy of Shahrekord University under the grant number 96GRD1M31714.

## Appendix A
## Proof of Proposition 1

Let us denote $X = c_1/\left(c_2X_1 + c_3X_2X_3\right)$ where $X_1 = |h_{RR}|^2$, $X_2 = |h_{JR}|^2$ and $X_3 = \frac{|h_{SJ}|^2}{|h_{SR}|^2}$, and $Y = \frac{c_4Y_1}{c_5Y_2X_3}$, with $Y_1 = |h_{RD}|^2$ and $Y_2 = |h_{JD}|^2$. Accordingly, the cdf of $\tilde{\gamma}_D^{\mathsf{FD}}$ in (36) becomes

$$\begin{aligned} F_{\tilde{\gamma}_D^{\mathsf{FD}}}(z) &= \Pr(\min(X,Y) < z) = 1 - \Pr(\min(X,Y) > z) \\ &= 1 - \Pr(X > z, Y > z). \end{aligned} \tag{50}$$

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

$$\begin{aligned} \Pr(X > z, Y > z) = \int_0^\infty &\left(1 - F_{X|X_3}(z)\right)\left(1 - F_{Y|X_3}(z)\right) \\ &\times f_{X_3}(x)dx. \end{aligned} \tag{51}$$

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

$$\begin{aligned} 1 - F_{X|X_3}(z) &= 1 - \Pr\left(\frac{c_1}{c_2X_1 + c_3X_2X_3} < z\right) \\ &= \int_0^{\frac{c_1}{c_3X_3z}} F_{X_1}\left(\frac{c_1 - c_3xX_3z}{c_2z}\right) f_{X_2}(x)dx. \end{aligned} \tag{52}$$

Recall that $X_1$ and $X_2$ are Exponential RVs with mean 1, thus (52) can be derived as

$$1 - F_{X|X_3}(z) = \frac{c_2 - c_2e^{\frac{-c_1}{c_2z}} + (e^{\frac{-c_1}{c_3X_3z}} - 1)c_3X_3}{c_2 - c_3X_3}. \tag{53}$$

The second item in the integral (51) can be written similarly as

$$1 - F_{Y|X_3}(z) = 1 - \Pr\left(Y_1 < \frac{zc_5X_3}{c_4}Y_2\right) = \frac{c_4}{zc_5X_3 + c_4}. \tag{54}$$

The pdf of RV $X_3$ can be readily evaluated as

$$f_{X_3}(x) = \frac{1}{(x+1)^2}, \quad 0 \le x < \infty. \tag{55}$$

By substituting (53), (54) and (55) into (51) and then substituting the result into (50), we have

$$F_{\tilde{\gamma}_D^{FD}}(z) = 1 - c_4 \int_0^\infty \frac{c_2 - c_2 e^{\frac{-c_1}{c_2 z}} + (e^{\frac{-c_1}{c_3 x z}} - 1) c_3 x}{(c_2 - c_3 x)(z c_5 x + c_4)(x+1)^2} dx. \tag{56}$$

Now, after some simple algebraic manipulations and using the integral identities [43, Eq. (2.3.4)], [34, Eq. (3.353.3) and Eq. (3.352.4)], we obtain the desired result in (39).

## Appendix B
## Proof of Proposition 2

$\tilde{\gamma}_E$ in (38) can be written as

$$\tilde{\gamma}_E = \frac{b_1 V}{b_2 W}, \tag{57}$$

where $V$ and $W$ is defined in Section III-B. Thus, the cdf of $\tilde{\gamma}_E$ can be expressed as

$$F_{\tilde{\gamma}_E}(z) = \Pr\left(V < \frac{b_2 z W}{b_1}\right) = \int_0^\infty F_V\left(\frac{b_2 z w}{b_1}\right) f_W(w) dw. \tag{58}$$

Utilizing (29) and the following identity [44]

$$K_\nu(2\sqrt{x}) = \frac{1}{2} G_{02}^{20}\left(x \middle| \begin{matrix} - \\ \frac{\nu}{2}, \frac{-\nu}{2} \end{matrix}\right), \tag{59}$$

(58) can be computed as

$$\begin{aligned} &F_{\tilde{\gamma}_E}(z) \qquad (60)\\ &= 1 - 2\int_0^\infty \sqrt{\frac{b_2 z w}{b_1}} K_1\left(2\sqrt{\frac{b_2 z w}{b_1}}\right) G_{02}^{20}\left(w \middle| \begin{matrix} - - \\ 0, 0 \end{matrix}\right) dw. \end{aligned}$$

Applying the integral identity [34, Eq. (7.821.3)], the integral in (60) can be solved and we have

$$F_{\tilde{\gamma}_E}(z) = 1 - \frac{b_1}{b_2 z} G_{2,2}^{2,2}\left(\frac{b_1}{b_2 z} \middle| \begin{matrix} -1, 0 \\ 0, 0 \end{matrix}\right). \tag{61}$$

Finally, with the help of [34, Eq. (9.31)], (61) can be re-expressed as

$$F_{\tilde{\gamma}_E}(z) = 1 - G_{2,2}^{2,2}\left(\frac{b_2 z}{b_1} \middle| \begin{matrix} 0, 0 \\ 1, 0 \end{matrix}\right). \tag{62}$$

## Appendix C
## Proof of Corollary 3

When jammer is located midway between the source and relay, the received SINR at $D$ can be approximated as

$$\tilde{\gamma}_D^{\mathsf{FD}} \approx \min\left(\frac{1}{\kappa |h_{RR}|^2}, \frac{c_4 |h_{SR}|^2 |h_{RD}|^2}{c_5 |h_{SJ}|^2 |h_{JD}|^2}\right). \tag{63}$$

Accordingly, the asymptotic expression for the CDF of $\tilde{\gamma}_D^{\mathsf{FD}}$ can be obtained after some manipulations as

$$\begin{aligned} F_{\tilde{\gamma}_D^{\mathsf{FD}}}(z) &\approx 1 - G_{22}^{22}\left(\frac{c_5}{c_4} z \;\middle|\; \begin{matrix} 0 & 0 \\ 1 & 0 \end{matrix}\right) + e^{-\frac{1}{\kappa z}} \\ &= 1 - G_{22}^{22}\left(\frac{c_5}{c_4} z \;\middle|\; \begin{matrix} 0 & 0 \\ 1 & 0 \end{matrix}\right) + G_{10}^{01}\left(\kappa z \;\middle|\; \begin{matrix} 1 \\ - \end{matrix}\right), \end{aligned} \tag{64}$$

where we have used the identity [44, Eq. (8.4.3.2)] to obtain the second equality. Moreover, $F_{\tilde{\gamma}_E^{\mathsf{FD}}}(z)$, derived in Appendix B, can be re-expressed as

$$F_{\tilde{\gamma}_E^{\mathsf{FD}}}(z) = G_{22}^{22}\left(\frac{b_2 z}{b_1} \;\middle|\; \begin{matrix} 0 & 1 \\ 1 & 1 \end{matrix}\right). \tag{65}$$

Next, by substituting the $F_{\tilde{\gamma}_D^{\mathsf{FD}}}(z)$ and $F_{\tilde{\gamma}_E^{\mathsf{FD}}}(z)$ into (21), and using the identity $(1+x)^{-\delta} = \frac{1}{\Gamma(\delta)} G_{11}^{11}\left(x \middle| \begin{matrix} 1-\delta \\ 0 \end{matrix}\right)$ [44, Eq. (8.4.2.5)], asymptotic average secrecy rate for FDJ protocol can be expressed in terms on the Meijer's G functions as

$$\begin{aligned} \bar{R}_0^{\mathsf{FD}} \approx \frac{1-\alpha}{\ln 2} &\int_0^\infty G_{11}^{11}\left(x \middle| \begin{matrix} 0 \\ 0 \end{matrix}\right) G_{22}^{22}\left(\frac{b_2}{b_1} x \;\middle|\; \begin{matrix} 0 & 1 \\ 1 & 1 \end{matrix}\right) \\ &\times G_{22}^{22}\left(\frac{c_5}{c_4} x \;\middle|\; \begin{matrix} 0 & 0 \\ 1 & 0 \end{matrix}\right) dx - \frac{1-\alpha}{\ln 2} \int_0^\infty G_{11}^{11}\left(x \middle| \begin{matrix} 0 \\ 0 \end{matrix}\right) \\ &\times G_{22}^{22}\left(\frac{b_2}{b_1} x \;\middle|\; \begin{matrix} 0 & 1 \\ 1 & 1 \end{matrix}\right) G_{10}^{01}\left(\kappa x \;\middle|\; \begin{matrix} 1 \\ - \end{matrix}\right) dx. \end{aligned} \tag{66}$$

To this end, by using the integral identity [41, Eq. (07.34.21.0081.01)] we obtain the desired result in (41).

## Appendix D
## Proof of Corollary 4

Let us denote $Y_3 = \frac{c_4 |h_{RD}|^2}{c_5 |h_{SJ}|^2 |h_{JD}|^2}$. Thus, the cdf of $\tilde{\gamma}_D^{\mathsf{HD}}$ can be expressed as

$$\begin{aligned} F_{\tilde{\gamma}_D^{\mathsf{HD}}}(z) &= \Pr\left(\underbrace{|h_{SR}|^2}_{X_0} \underbrace{\min(c_1, Y_3)}_{Y_4} < z\right), \\ &= \int_0^\infty F_{Y_4}\left(\frac{z}{x}\right) f_{X_0}(x) dx. \end{aligned} \tag{67}$$

Using simple algebraic calculations, the cdf of $Y_4$ can be obtained as

$$F_{Y_4}(y) = \begin{cases} 1 & \text{if } y \geq c_1; \\ 1 - \frac{c_4}{c_5 y} e^{\frac{c_4}{c_5 y}} E_1\left(\frac{c_4}{c_5 y}\right) & \text{if } y < c_1. \end{cases} \tag{68}$$

Substituting (68) and $f_{X_0}(x) = e^{-x} u(x)$ into (67) we get

$$F_{\tilde{\gamma}_D^{\mathsf{HD}}}(z) = 1 - \frac{c_4}{c_5 z} \int_{\frac{z}{c_1}}^\infty x e^{-x\left(1 - \frac{c_4}{c_5 z}\right)} E_1\left(\frac{c_4 x}{c_5 z}\right) dx. \tag{69}$$

With the help of the asymptotic expression for $E_n(x)$ [35, Eq. (5.1.51)], we have

$$\begin{aligned} F_{\tilde{\gamma}_D^{\mathsf{HD}}}(z) &\approx 1 - \int_{\frac{z}{c_1}}^\infty \left(e^{-x} - \frac{c_5 z}{x c_4} e^{-x} + \frac{2(c_5 z)^2}{x^2 c_4^2} e^{-x} \right. \\ &\quad \left. - \frac{6(c_5 z)^3}{x^3 c_4^3} e^{-x} + \cdots\right) dx \qquad (70)\\ &\approx 1 + e^{-\frac{z}{c_1}} - \sum_{n=1}^\infty \left(\frac{n!(c_5 z)^n (-1)^n}{c_4^n} \int_{\frac{z}{c_1}}^\infty \frac{e^{-x}}{x^n} dx\right). \end{aligned}$$

Finally, with the help of the identity [34, Eq. (3.351.4)], we can compute

$$F_{\tilde{\gamma}_D^{\mathsf{HD}}(z)} \approx 1 + e^{-\frac{z}{c_1}} - \sum_{n=1}^\infty \frac{n!(c_5 z)^n (-1)^n \mathcal{G}(n)}{c_4^n}, \tag{71}$$

where

$$\mathcal{G}(n) = (-1)^n \frac{\mathsf{Ei}\left(-\frac{z}{c_1}\right)}{(n-1)!} + \frac{e^{-\frac{z}{c_1}}}{\left(\frac{z}{c_1}\right)^{n-1}} \times \sum_{k=0}^{n-2} \frac{(-1)^k \left(\frac{z}{c_1}\right)^k}{(n-1)(n-2)\cdots(n-1-k)}.$$

## 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] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[4] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3359–3378, June 2014.

[5] 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.

[6] T. M. Hoang, T. Q. Duong, H. A. Suraweera, C. Tellambura, and H. V. Poor, "Cooperative beamforming and user selection for improving the security of relay-aided systems," *IEEE Trans. Commun.*, vol. 63, no. 12, pp. 5039–5051, Dec. 2015.

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

[8] 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.

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

[10] 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.

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

[12] H. M. Wang, M. Luo, Q. Yin, and X. G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

[13] T. Riihonen, S. Werner, and R. Wichman, "Hybrid full-duplex/half-duplex relaying with transmit power adaptation," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 3074–3085, Sept. 2011.

[14] I. Krikidis, H. A. Suraweera, P. J. Smith, and C. Yuen, "Full-duplex relay selection for amplify-and-forward cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 11, pp. 4381–4393, Dec. 2012.

[15] 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.

[16] 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.

[17] M. Mohammadi, H. A. Suraweera, Y. Cao, I. Krikidis, and C. Tellambura, "Full-duplex radio for uplink/downlink wireless access with spatially random nodes," *IEEE Trans. Commun.*, vol. 63, no. 12, pp. 5250–5266, 2015.

[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] D. Bharadia and S. Katti, "Full-duplex MIMO radios," in *Proc. 11th USENIX Symp. Networked Syst. Design and Implementation (NSDI '14)*, Seattle, WA, Apr. 2014, pp. 359–372.

[20] 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.

[21] 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.

[22] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.

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

[24] H. Chen, Y. Li, J. L. Rebelatto, B. F. Uchoa-Filho, and B. Vucetic, "Harvest-then-cooperate: Wireless-powered cooperative communications," *IEEE Trans. Signal Process.*, vol. 63, pp. 1700–1711, Apr. 2015.

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

[26] 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.

[27] I. Krikidis, S. Timotheou, S. Nikolaou, G. Zheng, D. W. K. Ng, and R. Schober, "Simultaneous wireless information and power transfer in modern communication systems," *IEEE Commun. Mag.*, vol. 52, no. 11, pp. 104–110, Nov. 2014.

[28] 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, July 2013.

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

[30] 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.

[31] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[32] H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou, "Power-constrained secrecy rate maximization for joint relay and jammer selection assisted wireless networks," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2180–2193, 2017.

[33] Z. Mobini, M. Mohammadi, and C. Tellambura, "Security enhancement of wireless networks with wireless-powered full-duplex relay and friendly jammer nodes," in *Proc. IEEE Int. Con. Commun. Workshops (ICC' 2017)*, Paris, France, May 2017, pp. 1329–1334.

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

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

[36] H. Xing, K. K. Wong, A. Nallanathan, and R. Zhang, "Wireless powered cooperative jamming for secrecy multi-AF relaying networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 7971–7984, Dec 2016.

[37] H. Q. Ngo, H. A. Suraweera, M. Matthaiou, and E. G. Larsson, "Multipair full-duplex relaying with massive arrays and linear processing," *IEEE J. Sel. Areas Commun.*, vol. 32, pp. 1721–1737, Sep. 2014.

[38] Y. Huang, J. Wang, C. Zhong, T. Q. Duong, and G. K. Karagiannidis, "Secure transmission in cooperative relaying networks with multiple antennas," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6843–6856, Oct 2016.

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

[40] 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.

[41] Wolfram. The Wolfram Functions Site, accessed on Aug. 15, 2016. [Online]. Available: http://functions.wolfram.com/.

[42] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637–1652, Sept. 2014.

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

[44] ——, *Integral and Series, vol. 3: More Special Functions*. Gordon and Breach, New York-London, 1990.

**Zahra Mobini** (S'09, M'15) received the B.S. degree in electrical engineering from Isfahan University of Technology, Isfahan, Iran, in 2006, and the M.S and Ph.D. degrees, both in electrical engineering, from the M. A. University of Technology and K. N. Toosi University of Technology, Tehran, Iran, respectively. From November 2010 to November 2011, she was a Visiting Researcher at the Research School of Engineering, Australian National University, Canberra, ACT, Australia. She is currently an Assistant Professor with the Faculty of Engineering, Shahrekord University, Shahrekord, Iran. Her research interests include wireless communication systems, cooperative networks, and network coding.

**Mohammadali Mohammadi** (S'09, M'15) received the B.S. degree in electrical engineering from the Isfahan University of Technology, Isfahan, Iran, in 2005, and the M.S. and Ph.D. degrees in electrical engineering from K. N. Toosi University of Technology, Tehran, Iran in 2007 and 2012, respectively. From November 2010 to November 2011, he was a visiting researcher in the Research School of Engineering, the Australian National University, Australia, working on cooperative networks. He is currently an assistant professor in the Faculty of Engineering, Shahrekord University, Iran. His main research interests include cooperative communications, energy harvesting and Green communications, full-duplex communications and stochastic geometry.

**Chintha Tellambura** (F'11) received the B.Sc. degree (with first-class honor) from the University of Moratuwa, Sri Lanka, the MSc degree in Electronics from King's College, University of London, United Kingdom, and the PhD degree in Electrical Engineering from the University of Victoria, Canada. He was with Monash University, Australia, from 1997 to 2002. Presently, he is a Professor with the Department of Electrical and Computer Engineering, University of Alberta. His current research interests include the design, modelling and analysis of cognitive radio, heterogeneous cellular networks, 5G wireless networks and machine learning algorithms.

Prof. Tellambura served as an editor for both IEEE Transactions on Communications (1999-2011) and IEEE Transactions on Wireless Communications (2001-2007) and for the latter he was the Area Editor for Wireless Communications Systems and Theory during 2007-2012. He has received best paper awards in the Communication Theory Symposium in 2012 IEEE International Conference on Communications (ICC) in Canada and 2017 ICC in France. He is the winner of the prestigious McCalla Professorship and the Killam Annual Professorship from the University of Alberta. In 2011, he was elected as an IEEE Fellow for his contributions to physical layer wireless communication theory. In 2017, he was elected as a Fellow of Canadian Academy of Engineering. He has authored or coauthored over 500 journal and conference papers with an h-index of 66 (Google Scholar).