Secrecy Capacity for Multi-Antenna Wireless-Powered AF Relaying Systems

Abdelhamid Salem, and Leila Musavian
School of Computer Science and Electronic Engineering, University of Essex, Colchester, UK.
Emails: {abdelhamid.salem, Leila.musavian}@essex.ac.uk.

***Abstract*—This paper analyzes the ergodic secrecy capacity of an energy-constrained multiple-antennas amplify-and-forward (AF) relaying system in the presence of a passive eavesdropper. In the first phase, the source broadcasts information signal, while the destination sends an artificial jamming signal. The jamming signal has two main purposes: 1) enhancing the system security; 2) increasing the energy harvesting (EH) at the relay node. In the second phase, the relay uses the harvested energy to amplify and forward the received signal to the destination. For this system model, explicit mathematical expressions for the ergodic secrecy capacity are derived for three different common EH-relaying protocols, namely, power splitting relaying (PSR), antenna selection and power splitting (ASPS) receiver, and ideal relaying receiver (IRR). Monte-Carlo simulations are included to validate the analysis and the effect of different parameters on the system security are investigated. The results show that, the ASPS receiver outperforms PSR in terms of secrecy capacity.**

I. Introduction

WIRELESS power transfer has attracted considerable attention in recent years. This idea is based on the fact that radio frequency (RF) signals are able to carry information and energy at the same time. This technique is called simultaneous wireless information and power transfer (SWIPT) [1], [2]. This technique is attractive for battery-limited devices which are hard to access, to recharge or to be replaced, for instance, sensor nodes operating in dangerous places. The concept of SWIPT technique was first introduced in [1], where a tradeoff between the rates at which reliable information and energy signals over a noisy channel was studied. Later, the effect of additive white Gaussian noise (AWGN) and frequency selective fading on SWIPT performance was investigated in [2]. These works, however, assumed that processing information and harvesting energy are achieved simultaneously from the same received signals by using an ideal receiver; this assumption might be unrealistic due to the practical limitations. On contrary, more practical receivers, namely, time switching (TS) and power splitting (PS) receivers were proposed in [3]. Moreover, the efficiency of wireless power transfer in SWIPT depends on the wireless channel characteristics, and therefore, using multiple-antennas and co-operative techniques can enhance the system performance [3]. For instance, the performance of an amplify-and-forward (AF) relay network, with an EH-relay node solely relying on RF EH was studied in [4] and [5], wherein different efficient EH-relaying protocols, i.e., power splitting relaying (PSR), time switching relaying (TSR), and antenna selection and power splitting (ASPS) receiver were proposed. On the other hand, recently there has been considerable interest in enhancing the physical layer security (PLS) in SWIPT networks. For instance, cooperative jamming technique was considered in [6] to enhance the security and EH of SWIPT systems. In addition, in our previous work in [7], a comparison between the TSR, and PSR was provided and we found that the PSR outperforms TSR in terms of the secrecy capacity.

In this paper, the secrecy of an EH multiple-antennas AF relaying system is investigated in terms of the secrecy capacity. Three common EH relaying protocols are considered, namely, PSR, ASPS and ideal relaying receiver (IRR). A cooperative jamming technique is used to enhance the system security and to increase the harvesting energy. To elaborate, the communication between the transmitter and the receiver is achieved in two phases. In phase I, while the transmitter sends the information signal, the receiver transmits an artificial noise (AN) signal; therefore, the relay can harvest energy from two different signals. In phase II, the relay amplifies and forwards the received signal to the destination by using the harvested energy from Phase I. Since the receiver has full knowledge of the AN signal and the system parameters, the AN component can be accurately eliminated from its received signal. The contribution of this work is as follows, firstly explicit mathematical expressions for the ergodic secrecy capacity of the PSR-, ASPS- and IRR-based systems of the proposed relaying model are derived. The analysis are confirmed by Monte-Carlo simulations. Further, we investigate the impact of different system parameters on the system security.

The notations used in this paper are: bold lowercase letters denote vectors. Transpose operation, and conjugate transpose are denoted by $(.)^{\dagger}$, and $(.)^{H}$, respectively. The notation $|.|$ represents the absolute value and $\|.\|$ denotes Euclidean norm. $\log_2(.)$ represents logarithm of base-2. Circularly symmetric, complex Gaussian distribution with mean μ and variance σ^2 is denoted by $\mathcal{CN}\left(\mu,\sigma^2\right)$; $\mathbb{E}(.)$ is expectation operation and $\in \mathbb{C}^{n\times m}$ represent $n\times m$ matrix.

II. System Model

We consider a wireless system model consisting of a single antenna source node, a single antenna legitimate receiver node and a multiple-antennas, N_r, AF relay node in the presence of a passive eavesdropper equipped with a single antenna, as shown in Fig. 1. In this system, the relay is EH-node and depends only on the harvested energy to amplify and forward the received signals to the destination, while the source and

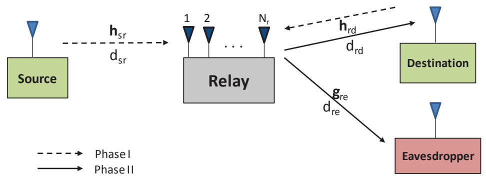


Figure 1: System model for energy-constrained multiple-antennas relay.

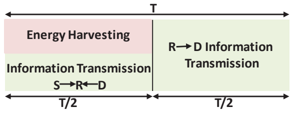


Figure 2: Frame structure of PSR protocol.

destination nodes both have fixed power supplies. The channel coefficients between the nodes are presented in Fig. 1, where $\mathbf{h}_{sr} \in \mathbb{C}^{N_r \times 1}$ denotes the channel vector between the source and relay node, $\mathbf{h}_{rd} \in \mathbb{C}^{1 \times N_r}$ is the channel vector between the relay and destination, and $\mathbf{g}_{re} \in \mathbb{C}^{1 \times N_r}$ denotes the channel vector between the relay and the eavesdropper. All channels are assumed to be quasi-static block fading, following a Rayleigh distribution magnitude with the forward-backward channels being symmetric. The distances between the nodes, i.e., source-to-relay, relay-to-destination, and relay-to-eavesdropper are denoted by d_{sr}, d_{rd} and d_{re}, respectively. We assume that the channel state information (CSI) of the legitimate system nodes are unknown at the eavesdropper [8] and the eavesdropper's CSI is unknown at the other nodes. Due to the deep shadowing, it is also assumed that all communications in the system are achieved through the relay and there are no direct links between the source and destination, and between the source and eavesdropper. This assumption has been extensively studied in literature for the cooperative systems [9].

In order to measure the system security, we consider the secrecy capacity, C_s, which is the maximum difference between the mutual information of the legitimate receiver and eavesdropper. Therefore, the ergodic secrecy capacity for the proposed system model is given by [10, page 4692]

$$\bar{C}_s = \left[\mathbb{E}\left(C_d\right) - \mathbb{E}\left(C_e\right)\right]^+ , \qquad (1)$$

where $[x]^+ =$ max $(0, x)$, C_d is the destination capacity, and C_e is the eavesdropper capacity. The ergodic secrecy capacity for the PSR, ASPS and IRR protocols are derived in the following sections.

III. Power Splitting Relaying (PSR)

Fig. 2 illustrates frame structure for the PSR protocol, where T is the total block time. Half of this time, $T/2$, is used for information transmission from the transmitter to the relay and the other half is used for information transmission from the relay to the receiver. In the first half, a part of the received signal power, ρP, is used for EH and the other part, $(1-\rho)\,P$, is allocated for the information transmission, with $0 \leq \rho \leq 1$. During the second time slot, the relay consumes all the harvested energy to amplify and forward the received signal to the destination. Consequently, the received signal at the input of EH receiver of the relay is

$$\mathbf{y}_{r_{EH}} = \sqrt{\frac{\rho\, P_s}{d_{sr}^m}}\mathbf{h}_{sr} s + \sqrt{\frac{\rho\, P_d}{d_{rd}^m}}\mathbf{h}_{rd}^{\dagger}\upsilon_d + \sqrt{\rho}\mathbf{n}_a, \qquad (2)$$

where s is the transmitted signal from the source with, $\mathbb{E}\left[|s|^2\right] = 1$, P_s is the source power, υ_d is the AN signal transmitted by the legitimate receiver, $\mathbb{E}\left[|\upsilon_d|^2\right] = 1$, P_d is the destination power, m is the path loss exponent and $\mathbf{n}_a \sim \mathcal{CN}\left(0,\, \sigma_a^2 \mathbf{I}_{N_r}\right)$ is the AWGN vector introduced by the receiver antennas at the relay [5]. From (2), the energy harvested, E_h, at the relay node is given by [7]

$$E_h = \frac{\eta\,\rho\,T}{2}\left[\frac{P_s}{d_{sr}^m}\left\|\mathbf{h}_{sr}\right\|^2 + \frac{P_d}{d_{rd}^m}\left\|\mathbf{h}_{rd}\right\|^2 + N_r\sigma_a^2\right]. \qquad (3)$$

where $0 < \eta \leq 1$ is the EH efficiency. The signal at the relay's information receiver can be expressed by

$$\mathbf{y}_r = \sqrt{\frac{(1-\rho)\,P_s}{d_{sr}^m}}\,\mathbf{h}_{sr} s + \sqrt{\frac{(1-\rho)\,P_d}{d_{rd}^m}}\,\mathbf{h}_{rd}^{\dagger}\upsilon_d + \mathbf{n}_r, \qquad (4)$$

where $\mathbf{n}_r \sim \mathcal{CN}\left(0,\, \sigma_r^2 \mathbf{I}_{N_r}\right)$ is an $N_r \times 1$ AWGN vector at the relay, and is given by $\mathbf{n}_r = \sqrt{1-\rho}\mathbf{n}_a + \mathbf{n}_c$, while $\mathbf{n}_c \sim \mathcal{CN}\left(0,\, \sigma_c^2 \mathbf{I}_{N_r}\right)$ denotes the noise vector introduced by the information receiver [4], [5]. The transmitted signal by the relay in the second phase is, $\mathbf{x}_r = G\,\mathbf{y}_r$, where $G = \sqrt{P_r \beta_p}$ denotes the relay gain, P_r is the relay power and $\beta_p = \left(\frac{(1-\rho)P_s}{d_{sr}^m}\left\|\mathbf{h}_{sr}\right\|^2 + \frac{(1-\rho)P_d}{d_{rd}^m}\left\|\mathbf{h}_{rd}\right\|^2 + N_r\sigma_r^2\right)^{-1}$. Since the legitimate receiver has full knowledge of the AN signal and the system parameters, i.e., the distance between the nodes, the channel coefficients, and the relay gain, the AN term can be easily eliminated at the destination; as a result, the received signal at the destination, y_d, can be written as [8]

$$y_d = \sqrt{\frac{(1-\rho)\,P_s P_r \beta_p}{d_{sr}^m d_{rd}^m}}\mathbf{h}_{rd}\mathbf{h}_{sr}\, s + \frac{\sqrt{P_r\beta_p}\mathbf{h}_{rd}}{\sqrt{d_{rd}^m}}\mathbf{n}_r + n_d. \qquad (5)$$

where n_d is AWGN at the destination with variance σ_d^2. On the other side, the received signal at the eavesdropper is given by [8]

$$y_e = \sqrt{\frac{(1-\rho)\,P_s P_r \beta_p}{d_{sr}^m d_{re}^m}}\mathbf{g}_{re}\,\mathbf{h}_{sr}\, s + \frac{\sqrt{(1-\rho)\,P_d P_r \beta_p}}{\sqrt{d_{rd}^m d_{re}^m}}\mathbf{g}_{re}\mathbf{h}_{rd}^{\dagger}\,\upsilon_d + \frac{\sqrt{P_r\beta_p}\mathbf{g}_{re}}{\sqrt{d_{re}^m}}\,\mathbf{n}_r + n_e. \qquad (6)$$

The relay power is calculated as $P_r = \frac{E_h}{T/2}$. By using (3), P_r can be written as $P_r = \eta\,\rho\left[\frac{P_s}{d_{sr}^m}\left\|\mathbf{h}_{sr}\right\|^2 + \frac{P_d}{d_{rd}^m}\left\|\mathbf{h}_{rd}\right\|^2 + N_r\sigma_a^2\right]$. By substituting P_r into (5) and (6), it is easy to find the signal-to-interference noise ratios (SINRs) at the destination and the eavesdropper nodes, respectively, as,

$$\gamma_d = \frac{a \left|\mathbf{h}_{rd}\mathbf{h}_{sr}\right|^2}{b \left\|\mathbf{h}_{rd}\right\|^2 + c \left\|\mathbf{h}_{rd}\right\|^2 + r}, \tag{7}$$

$$\gamma_e = \frac{a_1 \left|\mathbf{g}_{re}\mathbf{h}_{sr}\right|^2}{b_1 \left|\mathbf{g}_{re}\mathbf{h}_{rd}^{\dagger}\right|^2 + c_1 \left\|\mathbf{g}_{re}\right\|^2 + r_1 \left\|\mathbf{g}_{re}\right\|^2 + \omega}, \tag{8}$$

where $a = \eta\,\rho\,(1-\rho)\,P_s$, $b = \eta\,\rho\,d_{sr}^m\sigma_c^2$, $c = \eta\,\rho\,(1-\rho)\;d_{sr}^m\sigma_a^2$, $r = (1-\rho)\;d_{sr}^m d_{rd}^m\sigma_d^2$, $a_1 = \eta\,\rho\,(1-\rho)\,P_s d_{rd}^m$, $b_1 = \eta\,\rho\,(1-\rho)\;d_{sr}^m P_d$, $c_1 = \eta\,\rho\,(1-\rho)\,d_{sr}^m d_{rd}^m\sigma_a^2$, $r_1 = \eta\,\rho\,d_{sr}^m d_{rd}^m\sigma_c^2$ and $\omega = (1-\rho)\;d_{sr}^m d_{rd}^m d_{re}^m\sigma_e^2$.

Theorem 1. *The ergodic secrecy capacity for the PSR protocol is given by*

$$\bar{C}_s^{[PSR]} = \left[\mathbb{E}\left[C_d^{PSR}\right] - \mathbb{E}\left[C_e^{PSR}\right]\right]^+, \tag{9}$$

where $\mathbb{E}\left[C_d^{PSR}\right]$ and $\mathbb{E}\left[C_d^{PSR}\right]$ are given, respectively, by (10) and (12), shown at the top of the next page, which can be approximated using Gaussian Quadrature rule as in (11) and (13) where z_i and H_i are the i^{th} zero and the weighting factor of the Laguerre polynomials, respectively, [11].

Proof: To start with (7) can be written as $\gamma_d = \frac{X}{b+c+Y}$, where $X = a\frac{\left|\mathbf{h}_{rd}\mathbf{h}_{sr}\right|^2}{\left\|\mathbf{h}_{rd}\right\|^2}$ and $Y = \frac{r}{\left\|\mathbf{h}_{rd}\right\|^2}$. Consequently, the ergodic capacity at the destination can be given as

$$\mathbb{E}\left[C_d^{PSR}\right] = \frac{1}{2}\,\mathbb{E}\left[\log_2\left(1 + \frac{X}{b+c+Y}\right)\right]. \tag{14}$$

From [12], the ergodic capacity for any random variables x, $y > 0$, can be calculated by

$$\mathbb{E}\left[\ln\left(1 + \frac{x}{y}\right)\right] = \int_0^\infty \frac{1}{z}\left(\mathcal{M}_y(z) - \mathcal{M}_{y+x}(z)\right)dz, \tag{15}$$

where $\mathcal{M}_x(z)$ is the moment generating function (MGF) of the random variable x. Therefore, (14) can be rewritten as

$$\mathbb{E}\left[C_d^{PSR}\right] = \frac{1}{2\,\ln(2)}\int_0^\infty \frac{1}{z}\mathcal{M}_{b+c+Y}(z)\left(1 - \mathcal{M}_X(z)\right)dz. \tag{16}$$

Conditioned on $\mathbf{h}_{rd}$, X has exponential distribution with parameter $\lambda_x > 0$ [7], its MGF is, $\mathcal{M}_X(z) = \frac{\lambda_x}{\lambda_x + (az)}$. Since the random variable $\left\|\mathbf{h}_{rd}\right\|^2$ follows chi-square distribution, the MGF of, $b + c + Y$ can be written as, $\mathcal{M}_{b+c+Y}(z) = \frac{2\,e^{-(b+c)}\,(r\,z)^{N_r/2}\,K_{N_r}\left(2\sqrt{r\,z}\right)}{\Gamma(N_r)}$, where $\Gamma(.)$ denotes the Gamma function and $K_{N_r}(.)$ is the N_r^{th} order modified Bessel function of the second kind. By substituting $\mathcal{M}_X(z)$ and $\mathcal{M}_{b+c+Y}(z)$ into (16), we can find the destination ergodic capacity as in (10). Following similar steps, we can find the ergodic capacity at the eavesdropper as in (12). ■

IV. Antenna Selection and Power Splitting Receiver (ASPS)

In ASPS receiver, the N_r antennas are divided into two groups and the received signal at the relay $\mathbf{y}_r$ is divided into two sub-signals: $\mathbf{y}_{r_A}$and $\mathbf{y}_{r_B}$. The first antennas group (1 to n) is used to harvest energy and forward signals by PS technique, where a fraction of the received sub-signal power $\lambda\,P$, $0 \leq \lambda \leq 1$, is allocated for EH and the remaining power, $(1-\lambda)\,P$, is allocated for the information transmission. The second antennas group (n+1 to N_r) are used only for EH. Our investigation in this paper is based on[1], $n = \frac{N_r}{2}$. Therefore, in the first phase, the received signal at the relay is expressed by

$$\mathbf{y}_r = \sqrt{\frac{P_s}{d_{sr}^m}}\mathbf{h}_{sr}s + \sqrt{\frac{P_d}{d_{rd}^m}}\mathbf{h}_{rd}^{\dagger}\upsilon_d + \mathbf{n}_a, \tag{17}$$

where $\mathbf{y}_r = \left[y_{r1}, y_{r_2}, \ldots.., y_{r_{N_r}}\right]^{\dagger}$. The harvested power from $\mathbf{y}_r$ is hence given by

$$P_r = \eta\left[\frac{P_s}{d_{sr}^m}\left(\lambda\sum_{i=1}^{n}\left|h_{sri}\right|^2 + \sum_{i=n+1}^{N_r}\left|h_{sri}\right|^2\right) + \frac{P_d}{d_{rd}^m}\left(\lambda\sum_{i=1}^{n}\left|h_{rdi}\right|^2 + \sum_{i=n+1}^{N_r}\left|h_{rdi}\right|^2\right)\right], \tag{18}$$

where h_{sri} is the channel between the source and antenna i and h_{rdi} is the channel between the destination and Antenna i. During the second phase, the relay forwards the signal, $\mathbf{x}_r = G\left(\sqrt{1-\lambda}\mathbf{y}_{r_A} + \mathbf{n}_c\right)$, where $\mathbf{y}_{r_A} = \left[y_{r1}, y_{r_2}, \ldots.., y_{r_n}\right]^{\dagger}$and $G = \sqrt{P_r\beta_p}$ and $\beta_p = \left(\frac{(1-\lambda)P_s\sum_{i=1}^{n}\left|h_{sri}\right|^2}{d_{sr}^m} + \frac{(1-\lambda)P_d\sum_{i=1}^{n}\left|h_{rdi}\right|^2}{d_{rd}^m} + N_r\sigma_c^2\right)^{-1}$. The received signal at the destination after removing the AN can be written as

$$y_d = \sqrt{\frac{(1-\lambda)\,P_sP_r\beta_p}{d_{sr}^m d_{rd}^m}}\mathbf{h}_{rd,1}\mathbf{h}_{sr,1}\,s + \frac{\sqrt{P_r\beta_p}}{\sqrt{d_{rd}^m}}\mathbf{h}_{rd,1}\mathbf{n}_r + n_d, \tag{19}$$

where $\mathbf{h}_{sr,1}$ is the channel vector between the source and the first antennas group, $\mathbf{h}_{rd,1}$ is the channel vector between the destination and the first antennas group and $\mathbf{n}_r = (1-\lambda)\,\mathbf{n}_a + \mathbf{n}_c$. The received signal at the eavesdropper is hence given by

$$y_e = \sqrt{\frac{(1-\lambda)\,P_sP_r\beta_p}{d_{sr}^m d_{re}^m}}\mathbf{g}_{re1}\mathbf{h}_{sr,1}s + \sqrt{\frac{(1-\lambda)\,P_dP_r\beta_p}{d_{rd}^m d_{re}^m}}\mathbf{g}_{re1}\mathbf{h}_{rd,1}\upsilon_d + \frac{\sqrt{P_r\beta_p}}{\sqrt{d_{re}^m}}\mathbf{g}_{re1}\mathbf{n}_r + n_e, \tag{20}$$

where $\mathbf{g}_{re1}$ is the channel vector between the eavesdropper and the first antennas group. Substituting (18) into (19) and (20), we can obtain the SINRs at the destination and the

[1] For more details about ASPS receiver, please refer to [5].

$$\mathbb{E}\left[C_d^{PSR}\right] = \frac{1}{2\,\ln(2)}\int_0^\infty \frac{1}{z}\left(1-\frac{\lambda_x}{\lambda_x+az}\right)\,\frac{2\,e^{-z(b+c)}\,(r\,z)^{N_r/2}\,K_{N_r}\left(2\sqrt{r\,z}\right)}{\Gamma\left(N_r\right)}dz. \tag{10}$$

$$\mathbb{E}\left[C_d^{PSR}\right] \approx \frac{1}{2\ln(2)}\,\sum_{i=1}^{n}\frac{\mathrm{H}_i}{z_i}\left(1-\frac{\lambda_x\,(b+c)}{(b+c)\,\lambda_x+az_i}\right)\,\frac{2\,\left(\frac{r\,z_i}{(b+c)}\right)^{N_r/2}\,K_{N_r}\left(2\sqrt{\frac{r\,z_i}{(b+c)}}\right)}{\Gamma\left(N_r\right)} \tag{11}$$

$$\mathbb{E}\left[C_e^{PSR}\right] = \frac{1}{2\,\ln(2)}\int_0^\infty \frac{1}{z}\left(1-\frac{\lambda_\Phi}{\lambda_\Phi+a_1z}\right)e^{-z(c_1+r_1)}\left(\frac{\lambda_\Upsilon}{\lambda_\Upsilon+b_1z}\right)\,\frac{2\,\left(\omega\,z\right)^{N_r/2}\,K_{N_r}\left(2\sqrt{\omega\,z}\right)}{\Gamma\left(N_r\right)}dz. \tag{12}$$

$$\mathbb{E}\left[C_e^{PSR}\right] \approx \frac{1}{2\ln(2)}\,\sum_{i=1}^{n}\frac{\mathrm{H}_i}{z_i}\left(1-\frac{\lambda_\Phi\,(c_1+r_1)}{(c_1+r_1)\,\lambda_\Phi+a_1z_i}\right)\left(\frac{\lambda_\Upsilon\,(c_1+r_1)}{\lambda_\Upsilon\,(c_1+r_1)+b_1z_i}\right)\frac{2\,\left(\frac{\omega\,z_i}{(c_1+r_1)}\right)^{N_r/2}\,K_{N_r}\left(2\sqrt{\frac{\omega\,z_i}{(c_1+r_1)}}\right)}{\Gamma\left(N_r\right)} \tag{13}$$

eavesdropper nodes, respectively, as $\gamma_d = \frac{a_1|\mathbf{h}_{rd,1}\mathbf{h}_{sr,1}|^2}{a_2\|\mathbf{h}_{rd,1}\|^2+a_3}$, and $\gamma_e = \frac{b_1|\mathbf{g}_{re1}\mathbf{h}_{sr,1}|^2}{b_2|\mathbf{g}_{re1}\mathbf{h}_{rd,1}|^2+b_3\|\mathbf{g}_{re1}\|^2+b_4}$, where $a_1 = (1-\lambda)\,P_sP_r\beta_p$, $a_2 = P_r\beta_p\,d_{sr}^m\sigma_r^2$, $a_3 = d_{sr}^m d_{rd}^m\sigma_d^2$, $b_1 = (1-\lambda)\,P_sP_r\beta_p d_{rd}^m$, $b_2 = (1-\lambda)\,P_dP_r\beta_p\,d_{sr}^m$, $b_3 = P_r\beta_p\,\sigma_r^2\,d_{sr}^m d_{rd}^m$, $b_4 = d_{sr}^m d_{rd}^m d_{re}^m\sigma_e^2$ and $\sigma_r^2 = (1-\lambda)\,\sigma_a^2+\sigma_c^2$. For simplicity in this scheme we derive the ergodic secrecy capacity in interference limited (Int-Lim) systems.

Theorem 2. *The ergodic secrecy capacity for the ASPS receiver in interference limited systems can be obtained by*

$$\bar{C}_s^{[ASPS]} = \left[\mathbb{E}\left[C_d^{ASPS}\right]-\mathbb{E}\left[C_e^{ASPS}\right]\right]^+, \tag{21}$$

where $\mathbb{E}\left[C_d^{ASPS}\right]$ is given by,

$$\mathbb{E}\left[C_d^{ASPS}\right] = \frac{1}{2\,\ln(2)}\int_0^\infty \frac{1}{z}\left(1-\frac{\lambda_\chi}{\lambda_\chi+a_1z}\right)e^{-z\,a_2}dz \tag{22}$$

$$\mathbb{E}\left[C_d^{ASPS}\right] \approx \frac{1}{2\,\ln(2)}\sum_{i=1}^{n}\frac{\mathrm{H}_i}{z_i}\left(1-\frac{\lambda_\chi a_2}{\lambda_\chi a_2+a_1z_i}\right) \tag{23}$$

and $\mathbb{E}\left[C_d^{ASPS}\right]$ is given as in (24) and (25).

Proof: To start with, the SINR at the destination can be simplified as, $\gamma_d = \frac{\chi}{a_2+\Upsilon}$, where $\chi = \frac{a_1|\mathbf{h}_{rd,1}\mathbf{h}_{sr,1}|^2}{\|\mathbf{h}_{rd,1}\|^2}$, $\Upsilon = \frac{a_3}{\|\mathbf{h}_{rd,1}\|^2}$. For simplicity in this scheme we derived the ergodic capacities in Int-Lim systems. Using (15), we can write the ergodic capacity as, $\mathbb{E}\left[C_d^{ASPS}\right] = \frac{1}{2\,\ln(2)}\int_0^\infty \frac{1}{z}\left(1-\mathcal{M}_\chi(z)\right)\mathcal{M}_{a_2}(z)\,dz$, where $\mathcal{M}_\chi(z) = \frac{\lambda_\chi}{\lambda_\chi+(a_1\times z)}$, $\mathcal{M}_{a_2}(z) = e^{-z\,a_2}$. Following similar steps, we can find the ergodic capacity at the eavesdropper as in (24). ■

V. Ideal Relaying Receiver (IRR)

In IRR, during the first time slot, $T/2$, the relay harvests the energy and process information and in the second time slot, $T/2$, the relay amplifies and forwards the received signal by using the harvested energy. The relay power can be written as, $P_r = \eta\left[\frac{P_s}{d_{sr}^m}\|\mathbf{h}_{sr}\|^2+\frac{P_d}{d_{rd}^m}\|\mathbf{h}_{rd}\|^2+N_r\sigma_a^2\right]$. The received signals at the legitimate receiver and the eavesdropper, respectively, are

$$y_d = \sqrt{\frac{P_sP_r\beta_i}{d_{sr}^m d_{rd}^m}}\mathbf{h}_{rd}\mathbf{h}_{sr}\,s+\sqrt{\frac{P_r\beta_i}{d_{rd}^m}}\mathbf{h}_{rd}\mathbf{n}_r+n_d, \tag{26}$$

and

$$y_e = \sqrt{\frac{P_sP_r\beta_i}{d_{sr}^m d_{re}^m}}\mathbf{g}_{re}\mathbf{h}_{sr}s+\sqrt{\frac{P_dP_r\beta_i}{d_{rd}^m d_{re}^m}}\mathbf{g}_{re}\mathbf{h}_{rd}^\dagger\upsilon_d + \sqrt{\frac{P_r\beta_i}{d_{re}^m}}\mathbf{g}_{re}\mathbf{n}_r+n_e \tag{27}$$

where $\beta_i = \left(\frac{P_s}{d_{sr}^m}\|\mathbf{h}_{sr}\|^2+\frac{P_d}{d_{rd}^m}\|\mathbf{h}_{rd}\|^2+N_r\sigma_r^2\right)^{-1}$. By substituting P_r into (26) and (27), the SINR expressions at the destination and eavesdropper, respectively, are $\gamma_d = \frac{a|\mathbf{h}_{rd}\mathbf{h}_{sr}|^2}{b\|\mathbf{h}_{rd}\|^2+c}$, and $\gamma_e = \frac{a_1|\mathbf{g}_{re}\mathbf{h}_{sr}|^2}{b_1\left|\mathbf{g}_{re}\mathbf{h}_{rd}^\dagger\right|^2+c_1\|\mathbf{g}_{re}\|^2+r_1}$, where $a = \eta\,P_s$, $b = \eta\,d_{sr}^m\sigma_r^2$, $c = d_{sr}^m d_{rd}^m\sigma_d^2$, $a_1 = \eta\,P_sd_{rd}^m$, $b_1 = \eta\,d_{sr}^mP_d$, $c_1 = \eta\,\sigma_r^2\,d_{sr}^m d_{rd}^m$, $r_1 = d_{sr}^m d_{rd}^m d_{re}^m\sigma_e^2$.

Theorem 3. *The ergodic secrecy capacity for the IRR can be given by*

$$\bar{C}_s^{[IRR]} = \left[\mathbb{E}\left[C_d^{IRR}\right]-\mathbb{E}\left[C_e^{IRR}\right]\right]^+, \tag{28}$$

where $\mathbb{E}\left[C_d^{IRR}\right]$ and $\mathbb{E}\left[C_e^{IRR}\right]$ are given in (29) and (31), respectively, which can be approximated using Gaussian Quadrature rule as in (30) and (32), respectively, [11].

Proof: To start with the SINR at the destination can be written as $\gamma_d = \frac{X}{b+Y}$, where $X = a\frac{|\mathbf{h}_{rd}\mathbf{h}_{sr}|^2}{\|\mathbf{h}_{rd}\|^2}$ and $Y = \frac{c}{\|\mathbf{h}_{rd}\|^2}$. From (15), we can write, $\mathbb{E}\left[C_d^{IRR}\right] = \frac{1}{2\,\ln(2)}\int_0^\infty \frac{\mathcal{M}_{b+Y}(z)}{z}\left(1-\mathcal{M}_X(z)\right)dz$, where $\mathcal{M}_X(z) = \frac{\lambda_x}{\lambda_x+a\,z}$

$$\mathbb{E}\left[C_e^{ASPS}\right] = \frac{1}{2\,\ln(2)}\int_0^\infty \frac{e^{-zb_3}}{z}\left(1-\frac{\lambda_\chi}{\lambda_\chi+b_1 z}\right)\left(\frac{\lambda_y}{\lambda_y+b_2 z}\right)dz \tag{24}$$

$$\mathbb{E}\left[C_e^{ASPS}\right] \approx \frac{1}{2\,\ln(2)}\sum_{i=1}^{n}\frac{\mathrm{H}_i}{z_i}\left(1-\frac{\lambda_\chi b_3}{\lambda_\chi b_3+b_1 z_i}\right)\left(\frac{\lambda_y b_3}{\lambda_y b_3+b_2 z_i}\right) \tag{25}$$

$$\mathbb{E}\left[C_d^{IRR}\right] = \frac{1}{2\,\ln(2)}\int_0^\infty \frac{1}{z}\left(1-\frac{\lambda_x}{\lambda_x+a\,z}\right)\frac{2e^{-zb}\,\left(c\,z\right)^{N_r/2}\,K_{N_r}\left(2\sqrt{c\,z}\right)}{\Gamma\left(N_r\right)}dz. \tag{29}$$

$$\mathbb{E}\left[C_d^{IRR}\right] \approx \frac{1}{2\,\ln(2)}\sum_{i=1}^{n}\frac{\mathrm{H}_i}{z_i}\left(1-\frac{\lambda_x b}{\lambda_x b+a\,z_i}\right)\frac{2\,\left(\frac{c\,z_i}{b}\right)^{N_r/2}\,K_{N_r}\left(2\sqrt{\frac{c\,z_i}{b}}\right)}{\Gamma\left(N_r\right)}. \tag{30}$$

$$\mathbb{E}\left[C_e^{IRR}\right] = \frac{1}{2\,\ln(2)}\int_0^\infty \frac{e^{-zc_1}}{z}\left(1-\frac{\lambda_\Phi}{\lambda_\Phi+a_1\,z}\right)\frac{\lambda_\Upsilon}{\lambda_\Upsilon+b_1 z}\,\frac{2\,\left(r_1\,z\right)^{N_r/2}\,K_{N_r}\left(2\sqrt{r_1\,z}\right)}{\Gamma\left(N_r\right)}dz. \tag{31}$$

$$\mathbb{E}\left[C_e^{IRR}\right] \approx \frac{1}{2\,\ln(2)}\sum_{i=1}^{n}\frac{\mathrm{H}_i}{z_i}\left(1-\frac{\lambda_\Phi c_1}{\lambda_\Phi c_1+a_1\,z_i}\right)\frac{\lambda_\Upsilon c_1}{\lambda_\Upsilon c_1+b_1 z_i}\,\frac{2\,\left(\frac{r_1\,z_i}{c_1}\right)^{N_r/2}\,K_{N_r}\left(2\sqrt{\frac{r_1\,z_i}{c_1}}\right)}{\Gamma\left(N_r\right)}dz. \tag{32}$$

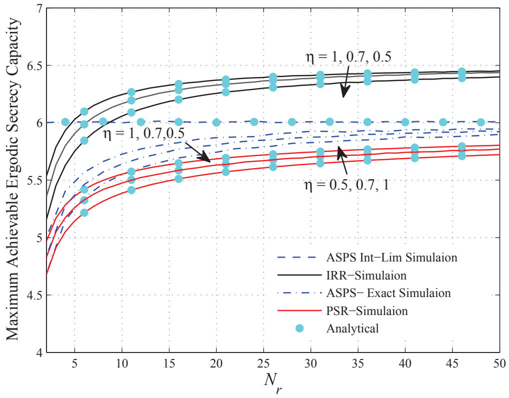


Figure 3: The maximum achievable ergodic secrecy capacity versus N_r for different values of η (Int-Lim denotes interference limited system).

, and $\mathcal{M}_{b+Y}\left(z\right) = \frac{2\,e^{-zb}\left(c\,z\right)^{N_r/2}K_{N_r}\left(2\sqrt{c\,z}\right)}{\Gamma\left(N_r\right)}$. Following similar steps, we can find the ergodic capacity at the eavesdropper as in (31).

■

VI. Numerical results

In this section, we present some numerical results to evaluate the analytical expressions derived and to investigate the effect of the main system parameters on the secrecy capacity. Unless stated otherwise, the distances d_{sr}, d_{rd} and d_{re} are normalized to unity, $\eta = 1$, $P_s = 30$ dBm, $P_d = 30$ dBm, and $m = 2.7$. For simplicity and without loss of generality, the noise variances at all the nodes are equal $\sigma_r = \sigma_d = \sigma_e = 10$ dBm and $\sigma_a = \sigma_c = \sigma_r/2$; also all the channel parameters λ_x, λ_χ, λ_Φ, λ_y and λ_Υ are set to 1.

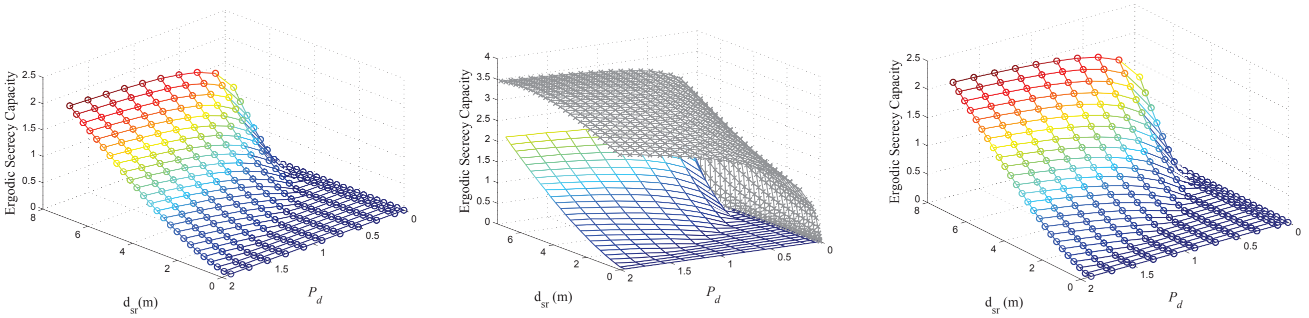
A. Effect of Relay Antennas and EH-Efficiency

In Fig. 3, the maximum achievable ergodic secrecy capacity is plotted with respect to the number of relay antennas, N_r, for various values of η. From these results, it is clearly visible that the IRR outperforms the ASPS and PSR in terms of the ergodic secrecy capacity for same system parameters values. It can also be seen that, for all systems, C_s enhances when either η or N_r increases and this is because increasing η and/or N_r will always reduce the optimal values of ρ and λ, which is expected since higher values of η or N_r means that more amount of energy can be harvested with smaller power ratios for PSR and ASPS. Therefore, smaller values of ρ and λ are required to attain the optimal system performance.

B. Effect of Relay/Eavesdropper Locations and AN Power

In order to investigate the effect of the relay/eavesdropper locations and the AN power, P_d, on the system secrecy, we study a simple one-dimensional model. In this simple model, the legitimate receiver is placed at (10, 0) meter away from the source (0, 0) meter whilst the relay and the eavesdropper positions are varied.

1) Effect of Relay Location and AN Power: Firstly, the eavesdropper is located at (7.5,0) meter and the relay position varies from (0, 0) meter to (7.5, 0) meter. Fig. 4 depicts a 3D surface plot for the ergodic secrecy capacity versus d_{sr} and P_d for the three protocols when ρ and λ are optimized. In this figure we adopt the following system parameters $N_r = 8$ and $P_s = 35$ dBm. The common observation in the three schemes is that, when the relay node is close to the source, the optimal secrecy capacity is at its minimum and the optimal secrecy capacity enhances as the relay node moves away toward the legitimate receiver. This is because when the relay is far away from the legitimate receiver, the received AN signal at the relay

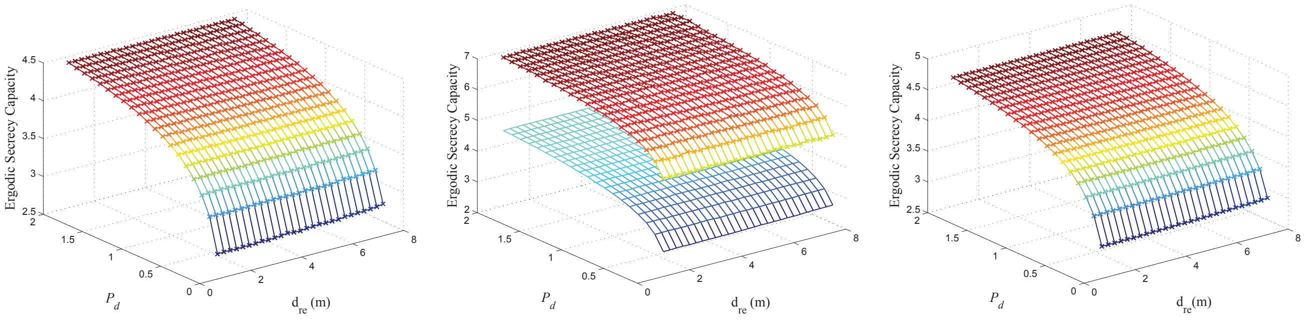


(a) PSR.

(b) ASPS Exact (the lower) and Int-Lim (the upper).

(c) IRR.

Figure 4: Optimal secrecy capacity versus d_{sr} and P_d for the PSR, ASPS and IRR-based systems (markers represent numerical results).



(a) PSR.

(b) ASPS Exact (the lower) and Int-Lim (the upper).

(c) IRR.

Figure 5: Optimal secrecy capacity versus d_{re} and P_d for the PSR, ASPS and IRR-based systems (markers represent numerical results).

in the first phase will be weak. As a consequence of this, the AN signal cannot provide high protection for the information signal in the second phase.

2) Effect of Eavesdropper Location and AN Power: In the second scenario, we fix the relay position at (5, 0) meter and the eavesdropper position varies from (6,0) meter to (13, 0) meter. Fig. 5 represents a 3D surface plot for the ergodic secrecy capacity versus d_{re} and P_d for the three protocols when ρ and λ are optimized. To be able to explain this impact more clearly, we reduce the noise variance to $\sigma_r = \sigma_d = \sigma_e = 0$ dBm. As we can see from the figure now, the secrecy capacity enhances slightly as the eavesdropper moves away from the relay in all the EH schemes.

Finally, from the two scenarios it is clearly visible that increasing the AN power will always improve the system secrecy; Its benefit is more obvious in IRR scheme.

VII. Conclusion

In this paper, we have investigated physical layer security for EH-based AF relaying system. Three common EH protocols, namely, PSR, ASPS and IRR have been studied. For each EH-protocol, we derived explicit mathematical expressions for the ergodic secrecy capacity. Results have shown that, the ergodic secrecy capacity always improves as the relay antennas, the distance from the relay-to-the source/eavesdropper, and/or AN power increase.

References

[1] L. Varshney, “Transporting information and energy simultaneously,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 1612–1616, Jul. 2008.

[2] P. Grover and A. Sahai, “Shannon meets tesla: Wireless information and power transfer,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 2363–2367, Jun. 2010.

[3] R. Zhang and C. K. Ho, “MIMO broadcasting for simultaneous wireless information and power transfer,” *IEEE Trans. Wireless Commun.*, vol. 12, pp. 1989–2001, May 2013.

[4] A. Nasir, X. Zhou, S. Durrani, and R. Kennedy, “Relaying protocols for wireless energy harvesting and information processing,” *IEEE Wireless Commun.*, vol. 12, pp. 3622–3636, Jul. 2013.

[5] Z. Zhou, M. Peng, Z. Zhao, and Y. Li, “Joint power splitting and antenna selection in energy harvesting relay channels,” *IEEE Signal Process. Lett*, vol. 22, pp. 823–827, July 2015.

[6] Q. Zhang, X. Huang, Q. Li, and J. Qin, “Cooperative jamming aided robust secure transmission for wireless information and power transfer in miso channels,” *IEEE Trans. Commun.*, vol. 63, pp. 906–915, March 2015.

[7] A. Salem, K. A. Hamdi, and K. M. Rabie, “Physical layer security with rf energy harvesting in af multi antenna relaying networks,” in *submitted to TCOM IEEE*.

[8] K.-H. Park, T. Wang, and M.-S. Alouini, “On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming,” *IEEE J. Sel. Areas Commun.*, vol. 31, pp. 1741–1750, September 2013.

[9] Y. Zou, X. Wang, and W. Shen, “Optimal relay selection for physical-layer security in cooperative wireless networks,” *IEEE J.Sel. Areas Commun.*, vol. 31, pp. 2099–2111, October 2013.

[10] P. K. Gopala, L. Lai, and H. El Gamal, “On the secrecy capacity of fading channels,” *IEEE Trans. Inf. Theory*, vol. 54, pp. 4687–4698, Oct. 2008.

[11] I. S. G. . I. M. Ryzhik, *Table of Integrals, Series, and Products*. 1980.

[12] K. Hamdi, “A useful lemma for capacity analysis of fading interference channels,” *IEEE Trans. Commun.*, vol. 58, pp. 411–416, Feb. 2010.