Physical Layer Security with RF Energy Harvesting in AF Multi Antenna Relaying Networks

DOI:
10.1109/TCOMM.2016.2573829

Document Version
Accepted author manuscript

Citation for published version (APA):
Salem, A., Hamdi, K., & Rabie, K. M. (2016). Physical Layer Security with RF Energy Harvesting in AF Multi Antenna Relaying Networks. *I E E E Transactions on Communications*, *64*(7), 3025-3038. https://doi.org/10.1109/TCOMM.2016.2573829

Published in:
I E E E Transactions on Communications

Physical Layer Security with RF Energy Harvesting in AF Multi-Antenna Relaying Networks

Abdelhamid Salem, *Student Member, IEEE*, Khairi Ashour Hamdi, *Senior Member, IEEE* and Khaled M. Rabie, *Member, IEEE.*

***Abstract*—In this paper we analyze the secrecy capacity of a half-duplex energy harvesting (EH)-based multi-antenna amplify-and-forward (AF) relay network in the presence of a passive eavesdropper. During the first phase, while the source is in transmission mode, the legitimate destination transmits an auxiliary artificial noise (AN) signal which has here two distinct purposes, a) to transfer power to the relay b) to improve system security. Since the AN is known at the legitimate destination, it is easily canceled at the intended destination which is not the case at the eavesdropper. In this respect, we derive new exact analytical expressions for the ergodic secrecy capacity for various well-known EH relaying protocols, namely, time switching relaying (TSR), power splitting relaying (PSR) and ideal relaying receiver (IRR). Monte Carlo simulations are also provided throughout our investigations to validate the analysis. The impacts of some important system parameters such as EH time, power splitting ratio, relay location, AN power, EH efficiency and the number of relay antennas, on the system performance are investigated. The results reveal that the PSR protocol generally outperforms the TSR approach in terms of the secrecy capacity.**

***Index Terms*—Amplify-and-forward relays, cooperative communications, energy harvesting, secrecy capacity, wireless power transfer.**

I. Introduction

RADIO frequency (RF) energy harvesting (EH) in wireless communications has recently attracted considerable attention which becomes particularly more attractive in applications where battery-limited devices are not easily accessible, and replacing or recharging their batteries is inconvenient, costly and/or unsafe such as devices embedded inside human bodies and wireless sensors operating under dangerous conditions. This solution is based on the fact that RF signals can concurrently carry information and energy, hence allowing energy constrained nodes to simultaneously harvest energy and process information. This is referred to as simultaneous wireless information and power transfer (SWIPT) [1]–[5]. Motivated by this, nodes in future wireless networks are envisioned to be energy self-sufficient and more sustainable by harvesting RF signals from the surrounding environment.

The concept of SWIPT was first developed in [1], where a tradeoff between the rates at which energy and reliable information can be transmitted over a single noisy channel was studied. Later on, this work was extended in [2] to incorporate the effect of frequency-selective channels and additive white Gaussian noise. However, these studies assumed ideal receiver conditions which means that decoding information and extracting power can be obtained simultaneously from the same received signal. This assumption appears unrealistic in practice due to practical circuit design limitations. On the other hand, the authors in [3], [6] introduced two practical EH receivers, namely, time switching (TS) and power splitting (PS). In the former, the receiver switches between the energy harvester and information receiver whereas in the latter scheme, the receiver splits the signal into two streams, one for EH and the other for information decoding[1].

Similar to wireless information signals, power transfer efficiency in SWIPT systems is subject to channel fading and, therefore, multi-antenna and cooperative communication techniques can be exploited to further enhance the efficiency of such systems [6], [7]. For instance, the authors in [8] considered the throughput of a single-antenna amplify-and-forward (AF) relaying system with an energy-constrained relay which solely relies on harvesting energy from the received RF signal. In this work, two EH relaying protocols are proposed namely, time switching relaying (TSR) and power splitting relaying (PSR). In [9] different power allocation strategies for EH decode-and-forward (DF) relaying networks with multiple source-destination pairs were investigated. Furthermore, an EH relaying system was studied in [10] for the cases with/without the presence of co-channel interference where the multiple antennas relay node is powered by the source signal and signals from other sources. In [11] harvest-and-forward strategy was proposed to enhance the achievable rate in multi-antenna relay channels. In this strategy, the relay harvests energy and receives information signal simultaneously based on antenna selection (AS) and power splitting (PS) techniques, then the relay amplifies and forwards the processed information using the harvested energy. For more details, we refer the reader to [12] where the basic concepts of SWIPT was discussed and the application of advanced smart antenna technologies to SWIPT was investigated.

Moreover, recently, there has been an growing interest in studying physical layer security in SWIPT systems. The concept of physical layer security was first developed by Wyner in [13] where it was shown that secret communication is possible when the eavesdropper channel is a degraded version of the destination channel. For instance, cooperative jamming aided secure communication for SWIPT networks was studied in [14], [15], where the jamming signal is used to degrade the eavesdropper's channel and help the source to increase the harvested energy by the energy receiver. The authors of [16] proposed a harvest-and-jam (HJ) protocol in a SWIPT cooperative system consisting of four relay node wiretap channels with multi-antenna HJ helpers to maximize the secrecy rate subject to the relay transmit power constraint and the total harvested energy for each jamming helper. In addition, different secure relay beam-forming algorithms for SWIPT non-regenerative relay systems were studied in [17].

The authors are with the School of Electrical and Electronic Engineering, the University of Manchester, Manchester, M13 9PL, UK. (emails: {abdelhamid.salem, k.hamdi, khaled.rabie}@manchester.ac.uk).

[1]In practice, PS is based on a power splitter and TS requires a simpler switcher.

Unlike the existing work on this topic, in this paper we analyze the performance of a multi-antenna energy-constrained AF relay network in the context of physical layer security. Three most common EH relaying schemes are considered in this paper, namely TSR, PSR and IRR. Although there have been many physical layer security jamming schemes with different degrees of effectiveness and complexity, in this paper we consider the well-known self-back interference scheme in which the destination transmits artificial noise (AN) to confuse the eavesdropper [18], [19]. To elaborate, the end-to-end communication is accomplished over two phases. In phase I, while the source transmits its information signal, the legitimate destination also broadcasts an AN signal; during this phase the relay harvests energy from the two different sources. In phase II, however, the relay combines the two received signals and, using the harvested energy, amplifies and forwards this signal. Since the legitimate destination has perfect knowledge of the AN, unlike the illegitimate nodes, it can easily and accurately remove it.

The contribution of this paper is as follows. We first derive analytical expressions for the ergodic secrecy capacity of the TSR-, PSR- and IRR-based systems. Then, the optimal time switching factor of the TSR system and the optimal power splitting factor of PSR system that maximize the system secrecy capacity are determined in various scenarios. In all our investigations, Monte Carlo simulations are provided to confirm our analysis. Furthermore, the impacts of some important system parameters such as the EH time, power splitting ratio, source-to-relay distance, AN power, EH efficiency and the number of relay antennas, on the adopted performance metrics are investigated. Results show that the good selection of the time switching and the power splitting factors are the key for achieving best secrecy capacity. Also, increasing the AN power, the number of the relay antennas, the source-to-relay distance and/or the source-to-eavesdropper distance can enhance the secrecy capacity of the proposed system.

We focus our study in this paper on the physical layer security in SWIPT systems for the following main reasons. Firstly, cryptography techniques, which are also used to achieve secure communication, need secure channels between the legitimate nodes to exchange a private key. Secondly, the jamming signal, which is conventionally used to increase security, is also exploited here to boost the energy harvesting process, this idea is very interesting and worth investigating.

This paper is organized as follows. In section II, we describe the system model. Sections III, IV and V derive analytical expressions for the ergodic secrecy capacity of the TSR-, PSR- and IRR-based systems, respectively. Numerical examples and simulation results are presented and discussed in section VI. Finally, Section VII outlines the main conclusions of this work.

II. System Model

The system model under consideration is shown in Fig. 1 which is based on a two-hop relaying network consisting of a single-antenna source node sending information signals to a single-antenna destination node through N-antenna AF relay in the presence of a single-antenna passive eavesdropper. On one hand, the source and destination transmit information and noise signals with a fixed transmission power supply denoted as P_s and P_d, respectively. On the other hand, the relay is an EH node which solely relies on its RF harvested energy, E_h, to amplify and forward the received signal[2]. The channel coefficients between the nodes are denoted as shown in Fig. 1, where $\mathbf{h}_1$ is the $N \times 1$ source-to-relay channel vector, $\mathbf{h}_2$ is the $1 \times N$ relay-to-destination channel vector, g_1 is 1×1 source-to-eavesdropper channel, g_2 is 1×1 destination-to-eavesdropper channel and $\mathbf{g}_3$ is $1 \times N$ relay-to-eavesdropper channel vector; all the channels are modeled as quasi-static block fading channels, i.e. channels remain constant over block time T and vary independently and identically from one block to another, following a Rayleigh distribution. The distances from the source to relay, relay to destination, source to eavesdropper, destination to eavesdropper and relay to eavesdropper nodes are represented by d_1, d_2, d_3, d_4 and d_5, respectively.

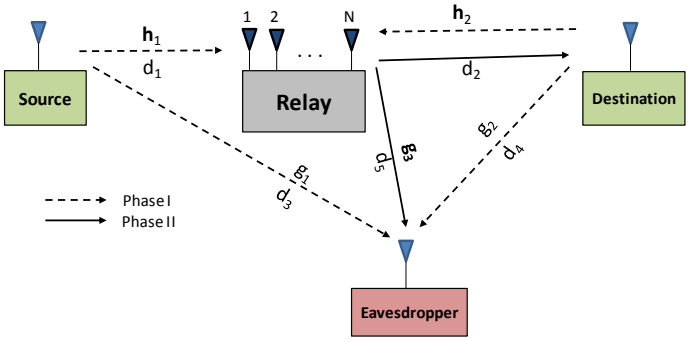
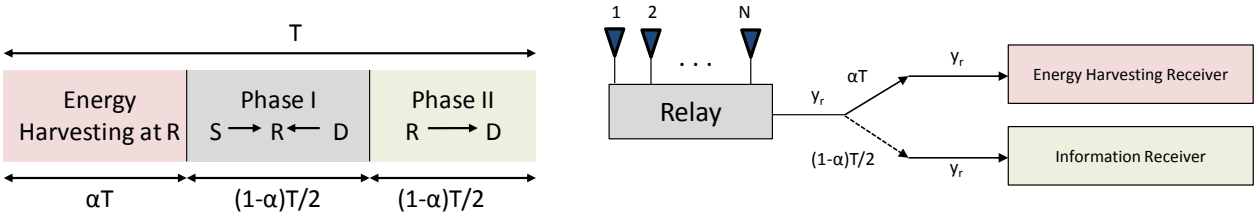


Figure 1: System model with multi-antenna relay.

It is assumed that all communications are performed through the relaying node and that there is no direct link between the source and destination due to the deep shadowing. Therefore, the communication between the source and destination is accomplished over two phases. In phase I, the relay simultaneously receives the information signal from the source and AN from the destination, both of which are used by the relay to harvest energy. During phase II, using the RF harvested energy, the relay amplifies and forwards the received signal to the intended destination. Due to the symmetry of time division systems, the forward and the backward channels are symmetric. It is also assumed that

- The channel state information (CSI) of the eavesdropper is unknown at the legitimate nodes.
- The eavesdropper does not have any knowledge of the channels between the legitimate nodes.
- The relay has full CSI of the main channels, i.e. source-to-relay and relay-to-destination links.
- There is perfect synchronization between the nodes and that the destination has perfect knowledge of the system parameters, e.g. channel gains and distances. Therefore, the AN power can always be adaptively controlled by the legitimate destination as required [20].

[2]The EH protocol at the relay is harvest-use based, i.e. there is no energy storage or rechargeable batteries at the relay and all the harvested energy is used instantly. It is worth mentioning that having storage capability will enable the node to store energy whenever the harvested energy is more than that of the node's consumption, which of course could considerably enhance the overall performance.



(a) Time frame structure.

(b) Block diagram.

Figure 2: TSR protocol for EH and information signal processing at the relay.

To measure the security level of a communication network, the secrecy capacity, C_s, is usually considered which is basically defined by the maximum difference between the mutual information of the main and eavesdropper channels [21]. The secrecy capacity C_s of a wiretap channel, has the following form [21]

$$C_s = \max \left[I\left(x;y\right) - I\left(x;z\right) \right]^+ \tag{1}$$

where $[l]^+ = \max\left(0, l\right)$, x is the input signal at the source, y and z are the output signals at the destination and eavesdropper, respectively. In addition, the ergodic secrecy capacity can be obtained based on the knowledge of the CSI at the transmitter as follow [22]

1- When the channel gains of both the legitimate destination (S-D) h_{sd} and the eavesdropper (S-E) h_{se} are known at the transmitter, the ergodic secrecy capacity is given by [22, Eq(4)] [21, Eq(2.31)]

$$\bar{C}_{s1} = \max_{P(h_{sd},h_{se})} \mathrm{E}\left[\left[C_d - C_e \right]^+ \right] \tag{2}$$

where C_d and C_e are the destination and eavesdropper capacities, respectively.

2- When only the channel gain of the legitimate destination is known at the transmitter, the ergodic secrecy capacity is given by [22, Eq(8)] [21, Eq(2.33)]

$$\bar{C}_{s2} = \max_{P(h_{sd})} \mathrm{E}\left[\left[C_d - C_e \right]^+ \right] \tag{3}$$

3- When the transmitter does not have any knowledge of both the main and eavesdropper channels (only destination CSI). The ergodic secrecy capacity in this case is given by [22, page 4692] [23, Eq(5)]

$$\bar{C}_{s3} = \left[\mathrm{E}\left(C_d \right) - \mathrm{E}\left(C_e \right) \right]^+ \tag{4}$$

Of course, the secrecy capacity in the first case is larger than those in the second and the third cases, i.e., the secrecy capacity in the third case is the lower bound of the first case, $\bar{C}_{s1} > \bar{C}_{s2} > \bar{C}_{s3}$. In this paper we assume that the destination has full state information of the main channel, and the ergodic secrecy capacity $\bar{C}_s$ is derived based on (4), where C_d and C_e are given by $C_d = \frac{1}{2}\log_2\left(1+\gamma_d\right)$ and $C_e = \frac{1}{2}\log_2\left(1+\gamma_e\right)$, respectively, whereas γ_d and γ_e denote the corresponding signal-to-noise ratios (SNRs). Therefore, the expression (4) implies that when the destination SNR is greater than that of the eavesdropper, the secrecy capacity will be the difference between the two channel capacities; otherwise, the secrecy capacity is zero. In the following, we derive the ergodic secrecy capacity for the three considered EH-based systems.

III. Time Switching Relaying (TSR) Protocol

In this protocol, as shown in Fig. 2, the time required to transmit a certain block from the source to the destination is T. The relay however harvests energy from the received signal for only a period of αT where $0 \leq \alpha \leq 1$. Half of the remaining time, $(1-\alpha)T/2$, is used for phase I and the other remaining half, $(1-\alpha)T/2$, is used for phase II. It is assumed that all the harvested energy during αT is used by the relay to forward the received signal[3]. To elaborate, in phase I, the received signal at the relay node can be given as

$$\mathbf{y}_r = \sqrt{\frac{P_s}{d_1^m}}\mathbf{h}_1 s + \sqrt{\frac{P_d}{d_2^m}}\mathbf{h}_2 \upsilon + \mathbf{n}_a \tag{5}$$

where P_s is the source transmitted power, s is the information signal normalized such that $\mathbb{E}\left[|s|^2\right] = 1$, P_d is the destination transmitted power, υ is the AN signal coming from the legitimate destination, and $\mathbb{E}\left[|\upsilon|^2\right] = 1$, m is the path loss exponent and $\mathbf{n}_a$ is the additive white Gaussian noise (AWGN) vector introduced by the receiver antennas at the relay, i.e. $\mathbf{n}_a \sim \mathcal{CN}\left(0, \sigma_a^2\mathbf{I}_N\right)$. During αT the harvested energy by the EH receiver is given by [3]

$$E_h = \eta\,\alpha\,T\left[\frac{P_s}{d_1^m}\left\|\mathbf{h}_1\right\|^2 + \frac{P_d}{d_2^m}\left\|\mathbf{h}_2\right\|^2 + N\sigma_a^2\right] \tag{6}$$

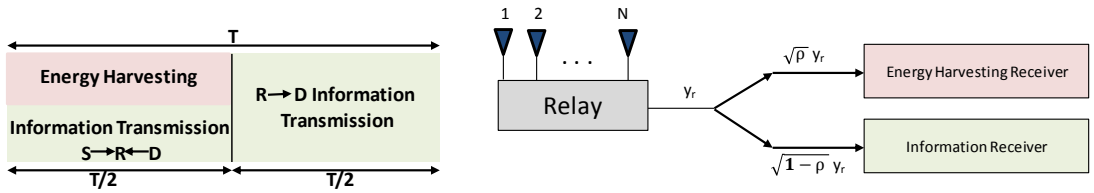
where $0 < \eta < 1$ is the EH efficiency factor which depends mainly on the EH circuitry and $\|.\|$ denotes Euclidean norm. After the base-band processing at the information receiver, the relay output signal before amplification can be expressed as

$$\mathbf{y}_r = \sqrt{\frac{P_s}{d_1^m}}\mathbf{h}_1 s + \sqrt{\frac{P_d}{d_2^m}}\mathbf{h}_2 \upsilon + \mathbf{n}_r \tag{7}$$

where $\mathbf{n}_r$ is an $N \times 1$ AWGN vector at the relay, i.e. $\mathbf{n}_r \sim \mathcal{CN}\left(0, \sigma_r^2\mathbf{I}_N\right)$, $\mathbf{n}_r = \mathbf{n}_a + \mathbf{n}_c$ and $\mathbf{n}_c$ is the noise vector introduced by the information receiver, i.e. $\mathbf{n}_c \sim \mathcal{CN}\left(0, \sigma_c^2\mathbf{I}_N\right)$ [8], [11]. Furthermore, the received signal at the eavesdropper in the first phase is given by

$$y_e^{(1)} = \sqrt{\frac{P_s}{d_3^m}}g_1 s + \sqrt{\frac{P_d}{d_4^m}}g_2 \upsilon + n_e \tag{8}$$

[3]In other words, the energy consumed by the relay circuitry to process the information signals is negligible in this study.



(a) Time frame structure.

(b) 2bBlock diagram.

Figure 3: PSR protocol for EH and information signal processing at the relay.

where n_e is the AWGN signal at the eavesdropper with variance σ_e^2, i.e., $n_e \sim \mathcal{CN}\left(0, \sigma_e^2\right)$. In phase II, the relay transmitted signal, $\mathbf{x}_r$, can be written as

$$\mathbf{x}_r = G\,\mathbf{y}_r \tag{9}$$

where G is the relay gain given by

$$G = \sqrt{P_r \beta_t}. \tag{10}$$

Here, P_r is the relay transmit power and

$$\beta_t = \frac{1}{\frac{P_s}{d_1^m}\left\|\mathbf{h}_1\right\|^2 + \frac{P_d}{d_2^m}\left\|\mathbf{h}_2\right\|^2 + N\sigma_r^2}. \tag{11}$$

Consequently, the received signal at the destination is

$$y_d = \sqrt{\frac{P_s P_r \beta_t}{d_1^m d_2^m}}\mathbf{h}_2\mathbf{h}_1\, s + \sqrt{\frac{P_d P_r \beta_t}{d_2^{2m}}}\mathbf{h}_2\mathbf{h}_2^{\dagger}\,\upsilon + \sqrt{\frac{P_r\beta_t}{d_2^m}}\,\mathbf{h}_2\mathbf{n}_r + n_d\,, \tag{12}$$

where n_d is the AWGN signal at the destination with variance σ_d^2, i.e. $n_d \sim \mathcal{CN}\left(0, \sigma_d^2\right)$ and $\dagger$ denotes the transpose operation. However, since the AN is known at the legitimate destination and full system information is available at the destination, υ can be easily removed at the destination; hence, y_d can be simplified to

$$y_d = \sqrt{\frac{P_s P_r \beta_t}{d_1^m d_2^m}}\mathbf{h}_2\mathbf{h}_1\, s + \sqrt{\frac{P_r\beta_t}{d_2^m}}\mathbf{h}_2\mathbf{n}_r + n_d. \tag{13}$$

On the other hand, the eavesdropper received signal is given as [20]

$$y_e^{(2)} = \sqrt{\frac{P_s P_r \beta_t}{d_1^m d_5^m}}\mathbf{g}_3\mathbf{h}_1\, s + \sqrt{\frac{P_d P_r \beta_t}{d_2^m d_5^m}}\mathbf{g}_3\mathbf{h}_2^{\dagger}\,\upsilon + \sqrt{\frac{P_r\beta_t}{d_5^m}}\,\mathbf{g}_3\mathbf{n}_r + n_e. \tag{14}$$

Now, the relay transmitted power P_r can be simply expressed in terms of the harvested energy as

$$P_r = \frac{E_h}{(1-\alpha)\,T/2} \tag{15}$$

and substituting the value of E_h in (6) into (15) yields

$$P_r = \frac{2\,\eta\,\alpha}{(1-\alpha)}\left[\frac{P_s}{d_1^m}\left\|\mathbf{h}_1\right\|^2 + \frac{P_d}{d_2^m}\left\|\mathbf{h}_2\right\|^2 + N\sigma_a^2\right]. \tag{16}$$

Now, substituting (16) into (13) and (14), then grouping the information signal and noise terms we obtain the SNR at the destination, γ_d, as given by

$$\gamma_d = \frac{2\,\eta\,\alpha\,P_s\left|\mathbf{h}_2\mathbf{h}_1\right|^2}{2\,\eta\,\alpha\,d_1^m\sigma_r^2\left\|\mathbf{h}_2\right\|^2 + (1-\alpha)\,d_1^m d_2^m\sigma_d^2}. \tag{17}$$

As we can see from (8) and (14), the eavesdropper has two opportunities to overhear the information signal in two different time slots. However, the eavesdropper has a limited ability to maximize the overall SNR, as it does not have any knowledge of the channels between the legitimate nodes.

Considering the worst case scenario in which the eavesdropper can know the systems' channels. Strictly speaking, in this case the eavesdropper can perform any technique with the signals received in the two phases in order to maximize the overall SNR. In this paper, in order to examine the efficiency of the proposed schemes, we study a simple case in which the eavesdropper performs maximal ratio combining (MRC) [4]. According to MRC, the eavesdropper combines the received signals by multiplying (8) and (14) with factors w_1 and w_2, respectively, as given by [24], [25]

$$y_e = w_1 y_e^{(1)} + w_2 y_e^{(2)} \tag{18}$$

where $w_1 = \frac{\sqrt{\frac{P_s}{d_3^m}}\,g_1^H}{\frac{P_d}{d_4^m}\left|g_2\right|^2 + \sigma_e^2}$ and $w_2 = \frac{\sqrt{\frac{P_s P_r \beta_t}{d_1^m d_5^m}}\,\mathbf{h}_1^H\mathbf{g}_3^H}{\frac{P_d P_r \beta_t}{d_2^m d_5^m}\left|\mathbf{g}_3\mathbf{h}_2\right|^2 + \frac{P_r\beta_t}{d_5^m}\sigma_r^2\left\|\mathbf{g}_3\right\|^2 + \sigma_e^2}$, while $(.)^H$ is the transpose conjugate operation. From (18) we can get the SNR at the eavesdropper γ_e as given by (19), shown at the top of the next page.

The ergodic secrecy capacity of this system can be obtained as

$$\bar{C}_s^{[TSR]} = \left[\mathbb{E}\left[C_d^{TSR}\right] - \mathbb{E}\left[C_e^{TSR}\right]\right]^+. \tag{20}$$

According to the best of the authors knowledge, the simplest form of $\mathbb{E}\left[C_d^{TSR}\right]$ and $\mathbb{E}\left[C_e^{TSR}\right]$ can be written respectively as in (21) and (22), shown at the top of the next page, where $\mathcal{M}_{\gamma_e^{(1)}}(z)$, $\mathcal{M}_{\gamma_e^{(2)}}^{TSR}(z)$ are given by (23) and (24), also shown at the top of the next page, and $a_1 = 2\,\eta\,\alpha\,P_s$, $b_1 = 2\,\eta\,\alpha\,d_1^m\sigma_r^2$,

[4]Please note that, in the system model there is no a direct (S-D) link, so we can increase the system security in this case by forcing the transmitter to transmit a jamming signal in the second phase.

$$\gamma_e = \underbrace{\frac{P_s d_4^m \left|g_1\right|^2}{P_d d_3^m \left|g_2\right|^2 + d_3^m d_4^m \sigma_e^2}}_{\gamma_e^{(1)}} + \underbrace{\frac{2\,\eta\,\alpha\,P_s d_2^m \left|\mathbf{g}_3\,\mathbf{h}_1\right|^2}{2\,\eta\,\alpha\,d_1^m P_d \left|\mathbf{g}_3 \mathbf{h}_2^\dagger\right|^2 + 2\,\eta\,\alpha\,d_1^m d_2^m \sigma_r^2 \left\|\mathbf{g}_3\right\|^2 + (1-\alpha)\,d_1^m d_2^m d_5^m \sigma_e^2}}_{\gamma_e^{(2)}}. \tag{19}$$

$c_1 = (1-\alpha)\ d_1^m d_2^m \sigma_d^2$, $a_2 = 2\,\eta\,\alpha\,P_s d_2^m$, $b_2 = \frac{2\,\eta\,\alpha\,d_1^m P_d}{2\,\eta\,\alpha\,P_s d_2^m}$, $c_2 = \frac{2\,\eta\,\alpha\,d_1^m d_2^m \sigma_r^2}{2\,\eta\,\alpha\,P_s d_2^m}$, $r = \frac{(1-\alpha)\,d_1^m d_2^m d_5^m \sigma_e^2}{2\,\eta\,\alpha\,P_s d_2^m}$ and $b_3 = \frac{P_d d_3^m}{P_s d_4^m}$, $c_3 = \frac{d_3^m \sigma_e^2}{P_s}$.

Proof: The proof is provided in Appendix A. ∎

IV. Power Splitting Relaying (PSR) Protocol

In this protocol the time required to transmit a certain block from the source to the destination T is divided into two equal durations, i.e. $T/2$, as illustrated in Fig. 3. During the first half time block $T/2$, the relay harvests energy and process information, and a fraction of the received signal power, ρP, at the relay is allocated for EH and the remaining received power, $(1-\rho)\,P$, is used for the information processing, where $0 \leq \rho \leq 1$. In the second $T/2$ time block, the relay uses the harvested energy to amplify and forward the received signal to the intended destination. As for phase I, the received signal at the EH receiver can be expressed as

$$\mathbf{y}_r = \sqrt{\frac{\rho\,P_s}{d_1^m}}\mathbf{h}_1 s + \sqrt{\frac{\rho\,P_d}{d_2^m}}\mathbf{h}_2 \upsilon + \sqrt{\rho}\mathbf{n}_a. \tag{25}$$

The energy harvested by the EH receiver is given by [3]

$$E_h = \frac{\eta\,\rho\,T}{2}\left[\frac{P_s}{d_1^m}\left\|\mathbf{h}_1\right\|^2 + \frac{P_d}{d_2^m}\left\|\mathbf{h}_2\right\|^2 + N\sigma_a^2\right]. \tag{26}$$

and the signal at the information receiver output can be expressed by

$$\mathbf{y}_r = \sqrt{\frac{(1-\rho)\,P_s}{d_1^m}}\,\mathbf{h}_1 s + \sqrt{\frac{(1-\rho)\,P_d}{d_2^m}}\,\mathbf{h}_2 \upsilon + \mathbf{n}_r \tag{27}$$

where $\mathbf{n}_r = \sqrt{1-\rho}\mathbf{n}_a + \mathbf{n}_c$. Now, the received signal at the eavesdropper in the first phase can be written as

$$y_e^{(1)} = \sqrt{\frac{P_s}{d_3^m}} g_1 s + \sqrt{\frac{P_d}{d_4^m}} g_2 \upsilon + n_e \tag{28}$$

In phase II, the relay transmits the following signal

$$\mathbf{x}_r = G\,\mathbf{y}_r \tag{29}$$

where G represents the relay gain given by

$$G = \sqrt{P_r \beta_p} \tag{30}$$

P_r is the relay power and β_p is given by

$$\beta_p = \frac{1}{\frac{(1-\rho)P_s}{d_1^m}\left\|\mathbf{h}_1\right\|^2 + \frac{(1-\rho)P_d}{d_2^m}\left\|\mathbf{h}_2\right\|^2 + N\sigma_r^2}. \tag{31}$$

Now, the received signal at the destination can be written as in (32).

Similar to the TSR scenario, υ can be easily removed at the destination; hence, y_d is simplified to

$$y_d = \sqrt{\frac{(1-\rho)\,P_s P_r \beta_p}{d_1^m d_2^m}}\mathbf{h}_2\mathbf{h_1}\,s + \frac{\sqrt{P_r\beta_p}\mathbf{h}_2}{\sqrt{d_2^m}}\mathbf{n}_r + n_d. \tag{33}$$

On the other hand, the eavesdropper received signal is given as

$$y_e^{(2)} = \sqrt{\frac{(1-\rho)\,P_s P_r \beta_p}{d_1^m d_5^m}}\mathbf{g}_3\,\mathbf{h}_1\,s + \frac{\sqrt{(1-\rho)\,P_d P_r \beta_p}}{\sqrt{d_2^m d_5^m}}\mathbf{g}_3\mathbf{h}_2^\dagger\,\upsilon + \frac{\sqrt{P_r\beta_p}\mathbf{g}_3}{\sqrt{d_5^m}}\,\mathbf{n}_r + n_e. \tag{34}$$

The relay transmitted power in terms of the harvested energy is obtained as

$$P_r = \frac{E_h}{T/2}. \tag{35}$$

Using (26), P_r can be expressed as

$$P_r = \eta\,\rho\left[\frac{P_s}{d_1^m}\left\|\mathbf{h}_1\right\|^2 + \frac{P_d}{d_2^m}\left\|\mathbf{h}_2\right\|^2 + N\sigma_a^2\right]. \tag{36}$$

Substituting (36) into (33) and (34), then grouping the information and noise signals, it is easy to obtained the SNR expressions at the destination and the eavesdropper nodes as given by (37) and (38), respectively.

The ergodic secrecy capacity of the PSR system is given as

$$\bar{C}_s^{[PSR]} = \left[\mathbb{E}\left[C_d^{PSR}\right] - \mathbb{E}\left[C_e^{PSR}\right]\right]^+ \tag{39}$$

while $\mathbb{E}\left[C_d^{PSR}\right]$ and $\mathbb{E}\left[C_d^{PSR}\right]$ are given by (40) and (41), respectively, where $\mathcal{M}_{\gamma_e^{(1)}}(z)$ is given by (23) and $\mathcal{M}_{\gamma_e^{(2)}}^{PSR}(z)$ is given by (42), and

$$a_1 = \eta\,\rho\,(1-\rho)\,P_s, \tag{43a}$$
$$b_1 = \eta\,\rho\,d_1^m \sigma_c^2, \tag{43b}$$
$$c_1 = \eta\,\rho\,(1-\rho)\ d_1^m \sigma_a^2, \tag{43c}$$
$$r_1 = (1-\rho)\ d_1^m d_2^m \sigma_d^2, \tag{43d}$$
$$a_2 = \eta\,\rho\,(1-\rho)\,P_s d_2^m, \tag{43e}$$
$$b_2 = \eta\,\rho\,(1-\rho)\,d_1^m P_d / a_2, \tag{43f}$$
$$c_2 = \eta\,\rho\,(1-\rho)\,d_1^m d_2^m \sigma_a^2 / a_2, \tag{43g}$$
$$r_2 = \eta\,\rho\,d_1^m d_2^m \sigma_c^2 / a_2, \text{ and} \tag{43h}$$
$$\omega = (1-\rho)\ d_1^m d_2^m d_5^m \sigma_e^2 / a_2, \tag{43i}$$

Proof: The proof is provided in Appendix B. ∎

$$\mathbb{E}\left[C_d^{TSR}\right] = \frac{1-\alpha}{2\,\ln(2)}\int_0^{\infty}\frac{1}{z}\left(1-\frac{\lambda_x}{\lambda_x+a_1 z}\right)\frac{2\,e^{-zb_1}\,(c_1 z)^{N/2}}{\Gamma(N)}\,K_N\left(2\sqrt{c_1 z}\right)(z)\,dz. \tag{21}$$

$$\mathbb{E}\left[C_e^{TSR}\right] = \frac{1-\alpha}{2\,\ln(2)}\int_0^{\infty}\frac{1}{z}\left(1-\mathcal{M}_{\gamma_e^{(1)}}(z)\,\mathcal{M}_{\gamma_e^{(2)}}^{TSR}(z)\right)e^{-z}dz. \tag{22}$$

$$\mathcal{M}_{\gamma_e^{(1)}}(z) = 1-\frac{z\lambda_{g_2}e^{\frac{\lambda_{g_2}}{b_3}(c_3+z)}\left[\Gamma\left(0,\frac{\lambda_{g_2}}{b_3}(c_3+z)\right)+\ln\left(\frac{b_3}{\lambda_{g_2}}\right)-\ln(c_3+z)+\ln\left(\frac{\lambda_{g_2}}{b_3}(c_3+z)\right)\right]}{b_3} \tag{23}$$

$$\mathcal{M}_{\gamma_e^{(2)}}^{TSR}(z) = 1-z\int_0^{\infty}e^{-zq}\frac{\lambda_\Upsilon}{\lambda_\Upsilon+(b_2*q)}.e^{-qc_2}.\frac{2\,(r\,q)^{N/2}}{\Gamma(N)}\,K_N\left(2\sqrt{r\,q}\right)dq. \tag{24}$$

$$y_d = \sqrt{\frac{(1-\rho)\,P_s P_r \beta_p}{d_1^m d_2^m}}\mathbf{h_2}\mathbf{h_1}\,s+\sqrt{\frac{(1-\rho)\,P_d P_r \beta_p}{d_2^{2m}}}\mathbf{h_2}\mathbf{h_2}^{\dagger}\,\upsilon+\frac{\sqrt{P_r\beta_p}\mathbf{h_2}}{\sqrt{d_2^m}}\mathbf{n}_r+n_d. \tag{32}$$

$$\gamma_d = \frac{\eta\,\rho\,(1-\rho)\,P_s\left|\mathbf{h_2}\mathbf{h_1}\right|^2}{\eta\,\rho\,d_1^m\sigma_c^2\left\|\mathbf{h_2}\right\|^2+\eta\,\rho\,(1-\rho)\;d_1^m\sigma_a^2\left\|\mathbf{h_2}\right\|^2+(1-\rho)\;d_1^m d_2^m\sigma_d^2}. \tag{37}$$

$$\gamma_e = \underbrace{\frac{P_s d_4^m\left|g_1\right|^2}{P_d d_3^m\left|g_2\right|^2+d_3^m d_4^m\sigma_e^2}}_{\gamma_e^{(1)}}+\underbrace{\frac{\eta\,\rho\,(1-\rho)\,P_s d_2^m\left|\mathbf{g_3}\mathbf{h_1}\right|^2}{\eta\,\rho\,(1-\rho)\;d_1^m P_d\left|\mathbf{g_3}\mathbf{h_2}^{\dagger}\right|^2+\eta\,\rho\,(1-\rho)\,d_1^m d_2^m\sigma_a^2\left\|\mathbf{g_3}\right\|^2+\eta\,\rho\,d_1^m d_2^m\sigma_c^2\left\|\mathbf{g_3}\right\|^2+(1-\rho)\;d_1^m d_2^m d_5^m\sigma_e^2}}_{\gamma_e^{(2)}}. \tag{38}$$

V. Ideal Relay Receiver

Unlike the TSR and PSR systems, the IRR system has the capability to independently and concurrently process the information signal and harvest energy from the same received signal[5]. Therefore, during the first $T/2$, the relay harvests energy and process information whereas in the second $T/2$ time block the relay uses this harvested energy to amplify and forward the received signal, as shown in Fig. 4. Consequently, the harvested energy and relay transmitted power can be expressed, respectively, as

$$E_h = \frac{\eta T}{2}\left[\frac{P_s}{d_1^m}\left\|\mathbf{h}_1\right\|^2+\frac{P_d}{d_2^m}\left\|\mathbf{h}_2\right\|^2+N\sigma_a^2\right]. \tag{44}$$

and

$$P_r = \frac{2\,E_h}{T} = \eta\left[\frac{P_s}{d_1^m}\left\|\mathbf{h}_1\right\|^2+\frac{P_d}{d_2^m}\left\|\mathbf{h}_2\right\|^2+N\sigma_a^2\right]. \tag{45}$$

The received signal at the eavesdropper in the first phase is given by

[5]It should be mentioned that IRR would require two independent antenna(s) which can be costly in practice. Additionally, as far as the current circuit designs are concerned, it is very difficult, if not impossible, yet to extract RF energy directly from the information signal [26].

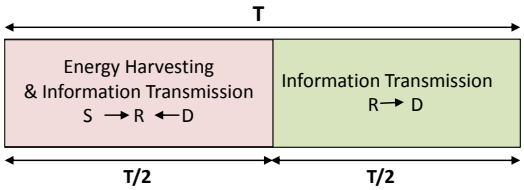


Figure 4: Time frame structure for IRR.

$$y_e^{(1)} = \sqrt{\frac{P_s}{d_3^m}}g_1 s+\sqrt{\frac{P_d}{d_4^m}}g_2\upsilon+n_e \tag{46}$$

In the second phase, the received signals at the destination and eavesdropper for the IRR system can be given by

$$y_d = \sqrt{\frac{P_s P_r \beta_i}{d_1^m d_2^m}}\mathbf{h}_2\mathbf{h}_1\,s+\sqrt{\frac{P_r\beta_i}{d_2^m}}\mathbf{h}_2\mathbf{n}_r+n_d \tag{47}$$

and

$$\mathbb{E}\left[C_d^{PSR}\right] = \frac{1}{2\,\ln(2)}\int_0^{\infty}\frac{1}{z}\left(1-\frac{\lambda_X}{\lambda_X+(a_1*z)}\right)e^{-(b_1+c_1)}\,\frac{2\,(r_1\,z)^{N/2}}{\Gamma(N)}K_N\left(2\sqrt{r_1\,z}\right)dz. \tag{40}$$

$$\mathbb{E}\left[C_e^{PSR}\right] = \frac{1}{2\,\ln(2)}\int_0^{\infty}\frac{1}{z}\left(1-\mathcal{M}_{\gamma_e^{(1)}}(z)\,\mathcal{M}_{\gamma_e^{(2)}}^{PSR}(z)\right)e^{-z}dz. \tag{41}$$

$$\mathcal{M}_{\gamma_e^{(2)}}^{PSR}(z) = 1 - z\int_0^{\infty}e^{-zq}e^{-q(c_2+r_2)}\frac{\lambda_\Upsilon}{\lambda_\Upsilon+(b_2*q)}\,\frac{2\,(\omega\,q)^{N/2}}{\Gamma(N)}K_N\left(2\sqrt{\omega\,q}\right)dq. \tag{42}$$

$$y_e^{(2)} = \sqrt{\frac{P_s P_r \beta_i}{d_1^m d_5^m}}\mathbf{g}_3\mathbf{h}_1\,s + \frac{\sqrt{P_d P_r \beta_i}}{\sqrt{d_2^m d_5^m}}\mathbf{g}_3\mathbf{h}_2^{\dagger}\,\upsilon + \frac{\sqrt{P_r\beta_i}}{\sqrt{d_5^m}}\mathbf{g}_3\mathbf{n}_r + n_e \tag{48}$$

respectively, where $\mathbf{n}_r = \mathbf{n}_a$ and

$$\beta_i = \frac{1}{\frac{P_s}{d_1^m}\|\mathbf{h}_1\|^2 + \frac{P_d}{d_2^m}\|\mathbf{h}_2\|^2 + N\sigma_r^2}. \tag{49}$$

Substituting (45) into (47) and (48), then grouping the information and noise terms, we get SNR expressions at the destination and eavesdropper as in (50) and (51), respectively.

$$\gamma_d = \frac{\eta\,P_s\,|\mathbf{h}_2\mathbf{h}_1|^2}{\eta\,d_1^m\sigma_r^2\,\|\mathbf{h}_2\|^2 + d_1^m d_2^m \sigma_d^2}. \tag{50}$$

Finally, the ergodic secrecy capacity of the IRR-based system can be obtained by

$$\bar{C}_s^{[IRR]} = \left[\mathbb{E}\left[C_d^{IRR}\right] - \mathbb{E}\left[C_e^{IRR}\right]\right]^+ \tag{52}$$

$\mathbb{E}\left[C_d^{IRR}\right]$ and $\mathbb{E}\left[C_e^{IRR}\right]$ can be expressed as in (53) and (54), respectively, where $\mathcal{M}_{\gamma_e^{(1)}}(z)$ is given by (23), $\mathcal{M}_{\gamma_e^{(2)}}(z)$ is given by (55) and

$$a_1 = \eta\,P_s, \tag{56a}$$
$$b_1 = \eta\,d_1^m\sigma_r^2, \tag{56b}$$
$$c_1 = d_1^m d_2^m \sigma_d^2, \tag{56c}$$
$$a_2 = \eta\,P_s d_2^m, \tag{56d}$$
$$b_2 = \eta\,d_1^m P_d/a_2, \tag{56e}$$
$$c_2 = \eta\,d_1^m d_2^m \sigma_r^2/a_2,\ and \tag{56f}$$
$$r_2 = d_1^m d_2^m d_5^m \sigma_e^2/a_2, \tag{56g}$$

Proof: The proof is provided in Appendix C. ∎

Equations (21), (22), (40), (41), (53) and (54) are exact explicit expressions for the ergodic capacities. Furthermore, to more clearly highlight the effect of various system parameters, Gaussian Quadrature rule can be straightforwardly applied. For instance (53), (54) and (55) can be rewritten as in (57), (58) and (59), where (z_i, q_i) and H_i are the i^{th} zero and the weighting factor of the Laguerre polynomials, respectively [27].

VI. Numerical results

In this section we present some numerical results for the mathematical expressions derived above and investigate the impact of various key system parameters on the system performance. To validate our analysis, Monte Carlo simulations with 10^6 independent trials are also presented throughout and in all our evaluations the channel coefficients are randomly generated in each simulation run. Unless otherwise stated, we set system parameters as follows $P_s = P_d = 30$ dBm, $\eta = 1$, $m = 2.7$[6] and d_1, d_2, d_3, d_4 and d_5 are normalized to unit value. For simplicity, but without loss of generality, equal noise variances are chosen at the destination and the eavesdropper nodes such that $\sigma^2 = \sigma_d^2 = \sigma_e^2 = -10$ dBm while $\sigma_a^2 = \sigma_c^2 = \sigma^2/2$; also λ_X, λ_Y, λ_Φ and λ_Υ are all set to 1. It should also be mentioned that the secrecy capacity integrals are efficiently evaluated using numerical integration.

A. Effect of α and ρ on Secrecy Capacity

In this section we investigate the impact of the EH time ratio, α, and power splitting factor, ρ, on the system performance. Fig. 5 shows the the ergodic secrecy capacity versus α and ρ for various values of N. The first observation one can see from these results is that the proposed TSR and PSR always provide better performance relative to the conventional systems, i.e. $N = 1$, irrespective of the values of α and ρ. It is also apparent that as the number of relay antennas increases the ergodic secrecy capacity enhances and that there exists an optimal value for α and ρ, for each number of the relay antennas N, that maximizes the ergodic secrecy capacity. This can be justified for each EH protocol as follows. For the TSR system, when α is too small there is less time for EH and hence small amount of energy is harvested which of course will result in poor secrecy capacity. At the other extreme, when α is too large, too much energy is harvested unnecessarily at the expense of information transmission time which, consequently, also leads to poor secrecy capacity. Similarly, for the PSR-based system, when ρ is too small, there is less power for EH. As a result, less transmission power is available at the relay, which leads to poor secrecy capacity. On the other hand, when ρ is too large, only small amount of power is available for the information transmission while more power is unnecessarily wasted on the EH and hence

[6]This corresponds to an urban cellular network environment [28].

$$\gamma_e = \underbrace{\frac{P_s d_4^m \left|g_1\right|^2}{P_d d_3^m \left|g_2\right|^2 + d_3^m d_4^m \sigma_e^2}}_{\gamma_e^{(1)}} + \underbrace{\frac{\eta\, P_s d_2^m \left|\mathbf{g}_3 \mathbf{h}_1\right|^2}{\eta\, d_1^m P_d \left|\mathbf{g}_3 \mathbf{h}_2^\dagger\right|^2 + \eta\, \sigma_r^2\, d_1^m d_2^m \left\|\mathbf{g}_3\right\|^2 + d_1^m d_2^m d_5^m \sigma_e^2}}_{\gamma_e^{(2)}}. \tag{51}$$

$$\mathbb{E}\left[C_d^{IRR}\right] = \frac{1}{2\,\ln(2)} \int_0^\infty \frac{1}{z} \left(1 - \frac{\lambda_X}{\lambda_X + a_1 z}\right) e^{-z b_1}\, \frac{2\,(c_1\, z)^{N/2}}{\Gamma(N)} K_N\left(2\sqrt{c_1\, z}\right) dz \tag{53}$$

$$\mathbb{E}\left[C_e^{IRR}\right] = \frac{1}{2\,\ln(2)} \int_0^\infty \frac{1}{z} \left(1 - \mathcal{M}_{\gamma_e^{(1)}}(z)\, \mathcal{M}_{\gamma_e^{(2)}}^{IRR}(z)\right) e^{-z} dz \tag{54}$$

$$\mathcal{M}_{\gamma_e^{(2)}}^{IRR}(z) = 1 - z \int_0^\infty e^{-z q} e^{-q c_2} \frac{\lambda_\Upsilon}{\lambda_\Upsilon + b_2 q}\, \frac{2\,(r_2\, q)^{N/2}}{\Gamma(N)} K_N\left(2\sqrt{r_2\, q}\right) dq. \tag{55}$$

$$\mathbb{E}\left[C_d^{IRR}\right] \approx \frac{1}{2\ln(2)}\, \frac{1}{b_1} \sum_{i=1}^{n} \mathrm{H}_i\, \frac{b_1}{z_i} \left(1 - \frac{\lambda_X b_1}{b_1 \lambda_X + a_1 z_i}\right) \frac{2\left(\frac{c_1\, z_i}{b_1}\right)^{N/2}}{\Gamma(N)} K_N\left(2\sqrt{\frac{c_1\, z_i}{b_1}}\right) \tag{57}$$

lesser secrecy capacity is noticed. This phenomena is discussed below in detail.

B. Optimized α and ρ and Maximum Achievable C_s

In this section we examine the optimal switching time/power splitting factors (α, ρ) and the corresponding maximum achievable ergodic secrecy capacity. Fig. 6a illustrates the optimal switching time factor (α^*) and power splitting factor (ρ^*) versus N for $\eta = 0.3,\ 0.5$ and 1. It should be pointed out that in this section the solid and dashed lines represent the analytical results whereas the simulated results are represented by markers. Having a closer look at these results, two main observations can be seen. First, increasing η will always reduce α^* and ρ^* which is intuitive because higher η means more energy can be harvested in shorter period of time for TSR and smaller power ratio for PSR, i.e. smaller α and ρ are required. The second observation is that α^* and ρ^* decrease with increasing the number of relay antennas. This can be intuitively explained by the fact that having more antennas will allow harvesting same amount of energy with shorter period of time for TSR and smaller power ratio for PSR. The maximum achievable ergodic secrecy capacity corresponding to α^* and ρ^* is plotted in Fig. 6b with respect to N for various values of η. In addition, results for the IRR system are shown in this figure. It is clear that the IRR system always has better performance relative to the TSR and PSR techniques under same system features. It is also noted that the C_s enhances when either η or N is increased for the same reasons mentioned previously.

C. Effect of Relay Location, Eavesdropper Location and AN Power

In order to investigate the impact of the relay location, the eavesdropper location and the AN power on the secrecy capacity of the TSR- and PSR-based systems, we consider a simple one-dimensional model as illustrated in Fig. 7, the source and the destination are located at (0, 0) m and (10, 0) m, respectively. The channels between the nodes are modeled by line-of-sight model including the path loss effect. It is assumed that the distance between the relay antennas is much smaller than the distance between the relay and the destination, eavesdropper and source nodes[7]. Hence, the path losses between the different relay antennas and the other nodes are the same.

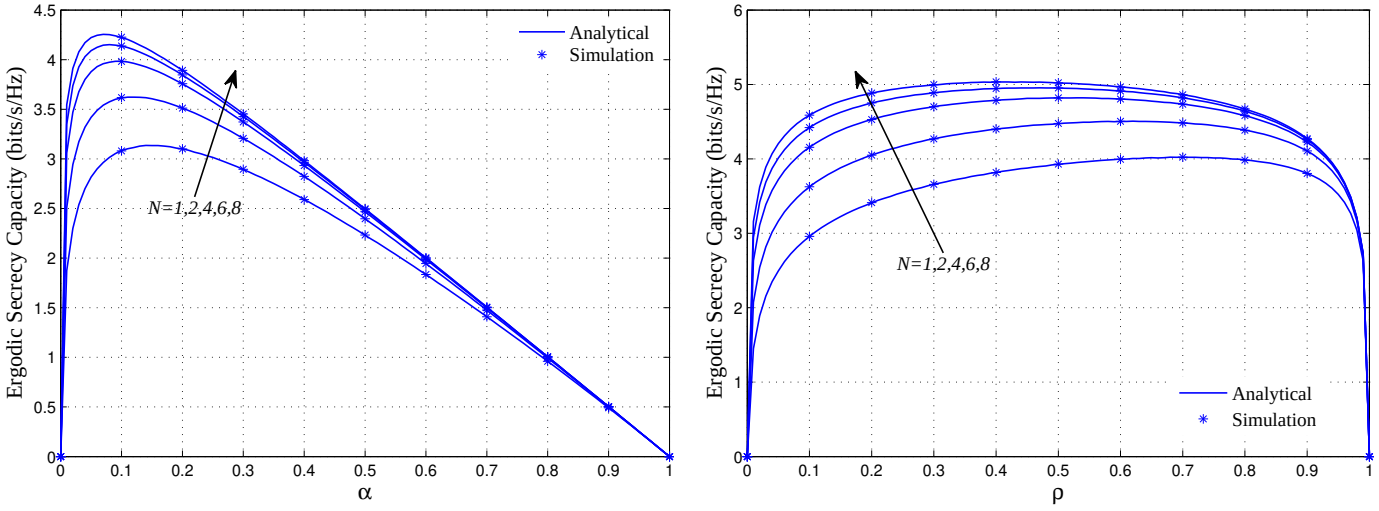
Firstly, the eavesdropper are placed at (7.5, 0) m away from the source (0, 0) m while the relay position is varied from (0, 0) m to (7.5, 0) m. In this respect, Fig. 8 depicts a 3D surface plot for the ergodic secrecy capacity as a function of d_1 and P_d for both the TSR- and PSR-based EH techniques when α and ρ are optimized. System parameters adopted in this section are $N = 8$, $\eta = 1$ and $P_s = 2$ W. In this section the solid lines represent the analytical results whereas the simulated results are represented by circles. The common observation one can see in the two systems is that the optimal secrecy capacity is at its minimum when the relay is exactly at the source node and improves as the relay moves towards the destination. This is because when the relay is far away from the destination, the AN signal at the relay will be too weak to protect the information source signal in phase II.

Secondly, the relay are placed at (5, 0) m away from the source (0, 0) m while the eavesdropper position is varied from (1, 0) m

[7]This is a common assumption in the analysis of relay networks.

$$\mathbb{E}\left[C_e^{IRR}\right] \approx \frac{1}{2\ln(2)} \sum_{i=1}^{n} \mathrm{H}_i \frac{1}{z_i} \left(1 - \mathcal{M}_{\gamma_e^{(1)}}(z_i)\, \mathcal{M}_{\gamma_e^{(2)}}^{IRR}(z_i)\right) \tag{58}$$

$$\mathcal{M}_{\gamma_e^{(2)}}^{IRR}(z) = 1 - \frac{z}{c_2} \sum_{i=1}^{n} \mathrm{H}_i e^{-\frac{z q_i}{c_2}} \frac{c_2\lambda_\Upsilon}{c_2\lambda_\Upsilon + b_2 q_i} \frac{2\left(\frac{r_2\, q_i}{c_2}\right)^{N/2}}{\Gamma(N)} K_N\left(2\sqrt{\frac{r_2\, q_i}{c_2}}\right). \tag{59}$$



(a) TSR-based system.

(b) PSR-based system.

Figure 5: Ergodic secrecy capacity with respect to α and ρ for the TSR- and PSR-based systems with various values of N.

to (7.5, 0) m. Fig. 9 represents a 3D surface plot for the ergodic secrecy capacity as a function of d_3 and P_d for both the TSR- and PSR-based EH techniques when α and ρ are optimized for the same system parameters. From this figure we can observe that, the optimal secrecy capacity is at its minimum when the eavesdropper is closed to the source node and enhances as the eavesdropper moves towards the destination. This can be justified by the fact that when the eavesdropper is far away from the destination, the AN signal strength at the eavesdropper in phase I will be too weak due to larger path loss.

Finally, from the two figures 8 and 9, it is clear that increasing the AN power will enhance the system secrecy capacity in both TSR- and PSR-based systems but it is more obvious in the former scheme.

VII. Conclusion

In this paper, we have analyzed the secrecy capacity in energy-constrained AF relay networks when the relay is equipped with multiple antennas. The analysis considered three EH relaying protocols, namely, TSR, PSR and IRR. In each case, we have derived accurate analytical expressions for the ergodic secrecy capacity. Also the time switching and power splitting factors were optimized to maximize the secrecy capacity in various system configurations. The results demonstrated that increasing the number of relay antennas can reduce the time switching and power splitting factors while maximizing the ergodic secrecy capacity. Furthermore, increasing the AN power as well as the source-to-relay distance and/or source-to-eavesdropper distance can considerably enhance the secrecy capacity performance.

Appendix A

This appendix derives the destination and eavesdropper ergodic capacities for the TSR-based system.

- Destination Ergodic Capacity

To begin with, it is more convenient to rewrite the destination ergodic capacity in (17) as follows

$$\gamma_d = \frac{a_1 \frac{|\mathbf{h}_2\mathbf{h}_1|^2}{\|\mathbf{h}_2\|^2}}{b_1 + \frac{c_1}{\|\mathbf{h}_2\|^2}} = \frac{X}{b_1 + Y} \tag{60}$$

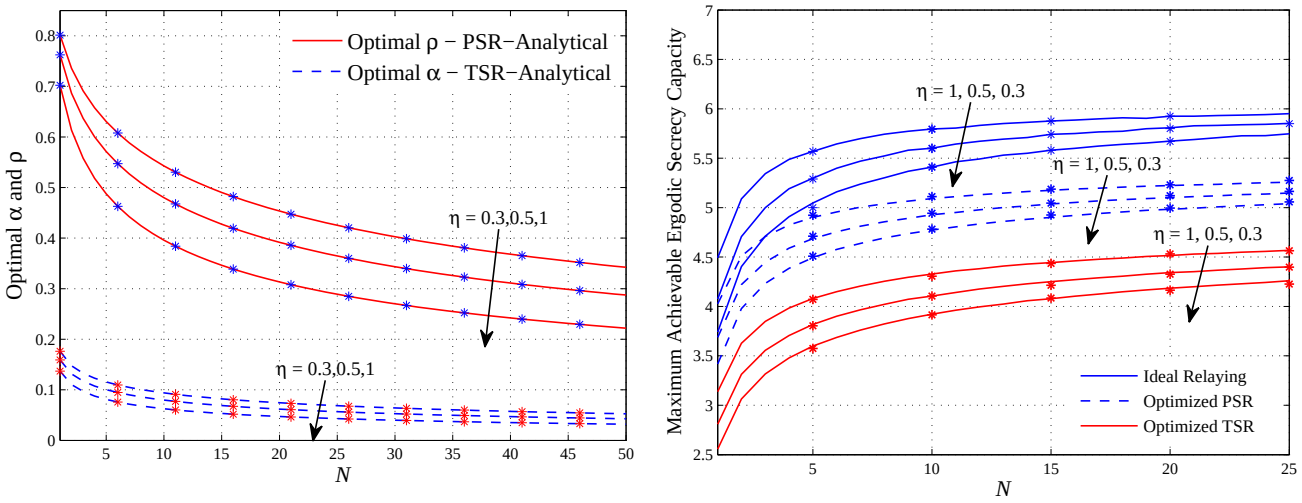
where $a_1 = 2\,\eta\,\alpha\,P_s$, $b_1 = 2\,\eta\,\alpha\,d_1^m\sigma_r^2$, $c_1 = (1-\alpha)\; d_1^m d_2^m \sigma_d^2$, $X = a_1 \frac{|\mathbf{h}_2\mathbf{h}_1|^2}{\|\mathbf{h}_2\|^2}$ and $Y = \frac{c_1}{\|\mathbf{h}_2\|^2}$. Consequently, we can get

$$\mathbb{E}\left[C_d^{TSR}\right] = \frac{1-\alpha}{2}\, \mathbb{E}\left[\log_2\left(1 + \frac{X}{b_1 + Y}\right)\right]. \tag{61}$$

It is presented in [29] that for any random variables $u, v > 0$

$$\mathbb{E}\left[\ln\left(1 + \frac{u}{v}\right)\right] = \int_0^\infty \frac{1}{z}\left(\mathcal{M}_v(z) - \mathcal{M}_{v+u}(z)\right) dz \tag{62}$$

where $\mathcal{M}_v(z)$ denotes the moment generating function (MGF) of v defined as



(a) Optimal values of α and ρ.

(b) Maximum achievable ergodic secrecy capacity.

Figure 6: Optimal values of α and ρ with the corresponding maximum achievable ergodic secrecy capacity versus the number of relay antennas for the TSR, PSR and IRR based systems with various values of η (stars represent simulation results).

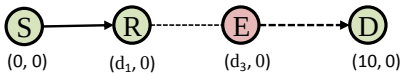


Figure 7: The system configuration used to highlight the impact of relay location, eavesdropper location and AN on the system secrecy capacity.

$$\mathcal{M}_v(z) = \int_{-\infty}^{\infty} e^{-zv} f(v)\, dv \tag{63}$$

where $f(v)$ is the probability density function. Using this definition in (62), and since X and Y are independent [30], (61) can be rewritten as

$$\mathbb{E}\left[C_d^{TSR}\right] = \frac{1-\alpha}{2\ln(2)} \int_0^{\infty} \frac{1}{z} \left(1 - \mathcal{M}_X(z)\right) \mathcal{M}_{b_1+Y}(z)\, dz \tag{64}$$

Because X has exponential distribution with parameter $\lambda_x > 0$ [30], its MGF is

$$\mathcal{M}_X(z) = \frac{\lambda_x}{\lambda_x + a_1 z}. \tag{65}$$

In addition, $\|\mathbf{h}_2\|^2$ has chi-square distribution, hence the MGF of $b_1 + Y$ can be given by [31]

$$\mathcal{M}_{b_1+Y}(z) = \frac{2\, e^{-zb_1} \left(c_1 z\right)^{N/2}}{\Gamma(N)} K_N\left(2\sqrt{c_1 z}\right) \tag{66}$$

where $\Gamma(.)$ is the Gamma function and $K_N(.)$ is the N^{th} order modified Bessel function of the second kind [27]. Substituting (65) and (66) into (64) yields (21).

- Eavesdropper Ergodic Capacity

Similarly, we now calculate the ergodic capacity at the eavesdropper by first simplifying (19) to

$$\gamma_e^{(1)} = \frac{P_s d_4^m \left|g_1\right|^2}{P_d d_3^m \left|g_2\right|^2 + d_3^m d_4^m \sigma_e^2} = \frac{\left|g_1\right|^2}{b_3 \left|g_2\right|^2 + c_3} \tag{67}$$

and

$$\gamma_e^{(2)} = \frac{\frac{\left|\mathbf{g}_3 \mathbf{h}_1\right|^2}{\|\mathbf{g}_3\|^2}}{b_2 \frac{\left|\mathbf{g}_3 \mathbf{h}_2^{\dagger}\right|^2}{\|\mathbf{g}_3\|^2} + c_2 + \frac{r}{\|\mathbf{g}_3\|^2}} = \frac{\Phi}{\Upsilon + c_2 + \zeta} \tag{68}$$

where $b_3 = \frac{P_d d_3^m}{P_s d_4^m}$, $c_3 = \frac{d_3^m d_4^m \sigma_e^2}{P_s d_4^m}$, $b_2 = \frac{2\,\eta\,\alpha\, d_1^m P_d}{2\,\eta\,\alpha\, P_s d_2^m}$, $c_2 = \frac{2\,\eta\,\alpha\, d_1^m d_2^m \sigma_r^2}{2\,\eta\,\alpha\, P_s d_2^m}$, $r = \frac{(1-\alpha)\, d_1^m d_2^m d_5^m \sigma_e^2}{2\,\eta\,\alpha\, P_s d_2^m}$, $\Phi = \frac{\left|\mathbf{g}_3 \mathbf{h}_1\right|^2}{\|\mathbf{g}_3\|^2}$, $\Upsilon = b_2 \frac{\left|\mathbf{g}_3 \mathbf{h}_2^{\dagger}\right|^2}{\|\mathbf{g}_3\|^2}$ and $\zeta = \frac{r}{\|\mathbf{g}_3\|^2}$. Using these definitions, the ergodic capacity at the eavesdropper for the TSR can now be expressed as

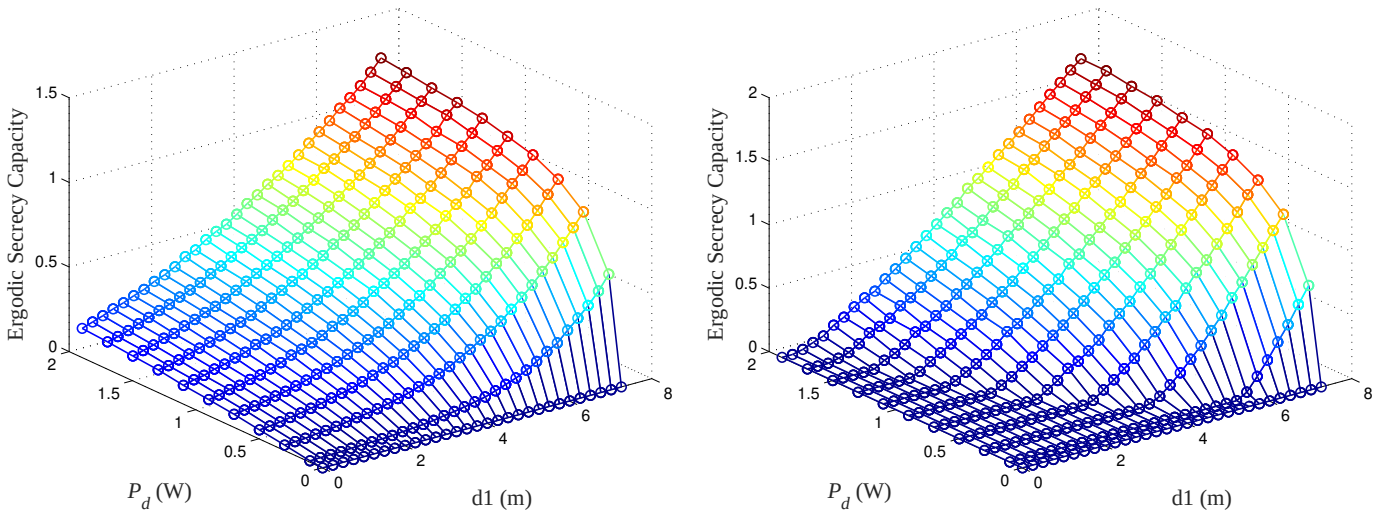
$$\mathbb{E}\left[C_e^{TSR}\right] = \frac{1-\alpha}{2}\, \mathbb{E}\left[\log_2\left(1 + \frac{\left|g_1\right|^2}{b_3 \left|g_2\right|^2 + c_3} + \frac{\Phi}{\Upsilon + c_2 + \zeta}\right)\right] \tag{69}$$

From [29], we can rewrite (69) as

$$\mathbb{E}\left[C_e^{TSR}\right] = \frac{1-\alpha}{2\ln(2)} \int_0^{\infty} \frac{1}{z} \left(1 - \mathcal{M}_{\gamma_e^{(1)}}(z)\, \mathcal{M}_{\gamma_e^{(2)}}^{TSR}(z)\right) e^{-z} dz. \tag{70}$$

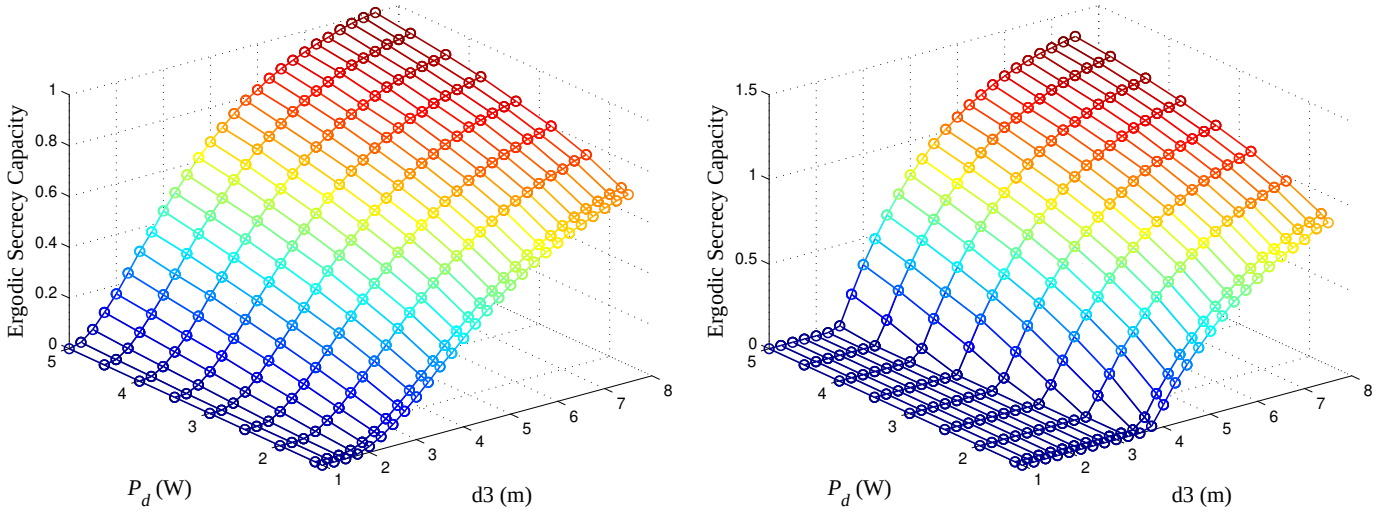
where $\mathcal{M}_{\gamma_e^{(1)}}(z)$ is the MGF of $\gamma_e^{(1)}$ and $\mathcal{M}_{\gamma_e^{(2)}}^{TSR}(z)$ is the MGF of $\gamma_e^{(2)}$. To derive MGF of $\gamma_e^{(1)}$, we start with

$$\mathcal{M}_{\gamma_e^{(1)}}(z) = \int_0^{\infty} e^{-z\gamma} f_{\gamma_e^{(1)}}(\gamma)\, d\gamma \tag{71}$$



(a) TSR. (b) PSR.

Figure 8: A 3D surface plot for the optimal secrecy capacity as a function of the source-to-destination distance and AN power for the TSR- and PSR-based systems. Circles represent simulated results.



(a) TSR. (b) PSR.

Figure 9: A 3D surface plot for the optimal secrecy capacity as a function of the source-to-eavesdropper distance and AN power for the TSR- and PSR-based systems. Circles represent simulated results.

Using integration by parts, we can get

$$\mathcal{M}_{\gamma_e^{(1)}}(z) = 1 - z\int_0^{\infty} e^{-z\gamma}\mathcal{M}_{b_3|g_2|^2+c_3}(\gamma)\,d\gamma \tag{72}$$

$\mathcal{M}_{b_3|g_2|^2+c_3}$ is found as [31]

$$\mathcal{M}_{b_3|g_2|^2+c_3}(\gamma) = \mathcal{M}_{|g_2|^2}(b_3\gamma)\; e^{-\gamma\, c_3} \tag{73}$$

Since $|g_2|^2$ has exponential distribution, $\mathcal{M}_{|g_2|^2}(b_3\gamma) = \frac{\lambda_{g_2}}{\lambda_{g_2}+b_3\gamma}$, and by substituting (73) into (72), we can get (23). Similarly, we can calculate the MGF of $\gamma_e^{(2)}$as

$$\mathcal{M}^{TSR}_{\gamma_e^{(2)}}(z) = 1 - z\int_0^{\infty} e^{-zq}\mathcal{M}_{\Upsilon+c_2+\zeta}(q)\,dq \tag{74}$$

Since Υ and $\|\mathbf{g}\|^2$ have exponential and chi-square distributions, respectively, the MGF of $\Upsilon + c_2 + \zeta$ can be given as

$$\mathcal{M}_{\Upsilon+c_2+\zeta}(q) = \underbrace{\frac{\lambda_\Upsilon}{\lambda_\Upsilon + b_2 q}}_{\mathcal{M}_\Upsilon(q)}.e^{-zc_2}.\underbrace{\frac{2\,(r\,q)^{N/2}}{\Gamma(N)}K_N\left(2\sqrt{r\,q}\right)}_{\mathcal{M}_\zeta(q)}. \tag{75}$$

Now, substituting (75) into (74), we can get $\mathcal{M}^{TSR}_{\gamma_e^{(2)}}(z)$. Finally, by substituting (74) and (23) into (70) we can find the eavesdropper ergodic capacity of the proposed TSR system.

Appendix B

This appendix derives the destination and eavesdropper ergodic capacities of the PSR-based system.

- Destination Ergodic Capacity

We first rewrite (37) in the following form

$$\gamma_d = \frac{a_1 \frac{|\mathbf{h_2 h_1}|^2}{\|\mathbf{h_2}\|^2}}{b_1 + c_1 + \frac{r_1}{\|\mathbf{h_2}\|^2}} = \frac{X}{b_1 + c_1 + Y} \tag{76}$$

while $X = a_1 \frac{|\mathbf{h_2 h_1}|^2}{\|\mathbf{h_2}\|^2}$ and $Y = \frac{r_1}{\|\mathbf{h_2}\|^2}$, a_1, b_1, c_1 and r_1 are defined in (43). Using (62), $\mathbb{E}\left[C_d^{PSR}\right]$ can be expressed as

$$\mathbb{E}\left[C_d^{PSR}\right] = \frac{1}{2\ln(2)} \int_0^\infty \frac{1}{z} \left(1 - \mathcal{M}_X(z)\right) \mathcal{M}_{b_1+c_1+Y}(z)\, dz \tag{77}$$

where $\mathcal{M}_X(z)$ and $\mathcal{M}_{b_1+c_1+Y}(z)$ are given, respectively, by

$$\mathcal{M}_X(z) = \frac{\lambda_X}{\lambda_X + (a_1 * z)} \tag{78}$$

and

$$\mathcal{M}_{b_1+c_1+Y}(z) = e^{-(b_1+c_1)} \frac{2\,(r_1 z)^{N/2}}{\Gamma(N)} K_N\left(2\sqrt{r_1 z}\right). \tag{79}$$

- Eavesdropper Ergodic Capacity

Similarly, we can derive $\mathbb{E}\left[C_e^{PSR}\right]$. First, we simplify $\gamma_e^{(2)}$ to

$$\gamma_e^{(2)} = \frac{\frac{|\mathbf{g_3 h_1}|^2}{\|\mathbf{g_3}\|^2}}{b_2 \frac{\left|\mathbf{g_3 h_2^\dagger}\right|^2}{\|\mathbf{g_3}\|^2} + c_2 + r_2 + \frac{\omega}{\|\mathbf{g_3}\|^2}} = \frac{\Phi}{\Upsilon + c_2 + r_2 + \varphi} \tag{80}$$

when $\Phi = \frac{|\mathbf{g_3 h_1}|^2}{\|\mathbf{g_3}\|^2}$, $\Upsilon = b_2 \frac{\left|\mathbf{g_3 h_2^\dagger}\right|^2}{\|\mathbf{g_3}\|^2}$, $\varphi = \frac{\omega}{\|\mathbf{g_3}\|^2}$, and b_2, c_2, r_2 and ω are defined in (43). Again, we can get the ergodic eavesdropper capacity by

$$\mathbb{E}\left[C_e^{PSR}\right] = \frac{1}{2\ln(2)} \int_0^\infty \frac{1}{z} \left(1 - \mathcal{M}_{\gamma_e^{(1)}}(z)\, \mathcal{M}_{\gamma_e^{(2)}}^{PSR}(z)\right) e^{-z} dz \tag{81}$$

where $\mathcal{M}_{\gamma_e^{(1)}}(z)$ is given by (23) and

$$\mathcal{M}_{\gamma_e^{(2)}}^{PSR}(z) = 1 - z \int_0^\infty \mathcal{M}_{\Upsilon+c_2+r_2+\varphi}(q)\; e^{-zq}\, dq \tag{82}$$

where

$$\mathcal{M}_{\Upsilon+c_2+r_2+\varphi}(q) = \frac{\lambda_\Upsilon e^{-q(c_2+r_2)}}{\lambda_\Upsilon + (b_2 * q)} \frac{2\,(\omega q)^{N/2}}{\Gamma(N)} K_N\left(2\sqrt{\omega q}\right) \tag{83}$$

Now, substituting (23) and (82) into (81) yields $\mathbb{E}\left[C_e^{PSR}\right]$.

APPENDIX C

Here we derive expressions for the destination and eavesdropper ergodic capacities of the IRR-based system.

- Destination Ergodic Capacity

For convenience, we first rewrite (50) as

$$\gamma_d = \frac{a_1 \frac{|\mathbf{h_2 h_1}|^2}{\|\mathbf{h_2}\|^2}}{b_1 + \frac{c_1}{\|\mathbf{h_2}\|^2}} = \frac{X}{b_1 + Y} \tag{84}$$

where $X = a_1 \frac{|\mathbf{h_2 h_1}|^2}{\|\mathbf{h_2}\|^2}$, $Y = \frac{c_1}{\|\mathbf{h_2}\|^2}$, a_1, b_1 and c_1 are given in (56). Using (62), we obtain

$$\mathbb{E}\left[C_d^{IRR}\right] = \frac{1}{2\ln(2)} \int_0^\infty \frac{1}{z} \left(1 - \mathcal{M}_X(z)\right) \mathcal{M}_{b_1+Y}(z)\, dz \tag{85}$$

where

$$\mathcal{M}_X(z) = \frac{\lambda_X}{\lambda_X + (a_1 * z)} \tag{86}$$

and

$$\mathcal{M}_{b_1+Y}(z) = e^{-z b_1} \frac{2\,(c_1 z)^{N/2}}{\Gamma(N)} K_N\left(2\sqrt{c_1 z}\right). \tag{87}$$

- Eavesdropper Ergodic Capacity

As for the ergodic capacity at eavesdropper, (51) can be simplified as

$$\gamma_e^{(2)} = \frac{\frac{|\mathbf{g_3 h_1}|^2}{\|\mathbf{g_3}\|^2}}{b_2 \frac{\left|\mathbf{g_3 h_2^\dagger}\right|^2}{\|\mathbf{g_3}\|^2} + c_2 + \frac{r_2}{\|\mathbf{g_3}\|^2}} = \frac{\Phi}{\Upsilon + c_2 + \zeta} \tag{88}$$

where $\Phi = \frac{|\mathbf{g_3 h_1}|^2}{\|\mathbf{g_3}\|^2}$, $\Upsilon = b_2 \frac{\left|\mathbf{g_3 h_2^\dagger}\right|^2}{\|\mathbf{g_3}\|^2}$, $\zeta = \frac{r_2}{\|\mathbf{g_3}\|^2}$, b_2, c_2 and r_2 are defined in (56). Given the definition in (62), we can express $\mathbb{E}\left[C_e^{IRR}\right]$ as

$$\mathbb{E}\left[C_e^{IRR}\right] = \frac{1}{2\ln(2)} \int_0^\infty \frac{1}{z} \left(1 - \mathcal{M}_{\gamma^{(1)}}(z)\, \mathcal{M}_{\gamma_e^{(2)}}^{IRR}(z)\right) e^{-z} dz \tag{89}$$

where $\mathcal{M}_{\gamma_e^{(1)}}$ is given by (23) and

$$\mathcal{M}_{\gamma_e^{(2)}}^{IRR}(z) = 1 - z \int_0^\infty e^{-zq} \mathcal{M}_{\Upsilon+c_2+\zeta}(q)\, dq \tag{90}$$

and $\mathcal{M}_{\Upsilon+c_2+\zeta}(q)$ is given by

$$\mathcal{M}_{\Upsilon+c_2+\zeta}(q) = \frac{\lambda_\Upsilon e^{-qc_2}}{\lambda_\Upsilon + (b_2 * q)} \frac{2\,(r_2 q)^{N/2}}{\Gamma(N)} K_N\left(2\sqrt{r_2 q}\right). \tag{91}$$

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] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," *IEEE Trans. Commun.*, vol. 61, pp. 4754–4767, Nov. 2013.

[4] L. Liu, R. Zhang, and K.-C. Chua, "Wireless information transfer with opportunistic energy harvesting," *IEEE Trans. Wireless Commun.*, vol. 12, pp. 288–300, Jan. 2013.

[5] Z. Xiang and M. Tao, "Robust beamforming for wireless information and power transmission," *IEEE Wireless Commun. Lett.*, vol. 1, pp. 372–375, Aug. 2012.

[6] 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.

[7] B. Medepally and N. Mehta, "Voluntary energy harvesting relays and selection in cooperative wireless networks," *IEEE Trans. Wireless Commun.*, vol. 9, pp. 3543–3553, Nov. 2010.

[8] 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.

[9] Z. Ding, S. Perlaza, I. Esnaola, and H. Poor, "Power allocation strategies in energy harvesting wireless cooperative networks," *IEEE Trans. Wireless Commun*, vol. 13, pp. 846–860, February 2014.

[10] G. Zhu, C. Zhong, H. Suraweera, G. Karagiannidis, Z. Zhang, and T. Tsiftsis, "Wireless information and power transfer in relay systems with multiple antennas and interference," *IEEE Trans. Commun.*, vol. PP, no. 99, pp. 1–1, 2015.

[11] 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.

[12] Z. Ding, C. Zhong, D. Ng, M. Peng, H. Suraweera, R. Schober, and H. Poor, "Application of smart antenna technologies in simultaneous wireless information and power transfer," *IEEE Commun. Mag.*, vol. 53, pp. 86–93, April 2015.

[13] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[14] 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.

[15] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Trans. Veh. Techno*, vol. PP, no. 99, pp. 1–1, 2015.

[16] H. Xing, Z. Chu, Z. Ding, and A. Nallanathan, "Harvest-and-jam: Improving security for wireless energy harvesting cooperative networks," in *Proc. IEEE Global Commun. (GLOBECOM)*, pp. 3145–3150, Dec 2014.

[17] Q. Li, Q. Zhang, and J. Qin, "Secure relay beamforming for simultaneous wireless information and power transfer in nonregenerative relay networks," *IEEE Trans. Veh. Technol.*, vol. 63, pp. 2462–2467, Jun 2014.

[18] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, Jun. 2008.

[19] Z. Ding, K. Leung, D. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting," *IEEE Trans. Wireless Commun*, vol. 10, pp. 1725–1729, June 2011.

[20] 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.

[21] Y.-W. Hong, P.-C. Lan, and C.-C. Kuo, *Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems*. 2014.

[22] 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.

[23] J. Li and A. P. Petropulu, "On ergodic secrecy rate for gaussian miso wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, pp. 1176–1187, April 2011.

[24] R. Zhao, Y. Huang, W. Wang, and V. Lau, "Ergodic achievable secrecy rate of multiple-antenna relay systems with cooperative jamming," *IEEE Trans. Wireless Commun.*, vol. PP, no. 99, pp. 1–1, 2015.

[25] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 310–320, Feb 2012.

[26] L. Xiao, P. Wang, D. Niyato, D. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Surveys Tutorials Commun.*, vol. PP, no. 99, pp. 1–1, 2015.

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

[28] H. Meyr, M. Mseneclaey, and S. A. Fechtel, *Digital Communication Receivers, Synchronization, Channel Estimation, and Signal Processing*. J. G. Proakis, Ed. Wiley Series in Telecommunications and signal Processing, 1998.

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

[30] J. Cui and A. Sheikh, "Outage probability of cellular radio systems using maximal ratio combining in the presence of multiple interferers," *IEEE Trans. Commun.*, vol. 47, pp. 1121–1124, Aug 1999.

[31] S. M. ROSS, *Introduction to probability models 10ed*. 2010.

[32] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, May 1978.

[33] X. Zhou and M. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, pp. 3831–3842, Oct. 2010.

[34] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, pp. 1202–1216, Mar. 2011.

[35] Z. Chen, B. Xia, and H. Liu, "Wireless information and power transfer in two-way amplify-and-forward relaying channels," in *Proc. IEEE Global Conf. Signal and Inf. Process. (GlobalSIP)*, pp. 168–172, Dec 2014.

[36] R. Wang and M. Tao, "Outage performance analysis of two-way relay system with multi-antenna relay node," in *Proc. IEEE Int. Conf. Commun. (ICC)*, pp. 3538–3542, Jun. 2012.

[37] M. Hasna and M.-S. Alouini, "End-to-end performance of transmission systems with relays over rayleigh-fading channels," *IEEE Trans. Wireless Commun.*, vol. 2, pp. 1126–1131, Nov. 2003.

[38] Y. Liu, L. Wang, M. Elkashlan, T. Duong, and A. Nallanathan, "Two-way relaying networks with wireless power transfer: Policies design and throughput analysis," in *Proc. IEEE Global Commun. (GLOBECOM)*, pp. 4030–4035, Dec. 2014.

[39] A. Ozgur, O. Leveque, and D. Tse, "Hierarchical cooperation achieves optimal capacity scaling in ad hoc networks," *IEEE Trans. Inf. Theory*, vol. 53, pp. 3549–3572, Oct 2007.

[40] 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.

[41] H. Hui, A. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Process. Lett.*, vol. 22, pp. 1147–1151, Aug 2015.

[42] X. Wang, K. Wang, and X.-D. Zhang, "Secure relay beamforming with imperfect channel side information," *IEEE Trans. Veh. Technol.*, vol. 62, pp. 2140–2155, Jun 2013.

[43] Z. Ding, I. Krikidis, B. Sharif, and H. Poor, "Wireless information and power transfer in cooperative networks with spatially random relays," *IEEE Trans. Wireless Commun.*, vol. 13, pp. 4440–4453, Aug 2014.

[44] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving wireless physical layer security via cooperating relays," *Signal Processing, IEEE Transactions on*, vol. 58, pp. 1875–1888, March 2010.

[45] S.-I. Kim, I.-M. Kim, and J. Heo, "Secure transmission for multiuser relay networks," *Wireless Communications, IEEE Transactions on*, vol. 14, pp. 3724–3737, July 2015.

Abdelhamid Salem (S'12), received the B.Sc. degree in Electrical and Electronic Engineering from the University of Benghazi, Benghazi, Libya, in 2002 and the M.Sc. degree (with distinction) in Communication Engineering from the University of Benghazi, Benghazi, Libya, in 2009, he is currently working toward the Ph.D. degree in wireless communications with The University of Manchester, United Kingdom . His current research interests include Physical Layer Security, signal processing for interference mitigation, energy harvesting, wireless power transfer, MIMO systems, wireless optical communication systems and power line communications.

Khairi Ashour Hamdi (M'99-SM'02) received the B.Sc. degree in electrical engineering from the Alfateh University, Tripoli, Libya, in 1981, the M.Sc. degree (with distinction) from the Technical University of Budapest, Budapest, Hungary, in 1988, and the Ph.D. degree in telecommunication engineering in 1993, awarded by the Hungarian Academy of Sciences. His current research interests include modelling and performance analysis of wireless communication systems and networks.

Khaled Maaiuf Rabie (S'12-M'15), received the B.Sc. degree (with Hons.) in Electrical and Electronic Engineering from the University of Tripoli, Tripoli, Libya, in 2008 and the M.Sc. degree (with Hons.) in Communication Engineering from the University of Manchester, Manchester, UK, in 2010. He is currently pursuing the Ph.D. degree with Microwave and Communications Systems (MCS) group at the University of Manchester.