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

DOI:
10.1109/TCOMM.2016.2573829

Document Version
Accepted author manuscript

Link to publication record in Manchester Research Explorer

Citation for published version (APA):

Published in:
IEEE Transactions on Communications

Citing this paper
Please note that where the full-text provided on Manchester Research Explorer is the Author Accepted Manuscript or Proof version this may differ from the final Published version. If citing, it is advised that you check and use the publisher's definitive version.

General rights
Copyright and moral rights for the publications made accessible in the Research Explorer are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

Takedown policy
If you believe that this document breaches copyright please refer to the University of Manchester’s Takedown Procedures [http://man.ac.uk/04Y6Bo] or contact uml.scholarlycommunications@manchester.ac.uk providing relevant details, so we can investigate your claim.
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 decoding1.

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].

1In 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-destination channel vector, the source-to-relay channel vector, the relay-to-destination 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 eavesdroper, destination to eavesdroper and relay to eavesdroper nodes are represented by $d_1$, $d_2$, $d_3$, $d_4$ and $d_5$, respectively.

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 eavesdroper is unknown at the legitimate nodes.
- The eavesdroper 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].

2The 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.
In this paper we assume that the destination has full state
third case is the lower bound of the first case,
\[ \bar{C}_s \]
where \( I(x; y) \) is the mutual information between the source and destination, 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)]
\[ \bar{C}_{s1} = \max_{P(h_{sd},h_{se})} \mathbb{E} \left[ \left| C_d - C_e \right|^+ \right] \]  
(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)]
\[ \bar{C}_{s2} = \max_{P(h_{sd})} \mathbb{E} \left[ \left| C_d - C_e \right|^+ \right] \]  
(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]
\[ \bar{C}_{s3} = \mathbb{E} \left[ C_d - C_e \right]^+ \]  
(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 \( C_d = \frac{1}{2} \log_2 (1 + \gamma_d) \) and \( C_e = \frac{1}{2} \log_2 (1 + \gamma_e) \), respectively, whereas \( \gamma_d \) and \( \gamma_e \) 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 \( \alpha T \), 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 \( \alpha T \) is used by the relay to forward the received signal. To elaborate, in phase I, the received signal at the relay node can be given as
\[ y_r = \sqrt{\frac{P_s}{d^a_1}} h_1 s + \sqrt{\frac{P_d}{d^a_2}} h_2 v + n_a \]  
(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, \( v \) is the AN signal coming from the legitimate destination, and \( \mathbb{E} \left[ |v|^2 \right] = 1 \). \( m \) is the path loss exponent and \( n_a \) is the additive white Gaussian noise (AWGN) vector introduced by the receiver antennas at the relay, i.e. \( n_a \sim \mathcal{CN}(0, \sigma_a^2 I_N) \). During \( \alpha T \) the harvested energy by the EH receiver is given by [3]
\[ E_h = \eta \alpha T \left( \frac{P_s}{d^a_1} \| h_1 \|^2 + \frac{P_d}{d^a_2} \| h_2 \|^2 + N \sigma_a^2 \right) \]  
(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
\[ y_r = \sqrt{\frac{P_s}{d^a_1}} h_1 s + \sqrt{\frac{P_d}{d^a_2}} h_2 v + n_r \]  
(7)
where \( n_r \) is an \( N \times 1 \) AWGN vector at the relay, i.e. \( n_r \sim \mathcal{CN}(0, \sigma_r^2 I_N) \). \( n_r = n_a + n_e \) and \( n_e \) is the noise vector introduced by the information receiver, i.e. \( n_e \sim \mathcal{CN}(0, \sigma_e^2 I_N) \) [8], [11]. Furthermore, the received signal at the eavesdropper in the first phase is given by
\[ y_e^{(1)} = \sqrt{\frac{P_s}{d^a_3}} g_1 s + \sqrt{\frac{P_d}{d^a_4}} g_2 v + n_e \]  
(8)
\(^3\)In other words, the energy consumed by the relay circuitry to process the information signals is negligible in this study.
where \( n_e \) is the AWGN signal at the eavesdropper with variance \( \sigma_e^2 \), i.e., \( n_e \sim \mathcal{CN}(0, \sigma_e^2) \). In phase II, the relay transmitted signal, \( x_r \), can be written as

\[
x_r = G y_r
\]

where \( G \) is the relay gain given by

\[
G = \sqrt{P_r \beta_t}.
\]

Here, \( P_r \) is the relay transmit power and

\[
\beta_t = \frac{P_r}{d_1^m} || h_1 ||^2 + \frac{P_d}{d_2^m} || h_2 ||^2 + N \sigma_d^2.
\]

Consequently, the received signal at the destination is

\[
y_d = \sqrt{\frac{P_s P_r \beta_t}{d_1^m d_2^m}} h_2 h_1 s + \sqrt{\frac{P_s P_r \beta_t}{d_1^m d_2^m}} h_2 h^\dagger v + \sqrt{\frac{P_s \beta_t}{d_2^m}} h_2 n_r + n_d, \quad (12)
\]

where \( n_d \) is the AWGN signal at the destination with variance \( \sigma_d^2 \), i.e., \( n_d \sim \mathcal{CN}(0, \sigma_d^2) \) 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, \( v \) can be easily removed at the destination; hence, \( y_d \) can be simplified to

\[
y_d = \sqrt{\frac{P_s P_r \beta_t}{d_1^m d_2^m}} h_2 h_1 s + \sqrt{\frac{P_s \beta_t}{d_2^m}} h_2 n_r + n_d. \quad (13)
\]

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

\[
y_e^{(2)} = \sqrt{\frac{P_s P_r \beta_t}{d_1^m d_5^m}} g_3 h_1 s + \sqrt{\frac{P_s P_d \beta_t}{d_2^m d_5^m}} g_3 h_1^\dagger v + \sqrt{\frac{P_s \beta_t}{d_5^m}} g_3 n_r + n_e. \quad (14)
\]

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

\[
P_r = \frac{E_h}{(1 - \alpha) T/2} \quad (15)
\]

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

\[
P_r = \frac{2 \eta \alpha}{(1 - \alpha)} \left[ \frac{P_s}{d_1^m} || h_1 ||^2 + \frac{P_d}{d_2^m} || h_2 ||^2 + N \sigma_d^2 \right]. \quad (16)
\]

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

\[
\gamma_d = \frac{2 \eta \alpha P_s || h_2 h_1 ||^2}{2 \eta \alpha d_1^m \sigma_e^2 || h_2 ||^2 + (1 - \alpha) d_1^m d_2^m \sigma_d^2}. \quad (17)
\]

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 \[24\], \[25\]

\[
y_e = w_1 y_e^{(1)} + w_2 y_e^{(2)} \quad (18)
\]

where \( w_1 = \sqrt{\frac{P_s P_r \beta_t}{d_1^m || g_3 ||^2 + \sigma_e^2}} \) and \( w_2 = \sqrt{\frac{P_s P_d \beta_t}{d_1^m || g_3 ||^2 + \sigma_e^2}} (\cdot)^H \), while \( (\cdot)^H \) is the transpose conjugate operation. From (18) we can get the SNR at the eavesdropper \( \gamma_e \) as given by (19), shown at the top of the next page.

The ergodic secrecy capacity of this system can be obtained as

\[
C_s^{[TSR]} = \left[ \mathbb{E} \left[ C_d^{[TSR]} \right] - \mathbb{E} \left[ C_e^{[TSR]} \right] \right] +. \quad (20)
\]

According to the best of the authors knowledge, the simplest form of \[26\] and \[27\] can be written respectively as in (21) and (22), shown at the top of the next page, where \( M_{\gamma_e}^{(1)} (z) \), \( M_{\gamma_e}^{[TSR]} (z) \) are given by (23) and (24), also shown at the top of the next page, and \( a_1 = 2 \eta \alpha P_s, b_1 = 2 \eta \alpha d_1^m \sigma_e^2 \).

\(^4\)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.
\[
\gamma_e = \frac{P_s d_m^m |g_1|^2}{\eta_\alpha d_{d3}^m |g_2|^2} + \frac{2 \eta_\alpha P_s d_m^m |g_3 h_1|^2}{\eta_\alpha d_{d1}^m P_d |g_3 h_2|^2} + \frac{2 \eta_\alpha P_s d_m^m |g_3 h_1|^2}{\eta_\alpha d_{d2}^m d_m^m \sigma_r^2}.
\]

(19)

\[c_1 = (1 - \alpha) d_1^m d_2^m \sigma_r^2, \quad a_2 = 2 \eta_\alpha P_s d_m^m, \quad b_2 = \frac{2 \eta_\alpha P_s d_m^m}{2 \eta_\alpha P_s d_m^m}, \quad c_2 = \frac{2 \eta_\alpha d_1^m d_2^m \sigma_r^2}{2 \eta_\alpha P_s d_m^m}, \quad r = \frac{1 - \alpha) d_1^m d_2^m d_m^m \sigma_r^2}{2 \eta_\alpha P_s d_m^m}, \quad b_3 = \frac{P_d d_m^m}{P_s d_m^m}, \quad c_3 = \frac{d_m^m \sigma_r^2}{P_s}.
\]

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, \( \rho P \), at the relay is allocated for EH and the remaining received power, \( (1 - \rho) P \), is used for the information signal 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

\[y_r = \sqrt{\rho P} d_1^m h_1 s + \sqrt{\rho P} d_2^m h_2 v + \sqrt{\rho P} n_s.
\]

(25)

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

\[E_h = \eta \rho T \left[ \frac{P_s}{d_1^m} ||h_1||^2 + \frac{P_d}{d_2^m} ||h_2||^2 + N \sigma_a^2 \right].
\]

(26)

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

\[y_r = \sqrt{(1 - \rho) P_s} d_1^m h_1 s + \sqrt{(1 - \rho) P_d} d_2^m h_2 v + n_r.
\]

(27)

where \( n_r = \sqrt{1 - \rho} n_s + n_c \). Now, the received signal at the eavesdropper in the first phase can be written as

\[y_e^{(1)} = \sqrt{\frac{P_s}{d_3^m}} g_1 s + \sqrt{\frac{P_d}{d_4^m}} g_2 v + n_e.
\]

(28)

In phase II, the relay transmits the following signal

\[x_r = G y_r
\]

(29)

where \( G \) represents the relay gain given by

\[G = \sqrt{P_r \beta_p}
\]

(30)

\[P_r \text { is the relay power and } \beta_p \text { is given by}
\]

\[\beta_p = \frac{1}{(1 - \rho) P_s} ||h_1||^2 + \frac{1}{(1 - \rho) P_d} ||h_2||^2 + N \sigma_r^2.
\]

(31)

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

Similar to the TSR scenario, \( v \) can be easily removed at the destination; hence, \( y_d \) is simplified to

\[y_d = \sqrt{(1 - \rho) P_s d_1^m d_2^m} g_3 h_1 s + \sqrt{P_r \beta_p d_2^m} \frac{\sqrt{P_r \beta_p} h_2}{\sqrt{d_2^m}} n_r + n_d.
\]

(33)

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

\[y_e^{(2)} = \sqrt{(1 - \rho) P_s d_1^m d_2^m} g_3 h_1 s + \sqrt{P_r \beta_p d_1^m d_2^m} g_3 h_2 v + \sqrt{P_r \beta_p d_1^m d_2^m} n_r + n_e.
\]

(34)

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

\[P_r = \frac{E_h}{T/2}.
\]

(35)

Using (26), \( P_r \) can be expressed as

\[P_r = \eta \rho \left[ \frac{P_s}{d_1^m} ||h_1||^2 + \frac{P_d}{d_2^m} ||h_2||^2 + N \sigma_a^2 \right].
\]

(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

\[C_s^{PSR} = \left[ E \left[ C_d^{PSR} \right] - E \left[ C_e^{PSR} \right] \right]^+
\]

(39)

while \( E \left[ C_d^{PSR} \right] \) and \( E \left[ C_e^{PSR} \right] \) are given by (40) and (41), respectively, where \( M_{\gamma_c} (z) \) is given by (23) and \( M_{\gamma_c}^{PSR} (z) \) is given by (42), and

\[a_1 = \eta \rho (1 - \rho) P_s, \quad b_1 = \eta \rho d_1^m \sigma_c^2, \quad c_1 = \eta \rho (1 - \rho) d_1^m \sigma_a^2, \quad r_1 = (1 - \rho) d_1^m d_2^m \sigma_a^2, \quad a_2 = \eta \rho (1 - \rho) P_s d_2^m, \quad b_2 = \eta \rho (1 - \rho) d_1^m P_s/\alpha_2, \quad c_2 = \eta \rho (1 - \rho) d_1^m d_2^m \sigma_a^2/\alpha_2, \quad r_2 = \eta \rho d_1^m d_2^m \sigma_a^2/\alpha_2, \quad \omega = (1 - \rho) d_1^m d_2^m d_3^m \sigma_a^2/\alpha_2.
\]

Proof: The proof is provided in Appendix B. ■
Energy Harvesting & Information Transmission

\[ E[C_{d}^{TSR}] = \frac{1 - \alpha}{2 \ln(2)} \int_{0}^{\infty} \left( 1 - \frac{\lambda_x}{\lambda_y + \alpha z} \right) \frac{2 e^{-z b_1} (c_1 z)^{N/2}}{\Gamma(N)} K_N(2\sqrt{c_1 z}) (z) \, dz. \] (21)

\[ E[C_{e}^{TSR}] = \frac{1 - \alpha}{2 \ln(2)} \int_{0}^{\infty} \left( 1 - \mathcal{M}_{\gamma_e^{(1)}}(z) \mathcal{M}_{\gamma_e^{(2)}}(z) \right) e^{-z} \, dz. \] (22)

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

\[ \mathcal{M}_{\gamma_e^{(2)}}(z) = 1 - z \int_{0}^{\infty} e^{-z q} \frac{\lambda_T}{\lambda_T + (b_2 + q)} e^{-q c_2} \frac{2 (r q)^{N/2}}{\Gamma(N)} K_N(2\sqrt{r q}) \, dq. \] (24)

\[ y_d = \sqrt{\frac{(1 - \rho) P_o P_s \beta_2}{d_1 m d_2}} \mathbf{h}_2 \mathbf{h}_1 s + \sqrt{\frac{(1 - \rho) P_s P_r \beta_3}{d_2 m}} \mathbf{h}_2 \mathbf{h}_2^* v + \frac{\sqrt{P_r \beta_3}}{\sqrt{d_2}} \mathbf{n}_r + n_d. \] (32)

\[ \gamma_d = \frac{\eta \rho (1 - \rho) P_s |\mathbf{h}_2 \mathbf{h}_1|^2}{\eta \rho d_1 m^2 \sigma_c^2 ||\mathbf{h}_2||^2 + \eta \rho (1 - \rho) d_2 m \sigma_a^2 ||\mathbf{h}_2||^2 + (1 - \rho) d_1 m d_2 \sigma_c^2}. \] (37)

\[ \gamma_e = \frac{P_s d_1 m |g_1|^2}{P_d d_3 m |g_2|^2 + d_4 m \sigma_c^2} + \frac{\eta \rho (1 - \rho) P_s d_2 m |g_3 \mathbf{h}_1|^2}{\eta \rho (1 - \rho) d_1 m P_d |g_3 \mathbf{h}_1|^2 + \eta \rho (1 - \rho) d_1 m \sigma_a^2 ||g_3||^2 + \eta \rho d_2 m \sigma_c^2 ||g_3||^2 + (1 - \rho) d_1 m d_2 \sigma_c^2}. \] (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. 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

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

and

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

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

\[ y_e^{(1)} = \sqrt{\frac{P_s}{d_3 m} g_1 s} + \sqrt{\frac{P_d}{d_4 m}} g_2 v + n_e \] (46)

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

\[ y_d = \sqrt{\frac{P_s P_r \beta_1}{d_1 m d_2}} \mathbf{h}_2 \mathbf{h}_1 s + \sqrt{\frac{P_r \beta_3}{d_2 m}} \mathbf{h}_2 \mathbf{n}_r + n_d \] (47)

and

\[ y_d = \sqrt{\frac{P_s P_r \beta_1}{d_1 m d_2}} \mathbf{h}_2 \mathbf{h}_1 s + \sqrt{\frac{P_r \beta_3}{d_2 m}} \mathbf{h}_2 \mathbf{n}_r + n_d \] (47)
\[ E[C_d^{PSR}] = \frac{1}{2 \ln(2)} \int_0^{\infty} \left( 1 - \frac{\lambda_X}{\lambda_X + (a_1 + z)} \right) e^{-(b_1 + c_1)z} \frac{2 \Gamma(N/2)}{\Gamma(N)} K_N(2\sqrt{r_1 z}) \, dz. \] (40)

\[ E[C_e^{PSR}] = \frac{1}{2 \ln(2)} \int_0^{\infty} \left( 1 - \mathcal{M}_{\gamma_1}(z) \mathcal{M}_{\gamma_2}(z) \right) e^{-z} \, dz. \] (41)

\[ \mathcal{M}_{\gamma_2}(z) = 1 - z \int_0^{\infty} e^{-zq} e^{-q(c_2 + r_2)} \frac{\lambda_T}{\lambda_T + (b_2 + q)} \frac{2 \Gamma(N/2)}{\Gamma(N)} K_N(2\sqrt{\omega q}) \, dq. \] (42)

\[ y_c^{(2)} = \sqrt{\frac{P_r \beta_i}{d_s^m d_5}} g_s h_1 s + \sqrt{\frac{P_r \beta_i}{d_s^m d_5}} g_s n_r + n_e \] (48)

\[ \beta_i = \frac{P_{rs}}{\eta d_s^m} ||h_1||^2 + \frac{P_{rs}}{d_s^m} ||h_2||^2 + N\sigma_r^2. \] (49)

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

\[ C_{d}^{IRR} = \left[ E[C_d^{IRR}] - E[C_e^{IRR}] \right]^+ \] (52)

\[ E[C_d^{IRR}] \text{ and } E[C_e^{IRR}] \] can be expressed as in (53) and (54), respectively, where \( \mathcal{M}_{\gamma_1}(z) \) is given by (23), \( \mathcal{M}_{\gamma_2}(z) \) is given by (55) and

\[ a_1 = \eta P_s, \] (56a)

\[ b_1 = \eta \frac{d_s^m}{\sigma_r^2} \] (56b)

\[ c_1 = \frac{d_s^m}{\sigma_r^2} \] (56c)

\[ a_2 = \eta P_s d_2^m, \] (56d)

\[ b_2 = \eta d_s^m P_d/a_2, \] (56e)

\[ c_2 = \eta \frac{d_s^m}{\sigma_r^2} \] (56f)

\[ r_2 = \frac{d_s^m}{\sigma_r^2} \] (56g)

\[ \text{Proof: The proof is provided in Appendix C.} \]

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 \( \sigma_a = \sigma_d = \sigma_e^2 = -10 \) dBm while \( \sigma_a^2 = \sigma_d^2 = \sigma_e^2/2 \); also \( \lambda_X, \lambda_Y, \lambda_\phi \) and \( \lambda_T \) are all set to 1. It should also be mentioned that the secrecy capacity integrals are efficiently evaluated using numerical integration.

A. Effect of \( \alpha \) and \( \rho \) on Secrecy Capacity

In this section we investigate the impact of the EH time ratio, \( \alpha \), and power splitting factor, \( \rho \), on the system performance. Fig. 5 shows the the ergodic secrecy capacity versus \( \alpha \) and \( \rho \) 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 \( \alpha \) and \( \rho \). 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 \( \alpha \) and \( \rho \), 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 \( \alpha \) 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. On the other hand, when \( \rho \) 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].
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 ($\alpha, \rho$) and the corresponding maximum achievable ergodic secrecy capacity. Fig. 6a illustrates the optimal switching time factor ($\alpha^*$) and power splitting factor ($\rho^*$) 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 $\eta$ will always reduce $\alpha^*$ and $\rho^*$ which is intuitive because higher $\eta$ means more energy can be harvested in shorter period of time for TSR and smaller power ratio for PSR, i.e. smaller $\alpha$ and $\rho$ are required. The second observation is that $\alpha^*$ and $\rho^*$ 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 $\alpha^*$ and $\rho^*$ is plotted in Fig. 6b with respect to $N$ for various values of $\eta$. 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 $\eta$ 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. 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 $\alpha$ and $\rho$ are optimized. System parameters adopted in this section are $N = 8$, $\eta = 1$ and $P_x = 2$ 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...
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 $\alpha$ and $\rho$ 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 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. 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.

VI. 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

\[
\gamma_d = \frac{a_1 \|b_1 b_1\|^2}{\|b_1\|^2 + \|c_1\|^2} = \frac{X}{b_1 + Y}
\]  

(60)

where $a_1 = 2 \eta \alpha P_s$, $b_1 = 2 \eta \alpha d_1^n \sigma_1^2$, $c_1 = (1 - \alpha) d_1^n d_2^n \sigma_2^2$, $X = a_1 \|b_2 b_1\|^2$, and $Y = \|c_1\|^2$. Consequently, we can get

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

(61)

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

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

(62)

where $\mathcal{M}_v(z)$ denotes the moment generating function (MGF) of $v$ defined as
Maximum achievable ergodic secrecy capacity.

\[ \mathcal{M}_e(z) = \int_{-\infty}^{\infty} e^{-zv} f(v) dv \]  

(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

\[ \mathbb{E}[C_{d}^{T S R}] = \frac{1 - \alpha}{2 \ln(2)} \int_{0}^{1} \left( 1 - \mathcal{M}_X(z) \right) \mathcal{M}_{b_{1}+Y}(z) dz \]  

(64)

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

\[ \mathcal{M}_X(z) = \frac{\lambda_x}{\lambda_x + \alpha_1 z} \]  

(65)

In addition, \( \|h_2\|^2 \) has chi-square distribution, hence the MGF of \( b_1 + Y \) can be given by [31]

\[ \mathcal{M}_{b_{1}+Y}(z) = 2 e^{-z b_1} (c_1 z)^{N/2} \frac{\Gamma(N)}{K_N(2\sqrt{c_1 z})} \]  

(66)

where \( \Gamma(\cdot) \) is the Gamma function and \( K_N(\cdot) \) 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

\[ \gamma_e = \frac{P_s d_3^{\alpha_m} |g_1|^2}{P_d d_3^{\alpha_m} |g_2|^2 + d_3^{m} d_4^{m} \sigma_0^2} = \frac{|g_1|^2}{b_3 |g_2|^2 + c_3} \]  

(67)

and

\[ \gamma_e = \frac{|g_3 h_3|^2}{b_2 |g_3|^2 + c_2 + r |g_3|^2} = \frac{\Phi}{\Upsilon + c_2 + \zeta} \]  

(68)

where \( b_3 = \frac{P_d d_3^{\alpha_m} d_4^{\alpha_m}}{P_s d_3^{\alpha_m}}, \ c_3 = \frac{d_3^{m} d_4^{m} \sigma_0^2}{P_s d_3^{\alpha_m}}, \ c_2 = \frac{2 \eta \alpha d_3^{m} P_s}{2 \eta \alpha P_s d_4^{m} d_2^{m}}, \ \Phi = \frac{|g_3 h_3|^2}{|g_3|^2}, \ \Upsilon = b_2 \frac{|g_3|^2}{|g_3|^2} \) and \( \zeta = \frac{r}{|g_3|^2} \). Using these definitions, the ergodic capacity at the eavesdropper for the TSR can now be expressed as

\[ \mathbb{E}[C_e^{T S R}] = \frac{1 - \alpha}{2} \mathbb{E}\left[ \log_2 \left( 1 + \frac{|g_1|^2}{b_3 |g_2|^2 + c_4} + \frac{\Phi}{\Upsilon + c_2 + \zeta} \right) \right] \]  

(69)

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

\[ \mathbb{E}[C_e^{T S R}] = \frac{1 - \alpha}{2 \ln(2)} \int_{0}^{\infty} \left( 1 - \mathcal{M}_{\gamma_e(1)}(z) \mathcal{M}_{\gamma_e(2)}(z) \right) e^{-z} dz. \]  

(70)

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

\[ \mathcal{M}_{\gamma_e(1)}(z) = \int_{0}^{\infty} e^{-z \gamma} f_{\gamma_e(1)}(\gamma) d\gamma \]  

(71)
Using integration by parts, we can get

\[ M_{\gamma_1}(z) = 1 - z \int_0^\infty e^{-\gamma} M_{b_1|g_2|^2+c_3} (\gamma) d\gamma \] (72)

\[ M_{b_1|g_2|^2+c_3} (\gamma) = M_{|g_2|^2} (b_3 \gamma) e^{-\gamma} c_3 \] (73)

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

\[ M_{\gamma_e(2)} (z) = 1 - z \int_0^\infty e^{-\gamma} M_{Y+c_2+\zeta} (q) dq \] (74)

Since \( Y \) and \( ||g||^2 \) have exponential and chi-square distributions, respectively, the MGF of \( Y + c_2 + \zeta \) can be given as

\[ M_{Y+c_2+\zeta} (q) = \frac{\lambda_Y}{\lambda_Y + b_2 q} e^{-\frac{\gamma c_2}{2}} \frac{2 (q)^{N/2}}{\Gamma (N)} K_N (2q) \] (75)

Now, substituting (75) into (74), we can get \( M_{\gamma_e(2)} (z) \). 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...
\[
\gamma_d = \frac{a_1 \frac{|b_2 h_1|^2}{\|b_2\|^2}}{b_1 + c_1 + X} = \frac{X}{b_1 + c_1 + Y}
\]  
(76)

while \( X = a_1 \frac{|b_2 h_1|^2}{\|b_2\|^2} \) and \( Y = \frac{r_1}{\|b_2\|^2} \), \( a_1, b_1, c_1 \) and \( r_1 \) are defined in (43). Using (62), \( \mathbb{E} [ C_d^{PSR} ] \) can be expressed as

\[
\mathbb{E} [ C_d^{PSR} ] = \frac{1}{2 \ln(2)} \int_0^{\infty} \frac{1}{Z} \left( 1 - M_X (z) \right) M_{b_1+c_1+Y} (z) \, dz
\]
(77)

where \( M_X (z) \) and \( M_{b_1+c_1+Y} (z) \) are given, respectively, by

\[
M_X (z) = \frac{\lambda_X}{\lambda_X + (a_1 + z)}
\]
(78)

and

\[
M_{b_1+c_1+Y} (z) = e^{-(b_1+c_1)} \frac{2}{\Gamma (N/2)} \frac{2^N}{2^{r_1} z} \frac{K_N (2 \sqrt{r_1} z)}{K_N (2 \sqrt{c_1} z)}.
\]
(79)

- Eavesdropper Ergodic Capacity

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

\[
\gamma_e^{(2)} = \frac{|g_3 h_1|^2}{|g_3|^2 + c_2 + \omega + \varphi} = \frac{\Phi}{\Upsilon} = \frac{\Phi}{\Upsilon}
\]
(80)

where \( \Phi = \frac{|g_3 h_1|^2}{|g_3|^2}, \ U = b_2 \frac{|g_3 h_1|^2}{|g_3|^2}, \ varphi = \omega \), and \( b_2, c_2, r_2 \) and \( \omega \) are defined in (43). Again, we can get the ergodic eavesdropper capacity by

\[
\mathbb{E} [ C_e^{PSR} ] = \frac{1}{2 \ln(2)} \int_0^{\infty} \frac{1}{Z} \left( 1 - M_{\gamma_e^{(1)}} (z) M_{\gamma_e^{(2)}} (z) \right) e^{-qz} \, dz
\]
(81)

where \( M_{\gamma_e^{(1)}} (z) \) is given by (23) and

\[
M_{\gamma_e^{(2)}} (z) = 1 - z \int_0^\infty M_{\Upsilon+c_2+r_2+\varphi} (q) e^{-qz} \, dq
\]
(82)

where

\[
M_{\Upsilon+c_2+r_2+\varphi} (q) = \frac{\lambda_T e^{-q (b_2 + q)}}{\Sigma (b_2 + q)} \frac{2}{\Gamma (N/2)} \frac{2^N}{2^{r_2} q} \frac{K_N (2 \sqrt{r_2} q)}{K_N (2 \sqrt{c_1} q)}.
\]
(83)

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

\section*{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

\[
\gamma_d = \frac{a_1 \frac{|b_2 h_1|^2}{\|b_2\|^2}}{b_1 + c_1 + X} = \frac{X}{b_1 + c_1 + Y}
\]
(84)

where \( X = a_1 \frac{|b_2 h_1|^2}{\|b_2\|^2} \), \( Y = \frac{c_1}{\|b_2\|^2} \), \( a_1 \), \( b_1 \) and \( c_1 \) are given in (56). Using (62), we obtain

\[
\mathbb{E} [ C_d^{IRR} ] = \frac{1}{2 \ln(2)} \int_0^\infty \frac{1}{Z} \left( 1 - M_X (z) \right) M_{b_1+Y} (z) \, dz
\]
(85)

and

\[
M_X (z) = \frac{\lambda_X}{\lambda_X + (a_1 + z)}
\]
(86)

- Eavesdropper Ergodic Capacity

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

\[
\gamma_e^{(2)} = \frac{|g_3 h_1|^2}{|g_3|^2} \frac{\Phi}{\Upsilon + c_2 + \zeta}
\]
(88)

where \( \Phi = \frac{|g_3 h_1|^2}{|g_3|^2} \), \( \Upsilon = b_2 \frac{|g_3 h_1|^2}{|g_3|^2} \), \( \zeta = \frac{r_1}{\|g_3 h_1\|^2} \), \( b_2 \), \( c_2 \) and \( r_2 \) are defined in (56). Given the definition in (62), we can express \( \mathbb{E} [ C_e^{IRR} ] \) as

\[
\mathbb{E} [ C_e^{IRR} ] = \frac{1}{2 \ln(2)} \int_0^\infty \left( 1 - M_{\gamma_e^{(1)}} (z) M_{\gamma_e^{(2)}} (z) \right) e^{-qz} \, dz
\]
(89)

where \( M_{\gamma_e^{(1)}} \) is given by (23) and

\[
M_{\gamma_e^{(2)}} (z) = 1 - z \int_0^\infty e^{-qz} M_{\Upsilon+c_2+\zeta} (q) \, dq
\]
(90)

and \( M_{\Upsilon+c_2+\zeta} (q) \) is given by

\[
M_{\Upsilon+c_2+\zeta} (q) = \frac{\lambda_T e^{-q (b_2 + q)}}{\Sigma (b_2 + q)} \frac{2}{\Gamma (N/2)} \frac{2^N}{2^{r_2} q} \frac{K_N (2 \sqrt{r_2} q)}{K_N (2 \sqrt{c_1} q)}.
\]
(91)

\section*{REFERENCES}


S. M. Ross, Introduction to probability models 10ed. 2010.


Khaled Maaouf 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.