Secure Communication for Separated and Integrated Receiver Architectures in SWIPT

Furqan Jameel*‡, Dushantha Nalin K. Jayakody†‡, Mark F. Flanagan§ and Chintha Tellambura¶
*Dept. of Electrical Engineering, COMSATS Institute of Information Technology, Islamabad, PAKISTAN
†School of Computer Science and Robotics, National Research Tomsk Polytechnic University, RUSSIA
‡College of Science and Engineering, Hamad Bin Khalifa University, Qatar Foundation, QATAR
§School of Electronics, Electrical and Communications Engineering, University College Dublin, IRELAND
¶Department of Electrical and Computer Engineering, University of Alberta, CANADA
Email: furqanjamil01@yahoo.com, {nalin.jayakody, mark.flanagan}@ieee.org and chintha@ece.ualberta.ca

***Abstract*—This paper investigates the outage probability of the achievable secrecy rate in the presence of multiple eavesdroppers that employ energy harvesting (EH) and information decoding (ID). We derive the theoretical outage probability of the achievable secrecy rate between the legitimate transmitter and receiver pair when both the main channel and wiretap channel experience Rician fading. This work also considers both ideal and imperfect channel state information as well as different EH architectures (i.e. separated and integrated receiver architecture) in the secrecy analysis. Furthermore, the use of transmit antenna selection (TAS) for enhancing message confidentiality is also studied. Numerical and simulation results are provided to validate our analysis.**

Keywords - Outage probability, Achievable secrecy rate, Transmit antenna selection (TAS), Rician fading.

I. Introduction

Simultaneous wireless information and power transfer (SWIPT) is gaining considerable interest in the research community in recent years. It enables devices to communicate and allows free mobility with the benefit of energy harvesting. However, SWIPT systems cannot be supported using a conventional design of transmitter and receiver [1]. To be more specific, we focus our attention towards two broad categories of receiver architectures in SWIPT literature, i.e., separated and integrated architecture [2]. In the separated receiver architecture, the information decoder and energy harvester act as dedicated and separate units. This not only increases the cost of receiver but also increases the complexity of hardware. In contrast, the integrated receiver architecture jointly processes the information and energy using a unified circuitry for both. This architecture reduces the cost and hardware complexity.

The broadcast nature of wireless channels implies that the transmitted information signals are also received by nodes other than the intended receiver, which results in the leakage of information. Encryption techniques at higher layers are used to secure transmitted information. However, high computational complexity of these cryptographic techniques consume significant amount of energy [3]. Recently, physical layer security (PLS) has been explored as a secure communication technique which exploits the characteristics of wireless channels, such as fading, noise, and interference [4]. In SWIPT systems, a power signal can be used to increase the error rate at the eavesdroppers so as to enhance wireless security. Hence, PLS techniques are naturally applicable to SWIPT. In this context, secrecy capacity in SWIPT was studied in [5] for multiple-input single-output (MISO) based systems in the presence of multiple eavesdroppers. In [6] the authors introduced artificial noise (AN) aided pre-coding scheme to maximize the secrecy rate. In [7] the authors studied the secrecy capacity of an energy harvesting orthogonal frequency division multiplexing (OFDM) network. In a similar work, authors in [8] investigated the secrecy performance of decode-and-forward (DF) relaying system. Secure beamforming was used in [9] for SWIPT in relay networks. A zero forcing based sub-optimal solution was presented to maximize the secrecy of amplify-and-forward (AF) two-way relay networks.

One can observe from the above mentioned works that most of the studies on SWIPT are limited to the separated receiver architecture [5]–[9]. Moreover, to the best of authors' knowledge, there have been no previous results reported on comparative secrecy analysis of the separated and integrated receiver architectures under imperfect channel estimation. Therefore, this work focuses on detailed evaluation of secrecy performance of a SWIPT system for different combinations of receiver architectures at the legitimate receiver and eavesdroppers. The main contribution of this paper is threefold:

- We derive the analytical expressions for the outage probability of the achievable secrecy rate between the legitimate transmitter and receiver pair when both the main channel and wiretap channel experience Rician fading.
- We investigate the secrecy performance in the following cases: 1) imperfect channel estimation; 2) separated/integrated receiver architecture.
- Finally, we study the antenna selection schemes by comparing transmit antenna selection (TAS) with the

This work was funded, in part, by the framework of Competitiveness Enhancement Program of the National Research Tomsk Polytechnic University No. TPU CEP-IC-110/2017. Authors also acknowledged the contribution of the COST Action on Inclusive Radio Communications (IRACON) No. CA15104.

benchmark scheme of baseline antenna selection (BAS) and quantify the performance improvements.

The remainder of the paper is organized as follows. Section II describes the system model. In Section III, the analysis of the secrecy outage probability is provided. Section IV discusses antenna selection schemes. In Section V numerical performance results are given. Finally, Section VI provides some concluding remarks.

II. System Model

We assume a downlink SWIPT system consisting of a transmitter also known as access point (AP) and an EH and ID node S in the presence of N eavesdroppers represented as $E = \{E_i | i = 1, 2, ...N\}$. The AP broadcasts an radio signal to S which is also received by E. Each node is assumed to be equipped with a single antenna and all the antennas experience statistically independent flat fading. The AP is assumed to have channel state information (CSI) for the channels to node S as well as that of wiretap channel between the AP and eavesdroppers which is a common assumption in the PLS literature (see [3], [5], [9] and references therein).

Being part of the same coverage range, E act as the potential eavesdroppers. Moreover, these eavesdroppers can actively combine and exchange information to decode the massage sent from the AP to S. It is also assumed that both S and the eavesdroppers use power splitting (PS) scheme to incorporate the process of EH and ID, as PS has been proven to be an optimal scheme under the practical consideration of circuit power consumption [2]. According to PS, the received signal at S and E is divided into two streams for ID and EH by a power splitting factor ρ and $1-\rho$, respectively, where $0 \leq \rho \leq 1$. Let us consider that the AP transmits its sampled and normalized signal s with $\mathbb{E}\{|s|^2\} = 1$ to S with power P. The signal received at S, can then be written as [2]

$$y_s = \sqrt{\rho_s}\left(\sqrt{\frac{P}{P_s^{\text{loss}}}}\hat{h}_s s + n_s\right) + z_s, \tag{1}$$

where $\hat{h}_s$ represents the estimated channel amplitude gain between the AP and S and ρ_s is the power splitting factor at S. Furthermore, n_s represents the zero mean AWGN with variance N_0 due to the receiver electronics at S. Furthermore, z_s is signal processing noise at S, given as $\mathcal{N}(0, \sigma_s^2)$. Additionally, $P_s^{\text{loss}} = \frac{(4\pi)^2 d_s^{\Xi}}{G_t G_r \lambda_c^2}$ is the path loss and d_s denote the distance between the AP and S and Ξ is the path loss exponent, G_t and G_r are antenna gains of the AP and S, λ_c is the carrier wavelength. Since the AP broadcasts its transmission, the signal received at i-th eavesdropper is written as

$$y_{ie} = \sqrt{\rho_{ie}}\left(\sqrt{\frac{P}{P_{ie}^{\text{loss}}}}\hat{h}_{ie} s + n_{ie}\right) + z_{ie}, \tag{2}$$

where P_{ie}^{loss} is the path loss at i-th eavesdropper and $\hat{h}_{ie}$ represents the estimated channel amplitude gain between the AP and i-th eavesdropper. Also, n_{ie} represents the zero mean AWGN with variance N_0. In addition to this, z_{ie} is signal processing noise at the eavesdropper, with zero mean and variance $\sigma_{ie}^2 = \sigma_e^2$ for all the eavesdroppers since they are assumed to use the same type of hardware. Finally, for tractable analysis we consider $n_{ie} = n_e$, $\rho_{ie} = \rho_e$ and $P_{ie}^{\text{loss}} = P_e^{\text{loss}}$, $\forall i \in N$, where $[N] = \{1, 2, \ldots, N\}$ is the set of positive integers. It is pertinent to note that due to the random nature of wireless channel and hardware impairments, perfect estimation of the wireless channel is not possible. Hence, in this paper we use a well known channel estimation model expressed as [10], [11]

$$\hat{h}_k = \sqrt{1-\delta_k^2} h_k + \delta_k v, \tag{3}$$

where $k \in (s, ie)$ and h_k represents the true channel amplitude gain. The accuracy of channel estimation is represented by the value $0 \leq \delta_k \leq 1$. It is worth mentioning that the channel estimation is assumed to be perfect for $\delta_k = 0$. In contrast, it is assumed to be completely inaccurate for $\delta_k = 1$. Additionally, v is a Gaussian random variable distributed as $\mathcal{N}(0, 1)$. In this paper, our focus is to analyze the secrecy performance of SWIPT, hence, we assume that δ_k is given *a priori*. Note that the AP does not have the true CSI of the links. On the contrary, the AP has the estimated CSI of the links which is related to the true but unknown CSI by δ_k. Hence, by substituting (3) in (2) and (1), we obtain $y_s = \sqrt{\rho_s}\left(\sqrt{\frac{P(1-\delta_s^2)}{P_s^{\text{loss}}}} h_s s + \sqrt{\frac{P}{P_s^{\text{loss}}}}\delta_s v s + n_s\right) + z_s$ and $y_{ie} = \sqrt{\rho_{ie}}\left(\sqrt{\frac{P(1-\delta_{ie}^2)}{P_e^{\text{loss}}}} h_{ie} s + \sqrt{\frac{P}{P_e^{\text{loss}}}}\delta_{ie} v s + n_{ie}\right) + z_{ie}$ for received signals at S and E_i, respectively. Now, the instantaneous SNR of main and i-th eavesdropper link can be written as

$$\gamma_s = \frac{\rho_s \Omega_s (1-\delta_s^2)}{(\Omega_s \rho_s \delta_s^2 + \rho_s N_0 + \sigma_s^2)} |h_s|^2, \tag{4}$$

$$\gamma_{ie} = \frac{\rho_e \Omega_e (1-\delta_{ie}^2)}{(\Omega_e \rho_s \delta_{ie}^2 + \rho_e N_0 + \sigma_e^2)} |h_{ie}|^2, \tag{5}$$

where $\Omega_s = P/(P_s^{\text{loss}})$ and $\Omega_e = P/(P_e^{\text{loss}})$. During each scheduling slot every all the eavesdroppers send their instantaneous SNR to a pre-selected eavesdropper. Subsequently, the eavesdropping node with the maximum instantaneous SNR is chosen to decode the secret message as it will ensure maximum rate of the wiretap link. Furthermore, we assume that $\delta_{ie} = \delta_e, \forall i \in N$ throughout this paper to facilitate our analysis. Hence the instantaneous SNR of the wiretap link can be re-written as

$$\gamma_e = \max_{i \in N} \gamma_{ie} = \frac{\rho_e \Omega_e (1-\delta_e^2)}{(\Omega_e \rho_s \delta_e^2 + \rho_e N_0 + \sigma_e^2)} \max_{i \in N} |h_{ie}|^2. \tag{6}$$

III. Secrecy Outage Probability Analysis

In the following we derive closed form expressions for secrecy outage probability. It may also be worth mentioning that we derive outage probability for four cases depending on the receiver architectures used at S and E i.e. $P_{\text{out}}^{\text{Sp-Sp}}$, $P_{\text{out}}^{\text{Sp-In}}$, $P_{\text{out}}^{\text{In-Sp}}$ and $P_{\text{out}}^{\text{In-In}}$ referring to the case of separated receiver at S and E, separated receiver at S and integrated receiver at E, integrated receiver at S and separated receiver at E and integrated receiver at S and E.

Using [12], the probability density function (PDF) of the main link can be obtained as

$$f_{\gamma_s}(\gamma_s) = \frac{(\Omega_s\rho_s\delta_s^2+\rho_sN_0+\sigma_s^2)(K_s+1)}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\exp\left(-K_s\right) \times \exp\left(-\frac{(\Omega_s\rho_s\delta_s^2+\rho_sN_0+\sigma_s^2)(K_s+1)\gamma_s}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right) \times I_0\left(2\sqrt{\frac{(\Omega_s\rho_s\delta_s^2+\rho_sN_0+\sigma_s^2)K_s(K_s+1)\gamma_s}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}}\right), \tag{7}$$

where $\bar{\gamma}_s = \Omega_s\mathbb{E}\{|h_s|^2\}$ is the average SNR of the main link and $I_0(.)$ is the modified Bessel function of the first kind and order zero [13]. Also K_s is the ratio of total power of Line of Sight (LOS) component to the total power of the scattered waves from each multipath cluster for the main link.

The cumulative distribution function (CDF) of instantaneous SNR of main and wiretap link is obtained as (8) and (9) at the top of next page. In (8) and (9) Q is the Marcum-Q function [13] which is given as $Q_1(a,b) = \int_b^\infty x\exp(-\frac{(x^2+a^2)}{2})I_0(ax)dx$. The PDF of γ_e can then be obtained by taking the derivative of (9) at the top of the next page, resulting in (10). In (9) and (10), $\bar{\gamma}_e = \Omega_e\mathbb{E}\{\max_{i\in N}|h_{ie}|^2\}$ is the average SNR and K_e is the ratio of total power of LOS to the total power of the scattered components of the wiretap link.

A. Separated Receivers at S and E

The achievable rate for the main and wiretap link can be written as $C_s = \log_2(1+\gamma_s)$ and $C_e = \log_2(1+\gamma_e)$, respectively [2, Eq.(21)]. The achievable secrecy rate C_{sec} is defined as the non-negative difference between the achievable rates of the main channel and wiretap channel, which is expressed as $C_{\text{sec}} = [C_s - C_e]^+$. A secrecy outage event occurs when C_{sec} falls below some target rate $R_s > 0$. The secrecy outage probability is then written as

$$\begin{aligned} P_{\text{out}}^{\text{Sp-Sp}} &= \Pr(C_{\text{sec}} < R_s) \\ &= \int_0^\infty \int_0^{2^{R_s}(1+\gamma_e)-1} f_{\gamma_e}(\gamma_e)f_{\gamma_s}(\gamma_s)d\gamma_s d\gamma_e, \\ &= \int_0^\infty f_{\gamma_e}(\gamma_e)F_{\gamma_s}(2^{R_s}(1+\gamma_e)-1)d\gamma_e. \end{aligned} \tag{11}$$

To simplify the integral in (11), we use the recently derived approximation of first order Marcum-Q function [14]

$$Q_1(a,b) \approx \exp[-\exp(\upsilon(a))b^{\mu(a)}], \tag{12}$$

where $\upsilon(.)$ and $\mu(.)$ are non-negative parameters expressed as

$$\upsilon(a) = \begin{cases} -\ln 2 - \frac{a^2}{2} + \frac{45\pi^2+72\ln 2+36\epsilon-496}{64(9\pi^2-80)}a^4, & \text{if } a \ll 1 \\ -0.8526 + 0.3504a - 0.7529a^2 & \text{otherwise} \end{cases} \tag{13}$$

and

$$\mu(a) = \begin{cases} 2 + \frac{9}{8(9\pi^2-80)a^4}, & \text{if } a \ll 1 \\ 2.1793 - 0.5916a + 0.5895a^2 & \text{otherwise} \end{cases}. \tag{14}$$

In (13), $\epsilon \approx 0.5772$ is the Euler-Mascheroni constant. Now replacing (10) and (8) in (11) and using [13, (1.211.1)] we get (15) at the top of next page. In (15) $\mathcal{I}(a,b) = \int_0^\infty \exp(-(K_e+1)a) \times \gamma_e^p \times [(K_e+1)a]^{\frac{\mu(\sqrt{2K_e})(N-1)}{2}} \exp[-\exp(\upsilon(\sqrt{2K_s}))((K_s+1)b)^{\frac{\mu(\sqrt{2K_s})}{2}}]d\gamma_e$ which is calculated using numerical methods. Also, $\Psi_1 = \frac{(\Omega_e\rho_e\delta_e^2+\rho_eN_0+\sigma_e^2)\gamma_e}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}$, $\Psi_2 = \frac{(\Omega_s\rho_s\delta_s^2+\rho_sN_0+\sigma_s^2)(2^{R_s}(1+\gamma_e)-1)}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}$ and $\Gamma(.)$ is the Gamma function [13].

B. Separated Receiver at S and Integrated Receiver at E

In this case, the achievable rate for the main and wiretap link becomes $C_s = \log_2(1+\gamma_s)$ and $C_e \approx \log_2(\gamma_e) + \frac{1}{2}\log_2\frac{e}{2\pi}$, respectively [2, Eq.(21),(28)]. Then using (11) we obtain

$$P_{\text{out}}^{\text{Sp-In}} \approx \int_0^\infty f_{\gamma_e}(\gamma_e)F_{\gamma_s}(2^{R_s}\gamma_eC-1)d\gamma_e, \tag{16}$$

where $C = \sqrt{\frac{e}{2\pi}}$. Substituting (10) and (8), outage probability is obtained as (17), where $\Psi_3 = \frac{(\Omega_s\rho_s\delta_s^2+\rho_sN_0+\sigma_s^2)(2^{R_s}\gamma_eC-1)}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}$.

C. Integrated Receiver at S and Separated Receiver at E

In this case, the achievable rate for the main and wiretap link can be written as $C_s \approx \log_2(\gamma_s) + \frac{1}{2}\log_2\frac{e}{2\pi}$ and $C_e = \log_2(1+\gamma_e)$, respectively [2, Eq.(21),(28)]. Then using a similar approach to (11) and after some simple mathematical steps, we get outage probability as (18) on the next page. In (18) $\mathcal{L}(a,b) = \int_{\frac{2^{R_s}}{C}}^\infty ((K_e+1)a)^{\frac{\mu(\sqrt{2K_e})(N-1)}{2}} \times (K_s(K_s+1)b)^q\exp(-(K_s+1)b)d\gamma_s$ which is calculated using numerical methods. Also, $\Psi_4 = \frac{(\Omega_e\rho_e\delta_e^2+\rho_eN_0+\sigma_e^2)(\frac{\gamma_sC}{2^{R_s}}-1)}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}$ and $\Psi_5 = \frac{(\Omega_s\rho_s\delta_s^2+\rho_sN_0+\sigma_s^2)\gamma_s}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}$.

D. Integrated Receivers at S and E

For this the achievable rate for the main and wiretap link becomes $C_s \approx \log_2(\gamma_s) + \frac{1}{2}\log_2\frac{e}{2\pi}$ and $C_e \approx \log_2(\gamma_e) + \frac{1}{2}\log_2\frac{e}{2\pi}$, respectively [2, Eq.(28)]. Then, with the help of (9) and (7), and using same approach as (11) and after some algebraic manipulations we obtain (19), where $\Psi_6 = \frac{(\Omega_e\rho_e\delta_e^2+\rho_eN_0+\sigma_e^2)\frac{\gamma_s}{2^{R_s}}}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}$.

IV. Antenna Selection

So far we have considered the system model in which the AP is equipped with only a single antenna. However, the AP with multiple antennas can be deployed to improve the security at S which is resource limited. In this context, we extend our system model to incorporate the case when the AP is equipped with $L > 1$ antennas. It is assumed that all antennas experience independent fading. In this case, a single antenna is chosen based on pre-defined criterion to minimize energy consumption at the transmitter and to reduce information decoding errors at the receiver. This scheme is called Antenna Selection (AS) [15]. In order to facilitate our analysis in this section, we define following notations: $C_{s,l}$ = Main link achievable rate at l-th antenna; $C_{e,l}$ = Wiretap link achievable rate at l-th antenna; $C_{\text{sec,l}} = C_{s,l} - C_{e,l}$= Achievable secrecy

$$F_{\gamma_s}(\gamma_s) = 1 - Q_1\left(\sqrt{2K_s}, \sqrt{\frac{2(\Omega_s\rho_s\delta_s^2 + \rho_s N_0 + \sigma_s^2)(K_s+1)\gamma_s}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}}\right). \tag{8}$$

$$F_{\gamma_e}(\gamma_e) = \Pr(\max_{i\in N}\gamma_{ie} < \gamma_e) = \left[1 - Q_1\left(\sqrt{2K_e}, \sqrt{\frac{(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)2(K_e+1)\gamma_e}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}}\right)\right]^N. \tag{9}$$

$$f_{\gamma_e}(\gamma_e) = \frac{dF_{\gamma_e}(\gamma_e)}{d\gamma_e} = \frac{N(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)}{(1-\delta_e^2)\bar{\gamma}_e} \times \exp\left(-K_e - \frac{(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)(K_e+1)\gamma_e}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right)$$
$$\times I_0\left(2\sqrt{\frac{(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)K_e(K_e+1)\gamma_e}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}}\right)\left[1 - Q_1\left(\sqrt{2K_e}, \sqrt{\frac{(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)2(K_e+1)\gamma_e}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}}\right)\right]^{N-1}. \tag{10}$$

$$P_{\text{out}}^{\text{Sp-Sp}} = 1 - \frac{N(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)(1+K_e)\exp(-K_e + \upsilon(\sqrt{2K_e})(N-1))}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\sum_{p=0}^{\infty}\frac{1}{p!\Gamma(p+1)}$$
$$\times\left[\frac{(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)K_e(K_e+1)}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right]^p \mathcal{I}(\Psi_1, \Psi_2). \tag{15}$$

rate due to selecting l-th antenna; $P_{\text{out,l}}^{\text{Sp-Sp}}, P_{\text{out,l}}^{\text{Sp-In}}, P_{\text{out,l}}^{\text{In-Sp}}, P_{\text{out,l}}^{\text{In-In}}$ = Outage probability due to selecting l-th antenna when S and E use the separated receiver; S uses the separated and E uses the integrated receiver; S uses the integrated and E uses the separated receiver; S and E use the integrated receiver, respectively.

A. Baseline Antenna Selection (BAS)

In this antenna selection scheme, the transmit antenna is selected using a pseudo-random antenna hopping sequence [16]. Hence, the secrecy outage probability during one transmission block is given by the mean secrecy outage probability of all the antennas.

$$P_{\text{out}}^{\Theta} = \frac{1}{L}\sum_{l=1}^{L} P_{\text{out,l}}^{\Theta}, \tag{20}$$

where $P_{\text{out,l}}^{\Theta} = \Pr(C_{\text{sec,l}}^{\Theta} < R_s)$ and $\Theta \in$ (Sp-Sp, Sp-In, In-Sp, In-In).

B. Transmit Antenna Selection (TAS)

In this antenna selection scheme, antenna selection is made on the basis of CSI feedback from S and E. To be precise, each node initially estimates its own CSI and sends this to AP. The AP then calculates the achievable secrecy rate for each antenna and chooses the antenna with highest secrecy rate for transmission. In this case, the secrecy outage probability can be derived by exploiting the independent fading at each antenna, as

$$P_{\text{out}}^{\Theta} = \Pr(\max_{l\in L} C_{\text{sec,l}} < R_S) \tag{21}$$
$$= \prod_{l=1}^{L}\Pr(C_{\text{sec,l}}^{\Theta} < R_S) \tag{22}$$
$$= \prod_{l=1}^{L} P_{\text{out,l}}^{\Theta}. \tag{23}$$

V. Numerical Results

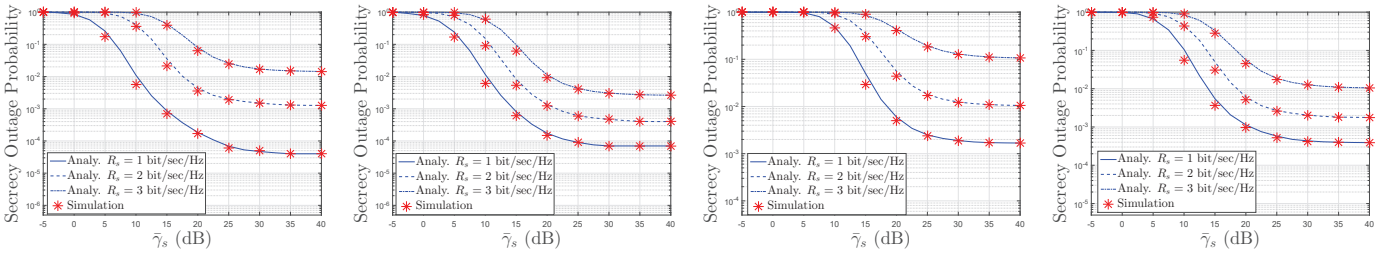
In this section we discuss the numerical results obtained as a result of the performance analysis in Section III and IV. Monte Carlo simulations in MATLAB were performed in order to obtain the simulation results. Unless stated otherwise, the system model parameters used for plotting analytical/simulation results are provided in Table I.

Figure 1 shows the secrecy outage probability as a function of $\bar{\gamma}_s$. Figure 1 (a) shows the outage probability when S and E are equipped with the separated receiver. It can be observed that an increase in $\bar{\gamma}_s$ causes a rapid decline in outage probability. Moreover, an increase in R_s results into an increase in outage probability. Similar observations can be made for Figure 1 (b), (c) and (d) where S and E are equipped with the separated and integrated, integrated and separated, and integrated and integrated receivers, respectively. Interestingly, it can be seen from Figure 1 (a), (b), (c) and (d) that an outage floor is introduced at higher values of main link SNR; this floor appears because of channel estimation errors at the

$$P_{\text{out}}^{\text{Sp-In}} = 1 - \frac{N(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)(1+K_e)\exp(-K_e + \upsilon(\sqrt{2K_e})(N-1))}{\rho_e(1-\delta_e^2)\bar{\gamma}_e} \sum_{p=0}^{\infty} \frac{1}{p!\Gamma(p+1)} \times \left[\frac{(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)K_e(K_e+1)}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right]^p \mathcal{I}(\Psi_1, \Psi_3). \tag{17}$$

$$P_{\text{out}}^{\text{In-Sp}} = 1 - \sum_{q=0}^{\infty} \frac{\exp[\upsilon(\sqrt{2K_e})(N-1) - K_s](\Omega_s\rho_s\delta_s^2 + \rho_s N_0 + \sigma_s^2)(K_s+1)}{\rho_s(q!)^2(1-\delta_s^2)\bar{\gamma}_s} \mathcal{L}(\Psi_4, \Psi_5). \tag{18}$$

$$P_{\text{out}}^{\text{In-In}} = 1 - \sum_{q=0}^{\infty} \frac{\exp[\upsilon(\sqrt{2K_e})(N-1) - K_s](\Omega_s\rho_s\delta_s^2 + \rho_s N_0 + \sigma_s^2)(K_s+1)}{\rho_s(q!)^2(1-\delta_s^2)\bar{\gamma}_s} \mathcal{L}(\Psi_6, \Psi_5), \tag{19}$$



(a) (b) (c) (d)

Fig. 1. Secrecy outage probability versus main link SNR when (a) S and E use the separated receiver (b) S uses the separated and E uses the integrated receiver (c) S uses the integrated and E uses the separated receiver (d) S and E use the integrated receiver.

TABLE I
SIMULATION PARAMETERS.

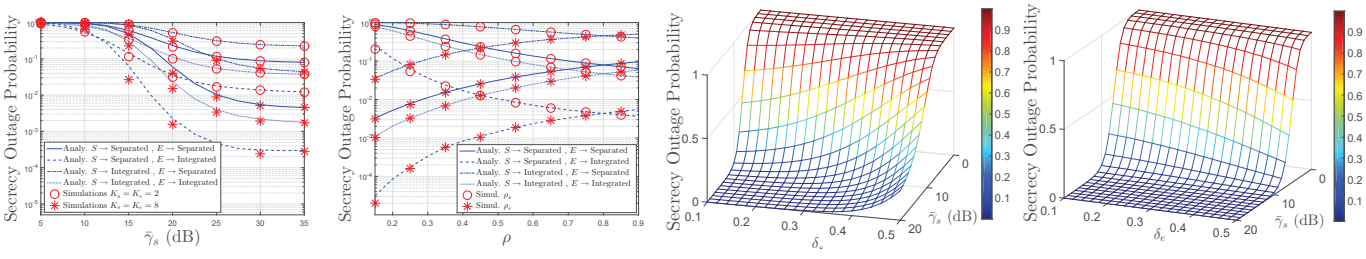
S No.	Simulation Parameter	Value
1.	Carrier Frequency	5 GHz[1]
2.	Antenna Gain $G_t = G_r$	1
3.	Channel Realizations	10^5
4.	Antenna Noise Variance N_0	1
5.	Signal Processing Noise Variance $\sigma_s^2 = \sigma_e^2$	1
6.	Target Secrecy Rate R_s	1 bit/sec/Hz
7.	Received Power Ω_s	15 dB
8.	Received Power Ω_e	0 dB
9.	Rician-K factor $K_s = K_e$	5
10.	Power splitting factor $\rho_s = \rho_e$	0.8
11.	Channel estimation accuracy $\delta_s = \delta_e$	0.2
12.	No. of eavesdroppers N	2

main and eavesdropper links. Also we observe that simulation results closely conform to the analytical results which shows the accuracy of our analytical expressions.

Figure 2 (a) shows the secrecy outage probability as a function of $\bar{\gamma}_s$. It can be seen that the secrecy outage performance gap is more for a larger value of $K_s = K_e$ as compared to its smaller values. It is worthwhile to note that minimum outage probability is achieved when the eavesdroppers are equipped with the integrated receivers and S is equipped with the separated receiver. Figure 2 (b) illustrates the impact of different values of ρ on secrecy performance of SWIPT. It may be highlighted that during the simulation of ρ_s, $\rho_e = 0.8$ and for the simulation for ρ_e, $\rho_s = 0.8$. The figure displays that for increasing values of ρ_s, the secrecy outage probability decreases. This is because a greater fraction of the received power is reserved for ID. In contrast, the secrecy outage probability increases with increasing ρ_e. This is due to the fact that more power is being reserved by the eavesdroppers to decode the signal which increases the secrecy outage probability. Figure 2 (c) and (d) emphasize the impact of δ_s and δ_e on the PLS of SWIPT. It may be noted that for increasing values of δ_s, $\delta_e = 0.1$ and vice versa. The graphs show that δ_s is predominant in determining the imperfect channel estimation for secrecy outage probability. The figures also show that increase in $\bar{\gamma}_s$ reduces the secrecy outage probability. However, with large estimation errors, it becomes difficult even at higher values of main link SNR to minimize the secrecy outage probability.

Figure 3 plots the secrecy outage probability against increasing values of L. It is worth mentioning that results are plotted when both S and E are equipped with the separated receiver for EH and ID. It can be seen from the figure that in case of BAS, the secrecy outage probability remains

[1]The motivation for selecting this range is due to its applicability in many wireless systems such as WLAN and vehicular communication [17].



(a) (b) (c) (d)

Fig. 2. Secrecy outage probability for (a) different values of K (b) different values of ρ (c) different values of δ_s (d) different values of δ_e

.

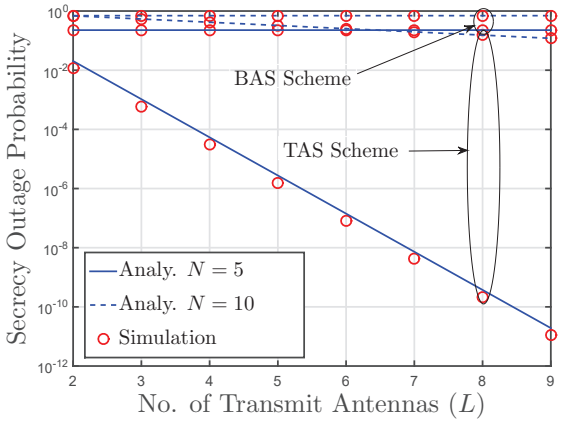


Fig. 3. Secrecy outage probability versus L. Other parameters are $K_s = K_e = 8$.

unchanged with the increase in number of transmit antennas. In contrast, the secrecy outage probability rapidly decreases with the increase in L which shows the advantage of using multiple antennas at transmitter. However, the secrecy outage probability increases with the increase in the number of eavesdroppers which degrades the performance improvements gained by using multiple antennas.

VI. Conclusion

In this paper, we analyzed the secrecy performance of a SWIPT system for different combinations of receiver architectures at S and E. We derived theoretical expressions of the secrecy outage probability under Rician fading and validated the derived expressions through extensive simulations. It is observed that an outage floor appears due to channel estimation errors when $\bar{\gamma}_s > 30$ dB such that the outage probability cannot be further reduced by increasing the SNR of the main link. Moreover, the largest secrecy rate is shown to be achieved when S is equipped with the separated receiver architecture and the eavesdroppers have the integrated receiver SWIPT architecture. It was also demonstrated that the PS factor of both S and E plays a prominent role in determining the secrecy performance in SWIPT.

References

[1] T. D. P. Perera, D. N. K. Jayakody, S. K. Sharma, S. Chatzinotas, and J. Li, "Simultaneous wireless information and power transfer (swipt): Recent advances and future challenges," *IEEE Communications Surveys Tutorials*, vol. PP, no. 99, pp. 1–1, 2017.

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

[3] F. Jameel, S. Wyne, and I. Krikidis, "Secrecy outage for wireless sensor networks," *IEEE Communications Letters*, 2017.

[4] F. Jameel and S. Wyne, "Secrecy outage of SWIPT in the presence of cooperating eavesdroppers," *AEU-International Journal of Electronics and Communications*, vol. 77, pp. 23–26, 2017.

[5] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," in *IEEE Global Communications Conference*. IEEE, 2013, pp. 1831–1836.

[6] B. Fang, Z. Qian, W. Zhong, and W. Shao, "AN-aided secrecy precoding for SWIPT in cognitive MIMO broadcast channels," *IEEE Communications Letters*, vol. 19, no. 9, pp. 1632–1635, 2015.

[7] M. Zhang, Y. Liu, and R. Zhang, "Artificial noise aided secrecy information and power transfer in OFDMA systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 4, pp. 3085–3096, 2016.

[8] F. Jameel, S. Wyne, and Z. Ding, "Secure Communications in Three-step Two-way Energy Harvesting DF Relaying," *IEEE Communications Letters*, vol. PP, no. 99, pp. 1–1, 2017.

[9] Q. Li, Q. Zhang, and J. Qin, "Secure relay beamforming for simultaneous wireless information and power transfer in nonregenerative relay networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 5, pp. 2462–2467, 2014.

[10] Y. Isukapalli and B. D. Rao, "Packet error probability of a transmit beamforming system with imperfect feedback," *IEEE Transactions on Signal Processing*, vol. 58, no. 4, pp. 2298–2314, 2010.

[11] T. Yoo and A. Goldsmith, "Capacity and power allocation for fading MIMO channels with channel estimation error," *IEEE Transactions on Information Theory*, vol. 52, no. 5, pp. 2203–2214, 2006.

[12] D. A. Zogas and G. K. Karagiannidis, "Infinite-series representations associated with the bivariate rician distribution and their applications," *IEEE Transactions on Communications*, vol. 53, no. 11, pp. 1790–1794, 2005.

[13] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*. Academic press, 2014.

[14] M. Z. Bocus, C. P. Dettmann, and J. P. Coon, "An approximation of the first order Marcum Q-function with application to network connectivity analysis," *IEEE Communications Letters*, vol. 17, no. 3, pp. 499–502, 2013.

[15] Z. Chen, J. Yuan, and B. Vucetic, "Analysis of transmit antenna selection/maximal-ratio combining in Rayleigh fading channels," *IEEE Transactions on Vehicular Technology*, vol. 54, no. 4, pp. 1312–1321, 2005.

[16] A. Hottinen, O. Tirkkonen, and R. Wichman, *Multi-antenna transceiver techniques for 3G and beyond*. John Wiley & Sons, 2004.

[17] Y. Song, Y.-C. Jiao, G. Zhao, and F.-S. Zhang, "Multiband CPW-fed triangle-shaped monopole antenna for wireless applications," *Progress In Electromagnetics Research*, vol. 70, pp. 329–336, 2007.