On the Secrecy Performance of SWIPT Receiver Architectures with Multiple Eavesdroppers

Furqan Jameel, Shurjeel Wyne, Syed Junaid Nawaz, Junaid Ahmed, and Kanapathippillai Cumanan

***Abstract*—Physical layer security (PLS) has been shown to hold promise as a new paradigm for securing wireless links. In contrast with the conventional cryptographic techniques, PLS methods exploit the random fading in wireless channels to provide link security. As the channel dynamics prevent a constant rate of secure communications between the legitimate terminals, the outage probability of the achievable secrecy rate is used as a measure of the secrecy performance. This work investigates the secrecy outage probability of a simultaneous wireless information and power transfer (SWIPT) system, which operates in the presence of multiple eavesdroppers that also have the energy harvesting capability. The loss in secrecy performance due to eavesdropper collusion, i.e., information sharing between the eavesdroppers to decode the secret message, is also analyzed. We derive closed-form expressions for the secrecy outage probability for Nakagami-m fading on the links and imperfect channel estimation at the receivers. Our analysis considers different combinations of the separated and the integrated SWIPT receiver architectures at the receivers. Numerical results are provided to validate our analysis.**

***Index Terms*—Achievable Secrecy Rate, Outage Probability, Nakagami-m Fading**

I. Introduction

Simultaneous wireless information and power transfer (SWIPT) systems have spurred considerable research interest in both academia and industry [1]. The SWIPT technique provides significant convenience to its users by efficiently utilizing the radio frequency (RF) signal for both information and power transfer [2]. However, SWIPT systems require a special receiver design to support the dual capability of energy harvesting (EH) and information decoding (ID). In the literature, two broad categories of SWIPT receiver architectures have been proposed namely the separated and the integrated receiver architectures [1]. The separated receiver architecture has dedicated separate units for ID and EH. However, this increases the complexity and cost of the receiver hardware [3]. In contrast, the integrated receiver architecture has a unified circuitry to perform ID and EH jointly, which reduces the hardware costs [3].

Varshney et al. in [4] were the first to propose the transmission of information and energy simultaneously. They developed a capacity-energy function to characterize the fundamental tradeoff in performance between simultaneous information and power transfer. In [5], the authors extended the work of [4] to frequency-selective channels with additive white Gaussian noise (AWGN). It was shown in [5] that a non-trivial tradeoff exists for information transfer versus energy transfer via power allocation. A SWIPT system under co-channel interference was studied in [6]. The authors derived optimal designs to achieve outage-energy tradeoffs and rate-energy tradeoffs. In [7] the authors considered the performance of a SWIPT system with imperfect channel state information (CSI) at the transmitter. Networks that employ pure wireless power transfer were studied in [8] and [9]. In [8], the authors studied a hybrid network that overlaid an uplink cellular network with randomly deployed power beacons, which charged mobiles wirelessly. The authors then derived the tradeoffs between different network parameters under an outage constraint on the data links.

The broadcast nature of wireless signals implies that nodes other than the intended receiver may also receive the transmitted message, which results in information leakage. Although cryptography-based techniques are conventionally used to secure transmitted information, the high computational complexity of these techniques consumes a significant amount of energy [10]. Recently, physical layer security (PLS) has been proposed as an alternative for securing wireless communications by exploiting the channel characteristics such as fading, noise, and interferences [11]. The secrecy performance of a cooperative network was investigated in [12], [13]; secrecy for interference limited networks was studied in [14] and for cognitive radio networks in [15], [16], [17]. In[18], the authors analyzed the secrecy performance of a multicast network in which the transmitter broadcasted its information to a set of legitimate users in the presence of multiple eavesdroppers. The authors then proposed power minimization and secrecy rate maximization schemes for the considered multicasting secrecy network. The security of large-scale networks has also been characterized in terms of connectivity [19], coverage [20] and capacity [21]. Researchers have also considered so-called artificial noise generation techniques to reduce the signal-to-interference ratio of the eavesdropper channel while minimizing the interference to the legitimate link [22], [23]. The authors in [24], [25] studied cooperative jamming, whereby a relay transmitted an interfering signal towards the eavesdropper while the source broadcasted its message. In [26], secure beamforming techniques have been explored to maximize the received power at the legitimate receiver. The PLS techniques are naturally applicable to SWIPT but the design of an optimal PLS techniques for SWIPT systems is a non-trivial task since it needs to also consider the efficiency of the wireless power transfer. In general, if a power receiver is

Furqan Jameel, Shurjeel Wyne, Syed Junaid Nawaz, and Junaid Ahmed are with the Department of Electrical Engineering, COMSATS Institute of Information Technology, Islamabad 45550, Pakistan.

Kanapathippillai Cumanan is with the Department of Electronic Engineering, University of York, Heslington, York, YO10 5DD, UK.

Manuscript received December XX, 2017...

a potential eavesdropper then any increase in the information signal power to improve the power transfer efficiency may also compromise the message secrecy [6]. Therefore, the inherent tradeoff between power efficiency and information security in a SWIPT system merits detailed examination. The authors in [27] investigated the maximization of secrecy throughput for SWIPT systems. In particular, they considered power allocation between EH and ID to provide an optimal secure SWIPT solution. In the same work an analytical expression for the secrecy outage probability was also derived. In [28], the authors investigated the secrecy performance of a SWIPT system with the separated receiver SWIPT architecture employed at the eavesdropper and $\kappa - \mu$ faded links. In [29] the authors introduced an artificial noise-aided precoding scheme to maximize the secrecy rate. In [30] the authors studied the secrecy capacity of an EH orthogonal-frequency-division-multiplexing network. All the sub-carriers were allocated an identical power and the power-splitting technique was used to coordinate ID and EH. In [31] the authors analyzed secure beamforming for an amplify-and-forward two-way relaying SWIPT network and proposed a zero-forcing based sub-optimal solution to maximize the secrecy of the considered network.

In the SWIPT literature most investigations have considered only the separated receiver architecture [27], [29], [30], [31]. Furthermore, multiple eavesdroppers when considered are often assumed to operate independently, whereas in many practical scenarios these eavesdroppers may collaborate to enhance their secret message decoding capability [32]. Finally, the achievable secrecy rate may degrade significantly under imperfect channel estimation at the legitimate receiver, whereas imperfect CSI at the eavesdropper can prove beneficial for the system's secrecy performance. To the best of the authors' knowledge, a comparative analysis of the secrecy performance of the separated and integrated SWIPT architectures with eavesdropper cooperation and imperfect CSI has not been performed previously. Specifically, the main contributions of the submitted work are listed as follows:

- We derive closed-form expressions for the secrecy outage probability with imperfect CSI knowledge at the receivers and different combinations of the separated and the integrated SWIPT architectures at the legitimate and the eavesdropping receivers.
- The tradeoff between secrecy performance and harvested energy is investigated.
- The loss in secrecy performance due to eavesdropper cooperation is analyzed and compared with the non-cooperative case.

The remainder of this paper is organized as follows. Section II presents the system model. In Section III the closed-form expressions for the outage probability are derived for different receiver architectures. Section IV provides numerical results along with relevant discussion. In Section V, some concluding remarks are given.

II. System Model

We consider the downlink of a SWIPT system as shown in Fig. 1 in which the Access Point (AP) transmits a secure message to the legitimate receiver S, which has simultaneous EH and ID capability. This transmission is also received by N eavesdropping nodes that are admitted into the network for EH-only but exploit their SWIPT receiver architectures in an attempt to intercept the secret communication between AP and S [33]. Since the eavesdroppers, denoted by $E = \{E_i | i = 1, 2, ...N\}$, are also part of the network - the AP is assumed to have CSI for the main channel to node S as well as for the N wiretap channels [33]. All nodes are considered to be equipped with single antennas.[1] Our analysis considers two types of receiver architectures for both S and E, i.e., the conventional separated receiver and the integrated receiver architecture [3] shown in Fig. 2. In the separated receiver, the RF signal after power-splitting (PS) is fed to separate circuitry for ID and EH, whereas in the integrated receiver PS between EH and ID takes place after the rectifier. The rectifier of the integrated receiver also down-converts the RF signal for ID, i.e., the down-conversion operation is integrated with the energy receiver in this architecture. For both receiver types, the fractional powers received for ID and EH are denoted by $0 \leq \rho < 1$ and $1 - \rho$, respectively.

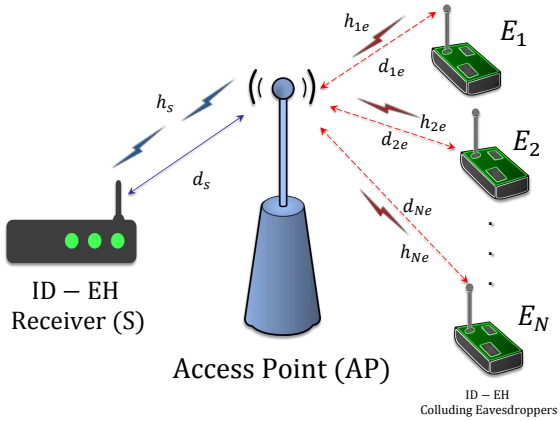

Fig. 1. System Model.

Consider that the AP transmits signal s with power P. The signal received at S can then be written as

$$y_s = \sqrt{\frac{P}{P_s^{loss}}} \hat{h}_s s + n_s, \tag{1}$$

where $\hat{h}_s$ represents the channel gain estimated by S and n_s denotes the zero-mean variance N_0 additive white Gaussian noise (AWGN) due to the receiver electronics at S. Additionally, $P_s^{loss} = \frac{(4\pi)^2 d_s^{\Xi}}{G_t G_r \lambda_c^2}$ is the path loss, where d_s denotes the distance between AP and S and Ξ is the path loss exponent. Furthermore, λ_c is the carrier wavelength and G_t and G_r are the antenna gains at AP and S, respectively.

Since S employs PS architecture, the received signal is further divided into two streams for ID and EH. The signal at the information decoder of S is given as

$$y_s = \sqrt{\rho_s} \left(\sqrt{\frac{P}{P_s^{loss}}} \hat{h}_s s + n_s \right) + z_s, \tag{2}$$

[1] Analysis for multi-antenna nodes [34] will be reported in future work.

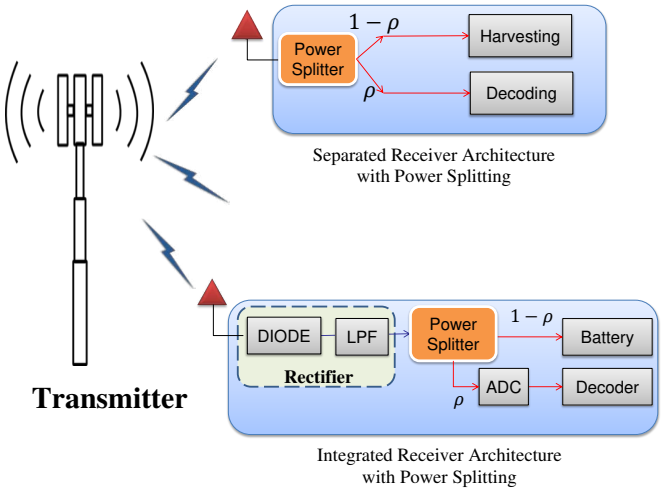

Fig. 2. Separated and integrated receiver architectures of SWIPT [3].

where ρ_s is the power splitting factor at S and z_s is the signal processing noise at S, also distributed normally as $\mathcal{N}(0, \sigma_s^2)$. Since $1 - \rho_s$ fraction of received power is used for energy harvesting, thus the amount of harvested energy at S, ignoring small amount of energy stored by antenna and signal processing noise, can be written as [3]

$$EH_s = \frac{\zeta_s(1-\rho_s)P|\hat{h}_s|^2}{P_s^{loss}}, \tag{3}$$

where ζ_s represents the power conversion efficiency at S. The AP transmission is also picked up by the eavesdroppers, the signal received at the information decoder of the i-th eavesdropper is written as

$$y_{ie} = \sqrt{\rho_{ie}}\left(\sqrt{\frac{P}{P_{ie}^{loss}}}\hat{h}_{ie}s + n_{ie}\right) + z_{ie}, \tag{4}$$

where $\hat{h}_{ie}$ represents the channel gain estimated by the i-th eavesdropper. Furthermore, $n_{ie} = n_e$ represents the thermal noise distributed as $\mathcal{N}(0, N_0)$ and $z_{ie} = z_e$ is the signal processing noise distributed as $\mathcal{N}(0, \sigma_e^2)$, at the i-th eavesdropper. Here the noise statistics are assumed identical due to all eavesdroppers using the same type of hardware. For a tractable analysis, we consider $P_{ie}^{loss} = P_e^{loss}$ and $\rho_{ie} = \rho_e \forall i \in N$. Similar to (3), the amount of harvested energy at the i-th eavesdropper can be written as [3]

$$EH_{ie} = \frac{\zeta_{ie}(1-\rho_{ie})P|\hat{h}_{ie}|^2}{P_{ie}^{loss}}, \tag{5}$$

where ζ_{ie} is the power conversion efficiency at the i-th eavesdropper. Moreover, without loss of generality, we consider $\zeta_{ie} = \zeta e$ throughout this work. Finally, the receiver nodes make an erroneous channel estimate due to their hardware impairments modeled as [35], [36]

$$\hat{h}_k = \sqrt{1-\delta_k^2}h_k + \delta_k v, \tag{6}$$

where $k \in \{s, ie\}$, h_k represents the true channel amplitude gain. The parameter $0 < \delta_k < 1$ is a measure of estimation accuracy with $\delta_k = 0$ for a perfect estimate. Additionally, v is a normal random variable distributed as $\mathcal{N}(0, 1)$. Now by substituting (6) into (2) we can express the signal received at S as

$$y_s = \sqrt{\rho_s}\left(\sqrt{\frac{P(1-\delta_s^2)}{P_s^{loss}}}h_s s + \sqrt{\frac{P}{P_s^{loss}}}\delta_s v s + n_s\right) + z_s, \tag{7}$$

and substituting (6) into (4) we can express the signal received at i-th eavesdropper as

$$y_{ie} = \sqrt{\rho_{ie}}\left(\sqrt{\frac{P(1-\delta_{ie}^2)}{P_e^{loss}}}h_{ie}s + \sqrt{\frac{P}{P_e^{loss}}}\delta_{ie} v s + n_{ie}\right) + z_{ie}. \tag{8}$$

Using the above equations, the instantaneous signal-to-noise ratio (SNR) of the main channel can be written as

$$\chi_s = \frac{\rho_s\Omega_s(1-\delta_s^2)}{(\Omega_s\rho_s\delta_s^2 + \rho_s N_0 + \sigma_s^2)}|h_s|^2, \tag{9}$$

and the SNR for the i-th wiretap channel can be expressed as

$$\chi_{ie} = \frac{\rho_e\Omega_e(1-\delta_{ie}^2)}{(\Omega_e\rho_s\delta_{ie}^2 + \rho_e N_0 + \sigma_e^2)}|h_{ie}|^2, \tag{10}$$

where $\Omega_s = P/(P_s^{loss})$ and $\Omega_e = P/(P_e^{loss})$. For subsequent analysis, $\delta_{ie} = \delta_e, \forall i \in N$ is considered.

III. Secrecy Outage Analysis

In this section closed form expressions for the secrecy outage probability are derived separately for four different cases that are based on the receiver types used at S and E. Specifically, P_{out}^{Sp-Sp} denotes outage probability for the case of separated receiver architectures at S and E, P_{out}^{Sp-In} denotes the outage for separated receiver at S and integrated receiver at E, P_{out}^{In-Sp} is the outage for integrated receiver at S and separated receiver at E, and P_{out}^{In-In} denotes outage probability for the case of integrated receivers at both S and E. Each of these four cases are discussed first for the non-cooperative eavesdropping scenario and later for cooperation among the eavesdroppers.

A. Non-cooperative Eavesdroppers

In this scenario, the worst-case of the eavesdropper with the maximum SNR is considered to decode the message. The instantaneous SNR of the wiretap link can be re-written as

$$\chi_e = \max_{i\in N}\chi_{ie} = \frac{\rho_e\Omega_e(1-\delta_e^2)}{(\Omega_e\rho_s\delta_e^2 + \rho_e N_0 + \sigma_e^2)}\max_{i\in N}|h_{ie}|^2. \tag{11}$$

where χ_{ie} is Gamma distributed [37] with probability density function (PDF) $f_{\chi_{ie}}(\gamma_{ie}) = \left[\frac{m_{ie}(\Omega_{ie}\rho_{ie}\delta_{ie}^2+\rho_{ie}N_0+\sigma_{ie}^2)}{\rho_{ie}(1-\delta_{ie}^2)\bar{\gamma}_{ie}}\right]^{m_{ie}} \times \exp\left(-\frac{m_{ie}(\Omega_{ie}\rho_{ie}\delta_{ie}^2+\rho_{ie}N_0+\sigma_{ie}^2)\gamma_{ie}}{\rho_{ie}(1-\delta_{ie}^2)\bar{\gamma}_{ie}}\right) \times \frac{(\gamma_{ie})^{m_{ie}-1}}{\Gamma(m_{ie})}$. Then, the cumulative distribution function (CDF) for the instantaneous SNR of the wiretap link (i.e. random variable χ_e falling below an arbitrary value γ_e), is given as

$$F_{\chi_e}(\gamma_e) = \Pr(\chi_e < \gamma_e). \tag{12}$$

Now using statistical independence of the wiretap channels and the CDF of a Gamma random variable [38], we obtain

$$\begin{aligned} F_{\chi_e}(\gamma_e) &= \Pr(\chi_{1e} < \gamma_e, \chi_{2e} < \gamma_e, \ldots, \chi_{Ne} < \gamma_e), \\ &= \left[1 - \exp\left(-\frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)\gamma_e}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right)\right. \\ &\quad \left.\times \sum_{r=0}^{m_e-1} \frac{1}{r!}\left[\frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)\gamma_e}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right]^r\right]^N, \end{aligned} \tag{13}$$

The corresponding PDF can be written as

$$\begin{aligned} f_{\chi_e}(\gamma_e) &= \frac{dF_{\chi_e}(\gamma_e)}{d\gamma_e} \\ &= \frac{N(\gamma_e)^{m_e-1}}{\Gamma(m_e)}\left[\frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right]^{m_e} \\ &\quad \times \left[1 - \exp\left(-\frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)\gamma_e}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right)\right. \\ &\quad \left.\times \sum_{r=0}^{m_e-1} \frac{1}{r!}\left\{\frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)\gamma_e}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right\}^r\right]^{N-1} \\ &\quad \times \exp\left(-\frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)\gamma_e}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right), \end{aligned} \tag{14}$$

where $\bar{\gamma}_e = \Omega_e\mathbb{E}\{\max_{i\in N}|h_{ie}|^2\}$ represents the average SNR of the wiretap link and m_e is the Nakagami-m fading severity parameter for the wiretap link.

The PDF of the instantaneous SNR of the main link can be obtained as [37]

$$\begin{aligned} f_{\chi_s}(\gamma_s) &= \left[\frac{m_s(\Omega_s\rho_s\delta_s^2 + \rho_s N_0 + \sigma_s^2)}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right]^{m_s} \\ &\quad \times \frac{(\gamma_s)^{m_s-1}\exp\left(-\frac{m_s(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)\gamma_s}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right)}{\Gamma(m_s)}. \end{aligned} \tag{15}$$

The corresponding CDF is given as [37]

$$\begin{aligned} F_{\chi_s}(\gamma_s) &= 1 - \exp\left(-\frac{m_s(\Omega_s\rho_s\delta_s^2 + \rho_s N_0 + \sigma_s^2)\gamma_s}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right)\sum_{r=0}^{m_s-1}\frac{1}{r!} \\ &\quad \times \left[\frac{m_s(\Omega_s\rho_s\delta_s^2 + \rho_s N_0 + \sigma_s^2)\gamma_s}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right]^r, \end{aligned} \tag{16}$$

where $\bar{\gamma}_s = \Omega_s\mathbb{E}\{|h_s|^2\}$ is the average SNR of the main link and m_s represents the Nakagami-m fading severity parameter for the main link.

1) Separated Receivers at S and E: The achievable rates for the main and wiretap links can be written as $C_s = \log_2(1+\chi_s)$ and $C_e = \log_2(1+\chi_e)$, respectively [3]. 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 $C_{sec} = [C_s - C_e]^+$. A secrecy outage event occurs when C_{sec} falls below some target rate $R_s > 0$ [39], [40]. The secrecy outage probability is then written as

$$\begin{aligned} P_{out}^{Sp-Sp} &= \Pr(C_{sec} < R_s) \\ &= \int_0^\infty \int_0^{2^{R_s}(1+\gamma_e)-1} f_{\chi_s}(\gamma_s) f_{\chi_e}(\gamma_e) d\gamma_s d\gamma_e, \\ &= \int_0^\infty F_{\chi_s}(2^{R_s}(1+\gamma_e)-1) f_{\chi_e}(\gamma_e) d\gamma_e. \end{aligned} \tag{17}$$

Now using (14) and (15) in (17) and with the help of [41, (8.352.4)], we obtain

$$\begin{aligned} P_{out}^{Sp-Sp} &= \frac{N}{\Gamma(m_e)}\left[\frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right]^{m_e} \\ &\quad \times \sum_{w=0}^{N-1}\binom{N-1}{w}\frac{(-1)^w}{\Gamma(m_e)\Gamma(m_s)} \times \mathcal{M}(\Psi_1, \Psi_2), \end{aligned} \tag{18}$$

where

$$\begin{aligned} \mathcal{M}(a,b) &= \int_0^\infty (\gamma_e)^{m_e-1}\exp(-m_e a)\Gamma(m_e, m_e a)^w \\ &\quad \times \Gamma(m_s, m_s b) d\gamma_e, \\ \Psi_1 &= \frac{(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)\gamma_e}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}, \\ \Psi_2 &= \frac{(\Omega_s\rho_s\delta_s^2 + \rho_s N_0 + \sigma_s^2)(2^{R_s}(1+\gamma_e)-1)}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}. \end{aligned}$$

Furthermore, $\Gamma(.,.)$ is the upper incomplete Gamma function and $\Gamma(.)$ is the Gamma function [41]. The function $\mathcal{M}(a,b)$ can be readily evaluated using any computational software.

2) Separated Receiver at S and Integrated Receiver at E: In this case the achievable rate for the main link is $C_s = \log_2(1+\chi_s)$. On the wiretap link, the integrated receiver's ID channel can be modeled as a free-space optical intensity channel [3]. The asymptotic high-SNR achievable rate for this channel is expressed as $C_e = \log_2(\chi_e) + \frac{1}{2}\log_2\frac{e}{2\pi}$, assuming that the signal processing noise dominates the antenna noise [3], [42]. Then using the approach of (17), we obtain

$$P_{out}^{Sp-In} = \int_0^\infty F_{\chi_s}(2^{R_s}\gamma_e C - 1) f_{\chi_e}(\gamma_e) d\gamma_e, \tag{19}$$

where $C = \sqrt{\frac{e}{2\pi}}$. Substituting (14) and (15) in (19) and using [41, (8.352.4)], we get

$$\begin{aligned} P_{out}^{Sp-In} &= \frac{N}{\Gamma(m_e)}\left[\frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right]^{m_e} \\ &\quad \times \sum_{w=0}^{N-1}\binom{N-1}{w}\frac{(-1)^w}{\Gamma(m_e)\Gamma(m_s)} \times \mathcal{M}(\Psi_1, \Psi_3). \end{aligned} \tag{20}$$

where $\Psi_3 = \frac{(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)(2^{R_s}\gamma_e C-1)}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}$.

3) Integrated Receiver at S and Separated Receiver at E: In this case, the main link has an asymptotic achievable rate of $C_s = \log_2(\chi_s) + \frac{1}{2}\log_2\frac{e}{2\pi}$ [3], [42], whereas the achievable rate for the wiretapper is $C_e = \log_2(1+\chi_e)$. Then using a

similar approach to (17) and after some manipulations, the outage probability is given as

$$P_{out}^{In-Sp} = 1 - \int_{\frac{2^{R_s}}{C}}^{\infty} F_{\chi_e}\left(\frac{\gamma_s C}{2^{R_s}} - 1\right) f_{\chi_s}(\gamma_s) d\gamma_s. \quad (21)$$

Substituting (13) and (15) in (21) and using the binomial theorem, we get

$$P_{out}^{In-Sp} = 1 - \sum_{z=0}^{N} \binom{N}{z} \frac{(-1)^z}{\Gamma(m_s)\Gamma(m_e)} \times \left[\frac{m_s(\Omega_s\rho_s\delta_s^2 + \rho_s N_0 + \sigma_s^2)}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right]^{m_s} \mathcal{T}(\Psi_4, \Psi_5), \quad (22)$$

where $\mathcal{T}(a,b) = \int_{2^{R_s}/C}^{\infty} \Gamma(m_e, m_e a)^z (\gamma_s)^{m_s - 1} \exp(-m_s b) d\gamma_s$ involves a single integral and can be readily evaluated in any computational software. Furthermore, $\Psi_4 = \frac{(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)(\frac{\gamma_s C}{2^{R_s}} - 1)}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}$ and $\Psi_5 = \frac{(\Omega_s\rho_s\delta_s^2 + \rho_s N_0 + \sigma_s^2)\gamma_s}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}$.

4) Integrated Receivers at S and E: In this case the main and wiretap links have asymptotic achievable rates of $C_s = \log_2(\chi_s) + \frac{1}{2}\log_2\frac{e}{2\pi}$ and $C_e = \log_2(\chi_e) + \frac{1}{2}\log_2\frac{e}{2\pi}$, respectively [3]. Then using the same approach as that for deriving (17), we obtain

$$P_{out}^{In-In} = 1 - \int_{2^{R_s}}^{\infty} F_{\chi_e}\left(\frac{\gamma_s}{2^{R_s}}\right) f_{\chi_s}(\gamma_s) d\gamma_s. \quad (23)$$

Replacing (13) and (15) in (23) and after some algebraic manipulations, we obtain

$$P_{out}^{In-In} = 1 - \sum_{z=0}^{N} \binom{N}{z} \frac{(-1)^z}{\Gamma(m_s)\Gamma(m_e)} \times \left[\frac{m_s(\Omega_s\rho_s\delta_s^2 + \rho_s N_0 + \sigma_s^2)}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right]^{m_s} \mathcal{T}(\Psi_6, \Psi_5), \quad (24)$$

where $\Psi_6 = \frac{(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)\frac{\gamma_s}{2^{R_s}}}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}$.

B. Cooperative Eavesdroppers

For the case of cooperative eavesdropping, the N eavesdroppers share information to form a virtual antenna array for receive beamforming such that a single-input multiple-output (SIMO) channel exists between the AP and the eavesdroppers [19]. The combined message ensures the maximum achievable rate of the wiretap link. In this case the instantaneous SNR of the combined wiretap signal can be written as

$$\chi_e = \sum_{i=1}^{N} \chi_{ie}. \quad (25)$$

The PDF of χ_e can be written as [43]

$$f_{\chi_e}(\gamma_e) = \left(\frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right)^{Nm_e} \frac{\gamma_e^{Nm_e-1}}{\Gamma(Nm_e)} \times \exp\left(-\frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\bar{\gamma}_e\right). \quad (26)$$

The CDF of the sum of independent, identically-distributed Gamma random variables is expressed as [38]

$$F_{\chi_e}(\gamma_e) = 1 - \exp\left(-\frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)\gamma_e}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right) \times \sum_{r=0}^{Nm_e-1} \frac{1}{r!}\left(-\frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)\gamma_e}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right)^r. \quad (27)$$

1) Separated Receivers at S and E: Using (26) and (15) in (17) and with the help of [41, (8.352.4)], the secrecy outage probability for this case is expressed as

$$P_{out}^{Sp-Sp} = 1 - \left(\frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right)^{Nm_e} \mathcal{U}(\Psi_1, \Psi_2), \quad (28)$$

where $\mathcal{U}(a,b) = \int_0^{\infty} \frac{\gamma_e^{Nm_e-1}}{\Gamma(Nm_e)} \exp(-m_e a) \frac{\Gamma(Nm_e, m_s b)}{\Gamma(Nm_e)} d\gamma_e$.

2) Separated Receiver at S, Integrated Receiver at E: Substituting (26) and (15) into (19), the secrecy outage probability for this case is expressed as

$$P_{out}^{Sp-In} = 1 - \int_0^{\infty} \left(\frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right)^{Nm_e} \times \frac{\gamma_e^{Nm_e-1}}{\Gamma(Nm_e)} \exp\left(-\frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\bar{\gamma}_e\right) \times \exp\left(-\frac{m_s(\Omega_s\rho_s\delta_s^2 + \rho_s N_0 + \sigma_s^2)(2^{R_s}\gamma_e C - 1)}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right) \times \sum_{r=0}^{m_s-1} \frac{1}{r!}\left[\frac{m_s(\Omega_s\rho_s\delta_s^2 + \rho_s N_0 + \sigma_s^2)(2^{R_s}\gamma_e C - 1)}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right]^r d\gamma_e. \quad (29)$$

After some simplifications and using [41, (8.352.4)], the secrecy outage probability is expressed as

$$P_{out}^{Sp-In} = 1 - \left(\frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right)^{Nm_e} \mathcal{U}(\Psi_1, \Psi_3). \quad (30)$$

3) Integrated Receiver at S and Separated Receiver at E: Substituting (27) and (15) in (21), the secrecy outage probability for this case is expressed as

$$P_{out}^{In-Sp} = 1 - \frac{\Gamma(m_s, \frac{m_s(\Omega_s\rho_s\delta_s^2 + \rho_s N_0 + \sigma_s^2)\gamma_s}{\rho_s(1-\delta_s^2)\bar{\gamma}_s})}{\Gamma(m_s)} - \int_{\frac{2^{R_s}}{C}}^{\infty} \exp\left(-\frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)\gamma_s C}{\rho_e(1-\delta_e^2)\bar{\gamma}_e 2^{R_s}} + \frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)}{\rho_e(1-\delta_e^2)\bar{\gamma}_e 2^{R_s}}\right) \times \sum_{r=0}^{Nm_e-1} \frac{1}{r!} \times \left(-\frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)\gamma_s C}{\rho_e(1-\delta_e^2)\bar{\gamma}_e 2^{R_s}} + \frac{m_e(\Omega_e\rho_e\delta_e^2 + \rho_e N_0 + \sigma_e^2)}{\rho_e(1-\delta_e^2)\bar{\gamma}_e 2^{R_s}}\right)^r \frac{(\gamma_s)^{m_s-1}}{\Gamma(m_s)} \times \left[\frac{m_s(\Omega_s\rho_s\delta_s^2 + \rho_s N_0 + \sigma_s^2)}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right]^{m_s} \times \exp\left(-\frac{m_s(\Omega_s\rho_s\delta_s^2 + \rho_s N_0 + \sigma_s^2)\gamma_s}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right) d\gamma_s. \quad (31)$$

After some algebraic manipulations, we obtain

$$P_{out}^{In-Sp} = 1 - \frac{\Gamma(m_s, \frac{m_s(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)\gamma_s}{\rho_s(1-\delta_s^2)\bar{\gamma}_s})}{\Gamma(m_s)} - \frac{[\frac{m_s(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}]^{m_s}}{\Gamma(m_s)}\mathcal{V}(\Psi_4, \Psi_5), \quad (32)$$

where $\mathcal{V}(a,b) = \int_{\frac{2^{R_s}}{C}}^{\infty} \frac{(\gamma_s)^{m_s-1}\exp(-m_s a)\Gamma(Nm_s, m_e b)}{\Gamma(Nm_s)} d\gamma_s$.

4) Integrated Receivers at S and E: Replacing (27) and (15) in (23) and using a similar approach as for the derivation of 32, the secrecy outage probability for this case is expressed as

$$P_{out}^{In-In} = 1 - \frac{\Gamma(m_s, \frac{m_s(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)\gamma_s}{\rho_s(1-\delta_s^2)\bar{\gamma}_s})}{\Gamma(m_s)} - \frac{[\frac{m_s(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}]^{m_s}}{\Gamma(m_s)}\mathcal{V}(\Psi_6, \Psi_5). \quad (33)$$

IV. Numerical Results and Discussion

We now provide some numerical results to validate the analytical expressions derived in Section III. The system parameters provided in Table I are used for result generation, unless stated otherwise.

S No.	Simulation Parameter	Value
1.	Channel Realizations	10^5
2.	Antenna Noise Variance N_0	0.1 dB
3.	Signal Processing Noise Variance $\sigma_s^2 = \sigma_e^2$	0 dB
4.	Target Secrecy Rate R_s	1 bit/sec/Hz
5.	Main Link Power Ω_s	30 dB
6.	Wiretap Link Power Ω_e	10 dB
7.	Nakagami-m shape factor $m_s = m_e$	2
8.	Power splitting factor $\rho_s = \rho_e$	0.8
9.	Channel estimation accuracy $\delta_s = \delta_e$	0.2
10.	No. of eavesdroppers N	5

TABLE I
Simulation Parameters.

Fig. 3 compares the secrecy performance for different combinations of receiver architectures at the legitimate receiver and the eavesdroppers. Fig. 3(a) shows that for any given value of $\bar{\gamma}_s$, the smallest secrecy outage probability is achieved when S is equipped with a separated and E with an integrated receiver architecture. on the other hand, the secrecy outage probability is the largest for the case when S is equipped with an integrated and E with a separated architecture, all other parameters remaining un-changed. The figure also shows that the outage probability increases with cooperation between the eavesdroppers. Fig. 3(a) shows that by increasing $\bar{\gamma}_s$ a steady reduction in the outage probability can be achieved. However, at large values ($\bar{\gamma}_s > 28$ dB), an outage floor is introduced for both the cooperative and non-cooperative cases, which shows that the outage probability does not decrease despite an increase in the main link SNR. This floor appears because of the channel estimation errors for the main link. By comparing Figs. 3(a) & (b), it can be observed that by increasing the target rate R_s, for a fixed $\bar{\gamma}_s$, the outage probability increases for all receiver architecture combinations. Finally, comparing the two sub-figures also reveals that the difference between the outage performance with and without eavesdropper cooperation diminishes as R_s is increased from 1 to 2 bps/Hz. All graphs shown in the figures exhibit a good match between the simulation and analytical results, which validates the accuracy of our derived analytical expressions.

Fig. 4 shows the secrecy outage probability surface plotted against $\bar{\gamma}_s$ and the Nakagami-m parameter, for different receiver architectures at S and E. Figure 4(a), for the case of non-cooperative eavesdroppers, shows that the secrecy outage probability decreases with an increase in $m_s = m_e$, which corresponds to a decreasing severity of the channel fading. Moreover, the figure shows that progressively larger values of the Nakagami parameter ($m_s = m_e = m > 2$, result in an increasing difference between the secrecy outage probabilities achieved by the 4 receiver combinations; the combination of S separated and E integrated receivers has the smallest outage as already observed in Fig. 3. By comparing Fig. 4(b), i.e., cooperative eavesdroppers with Fig. 4(a) for the non-cooperating case, it can be observed that for a given γ_s and identical system parameters, cooperation between the eavesdroppers significantly increases the secrecy outage probability relative to that for the non-cooperative case.

Fig. 5 shows the impact of the PS factor ρ on the secrecy outage probability. To separately demonstrate the effect of PS at S only, ρ_s is varied while the PS factor at the eavesdroppers is fixed at $\rho_e = 0.5$. Another set of curves shown in Fig. 5 describe the effect of PS at eavesdroppers only, while $\rho_s = 0.5$ is maintained for those curves. The figure shows that by increasing values of ρ_s the secrecy outage probability decreases. This is because a larger fraction of the received power is then used for ID at S. In contrast, the secrecy outage probability increases with increasing values of ρ_e. This is due to the fact that more power is then allocated by the eavesdroppers to decode the secret message, which diminishes the system's secrecy performance.

Fig. 6 shows the impact of the channel estimation errors on the secrecy outage probability. Figs. 6(a),(b) show that an increase in δ_s, the legitimate receiver's estimation error, degrades the secrecy performance. Whereas, Figs. 6(c),(d) show that an increase in δ_e, the eavesdropping receiver's estimation error, reduces the secrecy outage probability. This follows from the fact that the secrecy outage event is dependent on the decoding ability of both the legitimate and the eavesdropper nodes. An imperfect channel estimate at the eavesdropper increases its likelihood of incorrect decoding of the secret message, which reduces the information leakage. One may also observe from the figure that an increasing error in CSI estimate of the higher SNR main link has a more dominant effect on the secrecy outage probability than a similar increase in CSI error on the wiretapping receivers. This can be verified by comparing the relative shift in the secrecy outage curves between Fig. 6(a) and (b) with the relative shift in the secrecy outage between Fig. 6(c) and Fig. 6(d). This effect is more pronounced for the cooperating eavesdroppers case.

Fig. 7 shows the energy-secrecy capacity tradeoff for both cooperative as well as non-cooperative eavesdroppers. Each tradeoff curve is generated by varying ρ_s between 0.01 and

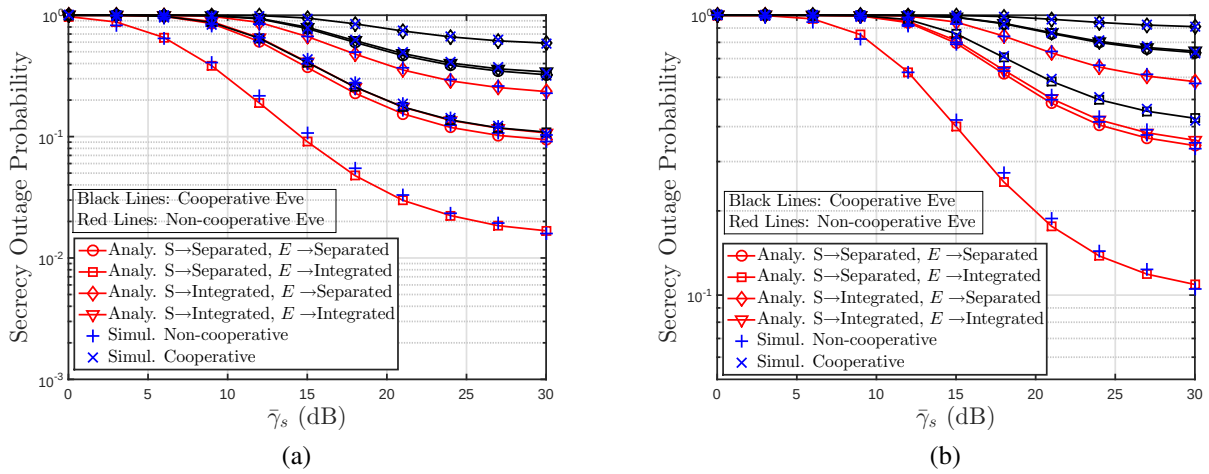

Fig. 3. Comparison of secrecy performance between different SWIPT receiver architectures. (a) $R_s = 1$ bps/Hz (b) $R_s = 2$ bps/Hz.

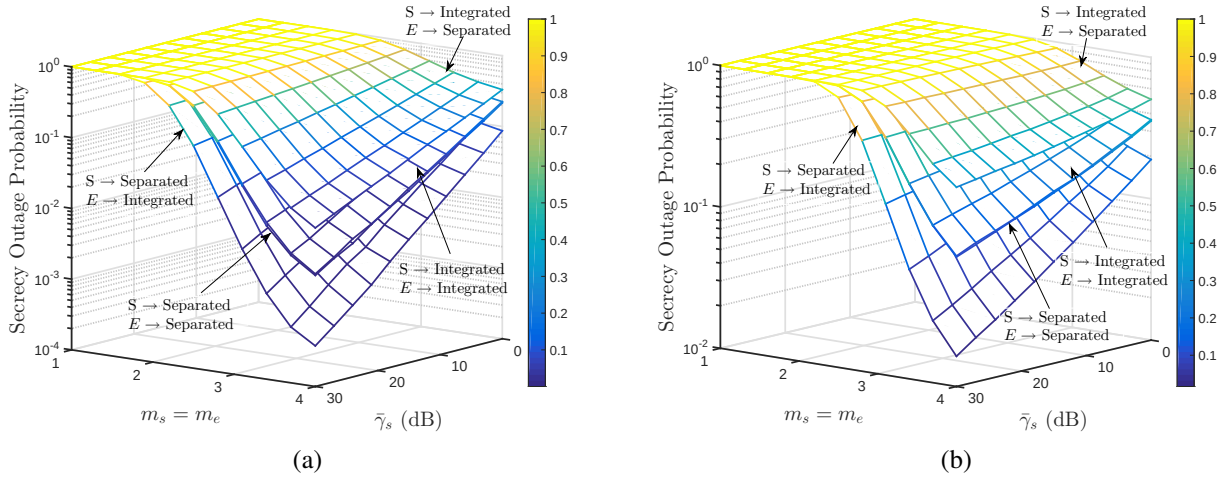

Fig. 4. Effect of Nakagami-m parameter and eavesdropper cooperation on secrecy performance, $\delta_s = \delta_e = 0.1$. (a) Non-cooperative eavesdroppers (b) Cooperative eavesdroppers.

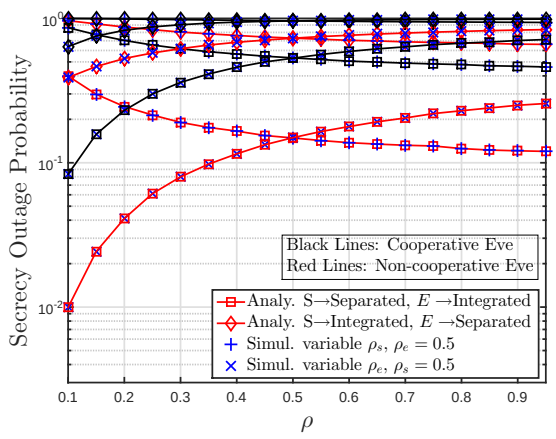

Fig. 5. Effect of power splitting factor ρ on the secrecy outage probability.

0.99 with fixed $\rho_e = 0.5$. However, plotting of each curve in Fig. 7 is restricted to its respective ρ_s sub-interval that produces a non-negative secrecy capacity. This results in different energy levels, harvested according to $(1-\rho_s)$, at zero secrecy capacity as shown in Fig. 7. One may observe from the figure that the enhanced eavesdropper performance due to cooperation diminishes the harvested energy conditional on a non-negative secrecy capacity. The figure also shows that $\delta_s = \delta_e = 0.001$ achieves a better energy-secrecy operating point than that of $\delta_s = \delta_e = 0.2$, which highlights the significance of having an accurate CSI estimate at the main receiver. Moreover, the figure shows that when the number of eavesdroppers N increases from 5 to 10, the area of the energy-secrecy capacity region decreases significantly for both the cooperative as well as the non-cooperative eavesdroppers. Finally, for a fixed number of eavesdroppers, the energy-secrecy capacity region for non-cooperative eavesdroppers is larger than that of the cooperative eavesdroppers. This highlights the fact that cooperation among the eavesdroppers considerably degrades the secrecy performance of the system.

V. Conclusion

This work has investigated the secrecy outage probability for a SWIPT system operating in the presence of cooperative

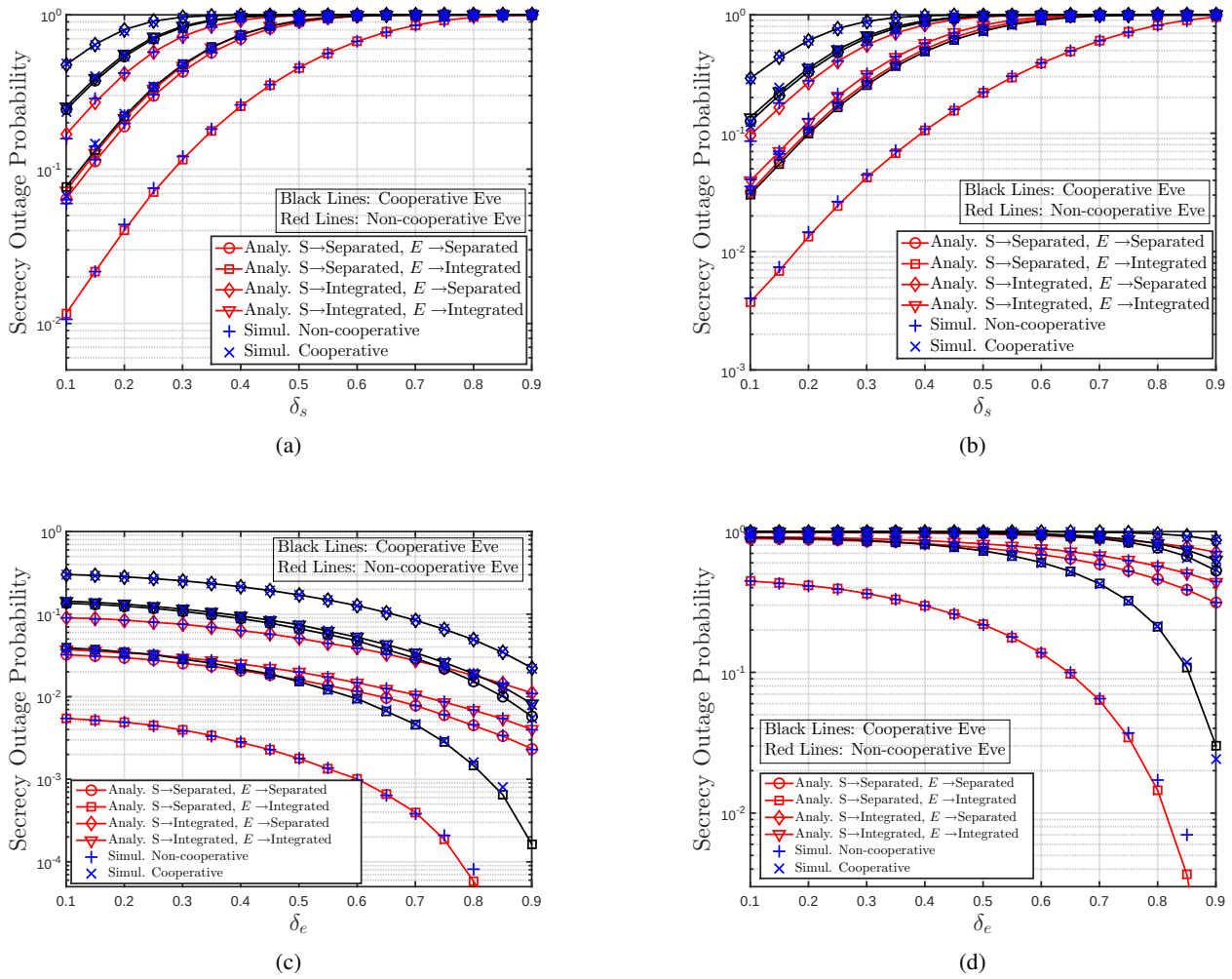

Fig. 6. Effect of imperfect CSI on the secrecy outage probability. (a) variable δ_s, fixed $\delta_e = 0.001$. (b) variable δ_s, fixed $\delta_e = 0.5$. (c) variable δ_e, fixed $\delta_s = 0.001$. (d) variable δ_e, fixed $\delta_s = 0.5$.

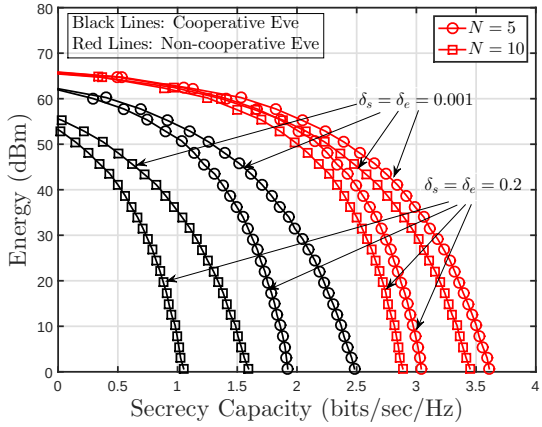

Fig. 7. Energy-Secrecy Capacity Region. ρ_s varied between 0.01 and 0.99, $\rho_e = 0.5$ and $\zeta_e = \zeta_s = 0.8$.

eavesdroppers and different combinations of the SWIPT receiver architectures considered at the legitimate receiver and the eavesdroppers. We derived closed-form expressions for the secrecy outage probability for each of these cases and showed that the smallest secrecy outage probability is achieved when the legitimate receiver has a separated architecture and the eavesdroppers have an integrated SWIPT receiver. The worst-case scenario is when the legitimate receiver has an integrated architecture and the eavesdroppers have separated SWIPT architectures; for a high main link SNR and Nakagami-$m = 4$, it was shown that the secrecy outage probabilities achieved for these two extreme cases differ by an order of magnitude. The effect of channel estimation errors was also investigated and it was shown that for the main link average SNR greater than 28 dB, an outage floor appears, i.e., the secrecy outage probability cannot be reduced further due to the channel estimation errors, despite an increase in the main link SNR. Finally, it was shown that cooperation between the eavesdroppers significantly increases the secrecy outage probability relative to that of the non-cooperative case for any combination of receiver architectures. Our results are useful for analyzing the secrecy performance of different SWIPT receiver architectures and eavesdropper cooperation.

ACKNOWLEDGMENT

This work is supported by the EU-funded project ATOM-690750, approved under call H2020-MSCA-RISE-2015.

REFERENCES

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

[2] K. Huang and E. Larsson, "Simultaneous information and power transfer for broadband wireless systems," *IEEE Transactions on Signal Processing*, vol. 61, no. 23, pp. 5972–5986, 2013.

[3] 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.

[4] L. R. Varshney, "Transporting information and energy simultaneously," in *proc. IEEE International Symposium on Information Theory*, 2008, pp. 1612–1616.

[5] P. Grover and A. Sahai, "Shannon meets Tesla: Wireless information and power transfer," in *proc. IEEE International Symposium on Information Theory*, 2010, pp. 2363–2367.

[6] L. Liu, R. Zhang, and K.-C. Chua, "Wireless information transfer with opportunistic energy harvesting," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 288–300, 2013.

[7] Z. Xiang and M. Tao, "Robust beamforming for wireless information and power transmission," *IEEE Wireless Communications Letters*, vol. 1, no. 4, pp. 372–375, 2012.

[8] K. Huang and V. K. Lau, "Enabling wireless power transfer in cellular networks: Architecture, modeling and deployment," *IEEE Transactions on Wireless Communications*, vol. 13, no. 2, pp. 902–912, 2014.

[9] S. Lee, R. Zhang, and K. Huang, "Opportunistic wireless energy harvesting in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 9, pp. 4788–4799, 2013.

[10] G. De Meulenaer, F. Gosset, F.-X. Standaert, and O. Pereira, "On the energy cost of communication and cryptography in wireless sensor networks," in *proc. IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 2008, pp. 580–585.

[11] K. Cumanan, H. Xing, P. Xu, G. Zheng, X. Dai, A. Nallanathan, Z. Ding, and G. K. Karagiannidis, "Physical layer security jamming: Theoretical limits and practical designs in wireless networks," *IEEE Access*, vol. 5, pp. 3603–3611, 2017.

[12] B. Juan, X. Tao, J. Xu, X. Zhang, and Q. Zhang, "Relay selection for secrecy connectivity in random wireless networks," *Wireless Communications and Mobile Computing*, vol. 16, no. 15, pp. 2263–2273, 2016.

[13] D. Deng, X. Li, L. Fan, W. Zhou, R. Qingyang Hu, and Z. Zhou, "Secrecy analysis of multiuser untrusted amplify-and-forward relay networks," *Wireless Communications and Mobile Computing*, vol. 2017, 2017, Article ID 9580639.

[14] X. He and A. Yener, "Secure degrees of freedom for Gaussian channels with interference: Structured codes outperform Gaussian signaling," in *proc. IEEE Global Telecommunications Conference*, 2009, pp. 1–6.

[15] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 5103–5113, 2013.

[16] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 28–33, 2013.

[17] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Communications*, vol. 6, no. 16, pp. 2676–2687, 2012.

[18] K. Cumanan, Z. Ding, M. Xu, and H. V. Poor, "Secrecy rate optimization for secure multicast communications," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1417–1432, Dec 2016.

[19] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networksPart I: Connectivity," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 125–138, 2012.

[20] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 256–266, 2011.

[21] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 3000–3015, 2012.

[22] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Processing Letters*, vol. 19, no. 2, pp. 71–74, 2012.

[23] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317–1322, 2011.

[24] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, "Secure communications with cooperative jamming: Optimal power allocation and secrecy outage analysis," *IEEE Transactions on Vehicular Technology*, vol. PP, no. 99, pp. 1–1, 2017.

[25] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 682–694, 2013.

[26] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Signal Processing Letters*, vol. 20, no. 1, pp. 35–38, 2013.

[27] H. Yu, S. Guo, Y. Yang, and B. Xiao, "Optimal target secrecy rate and power allocation policy for a swipt system over a fading wiretap channel," *IEEE Systems Journal*, vol. PP, no. 99, pp. 1–12, 2017.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] X. Chen, D. W. K. Ng, and H.-H. Chen, "Secrecy wireless information and power transfer: Challenges and opportunities," *IEEE Wireless Communications*, vol. 23, no. 2, pp. 54–61, 2016.

[33] F. Jameel, S. Wyne, and I. Krikidis, "Secrecy Outage for Wireless Sensor Networks," *IEEE Communications Letters*, vol. 21, no. 7, pp. 1565–1568, 2017.

[34] H. Zhang, Y. Huang, C. Li, and L. Yang, "Secure beamforming design for SWIPT in MISO broadcast channel with confidential messages and external eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 15, no. 11, pp. 7807–7819, 2016.

[35] 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.

[36] 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.

[37] G. K. Karagiannidis, D. A. Zogas, and S. A. Kotsopoulos, "On the multivariate Nakagami-m distribution with exponential correlation," *IEEE Transactions on Communications*, vol. 51, no. 8, pp. 1240–1244, 2003.

[38] R. Morsi, D. S. Michalopoulos, and R. Schober, "Multiuser scheduling schemes for simultaneous wireless information and power transfer over fading channels," *IEEE Transactions on Wireless Communications*, vol. 14, no. 4, pp. 1967–1982, 2015.

[39] 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.

[40] M.-N. Nguyen, N.-P. Nguyen, D. B. Da Costa, H.-K. Nguyen, and R. T. De Sousa, "Secure cooperative half-duplex cognitive radio networks with k-th best relay selection," *IEEE Access*, vol. 5, pp. 6678–6687, 2017.

[41] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*, 8th ed. Academic press, 2014.

[42] A. Lapidoth, S. M. Moser, and M. A. Wigger, "On the capacity of free-space optical intensity channels," *IEEE Transactions on Information Theory*, vol. 55, no. 10, pp. 4449–4461, 2009.

[43] V. A. Aalo, "Performance of maximal-ratio diversity systems in a correlated nakagami-fading environment," *IEEE Transactions on Communications*, vol. 43, no. 8, pp. 2360–2369, 1995.