Secrecy Limits of Energy Harvesting IoT Networks under Channel Imperfections

Furqan Jameel*, Zheng Chang†, Riku Jäntti*
* Department of Communications and Networking, Aalto University, 02150 Espoo, Finland.
† Faculty of Information Technology, University of Jyväskylä, Finland.

***Abstract*—Simultaneous wireless information and power transfer (SWIPT) has recently gathered much research interest from both academia and industry as a key enabler of energy harvesting Internet-of-things (IoT) networks. Due to a number of growing use cases of such networks, it is important to study their performance limits from the perspective of physical layer security (PLS). With this intent, this work aims to provide a novel analysis of the ergodic secrecy capacity of a SWIPT system is provided for Rician and Nakagami-m faded communication links. For a realistic evaluation of the system, the imperfections of channel estimations for different receiver designs of the SWIPT-based IoT systems have been taken into account. Subsequently, the closed-form expressions of the ergodic secrecy capacities for the considered scenario are provided and, then, validated through extensive simulations. The results indicate that an error ceiling appears due to imperfect channel estimation at high values of signal-to-noise ratio (SNR). More importantly, the secrecy capacity under different channel conditions stops increasing beyond a certain limit, despite an increase of the main link SNR. The in-depth analysis of secrecy-energy trade-off has also been performed and a comparison has been provided for imperfect and perfect channel estimation cases. As part of the continuous evolution of IoT networks, the results provided in this work can help in identifying the secrecy limits of IoT networks in the presence of multiple eavesdroppers.**

***Index Terms*—IoT Network, Eavesdroppers; Nakagami-m fading; Physical layer security; Rician fading; SWIPT**

I. Introduction

Internet-of-things (IoT) is gradually maturing due to a considerable amount of research interest received in recent years [1]. It seems evident that the myriad applications of IoT in healthcare, industrial automation, and agriculture, are going to usher an era of massive connectivity of millions of devices. According to the researchers, the increase in IT consolidation and the rapid adoption of reliable solutions are some of the main contributors to such massive connectivity of wireless IoT devices [2]. Modernization of legacy infrastructure is another focal point to provide seamlessly connected solutions that have a significant impact on the performance of such massive IoT networks. In this regard, ensuring the security of the IoT devices is at the forefront of critical issues. Due to this reason, a great number of research efforts are directed towards securing IoT devices against a number of attacks [3]. Another important aspect of such networks is energy consumption and reliability on rechargeable battery solutions. In particular, there is a growing demand to develop energy harvesting solutions to reduce the dependency and consumption of fossil fuels and move towards green communications [4]. To ensure such ubiquitous connectivity of green IoT networks, several interesting yet daunting issues need to be addressed for future IoT networks.

The first challenge stems in the form of prevention against eavesdropping attacks. Due to broadcast nature, it seems inevitable that the wireless links among IoT devices would be susceptible to the eavesdropping attacks. Moreover, since many of the IoT networks may operate privately in ad-hoc mode, the security techniques involving a trusted third party may not be realizable. In this regard, one of the promising solutions has been proposed in the form of physical layer security (PLS). The basic principle of PLS is to ensure link security by harnessing the randomness of the wireless channel [5]. This randomness of the wireless channel can be used to confuse the eavesdropper and reliably transfer the message to the intended receiver. Moreover, it can ensure good communication secrecy without requiring exhaustive cryptographic operations [6]. Besides this, message authentication can also be performed for ensuring the confidentiality of messages in the presence of malicious IoT devices.

The second issue is related to the limited life-cycle of wireless devices which can be addressed by employing efficient energy harvesting techniques [7]. The term energy harvesting which is sometimes called power harvesting is a technique that allows devices to harvest energy from already available sources. For RF energy harvesting, these sources include radio, cellular and television broadcasting signals that are mostly available and free to use for harvesting. This idea also gave birth to the transfer of power and data through electromagnetic (EM) waves [8]. As shown in Figure 1, the transfer of energy can take place using dedicated or ambient resources in the environment. The dedicated energy harvesting can be performed using dedicated towers to transfer energy to remote devices, whereas, ambient energy harvesting can be performed using radio frequency (RF) waves generated from wireless devices and fixed nodes. This dual nature of EM waves (i.e., ability to transfer information and energy) has given birth to a promising field of research namely simultaneous wireless information and power transfer (SWIPT) [7].

As mentioned earlier, the inherent nature of wireless IoT devices makes them vulnerable to eavesdropping attacks [9]. In this regard, it is worth noting increasing the power for ensuring the reliability of messages can have a negative impact on the secrecy performance of the network. In case, when a power receiver is a malicious IoT device, then improving the power transfer efficiency can reduce secrecy. It is because by increasing the power of the information signal, one may reduce

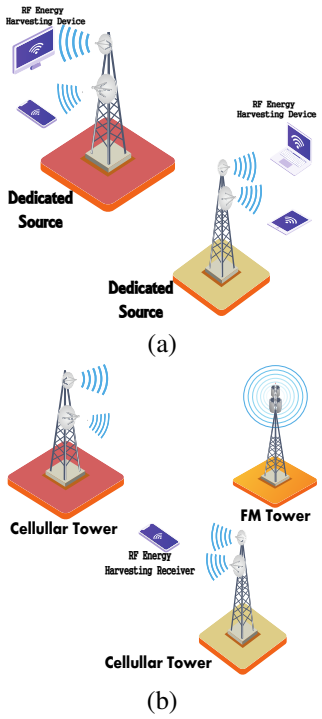


Fig. 1. RF energy harvesting architectures (a) dedicated energy harvesting (b) ambient energy harvesting.

the secrecy rate of the wireless links [10]. In this context, few studies have recently explored the concept of PLS and energy harvesting to efficiently use the transmit power. For instance, the authors of [11] proposed a band allocation scheme, whereby, the band reserved for energy harvesting cannot be used for information decoding. In another study, the concept of separated and integrated energy harvesting receiver design was proposed [12]. They introduced power splitting (PS) and time switching (TS) techniques for information processing and energy harvesting. Security in full-duplex (FD) relays with SWIPT systems was studied in [13]. An optimization problem was formulated for minimizing power consumption and ensuring link security for multiple-input-multiple-output (MIMO) FD relays. In another work [14], Bi *et al*. proposed a strategy based on energy accumulation and then jamming the eavesdropper reception. The authors of [15] provided a secrecy maximization scheme for energy harvesting relays. They first formulated a utility maximization problem and then solved it with the help of the Lagrange dual method.

The main contribution of this paper lies in the performance evaluation of energy harvesting and secure IoT. Specifically, we consider two fading channel models i.e., Rician and Nakagami-m fading. We derive closed-form expressions of ergodic secrecy capacity for both separated and integrated SWIPT-enabled IoT device architecture. In contrast to the conventional approach, we consider imperfect channel estimation for both legitimate and eavesdropping links. To validate our findings, we perform Monte-Carlo simulations in MATLAB.

The rest of the paper is arranged as follows. Section 2 provides details of the considered system model. In Section 3, a detailed analysis of ergodic secrecy capacity for both Nakagami-m and Rician fading has been provided. Section 4 provides analytical and simulation results along with their relevant discussion. Lastly, Section 5 presents some key conclusions.

II. System Model

Let us consider a downlink communication network constituting an access point (AP) and $N+1$ SWIPT-enabled IoT devices. Within any timeslot, the AP communicates with a legitimate IoT device ($\mathcal{S}$) while the other N IoT devices can be considered as eavesdroppers denoted as $\mathcal{E} = \{E_i | i = 1, 2, ...N\}$. All the IoT devices are equipped with single antennas having the capability to harvest energy and decode information from the received signal. In order to efficiently use the transmitted power from AP, during each time slot, the AP transmits information to $\mathcal{S}$ while the other devices are supposed to harvest energy from the radio waves. Being part of the same network, the energy harvesting IoT devices may act as eavesdroppers. Furthermore, in order to decode information and harvest energy $\mathcal{S}$ and $\mathcal{E}$ are assumed to use PS scheme [16]. As per PS policy, the signal at the receiving IoT device is divided into two streams for energy harvesting and information decoding. Particularly, the multiplicating PS factor ρ is used for information decoding and $1-\rho$ portion of the power is used for harvesting energy.

A. Fading Channel Models

For many tropospheric, urban, sub-urban and indoor communication systems, the channel is an amalgamation of noise, fading, and interference. Therefore, an appropriate selection of the channel fading model is important to analyze the performance of a wireless network. In this context, we adopt two renowned channel fading models namely, Rician and Nakagami-m distribution, for characterization of secrecy performance of SWIPT-enabled IoT devices. Rice distribution has been used to model environments where a strong stable line of sight component exists between source and destination. The theoretical model is the sum of two vectors, one with Rayleigh distributed modulus and other with known modulus with a large value. The Nakagami-m distribution is a multi-faceted distribution which is used to model numerous fading environments. It has proven to be highly flexible for matching empirical data of indoor and outdoor environments. It includes Rayleigh and One-sided Gaussian as special cases. Some studies also indicate that Nakagami-m can be used to approximate Rician fading for its shape parameter $m >> 1$ [17].

B. Signal Propagation

When AP, with power P, transmits its signal s to $\mathcal{S}$, the received signal is written as [18]

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

where $\hat{h}_s$ is the wireless channel gain between $\mathcal{S}$ and AP, and ρ_s is the PS factor for $\mathcal{S}$. The signal processing noise is denoted as z_s, n_s is the additive white Gaussian noise (AWGN) given as $\mathcal{N}(0, \sigma_s^2)$ and P_s^{loss} is the path loss. As explained earlier, the communication is overheard by the eavesdropping IoT devices. At the i-th eavesdropper, the received signal is expressed as

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

where $\hat{h}_{ie}$ is the channel gain and P_{ie}^{loss} is the path loss, z_{ie} represents the signal processing noise, and n_{ie} denotes the AWGN between the AP and i-th eavesdropper. We assume that the eavesdropper use similar hardware and $\sigma_{ie}^2 = \sigma_e^2 \; \forall \; E$. For tractability of analysis, we consider $n_{ie} = n_e$ and $\rho_{ie} = \rho_e$ and $P_{ie}^{loss} = P_e^{loss}$, $\forall \; i \; \in \; N$. In this paper, we consider imperfect channel estimation which is more practical as it is generally difficult to perfectly estimate wireless channel. Thus, a renowned channel estimation model has been used to incorporate channel imperfections in our system [19], [20]

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

where h_k is the estimated wireless channel gain and $k \in (s, ie)$. Also, δ_k denotes the channel accuracy factor wherein for $\delta_k = 0$ the channel is assumed to be accurately known and for $\delta_k = 1$ the channel estimation is completely inaccurate. Moreover, v is given by $\mathcal{N}(0, 1)$. Since we are focusing on the secrecy performance evaluation of the system, we assume that the value of δ_k is given a priori. By substituting above equation in (2) we obtain

$$y_s = \sqrt{\rho_s} \left(\sqrt{\frac{P(1-\delta_s^2)}{P_s^{loss}}} h_s s + \sqrt{\frac{P}{P_s^{loss}}} \delta_s v s + n_s \right) + z_s, \tag{4}$$

$$y_{ie} = \sqrt{\rho_{ie}} \left(\sqrt{\frac{P(1-\delta_{ie}^2)}{P_e^{loss}}} h_{ie} s + \sqrt{\frac{P}{P_e^{loss}}} \delta_{ie} v s + n_{ie} \right) + z_{ie}. \tag{5}$$

Using above equations, the instantaneous received SNR $\mathcal{S}$ can be expressed as

$$\gamma_s = \frac{\rho_s \Omega_s (1 - \delta_s^2)}{(\Omega_s \rho_s \delta_s^2 + \rho_s N_0 + \sigma_s^2)} |h_s|^2, \tag{6}$$

Similarly, the instantaneous received SNR at any eavesdropper is written as

$$\gamma_{ie} = \frac{\rho_e \Omega_e (1 - \delta_{ie}^2)}{(\Omega_e \rho_s \delta_{ie}^2 + \rho_e N_0 + \sigma_e^2)} |h_{ie}|^2, \tag{7}$$

where $\Omega_s = P/(P_s^{loss})$ and $\Omega_e = P/(P_e^{loss})$ are the average transmit power of main and wiretap link in (6) and (7), respectively. It is worth mentioning that among all the eavesdroppers, an eavesdropper with the best CSI has a better chance to decode the received message. Thus, the received SNR of eavesdropping link yields

$$\gamma_e = \max_{i \in N} \gamma_{ie} = \frac{\rho_e \Omega_e (1 - \delta_e^2)}{(\Omega_e \rho_s \delta_e^2 + \rho_e N_0 + \sigma_e^2)} \max_{i \in N} |h_{ie}|^2. \tag{8}$$

III. Ergodic Secrecy Capacity

An important security indicator is the average secrecy capacity C_{sec}. It is expressed as

$$\bar{C}_{sec} = \mathbf{E}\{C_{sec}\} = \mathbf{E}\{[C_s - C_e]^+\}. \tag{9}$$

Now, we first discuss both channels separately.

A. Ergodic Secrecy Capacity under Rician Fading

1) Separated $\mathcal{S}$ and $\mathcal{E}$: By using (9) we get

$$\begin{aligned} \bar{C}_{sec} &= \mathbf{E}\{[\log_2(1+\gamma_s) - \log_2(1+\gamma_e)]^+\} \\ &= \int_0^\infty \underbrace{\int_0^{\gamma_s} [\log_2(1+u) - \log(1+v)] f_{\gamma_e}(v) dv}_{\mathcal{G}_1} \\ &\quad \times f_{\gamma_s}(u) du. \end{aligned} \tag{10}$$

Now by using integration by parts, we get

$$\mathcal{G}_1 = \frac{1}{\ln 2} \int_0^u \frac{F_{\gamma_e}(v)}{1+v} dv. \tag{11}$$

Replacing (11) in (10) and changing the order of integration, we obtain

$$\begin{aligned} \bar{C}_{sec} &= \frac{1}{\ln 2} \int_0^\infty \frac{F_{\gamma_e}(v)}{1+v} \left[\int_v^\infty f_{\gamma_s}(v) du \right] dv \\ &= \frac{1}{\ln 2} \int_0^\infty \frac{F_{\gamma_e}(v)}{1+v} [1 - F_{\gamma_s}(v)] dv. \end{aligned} \tag{12}$$

Using [21], the probability density function (PDF) of the legitimate link is written as

$$\begin{aligned} f_{\gamma_s}(\gamma_s) &= \frac{(\Omega_s \rho_s \delta_s^2 + \rho_s N_0 + \sigma_s^2)(K_s + 1)}{\rho_s (1 - \delta_s^2) \bar{\gamma}_s} \\ &\quad \times \exp\left(- \frac{(\Omega_s \rho_s \delta_s^2 + \rho_s N_0 + \sigma_s^2)(K_s + 1) \gamma_s}{\rho_s (1 - \delta_s^2) \bar{\gamma}_s} \right) \\ &\quad \times I_0 \left(2 \sqrt{\frac{(\Omega_s \rho_s \delta_s^2 + \rho_s N_0 + \sigma_s^2) K_s (K_s + 1) \gamma_s}{\rho_s (1 - \delta_s^2) \bar{\gamma}_s}} \right) \\ &\quad \times \exp\left(-K_s\right). \end{aligned} \tag{13}$$

Similarly, the cumulative distribution function (CDF) of the received SNR at $\mathcal{S}$ is given as

$$\begin{aligned} &F_{\gamma_s}(\gamma_s) = \\ &1 - Q_1 \left(\sqrt{2K_s}, \sqrt{\frac{2(\Omega_s \rho_s \delta_s^2 + \rho_s N_0 + \sigma_s^2)(K_s + 1) \gamma_s}{\rho_s (1 - \delta_s^2) \bar{\gamma}_s}} \right), \end{aligned} \tag{14}$$

where $\bar{\gamma}_s = \Omega_s \mathbf{E}\{|h_s|^2\}$ denotes the mean value, $I_0(.)$ is the modified Bessel function of the first kind and order zero [22] and Q is the Marcum-Q function [22] which is given as

$$Q_1(a,b) = \int_b^\infty x \exp(-\frac{(x^2+a^2)}{2}) I_0(ax) dx. \quad (15)$$

Additionally, K_s is the ratio of the main link's power of the line of sight component to the scattered component.

By substituting (14) in (12), we get (16) at the top of next page. Now with the help of [22, (1.211.1),(3.194.3)], ergodic secrecy capacity can be obtained as

$$\bar{C}_{sec}^{Sp-Sp} = \frac{1}{\ln 2} \sum_{z=0}^{N} \binom{N}{z} (-1)^z \mathbf{B}\left(\frac{\mu(\sqrt{2K_e})}{2}, -\frac{\mu(\sqrt{2K_e})}{2}\right) \times \left[1 - z\exp(v(\sqrt{2K_e}))\left\{\frac{2(K_e+1)(\Omega_e\rho_e\delta_e^2+\rho_e N_0+\sigma_e^2)}{\rho_e\bar{\gamma}_e(1-\delta_e^2)}\right\}^{\frac{\mu(\sqrt{2K_e})}{2}}\right] - \frac{1}{\ln 2}\sum_{z=0}^{N}\binom{N}{z}(-1)^z \times \mathbf{B}\left(\frac{\mu(\sqrt{2K_s})}{2}, -\frac{\mu(\sqrt{2K_s})}{2}\right) \times \exp(v(\sqrt{2K_s}))\left[\frac{2(K_s+1)(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right]^{\frac{\mu(\sqrt{2K_s})}{2}}. \quad (17)$$

where $\mathbf{B}(.,.)$ is the incomplete Beta function [22].

2) Separated $\mathcal{S}$ and Integrated $\mathcal{E}$: Using the method presented above sub-section, we can easily derive the expression of ergodic secrecy capacity when $\mathcal{S}$ and $\mathcal{E}$ employ separated and integrated receivers, respectively. It is given by

$$\bar{C}_{sec} = \frac{1}{\ln 2}\int_0^\infty \frac{F_{\gamma_e}(v)}{Cv}[1 - F_{\gamma_s}(v)]dv. \quad (18)$$

Replacing (14) in (18) yields (19) at the top of next page. Using [22, (3.194.3)] along with Marcum Q approximation in (19), we get

$$\bar{C}_{sec}^{Sp-In} = \frac{1}{C\ln 2}\sum_{z=0}^{N}\binom{N}{z}(-1)^z \times \left[\mathbf{B}\left(\frac{\mu(\sqrt{2K_e})}{2}, -\frac{\mu(\sqrt{2K_e})}{2}\right) \times \left\{1 - z\exp(v(\sqrt{2K_e}))\left(2(K_e+1)\frac{(\Omega_e\rho_e\delta_e^2+\rho_e N_0+\sigma_e^2)}{\rho_e\bar{\gamma}_e(1-\delta_e^2)}\right)^{\frac{\mu(\sqrt{2K_e})}{2}}\right\} - \exp(v(\sqrt{2K_s}))\left(2(K_s+1)\frac{(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right)^{\frac{\mu(\sqrt{2K_s})}{2}} \times \mathbf{B}\left(\frac{\mu(\sqrt{2K_s})}{2}, -\frac{\mu(\sqrt{2K_s})}{2}\right)\right]. \quad (20)$$

B. Ergodic Secrecy Capacity under Nakagami-m Fading

The PDF of the main link is written as [23]

$$f_{\gamma_s}(\gamma_s) = \left[\frac{m_s(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right]^{m_s} \times \frac{(\gamma_s)^{m_s-1}\exp\left(-\frac{m_s(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)\gamma_s}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right)}{\Gamma(m_s)}, \quad (21)$$

Similarly, the CDF of received SNR at $\mathcal{S}$ is expressed as

$$F_{\gamma_s}(\gamma_s) = 1 - \exp\left(-\frac{m_s(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)\gamma_s}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right)\sum_{r=0}^{m_s-1}\frac{1}{r!} \times \left[\frac{m_s(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)\gamma_s}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right]^r. \quad (22)$$

where m_s represents the total number of multipath clusters for main link. Using the derivation for CDF and PDF of above section, we get CDF as

$$F_{\gamma_e}(\gamma_e) = \left[1 - \exp\left(-\frac{m_e(\Omega_e\rho_e\delta_e^2+\rho_e N_0+\sigma_e^2)\gamma_e}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right)\sum_{r=0}^{m_e-1}\frac{1}{r!} \times \left[\frac{m_e(\Omega_e\rho_e\delta_e^2+\rho_e N_0+\sigma_e^2)\gamma_e}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right]^r\right]^N, \quad (23)$$

In a similar way, the PDF of γ_e is obtained as

$$f_{\gamma_e}(\gamma_e) = \frac{N(\gamma_e)^{m_e-1}}{\Gamma(m_e)}\left[\frac{m_e(\Omega_e\rho_e\delta_e^2+\rho_e N_0+\sigma_e^2)}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right]^{m_e} \times \left[1 - \exp\left(-\frac{m_e(\Omega_e\rho_e\delta_e^2+\rho_e N_0+\sigma_e^2)\gamma_e}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right) \times \sum_{r=0}^{m_e-1}\frac{1}{r!}\times\left\{\frac{m_e(\Omega_e\rho_e\delta_e^2+\rho_e N_0+\sigma_e^2)\gamma_e}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right\}^r\right]^{N-1} \times \exp\left(-\frac{m_e(\Omega_e\rho_e\delta_e^2+\rho_e N_0+\sigma_e^2)\gamma_e}{\rho_e(1-\delta_e^2)\bar{\gamma}_e}\right). \quad (24)$$

where m_e represents the total number of multipath clusters for wiretap link.

1) Separated $\mathcal{S}$ and $\mathcal{E}$: By replacing (22) and (23) in (12), we obtain

$$\bar{C}_{sec}^{Sp-SP} = \frac{1}{\ln 2}\int_0^\infty \frac{F_{\gamma_e}(\gamma_e)}{1+\gamma_e}[1 - F_{\gamma_s}(\gamma_e)]d\gamma_e = \frac{1}{\ln 2}\int_0^\infty \frac{1}{1+\gamma_e}\left[1 - \exp\left(-\frac{(\Omega_e\rho_e\delta_e^2+\rho_e N_0+\sigma_e^2)\gamma_e}{\rho_e\bar{\gamma}_e(1-\delta_e^2)}\right) \times \sum_{r=0}^{m_e-1}\frac{1}{r!}\left\{\frac{(\Omega_e\rho_e\delta_e^2+\rho_e N_0+\sigma_e^2)\gamma_e}{\rho_e\bar{\gamma}_e(1-\delta_e^2)}\right\}^r\right]^N \times \Gamma\left(m_s, \frac{m_s(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)\gamma_e}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right)d\gamma_e. \quad (25)$$

Using [22, (8.352.4)] we obtain

$$\bar{C}_{sec}^{Sp-SP} = \frac{1}{\ln 2}\sum_{z=0}^{N}\binom{N}{z}\frac{(-1)^z}{\Gamma(m_s)\Gamma(m_e)}\sum_{a=0}^{m_e-1} \times \sum_{b=0}^{m_s-1}\frac{(m_e-1)!(m_s-1)!}{(a!)^z b!}\int_0^\infty \frac{1}{1+\gamma_e} \times \exp\left(-a\frac{(\Omega_e\rho_e\delta_e^2+\rho_e N_0+\sigma_e^2)\gamma_e}{\rho_e\bar{\gamma}_e(1-\delta_e^2)} - \frac{m_s(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)\gamma_e}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right) \times \frac{(\Omega_e\rho_e\delta_e^2+\rho_e N_0+\sigma_e^2)}{\rho_e\bar{\gamma}_e(1-\delta_e^2)}\frac{m_s(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)\gamma_e^2}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}d\gamma_e. \quad (26)$$

According to the author's best knowledge, the above integral cannot be further simplified. But it can be readily evaluated with MATLAB, Mathematica or any other standard computational software.

$$\bar{C}_{sec}^{Sp-Sp} = \frac{1}{\ln 2}\sum_{z=0}^{N}\binom{N}{z}(-1)^z \int_0^{\infty} \frac{1}{1+\gamma_e} \times \exp\left[-z\exp(\upsilon(\sqrt{2K_e}))\left\{\frac{2(K_e+1)(\Omega_e\rho_e\delta_e^2+\rho_e N_0+\sigma_e^2)\gamma_e}{\rho_e\bar{\gamma}_e(1-\delta_e^2)}\right\}^{\frac{\mu(\sqrt{2K_e})}{2}}\right]$$
$$\times \exp\left[-\exp(\upsilon(\sqrt{2K_s}))\left\{\frac{2(K_s+1)(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)\gamma_e}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right\}^{\frac{\mu(\sqrt{2K_s})}{2}}\right] d\gamma_e. \quad (16)$$

$$\bar{C}_{sec}^{Sp-In} = \frac{1}{\ln 2}\times\sum_{z=0}^{N}\binom{N}{z}(-1)^z \times \int_0^{\infty} \frac{1}{C\gamma_e} \times \exp\left[-z\exp(\upsilon(\sqrt{2K_e}))\left[\frac{2(K_e+1)(\Omega_e\rho_e\delta_e^2+\rho_e N_0+\sigma_e^2)\gamma_e}{\rho_e\bar{\gamma}_e(1-\delta_e^2)}\right]^{\frac{\mu(\sqrt{2K_e})}{2}}\right]$$
$$\times \exp\left[-\exp(\upsilon(\sqrt{2K_s}))\left[\frac{2(K_s+1)(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)\gamma_e}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right]^{\frac{\mu(\sqrt{2K_s})}{2}}\right] d\gamma_e. \quad (19)$$

2) Separated $\mathcal{S}$ and Integrated $\mathcal{E}$: Substituting (22) and (23) in (18) yields

$$\bar{C}_{sec}^{Sp-In} = \frac{1}{\ln 2}\int_0^{\infty}\frac{F_{\gamma_e}(\gamma_e)}{C\gamma_e}[1-F_{\gamma_s}(\gamma_e)]d\gamma_e.$$
$$= \frac{1}{\ln 2}\sum_{z=0}^{N}\binom{N}{z}\frac{(-1)^z}{\Gamma(m_s)\Gamma(m_e)}\sum_{a=0}^{m_e-1}\sum_{b=0}^{m_s-1}\frac{(m_e-1)!(m_s-1)!}{C(a!)^z b!}$$
$$\times\int_0^{\infty}\exp\left(-a\frac{(\Omega_e\rho_e\delta_e^2+\rho_e N_0+\sigma_e^2)\gamma_e}{\rho_e\bar{\gamma}_e(1-\delta_e^2)}-\frac{m_s(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)\gamma_e}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right)$$
$$\times\frac{m_e m_s(\Omega_e\rho_e\delta_e^2+\rho_e N_0+\sigma_e^2)(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)\gamma_e}{\rho_e\rho_s(1-\delta_e^2)\bar{\gamma}_e(1-\delta_s^2)\bar{\gamma}_s}d\gamma_e. \quad (27)$$

Now with the help of [22, (3.326.2)], we get

$$\bar{C}_{sec}^{Sp-In} = \frac{1}{\ln 2}\sum_{z=0}^{N}\binom{N}{z}\frac{(-1)^z}{\Gamma(m_s)\Gamma(m_e)}\sum_{a=0}^{m_e-1}\sum_{b=0}^{m_s-1}$$
$$\times\frac{(m_e-1)!(m_s-1)!}{\left[a\frac{(\Omega_e\rho_e\delta_e^2+\rho_e N_0+\sigma_e^2)\gamma_e}{\rho_e\bar{\gamma}_e(1-\delta_e^2)}-\frac{m_s(\Omega_s\rho_s\delta_s^2+\rho_s N_0+\sigma_s^2)\gamma_e}{\rho_s(1-\delta_s^2)\bar{\gamma}_s}\right]C(a!)^z b!}. \quad (28)$$

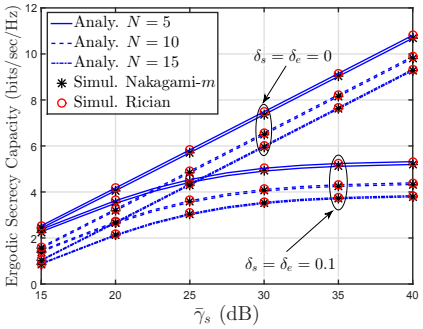
IV. Numerical Results

This section provides some numerical examples for the derived analytical results, which are also validated by simulations. Unless stated otherwise, the simulation parameters for generation of plots in this section are provided in Table I.

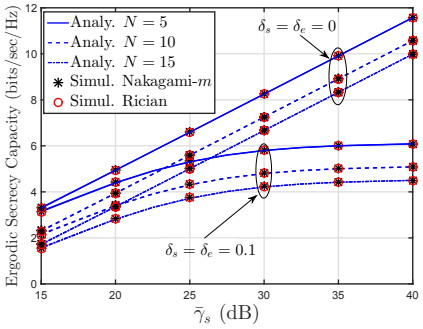
TABLE I
Simulation Parameters.

S No.	Parameter	Value
1.	Signal processing noise variance $\sigma_s^2 = \sigma_e^2$	0 dB
2.	Nakagami-m shape factor $m_s = m_e$	2
3.	Channel realizations	10^5
4.	Antenna noise variance N_0	0.1 dB
5.	Rician K factor $K_s = K_e$	5
6.	Main link power Ω_s	30 dB
7.	Channel estimation accuracy $\delta_s = \delta_e$	0.2
8.	No. of eavesdroppers N	5
9.	Wiretap link power Ω_e	10 dB
10.	Power splitting factor $\rho_s = \rho_e$	0.8

Figure 2 (a) plots the ergodic secrecy capacity against increasing $\bar{\gamma}_s$. Note that the ergodic secrecy capacity generally



(a)



(b)

Fig. 2. Ergodic Secrecy Capacity for Rician and Nakagami-m channels when (a) S and E employ separated design for receivers (b) S employs separated and E use integrated design for receivers.

increases with the increase in $\bar{\gamma}_s$. However, the increase in secrecy capacity is hampered due to imperfect channel estimation errors. Moreover, we observe that for particular values of $m_s = m_e$ and $K_s = K_e$, the secrecy capacity for Rician and Nakagami-m channel becomes similar when a large number of eavesdroppers are present in the network. Figure 2 (b) further shows the impact receiver design on secrecy performance of energy harvesting IoT devices. The secrecy capacity for Rician and Nakagami-m channel becomes the same despite the large difference in their shape parameters when $\mathcal{S}$ and $\mathcal{E}$ are equipped with separated and integrated

receivers. This shows that the impact of wireless channel reduces when $\mathcal{S}$ employs separated and $\mathcal{E}$ employ integrated receiver architecture.

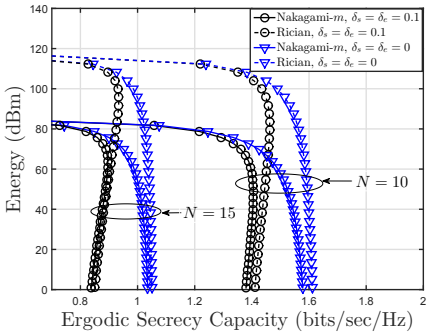


Fig. 3. Secrecy-energy region with S and E using separated design of receivers, where, $\zeta = 0.9$.

Figure 3 plots the secrecy-energy region for Nakagami-m and Rician fading channels. It can be observed that ideal channel estimation always achieves better secrecy-energy pair than that of imperfect channel estimation with $\delta_s = \delta_e = 0.1$. Moreover, when N increases from 10 to 15, the secrecy-energy performance significantly decreases. This shows that no. of eavesdroppers have a significant impact on a secrecy-energy pair. Furthermore, the gap between Nakagami-m and Rician channel shrinks for large no. of eavesdroppers.

V. Conclusion

In order to meet the future requirements of IoT networks, it is imperative that secure and environment-friendly solutions are proposed. With this intent, we have analyzed an information and power transfer IoT network from the link security perspective. Particularly, we derived closed-form expressions of ergodic secrecy capacity for two small-scale fading models. We also adopted a more practical approach by considering the availability of imperfect channel information at the transmitter. It was shown that the secrecy performance considerably deteriorates under imperfect channel estimation. In other words, an error ceiling is introduced whereby the secrecy capacity cannot be increased more even with the improvements in the SNR of the main link. This trend was observed for different receiver architectures of energy-harvesting IoT devices. Moreover, an increase in the number of eavesdroppers or channel estimation errors causes a significant reduction in the secrecy-energy region for both Rician and Nakagami-m channels. These findings can be considered important from the design perspective of secure RF energy harvesting future networks.

Acknowledgment

This work was supported in part by the Academy of Finland under Project No. 311760 and Project No. 319003.

References

[1] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[2] J. Hou, L. Qu, and W. Shi, "A survey on Internet of Things security from data perspectives," *Computer Networks*, vol. 148, pp. 295–306, 2019.

[3] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security," *IEEE Communications Surveys Tutorials*, vol. 21, no. 3, pp. 2734–2771, thirdquarter 2019.

[4] 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.

[5] F. Jameel, S. Wyne, and I. Krikidis, "Secrecy outage for wireless sensor networks," *IEEE Communications Letters*, vol. 21, no. 7, pp. 1565–1568, 2017.

[6] 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.

[7] 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.

[8] F. Jameel, Faisal, M. A. A. Haider, and A. A. Butt, "A technical review of simultaneous wireless information and power transfer (SWIPT)," in *2017 International Symposium on Recent Advances in Electrical Engineering (RAEE)*, Oct 2017, pp. 1–6.

[9] T. G. Nguyen, C. So-In, H. Tran, S. Sanguanpong *et al.*, "Secrecy Performance in the Internet of Things: Optimal Energy Harvesting Time Under Constraints of Sensors and Eavesdroppers," *Mobile Networks and Applications*, pp. 1–18, 2019.

[10] H. Ko and S. Pack, "Neighbor-Aware Energy-Efficient Monitoring System for Energy Harvesting Internet of Things," *IEEE Internet of Things Journal*, 2019.

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

[12] F. Jameel, D. N. K. Jayakody, M. F. Flanagan, and C. Tellambura, "Secure communication for separated and integrated receiver architectures in SWIPT," in *IEEE Wireless Communications and Networking Conference (WCNC)*, April 2018, pp. 1–6.

[13] O. Taghizadeh, A. Zamani, and R. Mathar, "Physical-layer security for simultaneous information and power transfer in full-duplex multi-user networks," in *Proceedings of the 20th International ITG Workshop on Smart Antennas (WSA 2016)*. VDE, 2016, pp. 1–8.

[14] Y. Bi and H. Chen, "Accumulate and jam: Towards secure communication via a wireless-powered full-duplex jammer," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1538–1550, 2016.

[15] W. Wu, B. Wang, Z. Deng, and H. Zhang, "Secure beamforming for full-duplex wireless powered communication systems with self-energy recycling," *IEEE Wireless Communications Letters*, vol. 6, no. 2, pp. 146–149, 2017.

[16] 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.

[17] M. Nakagami, "The m-distribution-A general formula of intensity distribution of rapid fading," *Statistical Method of Radio Propagation*, 1960.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

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

[23] 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.