Reconfigurable Intelligent Surface Assisted Energy Constraint Wireless System under UAV Eavesdropper with Full-Duplex Jammer

Kehinde O. Odeyemi [1, *], and Pius A. Owolawi [2]

[1] Department of Electrical and Electronic Engineering, Faculty of Technology, University of Ibadan, Nigeria
[2] Department of Computer Systems Engineering, Tshwane University of Technology, Pretoria-0001, South Africa;
Email: p.owolawi@gmail.com (P. A. O.)
*Correspondence: kesonics@yahoo.com (K.O.O.).

***Abstract*—This paper study the security performance of a Reconfigurable Intelligent Surface (RIS) energy constraint wireless system under the presence of Unmanned Aerial Vehicle (UAV) eavesdropper, where a full-duplex jammer destination is powered by a dedicated power beacon. A time switching scheme with full-duplex operation is considered for the legitimate energy constraint destination to generate jamming signal to interfere the eavesdropper. In particular, the analytical closed-form expression of Connection Outage Probability (COP), Security Outage Probability (SOP) and Secrecy Throughput (ST) are derived to evaluate the performance of the proposed system. To achieve more insight about the system, the ST asymptotic expression is obtained. Moreover, the accuracy of the derived analytical expressions is justified by the Monte-Carlo simulation. Our results illustrate that the number of reflecting elements N_E, amount of SIC ψ, and fading parameter m_{JE} significantly affect the security performance of the concerned system.**

***Keywords*—physical layer security, reconfigurable intelligent surface, energy harvest, cooperative jammer, full-duplex**

I. Introduction

Reconfigurable Intelligent Surface (RIS) has been advocated as an effective solution to enhance the performance of wireless communication especially where there is weak or no Line-of-Sight (LOS) between the transmitter and receiver [1]. This is achieved due to its capability to control radio propagation environment leading to system large coverage area with high spectral and energy efficiency [2]. RIS comprises of large number of small, low-cost and passive reflecting elements which induce phase shift on the incident waves before reflecting them to a particular direction [3]. Based on this, it found promising applications in many areas as it offers a cost-effective method for signal processing without additional power and radio frequency chain [4]. Moreover, the research has shown that RIS offers better system performance compared to conventional relaying and multiantenna technologies with reduction in system complexity and cost [5]. Thus, this make it easy to integrate RIS into existing wireless communications without requires any change of hardware [6].

Owing to characteristics nature of the wireless medium, transmission of confidential information is high susceptible to eavesdroppers' attack [7]. Today, there is tremendous growth in the deployment of UAV as main eavesdropper tools for wiretapping wireless links as a result of its cost-effectiveness, ease of operation and flexible mobility [8]. This constitutes greater threat to the ground transmitter than the terrestrial eavesdroppers due to UAV strong signal LOS and less restricted by the terrain characteristics [9]. To overcome this challenge, physical layer security (PLS) has been suggested in recent years as an efficient technique to secure information transmission in the wireless network without the use of authentication keys and encryption [10]. This technique exploits the intrinsic randomness of the channel characteristic to limit the amount of information that can be decoded by the eavesdropper [11]. Cooperative jamming is one of the most PLS strategies that involve an external helper or one of the communication devices transmits interference signal to degrade the channel quality of eavesdroppers [12, 13].

In energy constraint wireless systems, cooperative jamming require extra signal processing which incur greater power consumption and it is highly undesirable for the system [14]. To overcome this problem, energy harvesting has been proposed in literature to improve the lifetime of energy-limited devices in wireless networks [15]. As result of this, energy can be scavenged from the renewable energy sources in the environment such as thermal, wind, solar and so on and converted to electrical energy for the wireless devices [15]. However, this conventional energy harvesting methods are highly difficult to be controlled and unstable since they are mostly depending weather conditions [16]. Based on this, radio frequency (RF) wireless power transfer has be suggested as an alternative solution to provide a stable energy for communication devices [16, 17]. In open literature, there are several research studies on the PLS in the scenario of the cooperative jamming. The authors in [18] evaluated the

Manuscript received February 22, 2023; revised March 29, 2023; accepted April 10, 2023.

performance of cooperative jamming in downlink satellite network under the influence of hardware impairments. Also, the security performance of hybrid satellite-terrestrial muti-relay systems with artificial noise was studied in [19]. Wang *et al* [20] studied the PLS performance of a muti-hop hybrid satellite-terrestrial relay multiusers network with friendly jammer. However, all the aforementioned related works did not consider energy harvesting. To improve the system lifetime as a result of extra power incur by cooperative jammer, authors in [15] evaluated the security performance of energy harvesting wireless network with a cooperative jammer where multiple sources harvested energy for transmission to the base station under the presence of multiple eavesdroppers. Moreover, the PLS performance of a wireless powered communication network under the attack of multiple eavesdropper was presented in [21]. The authors proposed a full-duplex receiver which used harvested energy to emit jammer signal to the eavesdropper. Also, a power beacon aided wiretap channel was proposed in [14] where an energy limited source powered by a dedicated power beacon establishes secure communication with a legitimate user. The authors in [22] presented the security performance of a wireless powered communication network where jammer node harvested energy from the source to emit interference signal to multiple eavesdroppers. In addition, the PLS performance of an energy-constraint energy harvesting network with full-duplex self-jammer receiver was presented in [23]. In [13], the security performance of energy harvesting system enable full-duplex jamming network was studied under different energy harvesting schemes. However, the security performance of the stated research studied were not based on reconfigurable intelligent surface. In the context of RIS, the PLS of a RIS empowered wireless system was studied in [24] where a multiple antenna node send information to a legitimate user in the presence of an eavesdropper. Similarly, authors in [11] adopted RIS to enhance the security performance of a wireless systems where a base station communicates with multiple legitimate users in the presence of multiple eavesdropper. The analysis of the average secrecy capacity while comparing the efficiency of employing an RIS with both relaying systems: relay decode-and-forward (DF), and amplify-and-forward (AF) was carried out in [25]. In [26], the PLS performance of RIS-based wireless system was studied where the system security was improved with the number of meta-surface element of RIS in the presence of an eavesdropper. Wijewardena *et al.* [27] studied the security performance of a two-ways wireless network by exploiting RIS to communicate securely to the legitimate user under the presence of untrusted user. Moreover, the PLS performance of a RIS-assisted non-orthogonal multiple access network was evaluated in [6] under the influence of residual hardware impairment. However, all the aforementioned research studies on RIS under the PLS are not based on cooperative jammer and energy harvesting was not considered. Besides, their analysis was based on optimization techniques in maximizing the secrecy rates due to composite fading model of RIS that lead to intractable security metrics.

Motivated by the above observations, the security performance of a RIS aided energy constraint wireless system under the presence of UAV eavesdropper is presented, where a full-duplex jammer destination is powered by a dedicated power beacon. The main contributions of this study are summarized as follows:

(1) The exact closed-form expressions of the system performance metrics based on connection outage probability (COP), security outage probability (SOP) and secrecy throughput (ST) are derived.
(2) Also, the COP asymptotic expression is obtained at high signal-to-noise ratio (SNR) regime in order to achieve more insight about the system performance.
(3) Relative to the existing works, the PLS under the concept of RIS is based on cooperative jammer with energy harvesting and traceable security metrices are obtained.

The remainder of this paper is organized as follows. In Section II, the system and channel models are illustrated. The performance analysis of the system COP, SOP and ST are detailed in Section III with asymptotic expression. In Section IV, the numerical results and discussions are detailed. Lastly, the paper conclusion remarks are detailed in Section V.

II. System and Channel Models

A. System Description

A full-duplex RIS assisted energy constraint wireless network is illustrated in Fig. 1 where the source (S) transmit its information to the destination (D) through the RIS in the presence of UAV eavesdropper who wish to intercept the source information. At the same time, the destination harvests energy from the power beacon node and utilizes the energy to transmit interference signal to the UAV in order to secure the source information. It is assumed that every node in the network is equipped with a single antenna, but the RIS is made up of N_E reflective elements. Specifically, the destination is allocated with two separate antennas to operate in full-duplex mode of which one antenna is used to receive the source confidential information while the other for transmitting jammer signal to eavesdropper. In addition, due to unwanted obstacles and long transmission distances, it is believed that there is no direct link between the source and the legitimate destination. It also assumed that all the channels with the network are statically independent.

B. Signal Model

It is assumed that the destination is energy limited node and harvests energy through a dedicated power beacon (PB). In this case, time-switching protocol is adopted at the destination and the total transmission duration T_o is divided into two-phases, that is, energy transfer (ET) phase with αT_o duration and information receiving (IR) phase with $(1-\alpha)T_o$, where α denotes the time-switching ration in range $0 \leq \alpha \leq 1$. During the ET phase, the PB

transfer wireless energy to the FD destination and the received energy can be expressed as:

$$y_D = \sqrt{P_B} h_{PB} x_e + n_D \quad (1)$$

where P_B represents the beacon transmit power, h_{PB} denotes the channel gain between the PB and D, x_e represents energy bearing signal, n_D is the additive white Gaussian noise (AWGN) at the destination with zero mean and variance N_o^D. Hence, the total energy En_D received at the destination can be defined as:

$$En_D = \eta \alpha T_o P_B |h_{PB}|^2 \quad (2)$$

where $\eta \in \{0,1\}$ is the energy conversion efficiency and T_o indicates the time slot

Since the destination is energy limited node, energy harvested from the PB is used to radiate jammer signal. Thus, the total power P_D at the destination can be obtained as:

$$P_D = \frac{En_h}{(1-\alpha)T_o} = \beta P_B |h_{PB}|^2 \quad (3)$$

where $\beta = \frac{\eta\alpha}{1-\alpha}$

During the IR phase, the source transmits confidential information to the destination via the RIS which is overheard by the UAV eavesdropper. At the same time, the destination used the harvested energy to emit the jamming signal to the UAV eavesdropper and the signal received at the destination can be represented as:

$$y_D = \sqrt{P_s} \sum_{i=1}^{N_E} h_{s,i} h_{D,i} exp(j\phi_i)\, x_s + \sqrt{P_J} h_I x_o + n_D \quad (4)$$

where P_s is the source transmit power, x_s and x_o are the source information and jammer signal respectively, $h_{S,i} = \varsigma_i exp(-j\theta_i)$ is the channel gain of S-to-RIS link with ς_l denotes the amplitude of the link Rician fading and θ_i signifies the phase shift, $h_{D,i} = v_i exp(-j\varphi_i)$ represents the RIS-to-D channel gain with v_i denotes the amplitude of the link Rayleigh fading and φ_i signifies the phase shift, h_I denotes the self-interference channel gain at the destination.

According to [28], it is confirmed that the maximum SNR of the link is obtained by setting the $\phi_i = \theta_i + \varphi_i$. Thus, the received signal given in Eq. (4) can be rewritten as:

$$y_D = \sqrt{P_s} \left(\sum_{i=1}^{N_E} \alpha_i v_i \right) x_s + \sqrt{P_D} h_I x_o + n_D \quad (5)$$

Similarly, the signal received at the eavesdropper can be represented as:

$$y_E = \sqrt{P_s} h_{SE} x_s + \sqrt{P_D} h_{JE} x_o + n_E \quad (6)$$

where h_{SE} and h_{JE}, are respectively the channel gain of S-to-E and J-to-E links and n_E denotes AWGN at the UAV eavesdropper with zero mean and variance N_o^E.

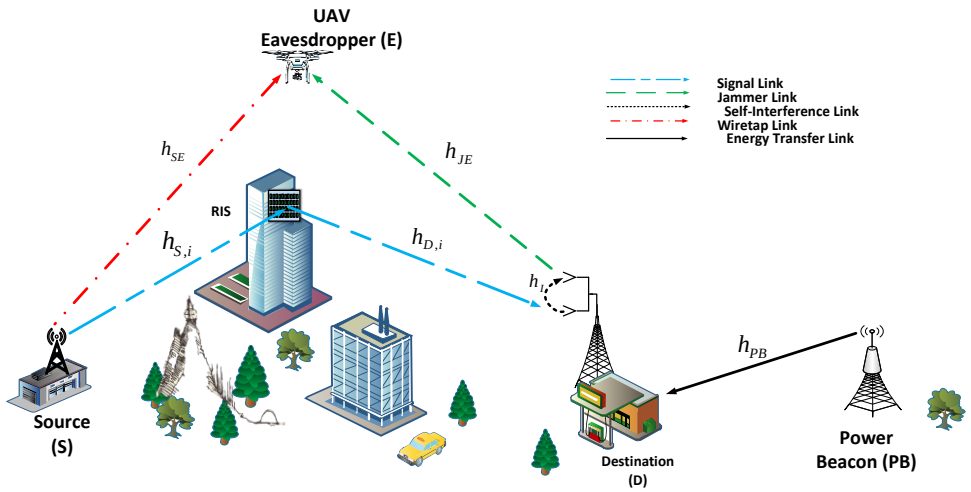

Figure 1. Model of Full-duplex RIS assisted energy constraint wireless network under UAV eavesdropper.

From Eq. (5), the receiving signal-to-interference-plus-noise ratios (SINR) at D can be obtained as:

$$\gamma_D = \frac{P_s \left| \sum_{i=1}^{N_E} \alpha_i v_i \right|^2}{P_J |h_I|^2 + N_o^D} \quad (7)$$

According to [23, 29], the $\mathbb{E}\{|h_{PB}|^2\}$ in Eq. (3) is confirmed to follow Erlang distribution with expectation the $\bar{\gamma}_{PB}$, thus the jammer power P_J at the destination can be written as:

$$P_J = \beta P_B \bar{\gamma}_{PB} \quad (8)$$

Thus, by substituting for P_J in Eq. (7), the receiving SINR at the destination can be expressed as:

$$\gamma_D = \frac{P_s \left| \sum_{i=1}^{N_E} \alpha_i v_i \right|^2}{\beta P_B \bar{\gamma}_{PB} |h_I|^2 + N_o^D} = \frac{\gamma_{SD}}{\bar{\bar{\gamma}}_I + 1} \quad (9)$$

where $\gamma_{SD} = \bar{\gamma}_{SD} \left| \sum_{i=1}^{N_E} \alpha_i v_i \right|^2$, $\bar{\gamma}_{SD} = \frac{P_s}{N_o^D}$ denotes the link average SNR, $\bar{\bar{\gamma}}_I = \bar{\gamma}_I |h_I|^2$, $\bar{\gamma}_I = \frac{\beta P_B \bar{\gamma}_{PB}}{N_o^D} - \psi$ with ψ denotes the amount of self-interference cancellation (SIC).

Similarly, from Eq. (6), the receiving SINR at the UAV eavesdropper can be expressed as:

$$\gamma_E = \frac{P_S|h_{SE}|^2}{\beta P_B \bar{\gamma}_{PB}\left|h_{JE}\right|^2 + N_o^E} = \frac{\gamma_{SE}}{\gamma_{JE}+1} \quad (10)$$

where $\gamma_{SE} = \bar{\gamma}_{SE}|h_{SE}|^2$, $\bar{\gamma}_{SE} = \frac{P_S}{N_o^E}$ denotes the link average SNR, $\gamma_{JE} = \bar{\gamma}_{JE}\left|h_{JE}\right|^2$ and $\bar{\gamma}_{JD} = \frac{\beta P_B \bar{\gamma}_{PB}}{N_o^E}$

C. Channel Models

As earlier mentioned, the S-to-RIS follows Rican distribution while the RIS-to-D link follows Rayleigh distribution. According to [28, 30], the combine PDF of the two links is subjected to an approximated generalized K-distribution and the CDF can be defined as:

$$F_{SD}(\gamma) = \Psi\gamma^{\rho_1} G_{1,3}^{2,1}\left(\frac{\mu^2}{\bar{\bar{\gamma}}_{SD}}\gamma\middle|_{\rho_2, -\rho_1, -\rho_2}^{1-\rho_1}\right) \quad (11)$$

where $\Psi = (\mu^{k_p+m_p})/\Gamma(k_p)\Gamma(m_p)(\bar{\gamma}_{SD})^{\rho_1}$, $\rho_1 = (k_p + m_p)/2$ and $\rho_2 = (k_p - m_p)/2$, k_q and m_q signify the distribution parameters and $\mu = \sqrt{k_q m_q/\Omega_q}$ with the Ω_q represents the mean power and $\Gamma(.)$ denotes the Gamma function. $\bar{\gamma}_R$ indicates the RIS link average SNR.

In addition, it is assumed that the source-to-UAV link is modelled by Rician distribution and the CDF is therefore Chi-square distributed which can be expressed as [31]:

$$F_{SE}(\gamma) = 1 - Q_1\left(\sqrt{2K}, \sqrt{\frac{2\theta\gamma}{\bar{\gamma}_{SE}}}\right) \quad (12)$$

where $\theta = K + 1$, K is the Rician fading factor, which denotes the ratio of LOS power to the non-line-of-sight (NLOS) power, and Q_1 denotes the first order Marcum function

Moreover, the jammer-to-UAV eavesdropper link is subjected to Nakagami-m distribution and the PDF of the link can be expressed as [32]:

$$f_{JE}(\gamma) = \Omega^m \frac{\gamma^{m-1}}{\Gamma(m)} exp(-\gamma\Omega) \quad (13)$$

where $\Omega = \mathrm{m}/\bar{\gamma}_{JE}$ and m denotes the fading parameter of the link.

Also, the self-interference channel gain is believed to follow Rayleigh fading and the PDF of the link is defined as [19]:

$$f_I(\gamma) = \frac{1}{\bar{\bar{\gamma}}_I} exp(-\gamma/\bar{\bar{\gamma}}_I) \quad (14)$$

III. Performance Analysis

In this paper, three secrecy metrics are considered for the performance evaluation of the proposed system and these include, COP, SOP and ST. Thus, the analytical closed-form expression of each is derived in this section.

A. COP Analysis

The COP is one of the secrecy indices which measures the probability of a link failure event where for which the destination SNR is less than a given threshold value $\gamma_{th1} = 2^{R_t} - 1$ with $R_t(bits/s/Hz)$ denotes as transmit rate. Thus, the COP of the proposed system can be given as [18]:

$$P_{COP} = Pr\{\gamma_D < \gamma_{th1}\} \quad (15)$$

By putting Eq. (9) into Eq. (15), the system COP can be defined as:

$$P_{COP} = Pr\left\{\frac{\gamma_{SD}}{\bar{\bar{\gamma}}_I + 1} < \gamma_{th1}\right\} \triangleq \int_0^\infty F_{SD}(\gamma_{th1}(x+1)) f_{JD}(x) dx \quad (16)$$

By invoking Eq. (11) and Eq. (14) into Eq. (16), the outage probability of the system can be expressed as:

$$P_{Out} = \frac{\Psi}{\bar{\bar{\gamma}}_I}\int_0^\infty \left(\gamma_{th1}(x+1)\right)^{\rho_1} exp\left(-\frac{x}{\bar{\bar{\gamma}}_I}\right) \times G_{1,3}^{2,1}\left(\frac{\mu^2}{\bar{\gamma}_{SD}}(\gamma_{th1}(x+1))\middle|_{\rho_2, -\rho_1, -\rho_2}^{1-\rho_1}\right) dx \quad (17)$$

By variable transformation, $z = \gamma_{th1}(x+1)$, $x = \frac{z}{\gamma_{th1}} - 1$ and $dx = dz/\gamma_{th1}$

Then, Eq. (17) can be expressed as:

$$P_{Out} = \frac{\Psi}{\bar{\bar{\gamma}}_I \gamma_{th1}} exp(1/\gamma_{th1}) \int_0^\infty z^{\rho_1} exp(-z/\bar{\bar{\gamma}}_I\gamma_{th1}) \times G_{1,3}^{2,1}\left(\frac{\mu^2}{\bar{\gamma}_{SD}} z\middle|_{\rho_2, -\rho_1, -\rho_2}^{1-\rho_1}\right) dz \quad (18)$$

By applying the integral identity detailed in Eq. (7.813(1)) in [33], the outage probability of the proposed system can be derived as:

$$P_{Out} = \Psi(\bar{\bar{\gamma}}_I\gamma_{th1})^{\rho_1} exp(1/\gamma_{th1}) \times G_{2,3}^{2,2}\left(\frac{\bar{\bar{\gamma}}_I\gamma_{th1}\mu^2}{\bar{\gamma}_{SD}}\middle|_{\rho_2, -\rho_1, -\rho_2}^{-\rho_1,\ 1-\rho_1}\right) \quad (19)$$

B. Asymptotic Expression

It can be observed that the analytical COP expression derived in Eq. (19) is complex and can give limited physical insight about the concerned system performance. In this case, the asymptotic expression of the system COP is developed at high SNR regime when $\bar{\gamma}_{SD} \to \infty$. By utilizing the asymptotic series expansion of the Meijer-G function at zero given in Eq. (9.303) in [33], then the system COP asymptotic expression can be obtained as:

$$P_{out}^{\infty} = \Psi(\bar{\bar{\gamma}}_I\gamma_{th1})^{\rho_1} exp(1/\gamma_{th1}) \times \sum_{l=1}^{2} \Delta_l \left(\frac{\bar{\bar{\gamma}}_I\gamma_{th1}\mu^2}{\bar{\gamma}_{SD}}\right)^{b_l} \quad (20)$$

where $\Delta_l = \frac{\prod_{t=1, t\neq l}^{2}\Gamma(\tau_{2,t}-\tau_{2,l})\Gamma(1-\tau_{1,t}-\tau_{2,1})}{\Gamma(1-\tau_{2,3}-\tau_{2,l})}$, $\tau_1 = 1-\rho_1$ and $\tau_2 = \rho_2, -\rho_1, -\rho_2$

C. SOP Analysis

The SOP of the system describes the security outage probability of event in which the eavesdropper SNR is more than the predefine threshold value $\gamma_{th2} = 2^{(R_t - R_s)} - 1$ with the $R_s(bits/s/Hz)$ signifies the secrecy rate. The SOP can thus be expressed as [13]:

$$P_{SOP} = Pr\{\gamma_E < \gamma_{th2}\} \tag{21}$$

By invoking Eq. (10) into Eq. (21), the system SOP can be defined further as:

$$P_{SOP} = Pr\left\{\frac{\gamma_{SE}}{\gamma_{JE}+1} > \gamma_{th2}\right\} \triangleq 1 - \int_0^\infty F_{SE}\big(\gamma_{th2}(y+1)\big) f_{JE}(y)dy \tag{22}$$

By substituting Eq. (12) and Eq. (13) into Eq. (22), the SOP of the system can be obtained as:

$$P_{SOP} = \frac{\Omega^m}{\Gamma(m)} \int_0^\infty Q_1\left(\sqrt{2K}, \sqrt{\frac{2\theta\big(\gamma_{th2}(y+1)\big)}{\bar{\gamma}_{SE}}}\right) \times y^{m-1} exp(-y\Omega)dy \tag{23}$$

By applying the identity detailed in [34, Eq. (29)], Marcum function can be approximated as follows:

$$Q_1(x,y) = \sum_{q=0}^{\Xi} \sum_{r=0}^{q} \frac{\xi_q q!}{r!} exp(-y^2/2)(y^2/2)^r \tag{24}$$

where $\Xi = 50\ max\{1, x, y\}$, and ξ_q can be defined as:

$$\xi_q = \frac{\Gamma(1+\Xi)\Xi^{1-2q}x^{2q}2^{-r}}{\Gamma(q+1)\Gamma(\Xi-q+1)\Gamma(q+1)exp(x^2/2)} \tag{25}$$

Thus, based on Eq. (24), the SOP given in Eq. (23) can be rewritten as:

$$P_{SOP} = \frac{\Omega^m}{\Gamma(m)} \sum_{q=0}^{\Xi} \sum_{r=0}^{q} \frac{\xi_q q!}{r!} \left(\frac{\theta\gamma_{th2}}{\bar{\gamma}_{SE}}\right)^r exp\left(-\frac{\theta\gamma_{th2}}{\bar{\gamma}_{SE}}\right) \times \int_0^\infty (y+1)^r exp\left(-\frac{\theta\gamma_{th2}}{\bar{\gamma}_{SE}}y\right) y^{m-1} exp(-y\Omega)dy \tag{26}$$

By binomial expansion theorem Eq. (1.111) in [33],

$$(y+1)^r = \sum_{k=0}^{r} \binom{r}{k} y^{r-k} \tag{27}$$

Then, Eq. (26) can be expressed further as:

$$P_{SO} = \frac{\Omega^m}{\Gamma(m)} \sum_{q=0}^{\Xi} \sum_{r=0}^{q} \sum_{k=0}^{r} \binom{r}{k} \frac{\xi_q q!}{r!} \left(\frac{\theta\gamma_{th2}}{\bar{\gamma}_{SE}}\right)^r exp\left(-\frac{\theta\gamma_{th2}}{\bar{\gamma}_{SE}}\right) \times \int_0^\infty y^{m+r-k-1} exp\left(-\left(\frac{\theta\gamma_{th2}}{\bar{\gamma}_{SE}} + \Omega\right)y\right) dy \tag{28}$$

By using the identity detailed in Eq. (3.325(3)) in [33], the proposed system SOP expression can be obtained as:

$$P_{SOP} = \frac{\Omega^m}{\Gamma(m)} \sum_{q=0}^{\Xi} \sum_{r=0}^{q} \sum_{k=0}^{r} \binom{r}{k} \frac{\xi_q q!}{r!} \left(\frac{\theta\gamma_{th2}}{\bar{\gamma}_{SE}}\right)^r exp\left(-\frac{\theta\gamma_{th2}}{\bar{\gamma}_{SE}}\right) \times \Gamma(m+r-k) \left(\frac{\bar{\gamma}_{SE}}{\theta\gamma_{th2} + \Omega\bar{\gamma}_{SE}}\right)^{m+r-k} \tag{29}$$

D. ST Analysis

Security throughput (ST) is used in wireless communication system to quantify the average rate of information that are reliably and securely transmitted. Therefore, it can be mathematically explained as the product of the secrecy rate and the probabilities of reliability and security of the transmission as follows [13, 23]:

$$\tau_{ST} = (1-\alpha)R_s[(1-P_{CO})(1-P_{SOP})] \tag{30}$$

By substituting Eq. (19) and Eq. (29) into Eq. (30), the ST of the proposed system can be obtained as:

$$\tau_{ST} = (1-\alpha)R_s \left[\Psi(\bar{\bar{\gamma}}_I\gamma_{th1})^{\rho_1} exp(-1/\gamma_{th1}) G_{1,3}^{2,1}\left(\frac{\bar{\bar{\gamma}}_I\gamma_{th1}\mu^2}{\bar{\gamma}_{SD}}\middle|_{\rho_2, -\rho_1, -\rho_2}^{1-\rho_1}\right)\right] \times \left[\frac{\Omega^m}{\Gamma(m)} \sum_{q=0}^{\Xi} \sum_{r=0}^{q} \sum_{k=0}^{r} \binom{r}{k} \frac{\xi_q q!}{r!} \left(\frac{\theta\gamma_{th2}}{\bar{\gamma}_{SE}}\right)^r exp\left(-\frac{\theta\gamma_{th2}}{\bar{\gamma}_{SE}}\right) \Gamma(m+r-k) \left(\frac{\bar{\gamma}_{SE}}{\theta\gamma_{th2} + \Omega\bar{\gamma}_{SE}}\right)^{m+r-k}\right] \tag{31}$$

IV. Numerical Results and Discussions

In this section, the numerical results of the concerned system based on the derived analytical closed-form expressions of COP, SOP and ST are presented. The accuracy of the derived expressions is verified by the Monte-Carlo simulation. The following system and channel parameter are set to be: $\alpha = 0.2$, $\eta = 0.4$, $R_s = 2\ bits/s/Hz$, $R_t = 4\ bits/s/Hz$, $\psi = 15\ dB$, $K = 1$, unless otherwise stated. Regarding the system without RIS, the source is assumed to be deployed with single antenna to communicate with destination via a relay over Nakagami-m fading channel.

Fig. 2 shows the COP performance of the system at different values of N_E, the number of reflecting elements in the RIS. The results show that the analysis results are consistent with the simulation results, justifying the accuracy of the derived expressions. We also find that increasing the number of RIS reflectors can significantly improve the COP performance of the system. In addition, the results depict that the system with RIS outperforms the system without RIS under the same conditions. Moreover, it can be seen that the analytical and asymptotic results are in perfect agreement at high SNR regime.

The COP performance of the concerned system under the effect of the amount of SIC ψ and number of reflective elements N_E is demonstrated in Fig. 3. The results show that there is a noticeable improvement in the system COP as amount of SIC ψ snice it reduces the amount of self-

interference at the destination. In all cases, increasing the number of reflective elements in the RIS also improves the COP performance of the system.

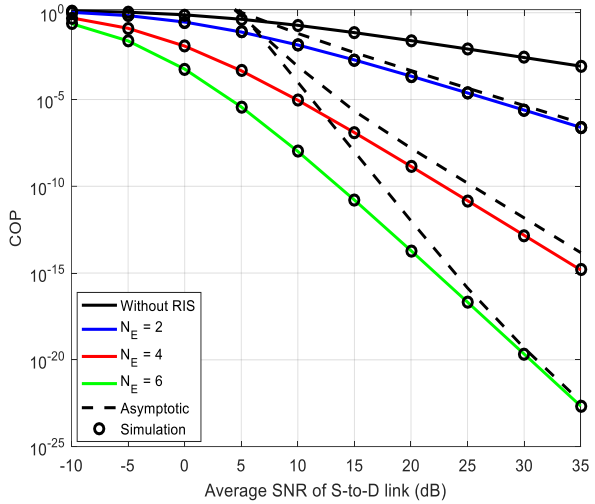

Figure 2. System COP performance under different values of number of reflecting elements N_E when $\psi = 15\ dB$.

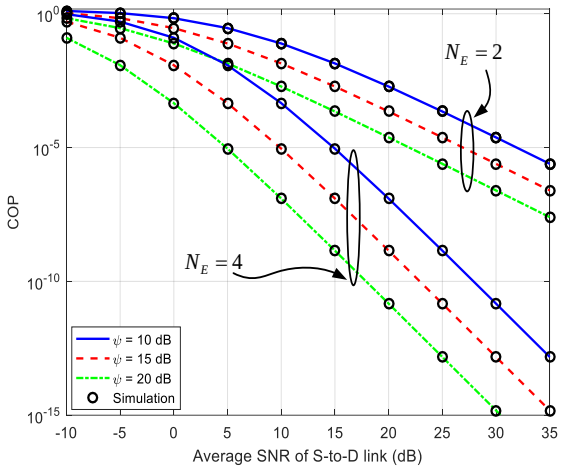

Figure 3. COP performance of the system under the influence of N_E for various values of ψ.

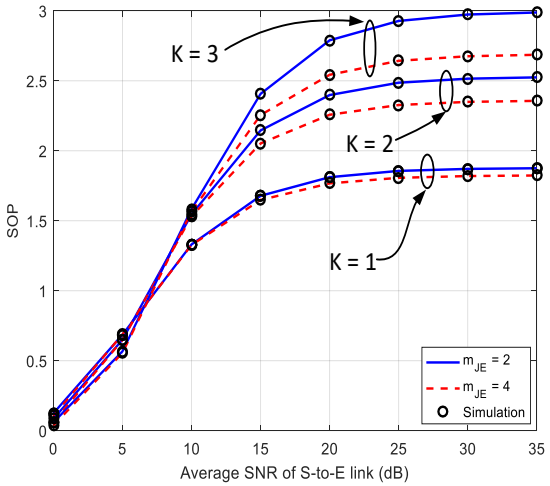

Figure 4. Influence of different values of K and m_{JE} on the system SOP performance.

In Fig. 4, the impact of m fading parameter on the J-to-E link under different values of K Rician factor is illustrated. The results show that the analytical and simulation results are in perfect agreement and verify the correctness of the derived SOP expression. From this result, it can be inferred that the SOP performance of the system decreases as the value of the K factor increases because more information is leaked to the UAV eavesdropper as result of strong LOS of the link. At any value of Rician factor, it is also observed that the increase in m fading parameter of the J-to-E link enhances the system SOP performance due to good quality of the link to emit jammer signal.

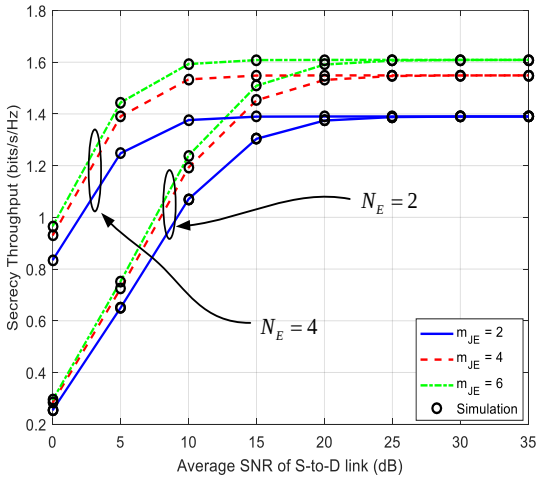

Figure 5. Impact of N_E and m_{JE} on the system ST performance when $\psi = 5\ dB$, $\bar{\gamma}_{SE} = 10\ dB$.

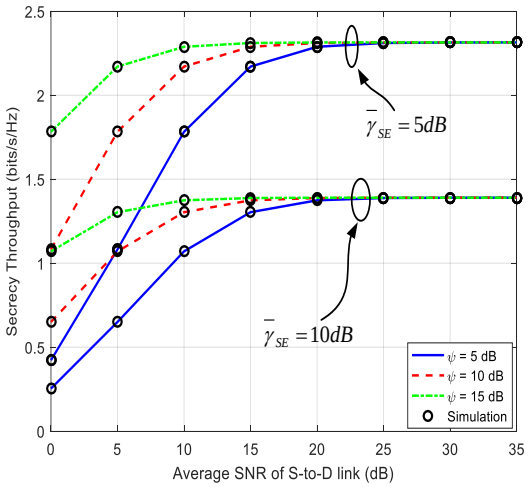

Figure 6. Effect of $\bar{\gamma}_{SE}$ on the system ST performance under various values of ψ when $m_{JE} = 2$.

The impact of number of reflecting elements at the RIS on the system ST performance under various values of m fading parameter of the J-to-E link is depicted in Fig. 5. As expected, the results prove that increasing in number of reflective elements N_E enhances the system ST performance. At a particular value of N_E, it is clearly observed that there is tremendous improvement in the

system ST performance with the increase in the m fading parameter of the J-to-E link. This is as a result of good quality channel to send jammer signal to confuse the UAV eavesdropper. In addition, the results show that the analytical and simulation results are in perfect agreement, verifying the accuracy of the derived SOP expression.

The ST performance of concerned system under the influence of amount of SIC ψ with different values of average SNR $\bar{\gamma}_{SE}$ on the S-to-E link is detailed in Fig. 6. The results depict that increasing the values of ψ produce a noticeable improvement in the system ST performance as a result of decrease in the self-interference at the destination. However, it can be observed that the increase in the values of $\bar{\gamma}_{SE}$ deteriorate the system ST performance since more information is obtained by the UAV eavesdropper.

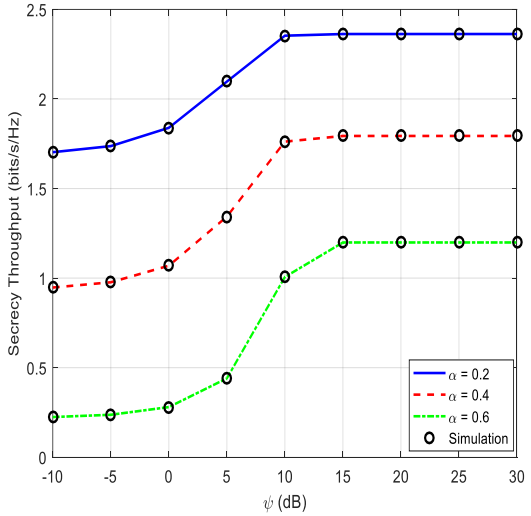

Figure 7. ST vs the amount of SIC ψ under various values of α when $\bar{\gamma}_{SD} = \bar{\gamma}_{SE} = 5\ dB$.

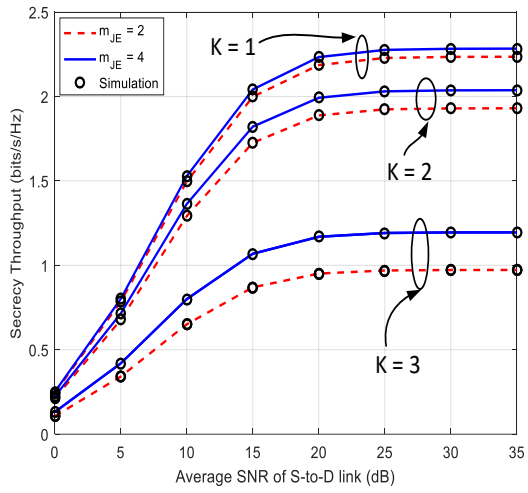

Figure 8. Influence of K factor on the system ST under different values of m_{JE} when $N_E = 4$, $\bar{\gamma}_{SE} = 15\ dB$ and $\psi = 10\ dB$.

The system performance of ST under different value of α as a function of amount of SIC ψ is presented in Fig. 7. It can be seen from the results that the system ST performance improves as the ψ increases due to decrease in self-interference at the destination. Also, it can be seen that there is significant enhancement in the system performance with the decrease in the value of α. Furthermore, it can be deduced that the simulation results agreed with the analytical results.

In Fig. 8, the impact of K Rician factor of the eavesdropper link and the m fading parameter of the J-to-E link is demonstrated. The results show that higher K values reduce the ST performance of the system. This is because UAV eavesdropper have a powerful LOS to retrieve confidential information from the source when the K factor is high. Also, it is observed that increase in the value of m_{JE} at a particular value of K improves the performance of the system ST.

V. Conclusion

In this paper, the security performance of a RIS energy constraint wireless system under the presence of UAV eavesdropper was presented where a full-duplex self-jammer emits interference signal to the eavesdropper. The analytical close-form expression of the system COP, SOP and ST are derived. Also, the system COP asymptotic expression is acquired to provide more insight into performance of the concerned system at high SNR regime. In addition, the correctness of the derived closed-form expressions is verified through the Monte-Carlo simulations. It can be deduced from the results that system and channel parameters such as the number of reflective elements in the RIS, network m-fading parameters, K-Rican coefficient for UAV sniffing attacks and amount of SIC have a significant impact on the system safety. The results also show that the system with RIS performs better than the system without RIS system.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Methodology, K.O.; software, K.O.; validation, K.O. P.A; formal analysis, K.O.; writing—original draft preparation, K.O.; writing—review and editing, K.O. and P.A.; supervision, P.A. all authors had approved the final version.

References

[1] I. Trigui, W. Ajib, W.-P. Zhu, and M. Di Renzo, "Performance evaluation and diversity analysis of RIS-assisted communications over generalized fading channels in the presence of phase noise," *IEEE Open Journal of the Communications Society*, 2022.

[2] G. D. Verma, A. Mathur, Y. Ai, and M. Cheffena, "Mixed dual-hop IRS-assisted FSO-RF communication system with H-ARQ protocols," *IEEE Communications Letters*, 2021.

[3] M. A. Jarrah, A. A. Dweik, E. Alsusa, Y. Iraqi, and M.-S. Alouini, "On the performance of IRS-Assisted multi-layer uav communications with imperfect phase compensation," *IEEE Transactions on Communications*, vol. 69, no. 12, pp. 8551-8568, 2021.

[4] J. Chen, Y. C. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: A programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82599-82612, 2019.

[5] K. O. Odeyemi, P. A. Owolawi, and O. O. Olakanmi, "Reconfigurable intelligent surface-assisted HAPS relaying communication networks for multiusers under AF protocol: A performance analysis," *IEEE Access*, vol. 10, pp. 14857-14869, 2022.
[6] Q. Chen, M. Li, X. Yang, R. Alturki, M. D. Alshehri, and F. Khan, "Impact of residual hardware impairment on the IoT secrecy performance of RIS-assisted NOMA networks," *IEEE Access*, vol. 9, pp. 42583-42592, 2021.
[7] K. O. Odeyemi and P. A. Owolawi, "Physical layer security in mixed RF/FSO system under multiple eavesdroppers collusion and non-collusion," *Optical Quantum Electronics*, vol. 50, no. 7, pp. 1-19, 2018.
[8] K. O. Odeyemi and P. A. J. Owolawi, "Secure hybrid satellite-UWOC cooperative relaying system under malicious unmanned aerial vehicle eavesdropper threat," *International Journal of Wireless Mobile Computing*, vol. 21, no. 1, pp. 66-75, 2021.
[9] J. Tang, G. Chen, and J. P. Coon, "Secrecy performance analysis of wireless communications in the presence of UAV jammer and randomly located UAV eavesdroppers," *IEEE Transactions on Information Forensics Security*, vol. 14, no. 11, pp. 3026-3041, 2019.
[10] X. Jiang, P. Li, B. Li, Y. Zou, and R. Wang, "Security-reliability tradeoff for friendly jammer aided multiuser scheduling in energy harvesting communications," *Security Communication Networks*, 2021.
[11] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, "Robust and secure wireless communications via intelligent reflecting surfaces," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 11, pp. 2637-2652, 2020.
[12] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, "Jamming strategies for physical layer security," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 148-153, 2017.
[13] R. Ma, H. Wu, J. Ou, S. Yang, and Y. Gao, "Power splitting-based SWIPT systems with full-duplex jamming," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9822-9836, 2020.
[14] X. Jiang, C. Zhong, Z. Zhang, and G. K. Karagiannidis, "Power beacon assisted wiretap channels with jamming," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8353-8367, 2016.
[15] T. G. Nguyen, C. So-In, and D.-B. Ha, "Secrecy performance analysis of energy harvesting wireless sensor networks with a friendly jammer," *IEEE Access*, vol. 5, pp. 25196-25206, 2017.
[16] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 401-415, 2015.
[17] Z. Chen, L. Hadley, Z. Ding, and X. Dai, "Improving secrecy performance of a wirelessly powered network," *IEEE Transactions on Communications*, vol. 65, no. 11, pp. 4996-5008, 2017.
[18] H. Wu, L. Zheng, Z. Li, R. Ma, and J. Ou, "Cooperative jamming in downlink satellite network with hardware impairments," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 12, p. e4372, 2021.
[19] M. Huang, F. Gong, N. Zhang, G. Li, and F. Qian, "Reliability and Security Performance Analysis of Hybrid Satellite-Terrestrial Multi-Relay Systems With Artificial Noise," *IEEE Access*, vol. 9, pp. 34708-34721, 2021.
[20] X. Wang, H. Zhang, and Z. Hou, "Physical Layer Secrecy Analysis of Multihop Hybrid Satellite-Terrestrial Relay Networks with Jamming," *Wireless Communications Mobile Computing*, vol. 2021, 2021.
[21] B. Ji, Y. Li, B. Zhou, C. Li, K. Song, and H. Wen, "Performance analysis of UAV relay assisted IoT communication network enhanced with energy harvesting," *IEEE Access*, vol. 7, pp. 38738-38747, 2019.
[22] J. Moon, H. Lee, C. Song, and I. Lee, "Secrecy performance optimization for wireless powered communication networks with an energy harvesting jammer," *IEEE Transactions on Communications*, vol. 65, no. 2, pp. 764-774, 2016.
[23] X. Tang *et al.*, "Energy-constrained SWIPT networks: Enhancing physical layer security with FD self-jamming," *IEEE Transactions on Information Forensics Security*, vol. 14, no. 1, pp. 212-222, 2018.
[24] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410-1414, 2019.
[25] N. Mensi, D. B. Rawat, and E. Balti, "Physical layer security for V2I communications: Reflecting surfaces vs. relaying," in *Proc. 2021 IEEE Global Communications Conference (GLOBECOM)*, 2021, pp. 1-6.
[26] D.-T. Do, A.-T. Le, N.-D. X. Ha, and N.-N. Dao, "Physical layer security for Internet of Things via reconfigurable intelligent surface," *Future Generation Computer Systems*, vol. 126, pp. 330-339, 2022.
[27] M. Wijewardena, T. Samarasinghe, K. T. Hemachandra, S. Atapattu, and J. S. Evans, "Physical layer security for intelligent reflecting surface assisted two–way communications," *IEEE Communications Letters*, vol. 25, no. 7, pp. 2156-2160, 2021.
[28] L. Yang, F. Meng, J. Zhang, M. O. Hasna, and M. Di Renzo, "On the performance of RIS-assisted dual-hop UAV communication systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 10385-10390, 2020.
[29] D. Wang, R. Zhang, X. Cheng, and L. Yang, "Capacity-enhancing full-duplex relay networks based on power-splitting (PS-) SWIPT," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 6, pp. 5445-5450, 2016.
[30] K. Odeyemi, P. Owolawi, and O. Olakanmi, "Reconfigurable intelligent surface in wireless-powered interference-limited communication networks," *Symmetry*, vol. 13, no. 6, p. 960, 2021.
[31] S. I. Alnagar, A. M. Salhab, and S. A. Zummo, "Unmanned aerial vehicle relay system: Performance evaluation and 3D location optimization," *IEEE Access*, vol. 8, pp. 67635-67645, 2020.
[32] N.-L. Nguyen, H.-N. Nguyen, A.-T. Le, D.-T. Do, and M. Voznak, "On performance analysis of NOMA-aided hybrid satellite terrestrial relay with application in small-cell network," *IEEE Access*, vol. 8, pp. 188526-188537, 2020.
[33] I. Gradshteyn, I. Ryzhik, and R. H. Romer, "Tables of integrals, series, and products," *American Association of Physics Teachers*, 1988.
[34] P. C. Sofotasios and S. Freear, "Novel expressions for the Marcum and one dimensional Q-functions," in *Proc. 2010 7th International Symposium on Wireless Communication Systems*, 2010, pp. 736-740: IEEE.