

Physical layer security of reconfigurable intelligent surface empowered wireless network with cooperative jammer

Kehinde Oluwasesan Odeyemi¹, Pius Adewale Owolawi², Olakanmi Oladayo Olufemi¹

¹Department of Electrical and Electronic Engineering, Faculty of Technology, University of Ibadan, Ibadan, Nigeria

²Department of of Computer Systems Engineering, Tshwane University of Technology, Pretoria, South Africa

Article Info

Article history:

Received May 12, 2022

Revised Aug 13, 2022

Accepted Sep 2, 2022

Keywords:

Connection outage probability

Cooperative jammer

Physical layer security

Reconfigurable intelligent surface

Secrecy throughput

Security outage probability

ABSTRACT

This paper evaluates the physical layer security performance of a reconfigurable intelligent surface (RIS) enabled wireless network in the presence of a passive eavesdropper. To secure the information transmission, a cooperative jammer is proposed to generate interference signal that degrade the performance of the eavesdropper. The source-to-RIS and RIS-to-destination links are subjected to Rician and Rayleigh fading distributions with phase errors, respectively, while other transmission links in the network follow the Nakagami-m fading distributions. The system phase error of the RIS is estimated by the von Mises distribution. To quantify the secrecy performance of the concerned system, the exact closed-form expressions in terms of connection outage probability (COP), security outage probability (SOP), and secrecy throughput (ST) are derived. In addition, the asymptotic expression of the system COP is obtained at high signal-to-noise ratio (SNR), providing more insight about the system performance. The accuracy of the derived expression is justified by Monte Carlo simulation. Also, the results clarify the analysis of the security performance, taking into account the impact of system and channel parameters on the system.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Kehinde Oluwasesan Odeyemi

Department of Electrical and Electronic Engineering, Faculty of Technology, University of Ibadan

Oduduwa Road, 200132, Ibadan, Nigeria

Email: kesonics@yahoo.com

1. INTRODUCTION

Recently, reconfigurable intelligent surface (RIS) has been considered as a new technology deployed to improve the coverage area, spectrum and power efficiency of wireless communication systems [1]. Its structure consists of large passive reflective elements that can introduce a phase shift to the incident signals before it is reflected in the desired direction [2]. Therefore, no additional power, radio frequency chains, and dedicated power supplies are required for signal processing compared to other traditional relay and multi-antenna technologies [3], [4]. Due to its light weight and shape conformance, RIS can be easily applied to building walls, windows, human clothing, and roadside signs [5]. As a result of these possibilities, RIS-supported transmission can be easily integrated to support existing and next-generation wireless networks. In open literature, RIS has been extensively studied to improve the transmission reliability of the wireless systems at weak or no line of sight (LSO) [6]. RIS was used to extend the coverage area of the unmanned aerial vehicle (UAV) communication system and evaluated the probability of system failure and error rate [7]. In addition, RIS was used to support the transmission of stratospheric platform stations in wireless multi-user systems in [3]. Under various relay protocols, Odeyemi *et al.* [8] studied the performance of RIS-supported power-line communication networks. The impact of interference on the performance of RIS support wireless systems is shown in [9]. Odeyemi *et al.* [10] studied the performance of RIS in supporting

the underwater communication systems. Moreover, Verma *et al.* [11] proposed a RIS-aided mixed dual-hop free space optical/radio frequency communication system where the impact of hybrid automatic repeat request protocol was studied on both link. In addition, the performance analysis of multi-layer UAV wireless communication assisted by RIS was presented in [2] where the error rate and outage probability of the system were evaluated under the imperfect phase compensation.

Due to the broadcast nature of wireless media, wireless transmission is extremely vulnerable to security measures by malicious users. As a result, physical layer security has been proposed as an alternative to traditional cryptographic techniques to protect wireless communication systems regardless of eavesdropping capabilities [12]. This concept involves leveraging the probabilistic characteristics of radio channels (that is, noise, fading, and interference) to reduce the likelihood that information will be decoded by eavesdroppers [13], [14]. Thus, cooperative jammer has been regarded as one of the efficient physical layer security methods in which either an external helper or a communication device emits artificial or interfering noise to reduce the channel quality of the eavesdropper [15]. In this case, several research efforts have been tailored towards the adoption of RIS in enhancing the physical layer security of wireless communication system. The physical layer security of a RIS empowered wireless system was studied in [16] where a multiple antenna node transmit information to a single antenna legitimate user in the presence of an eavesdropper. Similarly, Yu *et al.* [17] 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 physical layer security performance of RIS-based wireless system was studied where the system security was improved with the number of meta-surface element of RIS under the attack of an eavesdropper [18]. Wijewardena *et al.* [19] 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 physical layer security performance of a RIS-assisted non-orthogonal multiple access network was evaluated in [20] under the influence of residual hardware impairment. However, all of the above research studies on RIS under the physical layer security are not based on cooperative jammer and do not take phase errors into account. Their analysis was also based on optimization techniques to maximize the secrecy rates due to composite fading models of RIS and makes it difficult to manage the system security metrics. Regarding the phase error, the security performance of the RIS-assisted communication system with the phase error was presented in [21] but not subjected to cooperative jammer technique.

Motivated by the above observations, the physical layer security performance of a RIS empowered wireless network in the presence of an eavesdropper is presented. An external cooperative jammer is proposed to improve the system security performance by emitting interference signal that degrades the performance of the eavesdropper. The phase error of the RIS is estimated through the von Mises distribution and the system connection outage probability (COP), security outage probability (SOP), and secrecy throughput (ST) closed-form expressions are derived. To obtained more insight about the system performance, the COP asymptotic expression are derived.

The rest of this paper is arranged as follows; section 2 shows the system and channel models. The system performance analysis is provided in section 3 with asymptotic expression. In section 4, the numerical results are presented with discussions. Finally, section 5 contains the conclusions about the paper.

2. SYSTEM AND CHANNEL MODELS

2.1. System model

As depicted in Figure 1, a RIS empowered wireless network with a source (S), a legitimate destination (D), a jammer (J), and an eavesdropper (E) is presented. The source transmits confidential information to the destination via a RIS in the presence of an eavesdropper attempting to eavesdrop source's confidential information. At the same time, a cooperative jammer sends interference signal to prevent the source information from being intercepted by the eavesdropper. Due to availability of unwanted obstacles, it is believed that there is no direct connection between the S and D. Therefore, it is assumed that the RIS is highly positioned to prevent eavesdroppers from wiretapping on the connection. Furthermore, it is assumed that every node in the network has a single antenna. However, the RIS consists of a number of wall-mounted N_R reflective elements to aid in secure transmission between the source and destination. All the channels in the proposed network are assumed to be statistically independent with the connection between the source and the RIS, and RIS and destination are respectively denoted as $h_{S,i}$ and $h_{D,i}$. The link from the source to eavesdropper is represented by h_{SE} . Also, the channel from the jammer to eavesdropper and destination are respectively denoted as h_{JE} and h_{JD} .

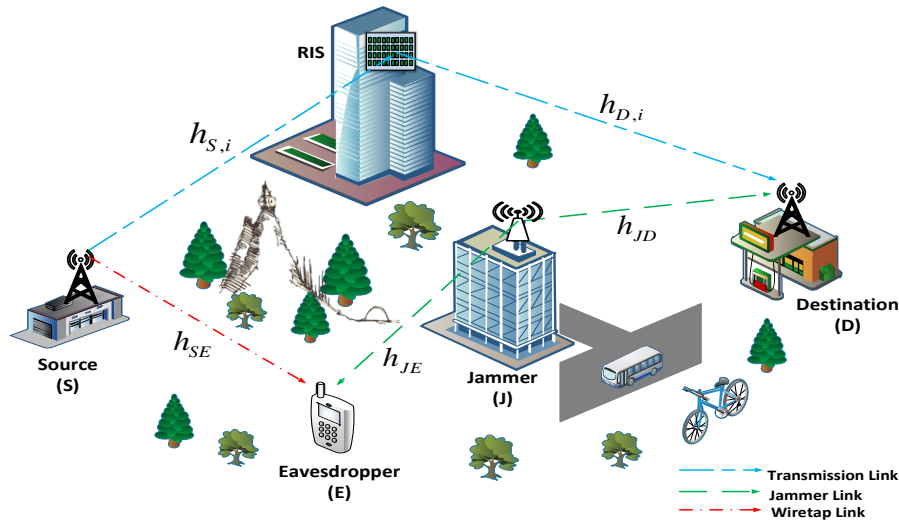


Figure 1. Model of RIS empowered wireless network with friendly jammer

2.2. Signal model

The source sends information to the destination via the RIS, and the signal received at the legitimate destination and eavesdropper can be respectively represented as:

$$y_D = \sqrt{P_S} \sum_{l=1}^{N_R} h_{S,l} \omega_l h_{D,l} \exp(j\phi_l) x_s + \sqrt{P_J} h_{JD} x_J + z_D \quad (1)$$

and

$$y_E = \sqrt{P_S} h_{SE} x_S + \sqrt{P_J} h_{JE} x_J + z_E \quad (2)$$

where P_S and P_J are the source and jammer transmit power respectively, x_s and x_J are the source information and interference signal respectively, $h_{S,l} = \alpha_l \exp(-j\theta_l)$ denotes the channel gain of S-to-RIS link with α_l represents the amplitude of the link Rician fading and θ_l signifies the phase shift, $h_{D,l} = \beta_l \exp(-j\psi_l)$ represents the RIS-to-D channel gain with the with β_l denotes the amplitude of the link Rayleigh fading and ψ_l signifies the phase shift, $\omega_l = \exp(j\vartheta_l)$ indicates the reflection coefficient produced by the l^{th} reflecting element of RIS, z_D and z_E are the complex additive white Gaussian noise (AWGN) at the destination and eavesdropper respectively with zero mean and variance σ_D^2 and σ_E^2 , $\phi_l = \theta_l + \psi_l - \vartheta_l$ signifies the phase deviation and is model by circular distribution. Thus, the signal-to-interference-plus-noise ratio (SINR) at the destination can be obtained from (1) as follows:

$$\gamma_D = \frac{P_S \left| \sum_{l=1}^{N_R} h_{S,l} \omega_l h_{D,l} \exp(j\phi_l) \right|^2}{P_J |h_{JD}|^2 + \sigma_D^2} \quad (3)$$

if the instantaneous signal-to-noise ratio (SNR) at the S-to-D and J-to-D are respectively defined as $\gamma_{SD} = P_S \left| \sum_{l=1}^{N_R} h_{S,l} \omega_l h_{D,l} \exp(j\phi_l) \right|^2 / \sigma_D^2$ and $\gamma_{JD} = P_J |h_{JD}|^2 / \sigma_D^2$, then the SINR at destination can be further expressed as:

$$\gamma_D = \frac{\gamma_{SD}}{\gamma_{JD} + 1} \quad (4)$$

from (2), the SINR at the eavesdropper can be expressed as:

$$\gamma_E = \frac{P_S |h_{SE}|^2}{P_J |h_{JE}|^2 + \sigma_E^2} \quad (5)$$

similarly, if $\gamma_{SE} = P_S |h_{SE}|^2 / \sigma_E^2$ and $\gamma_{JE} = P_J |h_{JE}|^2 / \sigma_E^2$, then (5) can be further expressed as:

$$\gamma_E = \frac{\gamma_{SE}}{\gamma_{JE}+1} \tag{6}$$

2.3. Channel models

With the incorporation of phase error, the combine probability density function (PDF) of the S-to-RIS and RIS-to-D is assumed to follow Gamma distribution defined as [22]:

$$f_{SD}(\gamma) = \frac{m_r^{m_r}}{(m_r-1)!\bar{\gamma}_{SD}^{m_r}} \gamma^{m_r-1} \exp\left(-\frac{m_r}{\bar{\gamma}_{SD}} \gamma\right) \tag{7}$$

where $m_r = \frac{N_R}{2} \frac{\phi_1^2 a^4}{\phi_2 - 2\phi_1^2 a^4}$ denotes the S-to-D fading parameter, $\phi_v = \frac{I_v(k)}{I_0(k)}$ is the characteristic function with I_0 the modified Bessel function of the first kind and order v , k indicates the concentration parameter of von Mises distribution, $\bar{\gamma}_{SD} = N_R^2 \phi_1^2 a^4 \gamma_o$ is the average SNR of the link and γ_o represent the average SNR of a single reflecting RIS element, $a_1 = \sqrt{\frac{\pi}{4(K+!)}} {}_1F_1(-1/2, 1, K)$ and $a_2 = \sqrt{\pi}/2$ are respectively denote the unit power of the $h_{S,i}$ and $h_{D,i}$ with $a = \sqrt{a_1 a_2}$. By using the integral identity detailed in [23], the CDF of the S-to-D link over RIS can be obtained from (7) as:

$$F_{SD}(\gamma) = 1 - \exp\left(-\frac{m_r}{\bar{\gamma}_{SD}} \gamma\right) \sum_{p=0}^{m_r-1} \frac{1}{p!} \left(\frac{m_r}{\bar{\gamma}_{SD}}\right)^p \gamma^p \tag{8}$$

similarly, the other links are subject to Nakagami-m distribution and the PDF can be expressed as [24]:

$$f_{\xi}(\gamma) = \frac{\gamma^{m_{\xi}-1}}{\Gamma(m_{\xi})\omega_{\xi}^{m_{\xi}}} \exp(-\gamma/\omega_{\xi}), \xi \in \{SE, JE \text{ and } JD\} \tag{9}$$

where $\omega_{\xi} = \bar{\gamma}_{\xi}/m_{\xi}$ with m_{ξ} and $\bar{\gamma}_{\xi}$ represent the links fading parameters and average SNR respectively. By integrating (9), the CDF of the links can be obtained as:

$$F_{\xi}(\gamma) = 1 - \exp\left(-\frac{\gamma}{\omega_{\xi}}\right) \sum_{n=0}^{m_{\xi}-1} \frac{\gamma^n}{\omega_{\xi}^{n+1} n!} \tag{10}$$

3. PERFORMANCE ANALYSIS

In this study, the concerned system is evaluated using three secrecy metrics which include, COP, SOP and ST, and the exact closed-form expression for each is obtained in this section.

3.1. Connection outage probability

The reliability of the system is quantified by COP which describes the probability of the connection outage event in which the destination SNR is less than the preset threshold value $\gamma_t = 2^{R_t} - 1$ with R_t (bits/s/Hz) denotes as transmit rate. Thus, the COP of the concerned system can be expressed as [25]:

$$P_{COP}(\gamma_t) = Pr\{\gamma_D < \gamma_t\} \tag{11}$$

by putting (4) into (11), the COP can be further expressed as:

$$P_{COP}(\gamma_t) = Pr\left\{\frac{\gamma_{SD}}{\gamma_{JD}+1} < \gamma_t\right\} \triangleq \int_0^{\infty} F_{SD}(\gamma_t(x+1)) f_{JD}(x) dx \tag{12}$$

putting (8) and (9) into (13), the $P_{COP}(\gamma_t)$ can be expressed as:

$$P_{COP}(\gamma_t) = 1 - \frac{1}{\Gamma(m_{JD})\omega_{JD}^{m_{JD}}} \sum_{p=0}^{m_r-1} \frac{1}{p!} \left(\frac{m_r}{\bar{\gamma}_{SD}}\right)^p \exp\left(-\frac{m_r}{\bar{\gamma}_{SD}}(\gamma_t(x+1))\right) \int_0^{\infty} (\gamma_t(x+1))^p \times x^{m_{JD}-1} \exp(-x/\omega_{JD}) dx \tag{13}$$

by binomial expansion in [23], (1.111), $(x+1)^p = \sum_{t=0}^p \binom{p}{t} x^{p-t}$ and (13) can be expressed as:

$$P_{COP}(\gamma_t) = 1 - \frac{1}{\Gamma(m_{JD})\omega_{JD}^{m_{JD}}} \sum_{p=0}^{m_r-1} \sum_{t=0}^p \binom{p}{t} \frac{1}{p!} \left(\frac{m_r \gamma_t}{\bar{\gamma}_{SD}}\right)^p \exp\left(-\frac{m_r \gamma_t}{\bar{\gamma}_{SD}}\right) \int_0^{\infty} x^{m_{JD}+p-t-1} \times \exp\left(-\left(\frac{m_r \gamma_t}{\bar{\gamma}_{SD}} + \frac{1}{\omega_{JD}}\right)x\right) dx \tag{14}$$

by utilizing the integral identity detailed in [23], (3.325(2)), (14) can be expressed as:

$$P_{COP}(\gamma_t) = 1 - \frac{1}{\Gamma(m_{JD})\omega_{JD}^{m_{JD}}} \sum_{p=0}^{m_r-1} \sum_{t=0}^p \binom{p}{t} \frac{1}{p!} \left(\frac{m_r \gamma_t}{\bar{\gamma}_{SD}}\right)^p \exp \times \Gamma(m_{JD} + p - t) \left(\frac{\bar{\gamma}_{SD}\omega_{JD}}{m_r \gamma_t \omega_{JD} + \bar{\gamma}_{SD}}\right)^{m_{JD}+p-t} \quad (15)$$

3.1.1. Asymptotic analysis

Since the COP expression derived in (14) is complicated, it is necessary to perform asymptotic analysis of the system at high SNR assuming $\bar{\gamma}_{SD} \rightarrow \infty$ in order to understand the system performance. At high SNR, the asymptotic expression for the S-to-D CDF in (16) can be defined as [26]:

$$F_{SD}(\gamma) \approx \left(\frac{m_r}{\bar{\gamma}_{SD}}\right)^{m_r} \frac{\gamma^{m_r}}{\Gamma(m_r)} \quad (16)$$

by putting (16) and (9) into (13), then the COP asymptotic expression can then be expressed as:

$$P_{COP}^{Asy} = \left(\frac{m_r}{\bar{\gamma}_{SD}}\right)^{m_r} \frac{1}{\Gamma(m_r)\Gamma(m_{JD})\omega_{JD}^{m_{JD}}} \int_0^\infty (\gamma_t(x+1))^{m_r} x^{m_{JD}-1} \exp(-x/\omega_{JD}) dx \quad (17)$$

by applying binomial theorem, (17) can be further expressed as:

$$P_{COP}^{Asy} = \left(\frac{m_r}{\bar{\gamma}_{SD}}\right)^{m_r} \frac{1}{\Gamma(m_r)\Gamma(m_{JD})\omega_{JD}^{m_{JD}}} \sum_{t=0}^{m_r} \binom{m_r}{t} \int_0^\infty x^{m_r+m_{JD}-t-1} \exp(-x/\omega_{JD}) dx \quad (18)$$

by using the integral identity detailed in [23], (3.325(2)), (18) can be solved as:

$$P_{COP}^{Asy} = \left(\frac{m_r}{\bar{\gamma}_{SD}}\right)^{m_r} \frac{1}{\Gamma(m_r)\Gamma(m_{JD})\omega_{JD}^{m_{JD}}} \sum_{t=0}^{m_r} \binom{m_r}{t} \Gamma(m_r + m_{JD} - t) \omega_{JD}^{(m_r+m_{JD}-t)} \quad (19)$$

3.2. Security outage probability

The SOP of the system illustrates the security outage probability of event in which the eavesdropper SNR is higher than the preset threshold value $\gamma_s = 2^{(R_t-R_s)} - 1$ with the R_s (bits/s/Hz) denotes as secrecy rate. The SOP can thus be expressed as [27]:

$$P_{SOP}(\gamma_s) = Pr\{\gamma_E > \gamma_s\} \quad (20)$$

by invoking (6) into (20), the SOP can be further expressed as:

$$P_{SOP}(\gamma_s) = Pr\left\{\frac{\gamma_{SE}}{\gamma_{JE}+1} > \gamma_s\right\} \triangleq 1 - \int_0^\infty F_{SE}(\gamma_s(y+1)) f_{JE}(y) dy \quad (21)$$

by putting (10) and (9) into (21), the SOP of the proposed system can be expressed as:

$$P_{SO} = \int_0^\infty \sum_{n=0}^{m_{SE}-1} \frac{(\gamma_s)^n}{\omega_{SE}^n n!} (y+1)^n \exp(-\gamma_s(y+1)/\omega_{SE}) \frac{y^{m_{JE}-1} \exp(-y/\omega_{JE})}{\Gamma(m_{JE})\omega_{JE}^{m_{JE}}} dy \quad (22)$$

by binomial expansion in [23], (1.111), $(y+1)^n = \sum_{q=0}^n \binom{n}{q} y^{n-q}$, then (22) can be further expressed as:

$$P_{SOP}(\gamma_s) = \frac{1}{\Gamma(m_{JE})\omega_{JE}^{m_{JE}}} \sum_{n=0}^{m_{SE}-1} \sum_{q=0}^n \binom{n}{q} \left(\frac{\gamma_s}{\omega_{JD}}\right)^n \frac{1}{n!} \exp(-\gamma_s/\omega_{JE}) \times \int_0^\infty y^{m_{JE}+n-q-1} \exp\left(-\left(\frac{\gamma_s}{\omega_{SE}} + \frac{1}{\omega_{JD}}\right)y\right) dy \quad (23)$$

by integral identity detailed in [23], (3.325(2)), hence (23) can be solved as:

$$P_{SOP}(\gamma_s) = \frac{1}{\Gamma(m_{JE})\omega_{JE}^{m_{JE}}} \sum_{n=0}^{m_{SE}-1} \sum_{q=0}^n \binom{n}{q} \left(\frac{\gamma_s}{\omega_{JD}}\right)^n \frac{1}{n!} \exp(-\gamma_s/\omega_{JE}) \times \Gamma(m_{JE} + n - q) \left(\frac{\omega_{SE}\omega_{JD}}{\gamma_s\omega_{JD} + \omega_{SE}}\right)^{m_{JE}+n-q} \quad (24)$$

3.3. Secrecy throughput

This is adopted in wireless communication system to measure the average rate of information that is transmitted reliably and securely. Mathematically, it is defined as the product of secrecy rate and the probabilities of reliability and security transmission as follows [26]:

$$\tau_{ST} = R_s \left[(1 - P_{COP}(\gamma_t))(1 - P_{SOP}(\gamma_s)) \right] \tag{25}$$

by substituting (18) and (24) into (25), the ST for the concerned system can be obtained as:

$$\tau_{ST} = R_s \left[\frac{1}{\Gamma(m_{JD})\omega_{JD}^{m_{JD}}} \sum_{p=0}^{m_r-1} \sum_{t=0}^p \binom{p}{t} \frac{1}{p!} \left(\frac{m_r \gamma_t}{\bar{\gamma}_{SD}}\right)^p \exp\left(-\frac{m_r \gamma_t}{\bar{\gamma}_{SD}}\right) \times \Gamma(m_{JD} + p - t) \left(\frac{\bar{\gamma}_{SD}\omega_{JD}}{m_r \gamma_t \omega_{JD} + \bar{\gamma}_{SD}}\right)^{m_{JD}+p-t} \right] \times \left[1 - \frac{1}{\Gamma(m_{JE})\omega_{JE}^{m_{JE}}} \sum_{n=0}^{m_{SE}-1} \sum_{q=0}^n \binom{n}{q} \left(\frac{\gamma_s}{\omega_{JD}}\right)^n \frac{1}{n!} \exp(-\gamma_s/\omega_{JE}) \times \Gamma(m_{JE} + n - q) \left(\frac{\omega_{SE}\omega_{JD}}{\gamma_s \omega_{JD} + \omega_{SE}}\right)^{m_{JE}+n-q} \right] \tag{26}$$

4. NUMERICAL RESULTS AND DISCUSSION

This section provides numerical results for the physical layer security of RIS-enabled wireless networks with cooperative jammers under the performance metrics COP, SOP, and ST. The accuracy of the derived analytical formula is verified by Monte Carlo simulation. Unless otherwise specified, the following system parameter values are set to $k = 2$, $N_R = 40$, $m_{SE} = m_{JE} = m_{JD} = 2$, $R_s = 2 \text{ bits/s/Hz}$, and $R_t = 4 \text{ bits/s/Hz}$.

Figure 2 shows the effect of the number of RIS reflective elements N_R on the COP performance of the system. The results show that the COP performance of the system improves with increasing N_R . From the results, we can conclude that the analysis and simulation results are consistent which indicate the correctness of the derived COP expression. In addition, the results show a perfect match between the analysis and asymptotic results over the high SNR regime. In addition, systems with RIS offers better COP performance than systems without RIS.

The influence of concentration parameter k of von Mises distribution on the system COP performance at various values of m fading parameter on the J-to-D link is illustrated in Figure 3. It can be observed that the increase in k parameter leads to better system COP performance with large value of k indicate same phase error. Moreover, the results outcome proves that at a particular value of k , there is significant improvement in the system COP with the increase in the m_{JD} of the J-to-D link. This is due to good channel quality for the jammer signal to reach the eavesdropper and show the impact of friendly jammer of the proposed system.

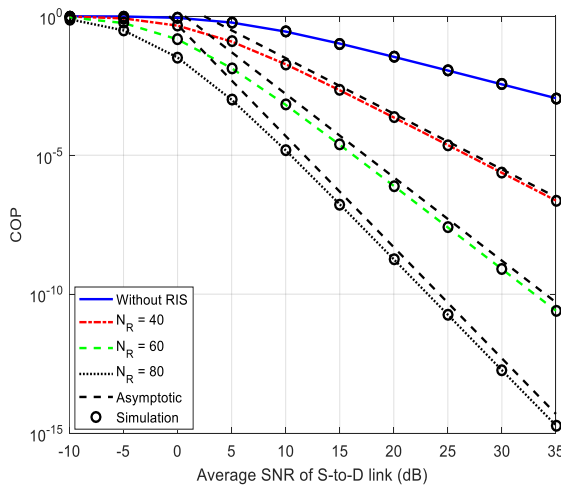


Figure 2. Impact of number of reflecting elements N_R in RIS of the system COP when $k = 8$, $\bar{\gamma}_{JE} = 15 \text{ dB}$

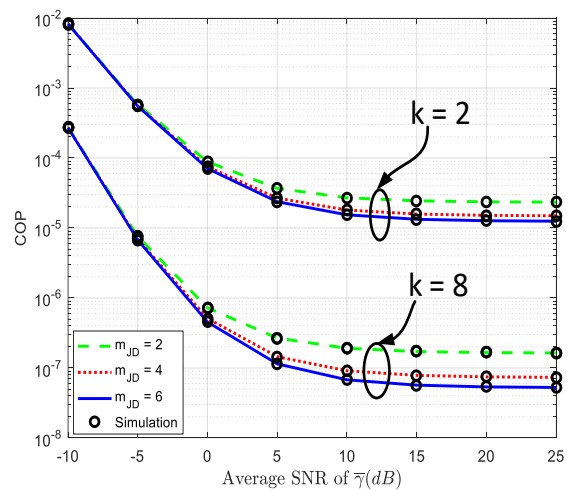


Figure 3. Influence of the k on the system COP performance under various values of m_{JD} when $N_R = 80$ and $\bar{\gamma}_{SD} = \bar{\gamma}_{JD} = \bar{\gamma}$

The performance of the system SOP under various values of m_{SE} and m_{JE} is depicted in Figure 4. The results show that the analytical results collaborate with the simulation results which validate the accuracy of the derived SOP expression. The results indicate that the system SOP yields better performance with the increase in the value of m_{JE} which shows the impact of jammer on the proposed system. Also, at a particular

value of m_{JE} , the system performance deteriorates with the increase in the values of m_{SE} due to favorable channel condition for the eavesdropper to overhead the source information.

In Figure 5, the results of the ST performance of the concerned system under various values of number of reflecting elements N_R and concentration parameter k of von Mises distribution is demonstrated. The results illustrate the increase in the RIS reflecting elements N_R leads to better system ST performance. In addition, it can be notice from the results that the increase in k parameter enhances the system ST performance with better phase errors. Also, it can be seen from the results that the analytical results perfectly match the simulation results.

The effect of m_{SE} and m_{JE} fading parameters on the system ST performance is presented in Figure 6. The results demonstrates that the system ST performance deteriorate with the increase in m_{SE} parameter of the S-to-E link due to good quality channel for the eavesdropper to overhear the source information. Also, the results clearly show that the system ST performance becomes better as the m_{JE} fading parameters of the J-to-E link due to good channel link for the jammer signal to confuse the eavesdropper.

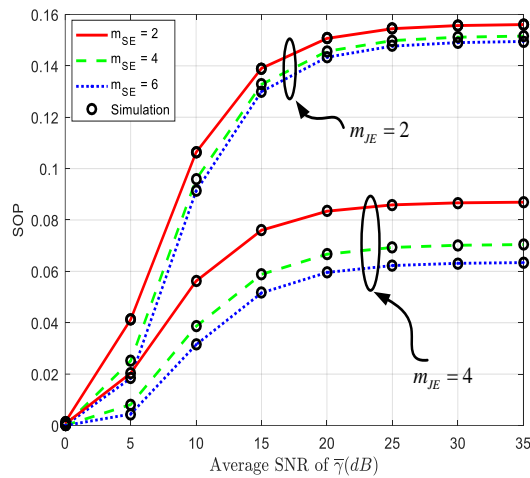


Figure 4. Impact of m_{SE} fading parameter on the system SOP performance at different values of m_{JE}

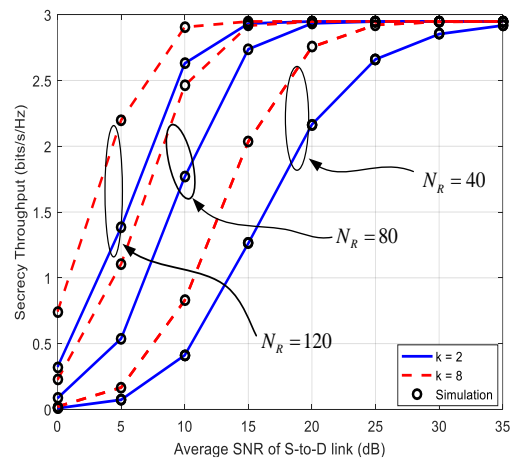


Figure 5. ST performance of the system under various values of k and N_R when $\bar{\gamma}_{JE} = 15 \text{ dB}$, $\bar{\gamma}_{JD} = 25 \text{ dB}$ and $\bar{\gamma}_{SE} = 10 \text{ dB}$

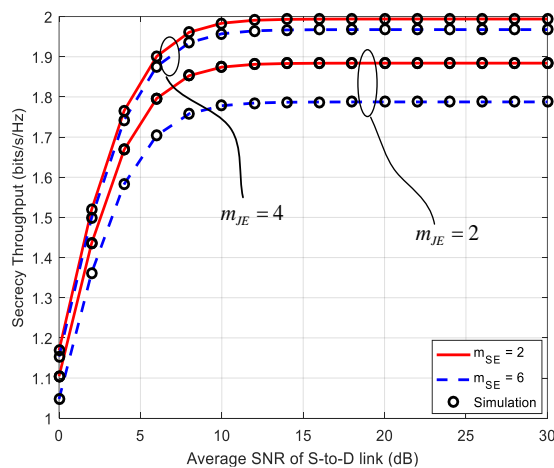


Figure 6. Effect of m_{SE} on the system ST performance under various values of m_{JE} when $\bar{\gamma}_{JE} = 15 \text{ dB}$, $\bar{\gamma}_{JD} = 15 \text{ dB}$, and $\bar{\gamma}_{SE} = 10 \text{ dB}$

5. CONCLUSION

This paper investigates the physical layer security performance of a RIS empowered wireless network in the presence of a passive eavesdropper. The exact closed-form expressions of the system secrecy

relative to COP, SOP, and ST are derived. The accuracy of the derived expressions is validated by Monte-Carlo simulations. To achieve better understanding of the system performance, the asymptotic expression of the system COP is obtained. This is consistent with the analytical results over the high signal-to-noise ratio. The results show that increasing the number of reflective elements in RIS and the concentration parameter k of the von Mises distribution significantly improves the performance of the system. The system security performance becomes deteriorates with the increase in eavesdropper m fading parameter. This is minimised with the increase in the value of m fading parameter on the jammer link which demonstrate the important of cooperative jammer for the proposed system.




REFERENCES

- [1] J. Chen, Y. -C. Liang, Y. Pei and H. Guo, "Intelligent reflecting surface: a programmable wireless environment for physical layer security," in *IEEE Access*, vol. 7, pp. 82599-82612, 2019, doi: 10.1109/ACCESS.2019.2924034..
- [2] M. Al-Jarrah, A. Al-Dweik, E. Alsusa, Y. Iraqi, and M.-S. Alouini, "On the performance of IRS-assisted multi-layer UAV communications with imperfect phase compensation," in *IEEE Transactions on Communications*, vol. 69, no. 12, pp. 8551-8568, Dec. 2021, doi: 10.1109/TCOMM.2021.3113008.
- [3] 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," in *IEEE Access*, vol. 10, pp. 14857-14869, 2022, doi: 10.1109/ACCESS.2022.3146885.
- [4] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications," in *IEEE Communications Letters*, vol. 23, no. 9, pp. 1488-1492, Sep. 2019, doi: 10.1109/LCOMM.2019.2924214.
- [5] F. A. P. de Figueiredo *et al.*, "Large intelligent surfaces with discrete set of phase-shifts communicating through double-Rayleigh Fading channels," in *IEEE Access*, vol. 9, pp. 20768-20787, 2021, doi: 10.1109/ACCESS.2021.3053773.
- [6] I. Trigui, W. Ajib, W. -P. Zhu, and M. D. Renzo, "Performance evaluation and diversity analysis of RIS-assisted communications over generalized fading channels in the presence of phase noise," in *IEEE Open Journal of the Communications Society*, vol. 3, pp. 593-607, 2022, doi: 10.1109/OJCOMS.2022.3160722.
- [7] L. Yang, F. Meng, J. Zhang, M. O. Hasna, and M. D. Renzo, "On the performance of RIS-assisted dual-hop UAV communication systems," in *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 10385-10390, Sep. 2020, doi: 10.1109/TVT.2020.3004598.
- [8] K. O. Odeyemi, P. A. Owolawi, and O. O. Olakanmi, "On the performance of reconfigurable intelligent surface aided power line communication system under different relay transmission protocols," *Progress In Electromagnetics Research C*, vol. 111, pp. 119-133, 2021, doi: 10.2528/PIERC21020803.
- [9] K. Odeyemi, P. Owolawi, and O. Olakanmi, "Reconfigurable intelligent surface in wireless-powered interference-limited communication networks," *Symmetry*, vol. 13, no. 6, p. 960, May 2021, doi: 10.3390/sym13060960.
- [10] K. O. Odeyemi, P. A. Owolawi, and O. O. Olakanmi, "Performance analysis of reconfigurable intelligent surface assisted underwater optical communication system," *Progress In Electromagnetics Research M*, vol. 98, pp. 101-111, Nov. 2020, doi: 10.2528/PIERM20101203.
- [11] G. D. Verma, A. Mathur, Y. Ai, and M. Cheffena, "Mixed dual-hop IRS-assisted FSO-RF communication system with H-ARQ protocols," in *IEEE Communications Letters*, vol. 26, no. 2, pp. 384-388, Feb. 2022, doi: 10.1109/LCOMM.2021.3129594.
- [12] X. Tang, Y. Cai, Y. Deng, Y. Huang, W. Yang, and W. Yang, "Energy-constrained SWIPT networks: enhancing physical layer security with FD self-jamming," in *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 212-222, Jan. 2019, doi: 10.1109/TIFS.2018.2848630.
- [13] 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," in *IEEE Access*, vol. 9, pp. 34708-34721, 2021, doi: 10.1109/ACCESS.2021.3058734.
- [14] X. Li, H.-N. Dai, M. K. Shukla, D. Li, H. Xu, and M. Imran, "Friendly-jamming schemes to secure ultra-reliable and low-latency communications in 5G and beyond communications," *Computer Standards & Interfaces*, vol. 78, p. 103540, Oct. 2021, doi: 10.1016/j.csi.2021.103540.
- [15] R. Ma, S. Yang, M. Du, H. Wu, and J. Ou, "Improving physical layer security jointly using full-duplex jamming receiver and multi-antenna jammer in wireless networks," *IET Communications*, vol. 13, no. 10, pp. 1530-1536, Jun. 2019, doi: 10.1049/iet-com.2018.5502.
- [16] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," in *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410-1414, Oct. 2019, doi: 10.1109/LWC.2019.2919685.
- [17] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, "Robust and secure wireless communications via intelligent reflecting surfaces," in *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 11, pp. 2637-2652, Nov. 2020, doi: 10.1109/JSAC.2020.3007043.
- [18] 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, Jan. 2022, doi: 10.1016/j.future.2021.08.012.
- [19] M. Wijewardena, T. Samarasinghe, K. T. Hemachandra, S. Atapattu, and J. S. Evans, "Physical layer security for intelligent reflecting surface assisted two-way communications," in *IEEE Communications Letters*, vol. 25, no. 7, pp. 2156-2160, Jul. 2021, doi: 10.1109/LCOMM.2021.3068102.
- [20] 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," in *IEEE Access*, vol. 9, pp. 42583-42592, 2021, doi: 10.1109/ACCESS.2021.3065760.
- [21] J. D. V. Sánchez, P. Ramírez-Espinosa, and F. J. López-Martínez, "Physical layer security of large reflecting surface aided communications with phase errors," in *IEEE Wireless Communications Letters*, vol. 10, no. 2, pp. 325-329, Feb. 2021, doi: 10.1109/LWC.2020.3029816.
- [22] M. -A. Badiu and J. P. Coon, "Communication through a large reflecting surface with phase errors," in *IEEE Wireless Communications Letters*, vol. 9, no. 2, pp. 184-188, Feb. 2020, doi: 10.1109/LWC.2019.2947445.
- [23] I. S. Gradshteyn, I. M. Ryzhik, and R. H. Romer, "Tables of integrals, series, and products," ed: American Association of Physics Teachers, 1988.




- [24] 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," in *IEEE Access*, vol. 8, pp. 188526-188537, 2020, doi: 10.1109/ACCESS.2020.3032139.
- [25] 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*, vol. 2021, Apr. 2021, doi: 10.1155/2021/5599334.
- [26] 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, Oct. 2021, doi: 10.1002/ett.4372.
- [27] R. Ma, H. Wu, J. Ou, S. Yang and Y. Gao, "Power splitting-based SWIPT systems with full-duplex jamming," in *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9822-9836, Sep. 2020, doi: 10.1109/TVT.2020.3002976.

BIOGRAPHIES OF AUTHORS






Kehinde Oluwasesan Odeyemi    received his B.Tech. degree in Electronic Engineering from Ladoke Akintola University of Technology Ogbomosho, Oyo State, Nigeria, in 2008. He later obtained an M.Eng. degree in the same field from the Federal University of Technology, Akure in 2012. In 2018, he received his Ph.D. degree in Electronic Engineering from the University of KwaZulu-Natal, Durban, South Africa. Currently, he is in the Department of Electrical and Electronic Engineering, University of Ibadan, Nigeria as a senior lecturer. He is a member of The Council for the Regulation of Engineering in Nigeria (COREN). He has written several research articles and served on the Technical Program Committee of several major IEEE conferences. His research interests are in the antenna design, optical wireless communication, MIMO communication, cooperative communication, physical layer security cognitive radio, unmanned aerial vehicles, and NOMA systems. He can be contacted at email: kesonics@yahoo.com.



Pius Adewale Owolawi    received his B.Tech. degree in Physics/Electronics from the Federal University of Technology, Akure, in 2001. He then obtained an M.Sc. and Ph.D. degrees in Electronic Engineering from the University of KwaZulu-Natal in 2006 and 2010, respectively. He holds several industry certifications such as CCNA, CCNP, CWNP, CFOA, CFOS/D, and MCITP. Member of several professional bodies like SAIEE, IEEE, and SA AMSAT. In 2007, he joined the Department of Electrical Engineering, Faculty of the Engineering, Mangosuthu University of Technology, South Africa. Thereafter, in 2017, he joined the Department of Computer Systems Engineering, Tshwane University of Technology, Pretoria, South Africa where is currently the acting head of department. His research interests are in the computational of electromagnetic, modeling of radio wave propagation at high frequency, fiber optic communication, radio planning and optimization techniques, and renewable energy. He has written several research articles and serves as a reviewer for many scientific journals. He can be contacted at email: p.owolawi@gmail.com.



Olakanmi Oladayo Olufemi    received his B.Tech. in Computer Engineering from Ladoke Akintola University of Technology, Nigeria in 2001 and M.Sc. in Computer Science from the University of Ibadan, Nigeria in 2006. He received Ph.D. degree in Electrical and Electronic Engineering from University of Ibadan, Nigeria in 2014. Currently, he is senior lecturer in the Department of Electrical and Electronic Engineering, University of Ibadan, Nigeria. A research fellow in Massachusetts Institute of Technology, USA. His research interests include security and privacy, and embedded systems. He can be contacted at email: olard4u@yahoo.com.