On Secrecy Performance of Mixed RF-FSO Systems With a Wireless-Powered Friendly Jammer

Yi Wang, Yang Tong, and Zhiwu Zhan

***Abstract*—This paper presents a study of the physical layer security performance of a mixed radio frequency-free space optical (RF-FSO) system with a wireless-powered friendly jammer. The RF links undergo the Nakagami-m fading, and the FSO link experiences the Exponentiated Weibull (EW) distribution. A two-hop decode-and-forward (DF) relay is present in the system. A single-antenna eavesdropper located on the RF link attempts to eavesdrop on the channel transmission information. There is a nearby multi-antenna jammer that can be charged wirelessly, and a save-then-transmit (ST) protocol is introduced in the jammer. The closed expressions for the secrecy outage probability (SOP) and the average secrecy capacity (ASC) of the mixed RF-FSO system are derived, and the correctness of the expressions is verified using the Monte-Carlo method. The influence of various key factors on the secrecy performance of the system is analyzed by simulations. The results show that increasing the average interference noise ratio, the number of interferer antennas, the time block allocation factor, and the size of the receiving aperture has a significant effect on the secrecy performance. This study provides a new system structure and a good theoretical basis for evaluating the physical layer security performance of mixed RF-FSO systems.**

***Index Terms*—RF/FSO, physical layer security, wireless powered jammer, save-then-transmit protocol.**

I. Introduction

THE rapid development of wireless communication is leading to an accelerated growth in the demand for wireless communication equipment. Consequently, the problem of spectrum scarcity is getting more and more attention. Compared to radio frequency (RF), free-space optical (FSO) communication also known as the atmospheric optical communication [1] is highly directional and secure, free from interference caused by frequencies and adjacent bands, and has the advantages of free licenses, low cost and high bandwidth. However, it is susceptible to pointing errors and various environmental factors, and is not suitable for long-distance communication [2], [3].

Manuscript received December 7, 2021; revised January 16, 2022; accepted January 20, 2022. Date of publication January 25, 2022; date of current version February 21, 2022. This work was supported in part by the National Natural Science Foundation of China under Grant 51704267, and in part by the Research Fund of State Key Laboratory of Coal Resources and Safe Mining, CUMT under Grant SKLCRSM21KF010. *(Corresponding author: Yi Wang.)*

The authors are with the Key Laboratory of Electromagnetic Wave Information Technology and Metrology of Zhejiang Province, College of Information Engineering, China Jiliang University, Hangzhou 310018, China, and also with the State Key Laboratory of Coal Resources and Safe Mining, China University of Mining and Technology, Xuzhou 221116, China (e-mail: wcy16@cjlu.edu.cn; tongyang199701@163.com; 1623893004@qq.com).

Digital Object Identifier 10.1109/JPHOT.2022.3146019

Mixed radio frequency-free space optical (RF-FSO) systems have been proposed in search of complementarity. The corresponding advantages of high capacity, scalability and low cost have attracted strong academic interest, and these systems are considered to provide a communication model with a wide range of prospects [4], [5]. Considering the broadcast nature of the wireless RF channel in mixed systems, the secrecy performance of the system is at risk in the presence of malicious eavesdroppers. Thus, it is becoming increasingly important to ensure the secure transmission of the confidential information. The physical layer security of mixed RF-FSO systems has started to receive a significant amount of attention because the security at this layer does not rely on any encryption algorithm, has low complexity, and only needs to exploit the physical characteristics of the wireless channel to achieve perfect confidential communication.

So far, the RF-FSO systems have been studied considering the impact of single-input multiple-output (SIMO), multiple-input multiple-output (MIMO) and transmit antenna selection (TAS) schemes, and simultaneous wireless information and power transfer (SWIPT) techniques on the physical layer security of mixed systems under different channels, respectively. El-Malek *et al.* first analyzed the security reliability tradeoff (SRT) of a mixed RF-FSO system with a mixed multi-user opportunistic user scheduling scheme. The authors derived a closed expression for the interception probability (IP) to describe the system's secrecy performance [6]. Lei *et al.* derived secrecy outage probability (SOP) and average secrecy capacity (ASC) under fixed-gain relaying and variable-gain relaying. The authors considered the effect of pointing error and two detection techniques, and analyzed the secrecy performance of the system under the assumption that the RF link suffered from the Nakagami-m fading and the FSO link experienced the Gamma-Gamma fading [7].

Yang *et al.* derived the SOP and ASC considering the RF and FSO links to be experiencing the η-μ and M-distributed fading [8]. In [9], the author proposed a mixed SIMO SWIPT RF and FSO fixed-gain relaying system, analyzed the security issues in the case of an energy harvester acting as an eavesdropper, and derived the SOP and ASC. Odeyemi *et al.* proposed a cognitive-based mixed system where the RF links suffered from the Rayleigh fading and the FSO link experienced the Gamma-Gamma fading, and derived the SOP and ASC [10].

All the aforementioned techniques increase the information transmission rate from the sender to the legitimate receiver. In this paper, we consider reducing the eavesdropping rate on the

receiver in the physical layer security transmission techniques. Therefore, we propose to introduce a wireless powered jammer with the save-then-transmit (ST) protocol in the mixed RF-FSO system to jam the potential eavesdropper.

- To the best of our knowledge, there is no existing literature that uses wireless powered jammers with the ST protocol for mixed RF-FSO systems secure communication and analyzes the secrecy performance of mixed RF-FSO systems. The main contributions of this paper are:
- We consider reducing the eavesdropping rate on the receiver in the physical layer security transmission techniques. The RF link is based on the adoption of the SIMO structure, introduce a jammer in the mixed RF-FSO system to jam the potential eavesdropper. The interference signal is transmitted into the zero space of the communication channel, eliminating the interference generated by the interferer to the signal received at the relay node. The cumulative distribution function (CDF) and the probability density function (PDF) of the signal-interference noise ratio (SINR) of the eavesdropper under the action of the interfering signal are derived.
- We introduce an energy harvesting solution of SWIPT to the jammer, overcoming the limitations of limited energy of communication nodes and the connection of power lines. A time protocol is considered in the transmission process, the energy harvesting and transmission process of the jammer becomes more controllable and stable.
- This paper presents a study of the physical layer secrecy performance of a mixed RF-FSO system in the presence of an eavesdropper and under the influence of a wireless-powered friendly jammer with ST protocol. The effects of the average interference noise ratio, the number of interferer antennas, the time block allocation factor, and the size of the receiving aperture at the destination end on the secrecy performance are analyzed by simulations. The uniform CDF of the end-to-end signal-to-noise ratio (SNR) of the SIMO communication system under the DF relay scheme is obtained, the analytical expressions for the system SOP and the ASC are further derived using the CDF and based on the Meijer-G function and the generalized Gauss-Laguerre formula. The accuracy of the expression is verified using the Monte-Carlo methods.

II. System Model

As shown in Fig. 1, we consider a mixed RF-FSO system in the presence of eavesdroppers. The system is based on the SIMO architecture under the influence of a wireless-powered friendly jammer with the ST protocol. The system consists of an RF source (S) with a single antenna, a DF relay (R) with N_R receptions and a single transmission, and a target node (D) with a single reception. The RF link in the S-R segment and the FSO link in the R-D segment experience the Nakagami-m fading distribution and EW distribution, respectively. A single-antenna eavesdropper (E) attempting to eavesdrop on channel transmissions is located on the RF link, and a jammer that can be wirelessly powered with N_J antennas is present nearby.

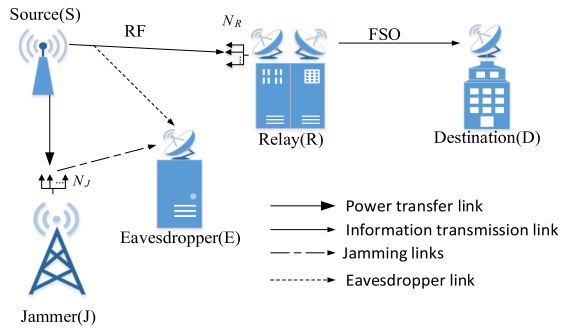

Fig. 1. Mixed RF-FSO system with a Wireless-Powered Friendly Jammer.

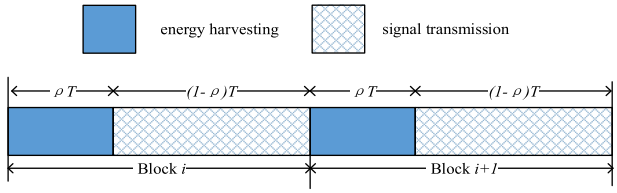

Fig. 2. ST Protocol.

The secure communication with wireless-powered jammer takes places in two phases: the energy harvesting phase and the information transfer phase. During the energy harvesting phase, the source node S sends a radio signal to the jammer. The jammer receives the radio signal, converts it to a direct current signal and stores the energy in its battery. During the information transfer phase, the jammer sends jamming signal to the eavesdropper by using the stored energy in the battery. At the same time, the source node S transmits the information signal to the relay node under the protection of the jamming signal, the relay node employed subcarrier intensity modulation (SIM) technique to convert RF signal to optical signal and transmits it to the legitimate destination.

The ST protocol [11] shown in Fig. 2 is used to design the total time block T for energy harvesting and transmitting interference signals. The jammer uses the time ρT to acquire energy from the transmitter and save it. The remaining time is used by the jammer to transmit a jamming signal to the potential eavesdropper.

The source node S sends a radio signal x_{SJ} of power P_S in the energy harvesting phase, which is then transmitted to the interferer node J through the RJ channel. The signal received by the interferer node J can be expressed as

$$y_{SJ} = \frac{1}{\sqrt{d_{SJ}^{\tau}}}\sqrt{P_S}h_{SJ}x_{SJ} + e_J \tag{1}$$

Where P_S is the transmitting power at the transmitter, x_{SJ} is the normalized signal of the source node, h_{SJ} is the channel coefficient between the source node S and the interferer node, d_{SJ}represents the distance from S to J, τ is the path loss exponent, and e_J denotes additive Gaussian white noise with zero mean and variance σ_J^2 at the interferer. Using (1) and ignoring the noise power, the harvested energy is given by [12]

$$\omega_J(h_{SJ}) = \rho\eta\left|\frac{1}{\sqrt{d_{SJ}^{\tau}}}\sqrt{P_J}h_{SJ}\right|^2 T \tag{2}$$

where η is the energy conversion efficiency of the jammer to convert the RF signal to direct current (DC).

In the signal transmission phase, the jammer has enough power to send interfering signals to the eavesdropper. The transmission power P_J satisfies

$$P_J(1-\rho)T \le \omega_J \tag{3}$$

Once the battery of the jammer accumulates energy in the charging stage, the interference signal will have a certain interference effect on the relay node for a single antenna jammer. For a multi-antenna jammer, it can be gathered using the artificial interference generation method in [13] that the jammer generates an $N_J \times (N_J-1)$ matrix W, which is an orthonormal basis of the null space of h_{JR}. It also generates a vector v with N_J-1 independent identically distributed complex Gaussian random elements with a normalized variance. Subsequently, the jammer sends Wv as the jamming signal. The signal received by the relay node R at this time can be expressed as

$$y_{SR} = \begin{cases} \frac{\sqrt{\mathrm{P}_S}}{\sqrt{d_{SR}^{\tau}}} h_{SR} x_{\mathrm{SR}} + \frac{\sqrt{\mathrm{P}_J}}{\sqrt{d_{JR}^{\tau}}} h_{JR} x_{JR} + e_R, & N_J = 1 \\ \frac{\sqrt{\mathrm{P}_S}}{\sqrt{d_{SR}^{\tau}}} h_{SR} x_{SR} + e_R, & N_J > 1 \end{cases} \tag{4}$$

where x_{SR} is the normalized signal transmitted by the source node S, h_{SR} is the channel coefficient between the source node S and the relay node, and e_R denotes additive Gaussian white noise with zero mean and variance σ_R^2 at the relay. When $N_J > 1$, the signal received at the relay is unaffected by the interference signal because it is transmitted into the zero space of h_{JR}. Based on the above analysis, the next cases consider the number of interferer antennas as $N_J > 1$.

The signal received at the eavesdropper under the action of the jammer can be expressed as follows:

$$y_{SE} = \frac{\sqrt{\mathrm{P}_S}}{\sqrt{d_{SE}^{\tau}}} h_{\mathrm{SE}} x_{\mathrm{SR}} + \frac{\sqrt{\mathrm{P}_J}}{\sqrt{d_{JE}^{\tau}}} h_{\mathrm{JE}} \frac{\mathbf{Wv}}{\sqrt{N_J - 1}} + e_E \tag{5}$$

A. RF Channel Model

The interference signal sent by the jammer will only affect the eavesdropper. The SINR at the eavesdropper can be obtained as

$$\gamma_{SJE} = \frac{\gamma_{SE}}{\gamma_{JE}+1} = \frac{\frac{P_S}{d_{SE}^{\tau}} |h_{SE}|^2}{\frac{P_J \|h_{JE}\mathbf{W}\|^2}{d_{JE}^{\tau}(N_J-1)} + 1} \tag{6}$$

All RF links suffer from the Nakagami-m fading, which is a more general channel fading that matches well with test results in many practical wireless environment tests. The PDF and CDF of the instantaneous SNR γ_k of the RF links are

$$f_{\gamma_k}(\gamma) = \frac{1}{\Gamma(m_k N_k)} \left(\frac{m_k}{\Omega_k}\right)^{m_k N_k} \gamma_k^{m_k N_k - 1} \exp\left(-\frac{m_k}{\Omega_k}\gamma_k\right) \tag{7}$$

$$F_{\gamma_k}(\gamma) = 1 - \exp\left(-\frac{m_k}{\Omega_k}\gamma_k\right) \sum_{t=0}^{m_k N_k - 1} \frac{1}{t!} \left(\frac{m_k}{\Omega_k}\gamma_k\right)^t \tag{8}$$

$k \in \{SR, SE, JE\}$, where $\gamma_{JE} = \frac{\rho\eta P_S |h_{SJ}|^2 \|h_{JE}W\|^2}{(1-\rho)\sigma_E^2 (N_J-1) d_{SJ}^{\tau} d_{JE}^{\tau}}$, $\gamma_{SE} = \frac{P_S}{\sigma_E^2 d_{SE}^{\tau}} |h_{SE}|^2$, $\Omega_{SR} = \frac{P_S \lambda_{SR}}{\sigma_R^2 d_{SJ}^{\tau}}$, $\Omega_{SE} = \frac{P_S \lambda_{SE}}{\sigma_E^2 d_{SE}^{\tau}}$, $\Omega_{JE} = \psi \frac{\lambda_{JE}}{d_{JE}^{\tau}}$, λ_k is the average power channel gains between the respective channels, and $\psi = \frac{\rho\eta P_S N_J}{(1-\rho)\sigma_E^2 d_{SJ}^{\tau}}$.

Considering the fading of J-E link is obvious since there is no line of sight (NLOS). In the calculations, consider $m_{JE} = 1$. Using (6), (7) and (8), the CDF of the instantaneous SNR was obtained as follows using the method provided in [14]:

$$\begin{aligned} F_{\gamma_{SJE}}(\gamma) = 1 - & \sum_{t=0}^{m_{SE}-1} \frac{1}{t!} \left[\frac{m_{SE}}{\Omega_{SE}(N_J-1)}\right]^t \frac{1}{\Gamma(N_J-1)} \sum_{k=0}^{t} \\ & \times \binom{t}{k} {\Omega_{JE}}^k \gamma^t \times \exp\left[-\frac{m_{SE}}{\Omega_{SE}(N_J-1)}\gamma\right] \\ & \times G_{1,1}^{1,1}\left[\frac{m_{SE}\Omega_{JE}}{\Omega_{SE}(N_J-1)}\gamma \,\middle|\, \begin{matrix} -k-N_J+2 \\ 0 \end{matrix}\right] \end{aligned} \tag{9}$$

Taking the derivative of the CDF given in (9) provides the corresponding PDF as

$$\begin{aligned} f_{\gamma_{SJE}}(\gamma) = & \frac{1}{\Gamma(m_{SE})\Gamma(N_J-1)} \left[\frac{m_{SE}}{\Omega_{SE}(N_J-1)}\right]^{m_{SE}} \sum_{k=0}^{m_{SE}} \\ & \times \binom{m_{SE}}{k} \Omega_{JE}^k \gamma^{m_{SE}-1} \times \exp\left[-\frac{m_{SE}}{\Omega_{SE}(N_J-1)}\gamma\right] \\ & \times G_{1,1}^{1,1}\left[\frac{m_{SE}\Omega_{JE}}{\Omega_{SE}(N_J-1)}\gamma \,\middle|\, \begin{matrix} -k-N_J+2 \\ 0 \end{matrix}\right] \end{aligned} \tag{10}$$

B. FSO Channel Model

The Exponentiated Weibull (EW) distribution is suitable for all turbulent situations and effectively models the data and experiments even in the presence of aperture smoothing effects. The expressions for the PDF and CDF of the EW distribution channel are [15]

$$\begin{aligned} f_{\gamma_{RD}}(\gamma) = & \frac{\alpha\beta}{\eta} \left(\frac{1}{\eta}\sqrt{\frac{\gamma}{\mu_r}}\right)^{\beta-1} \exp[-\left(\frac{1}{\eta}\sqrt{\frac{\gamma}{\mu_r}}\right)^{\beta}] \\ & \times \left\{1 - \exp\left[-\left(\frac{1}{\eta}\sqrt{\frac{\gamma}{\mu_r}}\right)^{\beta}\right]\right\}^{\alpha-1} \end{aligned} \tag{11}$$

$$F_{\gamma_{RD}}(\gamma) = \left\{1 - \exp\left[-\left(\frac{1}{\eta}\sqrt{\frac{\gamma}{\mu_r}}\right)^{\beta}\right]\right\}^{\alpha} \tag{12}$$

where $\alpha \approx 3.931(\frac{\mathrm{D}}{\rho_0})^{-0.519}$, $\beta \approx (\alpha\sigma_{\mathrm{I}}^2)^{-6/11}$ are the shape parameters related to the flicker index. Where D is the receiving aperture diameter, and $\rho_0 = (1.46 C_n^2 k^2 \mathrm{L_{RD}})^{-3/5}$ is the atmospheric coherence radius, L_{RD} is the transmission distance of the FSO link, $\mathrm{k} = 2\pi/\lambda$ is the wavenumber with λ being the optical wavelength, the σ_{I}^2 is the scintillation index, and C_n^2 is the atmospheric refractive index structure constant. $\eta = \frac{1}{\alpha\Gamma(1+1/\beta)\mathrm{g}(\alpha,\beta)}$ is a scale parameter, which

is related to the mean value of irradiance, where $\mathrm{g}(\alpha,\beta) = \sum_{\mathrm{i}=0}^{\infty} \frac{(-1)^{\mathrm{i}}(\mathrm{i}+1)^{-(1+\beta)/\beta}\Gamma(\alpha)}{\mathrm{i}!\Gamma(\alpha-\mathrm{i})}$.

III. End-to-End SNR Statistics

Under the DF relay, the end-to-end instantaneous SNR is expressed as follows:

$$\gamma_{\mathrm{SRD}} = \frac{\gamma_{SR}\gamma_{RD}}{\gamma_{SR}+\gamma_{RD}+1} \cong \min(\gamma_{SR},\gamma_{RD}) \tag{13}$$

The end-to-end CDF of the joint channel is

$$\begin{aligned} F_{\gamma_{SRD}}(\gamma) &= P_r[\min(\gamma_{SR},\gamma_{RD}) < \gamma] \\ &= F_{\gamma_{SR}}(\gamma) + F_{\gamma_{RD}}(\gamma) - F_{\gamma_{SR}}(\gamma)F_{\gamma_{RD}}(\gamma) \end{aligned} \tag{14}$$

Substituting (8) and (12) into (14) yields

$$\begin{aligned} F_{\gamma_{SRD}}(\gamma) = 1 &- \exp\left(-\frac{m_k}{\Omega_k}\gamma_k\right)\sum_{t=0}^{m_k N_k-1}\frac{1}{t!}\left(\frac{m_k}{\Omega_k}\gamma_k\right)^t \\ &+ \exp\left(-\frac{m_k}{\Omega_k}\gamma_k\right)\sum_{t=0}^{m_k N_k-1}\frac{1}{t!}\left(\frac{m_k}{\Omega_k}\gamma_k\right)^t \\ &\times\left\{1-\exp\left[-\left(\frac{1}{\eta}\sqrt{\frac{\gamma}{\mu_r}}\right)^{\beta}\right]\right\}^{\alpha} \end{aligned} \tag{15}$$

IV. Secrecy Outage Probability Analysis

When the instantaneous secrecy capacity is lower than the target secrecy rate R_S, an SOP event occurs. Therefore, the lower bound expression of the SOP for the mixed system [16]

$$P_{out}^{L}(R_s) = \int_0^{\infty} F_{SRD}(\theta\gamma) f_{SE}(\gamma_{SE}) d\gamma_{SE} \tag{16}$$

where $\theta = \exp(R_s)$. Substituting (10) and (15) into (16), the end-to-end SOP can be written as

$$P_{\gamma_{SRD}}(R_s) \triangleq G_1 - G_2 + G_3 \tag{17}$$

$$G_1 = \frac{1}{\Gamma(m_E)\Gamma(N_J-1)}\left[\frac{m_E}{\bar{\gamma}_{SE}(N_J-1)}\right]^{m_E} \times\sum_{k=0}^{m_E}\binom{m_E}{k}{\Omega_{JE}}^k\int_0^{\infty}\gamma_{SE}^{m_E-1} \times\exp\left[-\frac{m_E}{\Omega_{SE}(N_J-1)}\gamma_{SE}\right] \times G_{1,1}^{1,1}\left[\frac{m_E\Omega_{JE}}{\Omega_{SE}(N_J-1)}\gamma_{\mathrm{SE}}\middle|\begin{matrix}-k-N_J+2\\0\end{matrix}\right]d\gamma_{SE} \tag{18}$$

$$G_2 = \sum_{t=0}^{N_R m_{SR}-1}\frac{1}{t!}\left(\frac{m_{SR}\theta}{\Omega_{SR}}\right)^t\frac{1}{\Gamma(m_E)\Gamma(N_J-1)} \times\left[\frac{m_{SE}}{\Omega_{SE}(N_J-1)}\right]^{m_{SE}}\sum_{k=0}^{m_{SE}}\binom{m_{SE}}{k}{\Omega_{JE}}^k \times\int_0^{\infty}\gamma_{SE}^{t+m_E-1} \times\exp\left[-\left(\frac{m_{SR}\theta}{\Omega_{SR}}+\frac{m_{SE}}{\Omega_{SE}(N_J-1)}\right)\gamma_{SE}\right] \times G_{1,1}^{1,1}\left[\frac{m_{SE}\Omega_{JE}}{\Omega_{SE}(N_J-1)}\gamma_{\mathrm{SE}}\middle|\begin{matrix}-k-N_J+2\\0\end{matrix}\right]d\gamma_{SE} \tag{19}$$

$$G_3 = \sum_{t=0}^{N_R m_{SR}-1}\frac{1}{t!}\left(\frac{m_{SR}\theta}{\Omega_{SR}}\right)^t\frac{1}{\Gamma(m_{SE})\Gamma(N_J-1)} \times\left[\frac{m_{SE}}{\Omega_{SE}(N_J-1)}\right]^{m_{SE}}\sum_{k=0}^{m_{SE}}\binom{m_{SE}}{k}{\Omega_{JE}}^k \times\int_0^{\infty}\gamma_{SE}^{t+m_{SE}-1} \times\exp\left[-\left(\frac{m_{SR}\theta}{\Omega_{SR}}+\frac{m_{SE}}{\Omega_{SE}(N_J-1)}\right)\gamma_{SE}\right] \times G_{1,1}^{1,1}\left[\frac{m_{SE}\Omega_{JE}}{\Omega_{SE}(N_J-1)}\gamma_{\mathrm{SE}}\middle|\begin{matrix}-k-N_J+2\\0\end{matrix}\right] \times\left\{1-\exp\left[-\left(\frac{1}{\eta}\sqrt{\frac{\theta\gamma_{SE}}{\mu_r}}\right)^{\beta}\right]\right\}^{\alpha}d\gamma_{SE} \tag{20}$$

$$\begin{aligned} P_{\gamma_{\mathrm{SRD}}}(R_s) = {} & \frac{1}{\Gamma(m_{SE})\Gamma(N_J-1)}\sum_{k=0}^{m_{SE}}\binom{m_{SE}}{k}{\Omega_{JE}}^k \times G_{2,1}^{1,2}\left[\Omega_{JE}\middle|\begin{matrix}-k-N_J+2,1-m_{\mathrm{SE}}\\0\end{matrix}\right] - \sum_{t=0}^{N_S m_{SR}-1}\frac{1}{t!}\left(\frac{m_{SR}\theta}{\Omega_{SR}}\right)^t \\ & \times\frac{1}{\Gamma(m_{SE})\Gamma(N_J-1)}\left[\frac{m_{SE}}{\Omega_{SE}(N_J-1)}\right]^{m_{SE}}\sum_{k=0}^{m_{SE}}\binom{m_{SE}}{k}{\Omega_{JE}}^k \\ & \times\left(\begin{array}{l} \left[\frac{m_{\mathrm{SR}}\theta(N_J-1)\Omega_{SE}+m_{\mathrm{SE}}\Omega_{SR}}{\Omega_{SE}\Omega_{SR}(N_J-1)}\right]^{-m_{SE}-t} \\ \times G_{2,1}^{1,2}\left[\frac{\Omega_{SE}\Omega_{SR}m_{SE}}{m_{SR}\theta(N_J-1)\Omega_{SE}+m_{SE}\Omega_{SR}}\middle|\begin{matrix}-k-N_J+2,1-m_{\mathrm{SE}}\\0\end{matrix}\right] \\ -\sum_{j=1}^{t}H_j\gamma_j^{t+m_{SE}-0.5}\exp\left[-\left(\frac{m_{SR}\theta}{\Omega_{SR}}+\frac{m_{SE}}{\Omega_{SE}(N_J-1)}-1\right)\gamma_j\right] \\ \times G_{1,1}^{1,1}\left[\frac{m_{SE}\Omega_{JE}}{\Omega_{SE}(N_J-1)}\gamma_{\mathrm{j}}\middle|\begin{matrix}-k-N_J+2\\0\end{matrix}\right]\left\{1-\exp\left[-\left(\frac{1}{\eta}\sqrt{\frac{\theta\gamma_j}{\mu_r}}\right)^{\beta}\right]\right\}^{\alpha} \end{array}\right) \end{aligned} \tag{21}$$

By applying the integral constancy equation given in [17], the exponential function is converted to Meijer-G. Subsequently, the theory given in [18] and the generalized Gauss-Laguerre formula [19] are combined. By substituting (18)-(20) into (17) and after a few mathematical simplifications using the above calculation method, the end-to-end SOP can be obtained as shown in (21) at the bottom of the previous page where $H_j = \frac{\Gamma(n+1/2)x_j}{n!(n+1)^2[L_n^{(-1/2)}(x_j)]^2}$, and x_j is the jth root of the generalized Laguerre polynomial $L_n^{(-\frac{1}{2})}(x)$.

Then, using the calculation method in [17] after a few mathematical simplifications, we can obtain the asymptotic SOP when $\bar{\gamma} \to \infty$, as shown in (22) at the bottom of the page, where $\Psi = \frac{m_{SR}\theta(N_J-1)\Omega_{SE}+m_{SE}\Omega_{SR}}{\Omega_{SE}\Omega_{SR}(N_J-1)}$, $\Phi = \prod_{m=1,m\neq h}^{2}\Gamma(K_{1,h}-K_{1,m})\prod_{m=1}^{2}\Gamma(1+K_{2,m}-K_{1,h})$, $K_1 = -k-N_J+21-m_{SE}$, $K_2 = 0$.

V. Average Secrecy Capacity Analysis

The ASC is an important indicator for assessing the secrecy performance of active eavesdropping. It can be expressed as follows

$$\bar{C}_S = \int_0^\infty \frac{F_{SE}(\gamma)}{1+\gamma}\left(1-F_{eq}(\gamma)\right)d\gamma_{SE} \tag{23}$$

Substituting (9) and (15) into (23) and after a few mathematical simplifications mentioned above, we obtain

$$\begin{aligned}\bar{C}_S = &\sum_{p=0}^{N_S m_{SR}-1}\frac{1}{p!}\left(\frac{m_{SR}}{\Omega_{SR}}\right)^p\\ &\left(G_{1,2}^{2,1}\left[\frac{m_{SR}}{\Omega_{SR}}\middle|\begin{matrix}-p\\0,-p\end{matrix}\right]-\sum_{j=1}^{t}H_j\frac{\gamma_{\rm j}^{p+0.5}}{1+\gamma_{\rm j}}\right.\\ &\left.\times\exp\left[-\left(\frac{m_{SR}}{\Omega_{SR}}-1\right)\gamma_j\right]\left\{1-\exp\left[-\left(\frac{1}{\eta}\sqrt{\frac{\gamma_j}{\mu_r}}\right)^\beta\right]\right\}^\alpha\right)\\ &-\sum_{t=0}^{m_{SE}-1}\frac{1}{t!}\left[\frac{m_{SE}}{\Omega_{SE}(N_J-1)}\right]^t\frac{1}{\Gamma(N_J-1)}\sum_{k=0}^{t}\binom{t}{k}{\Omega_{JE}}^k\\ &\times\sum_{p=0}^{N_S m_{SR}-1}\frac{1}{p!}\left(\frac{m_{\rm SR}}{\Omega_{SR}}\right)^p\sum_{j=1}^{t}H_j\frac{\gamma_{\rm j}^{p+0.5}}{1+\gamma_{\rm j}}\\ &\times\exp\left[-\left(\frac{m_{SR}\theta}{\Omega_{SR}}+\frac{m_{SE}}{\Omega_{SE}(N_J-1)}-1\right)\gamma_j\right]\\ &\times G_{1,1}^{1,1}\left[\frac{m_{SE}\Omega_{JE}}{\Omega_{SE}(N_J-1)}\gamma_{\rm j}\middle|\begin{matrix}-k-N_J+2\\0\end{matrix}\right]\\ &\times\left(1-\left\{1-\exp\left[-\left(\frac{1}{\eta}\sqrt{\frac{\gamma_j}{\mu_r}}\right)^\beta\right]\right\}^\alpha\right)\end{aligned} \tag{24}$$

Similarly with (22), we can obtain the asymptotic ASC

$$\begin{aligned}\bar{C}_S = &\sum_{p=0}^{N_S m_{SR}-1}\frac{1}{p!}\left(\frac{m_{SR}}{\Omega_{SR}}\right)^p\sum_{h=1}^{2}\left(\frac{m_{SR}}{\Omega_{SR}}\right)^{K_{1,h}}\\ &\times\prod_{m=1,m\neq h}^{2}\Gamma(K_{2,m}-K_{2,h})\\ &\times\prod_{m=1}^{2}\Gamma(1+K_{1,h}-K_{2,m})-\sum_{t=0}^{m_{SE}-1}\frac{1}{t!}\\ &\times\left[\frac{m_{SE}}{\Omega_{SE}(N_J-1)}\right]^t\frac{1}{\Gamma(N_J-1)}\sum_{k=0}^{t}\binom{t}{k}{\Omega_{JE}}^k\\ &\times\sum_{p=0}^{N_S m_{SR}-1}\frac{1}{p!}\left(\frac{m_{\rm SR}}{\Omega_{SR}}\right)^p\sum_{j=1}^{t}H_j\frac{\gamma_{\rm j}^{p+0.5}}{1+\gamma_{\rm j}}\\ &\times\exp\left[-\left(\frac{m_{SR}\theta}{\Omega_{SR}}+\frac{m_{SE}}{\Omega_{SE}(N_J-1)}-1\right)\gamma_j\right]\\ &\times\Gamma(k+N_J-1)\left(\frac{m_{SE}\Omega_{JE}\gamma_j}{\Omega_{SE}(N_J-1)}+1\right)^{-k-N_J+1}\end{aligned} \tag{25}$$

Where $K_1 = -p, K_2 = 0, -p$.

VI. Simulation Results

In this section, the simulation results of the RF-FSO system under the influence of various parameters are described. The Monte-Carlo simulations are also carried out to verify the accuracy of the numerical results. Assume that on the RF link $d_{SJ} = d_{JE} = d_{SE} = d_{SR} = 10$ m, the FSO link distance is 1 km, the wavelength is 785 nm, the optical wavenumber $k = 2\pi/\lambda$,

$$\begin{aligned}P_{\gamma_{SRD}}(R_s) = &\frac{1}{\Gamma(m_{SE})\Gamma(N_J-1)}\sum_{k=0}^{m_{SE}}\binom{m_{SE}}{k}{\Omega_{JE}}^k\sum_{h=1}^{2}(\Omega_{JE})^{K_{1,h}}\Phi-\frac{1}{\Gamma(m_{SE})\Gamma(N_J-1)}\\ &\times\left[\frac{m_{SE}}{\Omega_{SE}(N_J-1)}\right]^{m_{SE}}\sum_{k=0}^{m_{SE}}\binom{m_{SE}}{k}{\Omega_{JE}}^k\\ &\times\left(\begin{matrix}\sum_{t=0}^{N_S m_{SR}-1}\frac{1}{t!}\left(\frac{m_{SR}\theta}{\Omega_{SR}}\right)^t\left[\frac{1}{\Psi}\right]^{-m_{SE}-t}\sum_{h=1}^{2}(\Psi)^{K_{1,h}}\Phi-\sum_{j=1}^{t}H_j\gamma_j^{m_{SE}-0.5}\\ \times\exp\left[-\left(\frac{m_{SE}}{\Omega_{SE}(N_J-1)}-1\right)\gamma_j\right]\left(\frac{m_{SE}\Omega_{JE}\gamma_j}{\Omega_{SE}(N_J-1)}+1\right)^{-k-N_J+1}\\ \times\Gamma(k+N_J-1)\left\{1-\exp\left[-\left(\frac{1}{\eta}\sqrt{\frac{\theta\gamma_j}{\mu_r}}\right)^\beta\right]\right\}^\alpha\end{matrix}\right)\end{aligned} \tag{22}$$

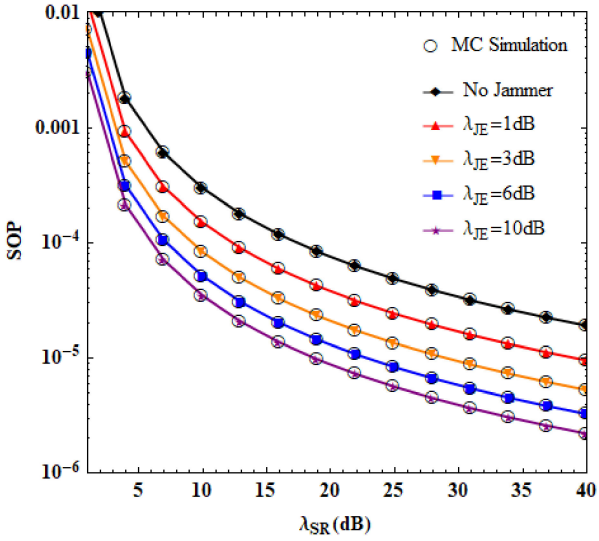

Fig. 3. Simulation diagram of the SOP with different λ_{JE} for eavesdroppers in the RF/FSO system.

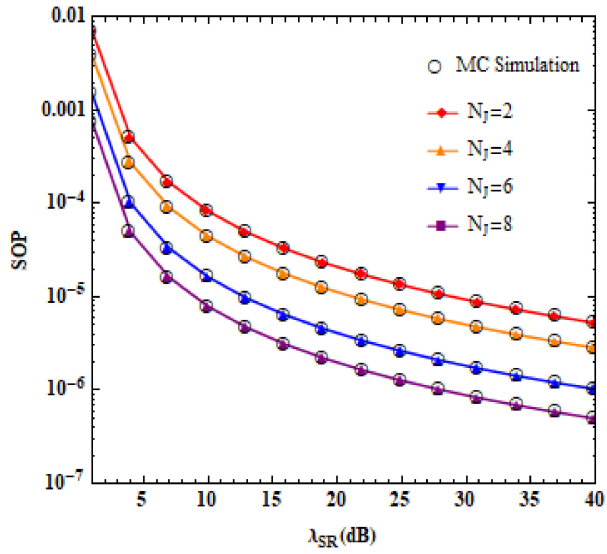

Fig. 4. Simulation diagram of the SOP with different number of antennas of the jammer in the RF/FSO system.

the refractive-index structure constant $C_n^2 = 2.1 \times 10^{-14}$, the instantaneous SNR of the FSO and eavesdropping links are $\mu_r = 20\,\text{dB}$ and $\lambda_{SE} = -10\,\text{dB}$, respectively, and the target secrecy rate $R_s = 0.01$ nat/s. When the receiving aperture $D = 10\,textmm$, the EW channel parameters under weak turbulence are respectively taken as $(\alpha, \beta, \eta) = (4.60, 1.17, 0.52)$. The other parameters are $\xi = 0.8$, $\tau = 1, \rho = 0.8$, $m_{SR} = m_{SE} = 2$, $N_J = 2$, $N_R = 1$, $\lambda_{JE} = 3\,\text{dB}$. In the following simulations, the aforementioned parameters are used unless mentioned otherwise. The value of j is set to 30 when calculating the generalized Laguerre orthogonal numerical integration method in order to make the series converge. The Monte-Carlo simulation results are provided in order to verify the validity of the analytical expressions. The numerical results agree with the simulation results, which verifies the accuracy of the proposed expression.

Fig. 3 shows the SOP of the RF-FSO system under different λ_{JE} values in the presence of the eavesdropper. When $\lambda_{SR} = 30dB$, $\lambda_{JE} = 1,\ 3,\ 6\ and\ 10dB$, the system SOP values are 1.69×10^{-5}, 9.35×10^{-6}, 5.80×10^{-6} and 3.90×10^{-6}. The system SOP is 3.38×10^{-5} in the absence of any interferer. The SOP of the system decreases significantly as λ_{JE} increases. It can be observed that the use of jammers to send jamming signals to the eavesdroppers positively affects the secrecy performance of the system. However, with the increasing of λ_{JE}, the improvement become limited. Introducing jammers and choosing reasonable transmit power can effectively improve the secrecy performance of the system.

Fig. 4 shows the SOP of the RF-FSO system with different numbers of jammer antennas. When $\lambda_{SR} = 30dB$ and the number of interferer antennas are $N_J = 2,\ 4,\ 6\ and\ 8$, the SOP values are 9.35×10^{-6}, 5.03×10^{-6}, 1.82×10^{-6} and 8.82×10^{-7}. It can be observed that the system SOP is significantly reduced by increasing the number of jammer antennas. The transmitter's power is lower under the scheme with a higher number of interferer antennas for the same value of SOP. This provides a good solution for designing the jammer equipment and reducing the consumption at the transmitter side.

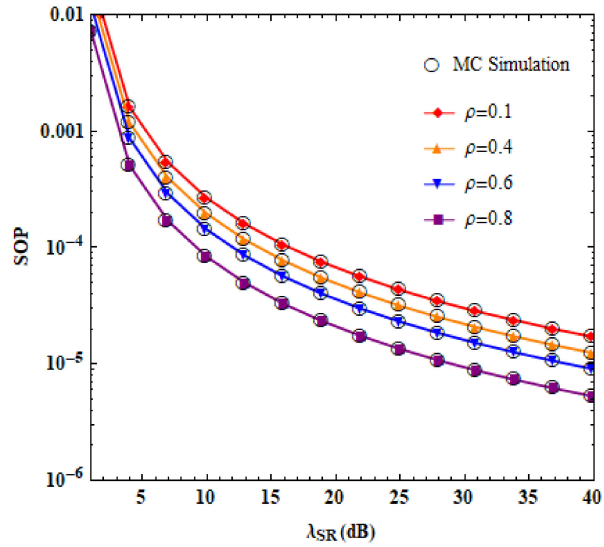

Fig. 5. Simulation diagram of the SOP under different time block allocation factors of the jammer in the RF/FSO system.

Fig. 5 shows the SOP of the RF-FSO system when the jammer uses different time block allocation factors. When $\lambda_{SR} = 30dB$, and the jammer time block allocation factors are $\rho = 0.10.4,\ 0.6\ and\ 0.8$, the SOP values are 3.01×10^{-5}, 2.20×10^{-5}, 1.60×10^{-5} and 9.35×10^{-6}. The SOP decreases and the ASC increases as the time block allocation factor increases. As ρ is monotonically related to the energy transferred to the interferer storage, we can note from the figure that the value of ρ increases. This increase represents that the longer the jammer receives the energy, the higher the amount of energy that is stored. Subsequently, a higher amount of energy is used to transmit the jamming signal in the remaining limited time, which progressively improves the jamming effect of the jammer

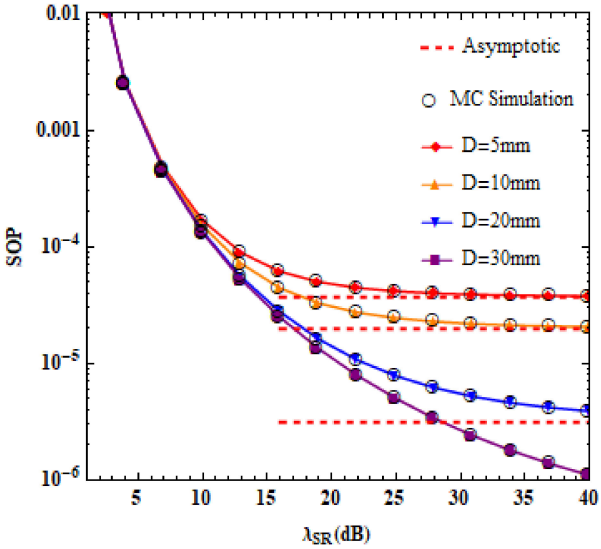

Fig. 6. Simulation diagram of the SOP with different receive aperture sizes at the destination in the RF/FSO system. ($N_R = 2, \lambda_{SE} = 0dB$).

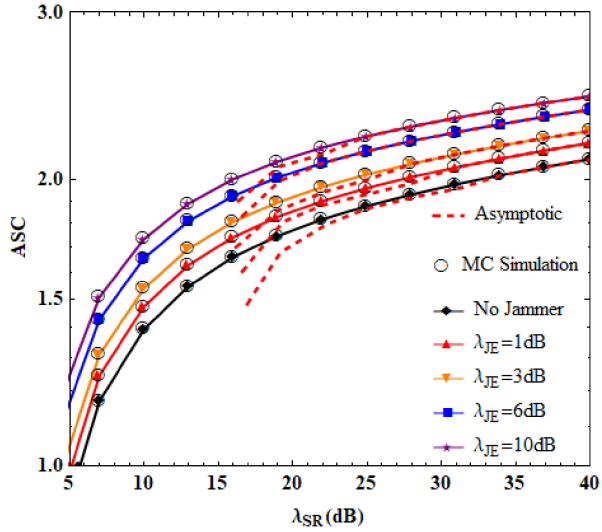

Fig. 7. Simulation diagram of the ASC under different λ_{JE} for eavesdroppers in the RF/FSO system. ($\lambda_{SE} = 0dB$).

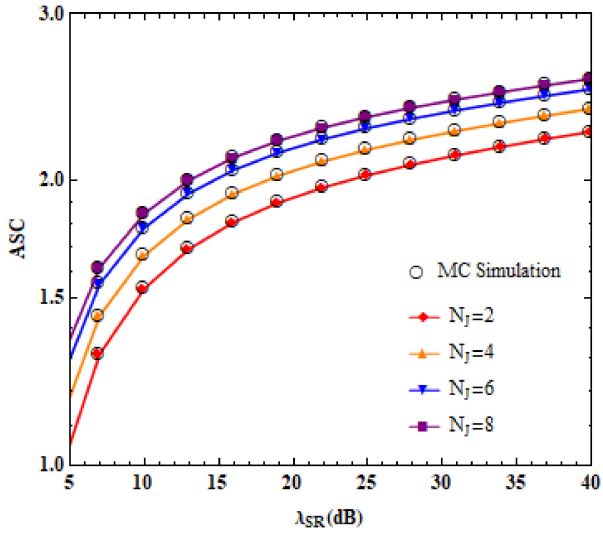

Fig. 8. Simulation diagram of the ASC under different number of antennas of the jammer in the RF/FSO system. ($\lambda_{SE} = 0dB$).

on the eavesdropper and results in a better system secrecy performance. On the contrary, the secrecy performance is relatively degraded when the value of ρ decreases. Reasonable setting of ρ according to the actual situation can effectively improve the secrecy performance. Besides, with the introduction of the ST protocol, the energy harvesting and transmission process of the jammer becomes more controllable and stable.

Fig. 6 shows the simulation of the SOP of the RF-FSO system with different receiver aperture sizes at the destination. When $\lambda_{SR} < 10dB$, the SOP hardly varies with the change in the size of the receiving aperture. On the other hand, when $\lambda_{SR} > 10dB$, the effect of the size of the receiving aperture on the SOP diverges significantly with increasing λ_{SR}. As the receiving aperture increases, the SOP is significantly reduced, and the SOP values under different receiving aperture values indicate a stable performance under a high SNR. It can be observed that increasing the size of the FSO link receiving aperture in practical applications can effectively improve the secrecy performance of the system. The large receiving aperture can increase the incident optical power and collect a higher amount of optical signal power. At this time, large receiving aperture leads to a risk of eavesdropping on the FSO link. Thus, selecting proper receiving aperture size can realize the trade-off between operating cost and secrecy performance.

Fig. 7 shows the ASC of the RF-FSO system with the eavesdropper subjected to different λ_{JE} values. When $\lambda_{SR} = 30\,\text{dB}$ and $\lambda_{JE} = 1,\ 3,\ 6$ and $10\,\text{dB}$, the ASC values are $2.05,\ 2.11,\ 2.23$ and 2.31. In the absence of a jammer action, the ASC is 1.96. It can be noted that the average confidential capacity of the system is increased to some extent with the increase of λ_{JE}. It is further shown that the transmission of a jamming signal to the eavesdropper improves the secrecy performance, and the increase of the jammer transmitting power can improve the secrecy performance.

Fig. 8 shows the ASC of the RF-FSO system for different numbers of jammer antennas. When $\lambda_{SR} = 30\,\text{dB}$, and $N_J = 2,\ 4,\ 6$ and 8, the ASC values are $2.11,\ 2.24,\ 2.36$ and 2.42. It can be observed that increasing the number of jammer antennas also allows the effective improvement of the average confidential capacity. As the number of transmitting antennas of the jammer increases, the security and confidentiality performance of the system is improved.

VII. Conclusion

In this paper, we studied the secrecy performance of the RF-FSO mixed systems under the influence of wireless powered Jammer with the ST protocol. The SOP and ASC of the system were analyzed using theoretical derivation and simulation, and Monte-Carlo simulations verified the validity of the expressions. The effects of average interference-to-noise ratio, number of

interferer antennas, time block allocation factor, and destination receiving aperture size on the secrecy performance were mainly investigated. The simulation results showed that when the interference noise ratio of the interferer was increased, the SOP of the system was significantly reduced and the ASC was significantly increased. This behavior showed that the secrecy performance of the system could be enhanced by increasing the interference-to-noise ratio to improve the effect of the interference signal on the eavesdropper. When the number of jammer antennas was increased, the SOP of the system was significantly reduced, and the ASC was significantly increased with it. The system's secrecy performance improved while simultaneously providing a good solution to the design of jammer equipment. By introducing the ST protocol and adjusting the time block allocation factor, the energy harvesting and transmission process of the jammer becomes more controllable and stable. The longer the jammer receives the energy, a higher amount of energy is used to transmit the jamming signal in the remaining time, which progressively improves the jamming effect of the jammer on the eavesdropper. Reasonable setting of ρ according to the actual situation can effectively improve the secrecy performance. On the other hand, increasing the receiving aperture of the destination enabled collection of a higher amount of optical signal power. However, large receiving aperture leads to a risk of eavesdropping on the FSO link. Proper receiving aperture size can realize the trade-off between operating cost and secrecy performance. In summary, the secrecy performance of the mixed RF-FSO system was significantly improved in the presence of the wireless powered jammer with the time protocol, which can provide a new system structure and a good theoretical basis for engineering implementation.

REFERENCES

[1] A. Mansour, R. Mesleh, and M. Abaza, "New challenges in wireless and free space optical communications," *Opt. Lasers Eng.*, vol. 89, pp. 95–108, 2017.

[2] M. T. Dabiri, M. J. Saber, and S. Sadough, "On the performance of multiplexing FSO MIMO links in log-normal fading with pointing errors," *J. Opt. Commun. Netw.*, vol. 9, no. 11, pp. 974–983, 2017.

[3] J. Xu, "Underwater wireless optical communication: Why, what, and how?," *Chin. Opt. Lett.*, vol. 17, pp. 38–47, 2019.

[4] E. Lee, J. Park, D. Han, and G. Yoon, "Performance analysis of the asymmetric dual-hop relay transmission with mixed RF-FSO links," *Photo. Tech. Lett.*, vol. 23, no. 21, pp. 1642–1644, 2011.

[5] X. Yi, C. Shen, P. Yue, W. Yamin, and Z. Peng, "Performance analysis for a mixed RF and multihop FSO communication system in 5G C-RAN," *J. Opt. Commun. Netw.*, vol. 11, no. 8, pp. 452–464, 2019.

[6] A. H. Abd El-Malek, A. M. Salhab, S. A. Zummo, and M. Alouini, "Security-reliability trade-off analysis for multiuser SIMO mixed RF/FSO relay networks with opportunistic user scheduling," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 5904–5918, 2016.

[7] H. Lei *et al.*, "On secrecy performance of mixed RF-FSO systems," *IEEE Photon. J.*, vol. 9, no. 4, pp. 1–14, 2017.

[8] L. Yang, T. Liu, J. Chen, and M. Alouini, "Physical-layer security for mixed $\eta-\mu$ and *M*-Distribution dual-hop RF-FSO systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12427–12431, 2018.

[9] M. J. Saber, A. Keshavarz, J. Mazloum, A. M. Sazdar, and M. J. Piran, "Physical-layer security analysis of mixed SIMO SWIPT RF and FSO fixed-gain relaying systems," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2851–2858, Sept. 2019.

[10] K. O. Odeyemi, P. A. Owolawi, and O. O. Olakanmi, "Secrecy performance of cognitive underlay hybrid RF/FSO system under pointing errors and link blockage impairments," *Opt. Quantum Electron.*, vol. 52, no. 3, pp. 183.1–183.16, 2020.

[11] S. Luo, R. Zhang, and T. J. Lim, "Optimal save-then-transmit protocol for energy harvesting wireless transmitters," *IEEE Trans. Wireless Commun.*, vol. 12, no. 3, pp. 1196–1207, 2013.

[12] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989–2001, 2013.

[13] M. K. M. R. Zhou, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, 2010.

[14] X. Zhang, X. Zhou, and M. R. Mckay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, 2013.

[15] R. Barrios and F. Dios, "Exponentiated Weibull model for the irradiance probability density function of a laser beam propagating through atmospheric turbulence," *Opt. Laser Technol.*, vol. 45, pp. 13–20, 2013.

[16] H. Lei *et al.*, "On physical layer security over generalized gamma fading channels," *Commun. Lett.*, vol. 19, no. 7, pp. 1257–1260, 2016.

[17] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. New York, NY, USA: Academic, 2007.

[18] Wolfram, The wolfram functions site, 2015. [Online]. Available: https://functions.wolfram.com/HypergeometricFunctions/MeijerG/

[19] P. Concus, D. Cassatt, G. Jaehnig, and E. Melby, "Tables for the evaluation of $\int_0^\infty x^\beta e^{-x} f(x)dx$ by Gauss-Laguerre quadrature," *Math. Comput.*, vol. 17, no. 83, 1963, pp. 245–256.