photonics

MDPI

Article

Secrecy Performance Analysis of Mixed RF/FSO Systems Based on RIS Reflection Interference Eavesdropper

Yong Wang [1,2], Yi Wang [1,2,*] and Wangyue Lu [1,2]

[1] Guangxi Key Laboratory of Nuclear Physics and Nuclear Technology, Guangxi Normal University, Guilin 541004, China; p21030854048@cjlu.edu.cn (Y.W.); 1800306129@cjlu.edu.cn (W.L.)
[2] Key Laboratory of Electromagnetic Wave Information Technology and Metrology of Zhejiang Province, College of Information Engineering, China Jiliang University, Hangzhou 310018, China
* Correspondence: wcy16@cjlu.edu.cn

Abstract: This paper proposes and studies the physical layer security of a mixed radio frequency/free space optical (RF/FSO) system based on reconfigurable intelligent surface (RIS)-aided jamming to prevent eavesdropping. This work considers Nakagami-m fading for the RF links and Málaga (M) turbulence for the FSO links. A two-hop decode-and-forward (DF) relaying method was used and the eavesdropper actively eavesdropped on the information transmitted by the RF link. The eavesdropper was thwarted by a wireless-powered jammer that transmits jamming signals, which were reflected by the RIS to the eavesdropper to ensure secure communication in the mixed RF/FSO system. The expressions of secrecy outage probability (SOP) and average secrecy capacity (ASC) of the RIS-aided mixed RF/FSO system were derived for the system model discussed above. The Monte Carlo method was utilized to verify the accuracy of these expressions. In the RIS-aided mixed RF/FSO system, the effects of the time switching factor, energy conversion efficiency, and average interference noise ratio on the system secrecy outage probability were analyzed and compared to the RIS-free mixed RF/FSO system. Meanwhile, the influence of the number of RIS reflecting elements, link distances before and after reflection, and fading severity parameter on the security performance of a mixed RF/FSO system assisted by RIS were also investigated.

Keywords: RF/FSO; physical layer security; wireless powered jammer; RIS

Citation: Wang, Y.; Wang, Y.; Lu, W. Secrecy Performance Analysis of Mixed RF/FSO Systems Based on RIS Reflection Interference Eavesdropper. *Photonics* **2023**, *10*, 1193. https://doi.org/10.3390/photonics10111193

Received: 28 September 2023
Revised: 18 October 2023
Accepted: 19 October 2023
Published: 26 October 2023

1. Introduction

Free space optical (FSO) communication has obvious advantages in terms of data transmission rate, spectrum license, bandwidth availability, and cost-effectiveness, but atmospheric turbulence and attenuation, building jitter and the deviation of receiving equipment pose a significant challenge to long-distance communication over the FSO link [1,2]. In contrast, radio frequency (RF) communication is not sensitive to atmospheric turbulence, but its spectrum resources are limited. The advantages of these two types of communications can be integrated by using relay technology where a mixed RF/FSO system can be formed that combines RF communication with FSO communication to achieve long-distance transmission.

As the RF links are broadcast, there are security risks where an eavesdropper can eavesdrop on the transmitted information. Therefore, physical layer security (PLS) is currently a prominent topic [3], and especially the research on security performance in mixed RF/FSO systems is one of the hotspots [4]. For example, there are studies on relay gain schemes. Yang et al. investigated the different gain schemes at the relay mixed RF/FSO systems with an eavesdropper in the RF link, analyzing their secrecy outage probability (SOP) and average secrecy capacity (ASC) [5]. On this basis, Lei et al. also analyzed the influence of atmospheric turbulence and other related factors on the system secrecy performance, deriving both asymptotic and lower bound expressions for the SOP and ASC [6]. Channel

state information has also been studied. Lei et al. analyzed the mixed RF/FSO system secrecy outage performance with imperfect channel state information [7], and the authors in [8] also considered four transmitting antenna selection schemes on this basis to enhance the mixed RF/FSO system secrecy performance. PLS can also be enhanced by jamming with the communication of eavesdropper. Considering an eavesdropper user in the RF link, our team studied simultaneous wireless information and power transfer (SWIPT) structure that was introduced in the relay to control energy harvesting and information transmission. The collected energy was used to emit interference signals to reduce the receiving rate of the eavesdropper, which improved the communication system's secrecy performance [9]. The PLS performance of the eavesdropper based on the wireless-powered friendly jammer transmitting interference signals was studied in [10].

In recent years, an electromagnetic device with controllable electromagnetic characteristics has been proposed, namely reconfigurable intelligent surface (RIS) [11]. By introducing RIS into a mixed RF/FSO system, the performance of the system can be significantly enhanced. For example, G. Alnwaimi et al. in [12] deployed the RIS as a transmitter or reflector to send signals, respectively, and the proposed RF/FSO system using RIS offered 20~25 dB gain with respect to a conventional RF/FSO system. K.O. Odeyemi et al. investigated the RIS, and the results illustrated that increasing the RIS- reflecting elements in RF and FSO links could significantly reduce the outage probability (OP) and average bit error rate of the system [13]. In [14], the system performance of intelligent reflecting surface (IRS)-aided RF/FSO communication network was studied, and the influence of factors such as the number of IRS elements, pointing error, atmospheric turbulence, and other factors on system OP and average bit error rate were analyzed. Aman Sikri et al. employed a signal space diversity technique to enhance the spectral efficiency and the diversity order of distributed RIS-assisted dual-hop mixed RF/FSO systems [15]. Wang et al. used the RIS in the FSO link segment of a mixed system to form the optical RIS, and the performance of the mixed communication system assisted by it was analyzed in [16]. In [17], Wu et al. studied the secrecy performance of the FSO system and analyzed the influence of atmospheric turbulence, pointing error, and other related parameters, as well as the position of eavesdroppers in different eavesdropping scenarios. In [18,19], the RIS and source nodes were combined, respectively, to form one and multiple RIS-equipped sources. The above studies showed that the RIS could improve performance such as the OP of a system, but the application of RIS to the mixed RF/FSO system to resist eavesdropping and improve the security performance of the physical layer has not been reported in the literature.

Drawing from the aforementioned discussion, we propose a mixed RF/FSO system where the jamming signals via RIS reflection cause interference to the eavesdropper. It was found that the RIS could significantly improve the system security performance. The uniform cumulative distribution function (CDF) for the end-to-end signal-to-noise ratio (SNR) of the communication system was derived for the eavesdropper subjected to the interference signal reflected by the RIS. We further derived the expressions for the SOP and ASC, which were verified for accuracy using Monte Carlo methods. The changes in the important system parameters, such as time switching factor, energy conversion efficiency, and average interference noise ratio were analyzed by simulations. In addition, the impact on the system security performance before and after the use of RIS was compared. The influence of important parameters of the RIS on the secrecy performance of the system was further investigated. These parameters included the number of reflecting elements, the link distances before and after reflection, and the fading severity parameter.

2. System Model

Figure 1 shows the mixed RF/FSO system based on RIS reflection interference to the eavesdropper. The system comprised of an RF source (S) with a single antenna, a single antenna relay (R) and a destination node (D), a wireless-powered multi-antenna jammer (J), and an RIS (R') with N reflection elements. The RF and FSO links followed Nakagami-m and M fading distribution, respectively. A single antenna eavesdropper (E) in the RF link,

attempts to eavesdrop on information sent from S to R but is interfered by the jamming signals. These signals are emitted by the jammer via RIS reflection and guarantee secure communication throughout the system. We assumed that the channel state information for each node is known.

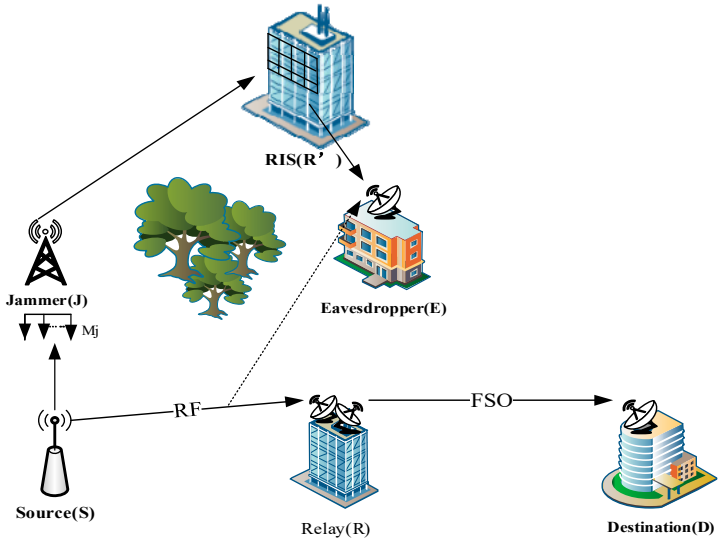

Figure 1. Mixed RF/FSO system based on RIS reflection interference eavesdropper.

We considered two-phase communication where the jammer considered fixed-rate transmission. The two phases are the energy-harvested phase and the information transmission phase. The SWIPT adopts a time-switching protocol in the whole process, meaning that during each time cycle T, energy collection is performed over λT, and information transmission is performed over $(1-\lambda)T$ [10]. Multiple receive antennas M_j (j = 1, 2, ...) were used at the jammer that receives the transmitted signal from the source node, and thus the signal received at J can be expressed as follows:

$$y_J = \frac{1}{\sqrt{d_{SJ}^{\tau}}}\sqrt{P_S}h_{SJ}x_S + n_J \tag{1}$$

where P_S refers to the transmission signal power of the S, x_S indicates the signal sent by the S, and h_{SJ}, d_{SJ} denotes the channel coefficients between the S and the J, and the distance between them, respectively. τ represent path loss index, and n_J is the additive Gaussian white noise with zero mean and variance σ_J^2 at the jammer. The energy harvested by the J can be expressed as:

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

where the time switching factor is represented by λ and ρ denotes the J energy conversion efficiency in converting the RF signal into direct current. In the information transmission phase, the energy consumed by the jammer to transmit signals cannot exceed the energy collected and stored in the previous phase. According to (2), the transmission power of the jammer P_J satisfies:

$$P_J(1-\lambda)T \le W_J \tag{3}$$

Using the N number of reflectors, the RIS redirects the incoming interference signal to the eavesdropper with an appropriate phase change, where $h_i = d_{JR'}^{\tau}\alpha_i e^{-j\theta_i}$ and $g_i = d_{R'E}^{\tau}\beta_i e^{-j\varphi_i}$ for $J - R'$ and $R' - E$ links, respectively. Here, α_i, θ_i represent the ampli-

tude and phase of the h_i channel, respectively. Similarly, β_i, φ_i denotes the amplitude and phase of the g_i channel, respectively. Therefore, the signal received by E can be expressed as:

$$y_E = \sum_{i=1}^{N} \sqrt{P_J} h_i v_i g_i x_J + \frac{1}{\sqrt{d_{SE}^{\tau}}} \sqrt{P_S} h_{SE} x_S + n_E \tag{4}$$

where x_J is the signal transmitted by the J, and h_{SE} and $d_{JR'}, d_{R'E}, d_{SE}$ indicate the channel coefficient and distances of the corresponding links, respectively. The RIS reflection coefficient of the ith reflection module is $v_i = \rho_i(\phi_i)e^{j\phi_i}$, the phase shift is $\phi_i \in [-\pi, \pi)$, and $\rho_i(\phi_i) \in [0, 1]$ represents the corresponding amplitude. The additive Gaussian white noise with zero mean and variance σ_E^2 at the eavesdropper is represented by n_E, respectively.

2.1. RF Channel Model

All RF links as well as the interference links experience the Nakagami-m fading because it can effectively model channel fading. According to [20] the PDF and CDF for the instantaneous SNR γ_k of the RF link are as follows:

$$f_{\gamma_k}(\gamma) = \frac{1}{\Gamma(m_k N_k)} \left(\frac{m_k}{\Omega_k}\right)^{m_k N_k} \gamma_k^{m_k N_k - 1} \exp\left(-\frac{m_k}{\Omega_k}\gamma_k\right) \tag{5}$$

$$F_{\gamma_k}(\gamma) = 1 - \exp\left(-\frac{m_k}{\Omega_k}\gamma_k\right) \sum_{t=0}^{m_k N_k - 1} \frac{1}{t!} \left(\frac{m_k}{\Omega_k}\gamma_k\right)^t \tag{6}$$

where $\Omega_{SR} = \frac{P_S \lambda_{SR}}{\sigma_R^2 d_{SR}^{\tau}}, \Omega_{SE} = \frac{P_S \lambda_{SE}}{\sigma_E^2 d_{SE}^{\tau}}, \Omega_{JR'} = \delta \frac{\lambda_{JR'}}{d_{JR'}^{\tau}}, \Omega_{R'E} = \delta \frac{\lambda_{R'E}}{d_{R'E}^{\tau}}$, and $k \in \{SR, SE, JR', R'E\}$, λ_k are the corresponding channel average power channel gains, and $\delta = \frac{\lambda \rho P_J M_j}{(1-\lambda)\sigma_E^2 d_{SJ}^{\tau}}$.

2.2. RF Interference Link

The jammer harvests the energy and then transmits the signal. Considering that the transmitted jamming signal will only be effective for the eavesdropper, we assume $\rho_i(\phi_i) = 1$, $\phi_i = \theta_i + \varphi_i$, which maximizes the SNR of the interfering link [21]. The interference signal is reflected by the RIS to interfere with the eavesdropper. According to [22], the instantaneous SNR of the interference link is:

$$\gamma = \sum_{i=1}^{N} (x_i y_i)^2 \frac{P_J}{N_0} = \sum_{i=1}^{N} W_i^2 \overline{\gamma} \tag{7}$$

where $W_i = x_i y_i$ and x_i, y_i correspond to two independent random variables that observe to the Nakagami-m distribution, N is the number of RIS reflecting elements, N_0 is the variance of additive white Gaussian noise, and $\overline{\gamma}$ is the average SNR of the interference link. Using the first term of Laguerre expansion, the PDF of $W = \sum_{i=1}^{N} W_i$ is given as:

$$f_W(z) = \frac{z^a}{b^{a+1}\Gamma(a+1)} \exp\left(-\frac{z}{b}\right) \tag{8}$$

where a and b are mean and variance of W, respectively, and given as follows:

$$a = \frac{(N+1)\Gamma(m+0.5)^4 - m^2\Gamma(m)^4}{m^2\Gamma(m)^4 - \Gamma(m+0.5)^4} \text{ and } b = m\Omega\left(\frac{\Gamma(m)^2\Gamma(m+1)^2 - \Gamma(m+0.5)^4}{\Gamma(m+0.5)^2\Gamma(m+1)^2}\right)$$

where $\Gamma(\cdot)$ is the Gamma function, $m \in \{1, 2, \ldots, \infty\}$ is the fading severity parameter, and Ω is the mean fading power. Changing the variable of (8), the PDF of γ under Nakagami-m distribution is obtained as:

$$f_\gamma(\gamma) \approx \frac{\gamma^{(a-1)/2}}{2\overline{\gamma}^{(a+1)/2} b^{a+1} \Gamma(a+1)} \exp\left(-b^{-1}\sqrt{\frac{\gamma}{\overline{\gamma}}}\right) \tag{9}$$

The CDF of (9) can be obtained as:

$$F_\gamma(\gamma) \approx \frac{1}{\Gamma(a+1)} G_{1,2}^{1,1}\left[b^{-1}\sqrt{\frac{\gamma}{\overline{\gamma}}} \middle| \begin{matrix} 1 \\ a+1, 0 \end{matrix}\right] \tag{10}$$

The fading of the J to E link is evident due to the no line of sight resulting from obstructions like bushes. Combining (10) and [23], the CDF of the instantaneous SNR of the whole interference link is obtained as follows:

$$\begin{aligned} F_{\gamma_{SJR'E}}(\gamma) = 1 - \frac{1}{\Gamma(a+1)\Gamma(M_j-1)} \sum_{k=0}^{m_{SE}-1} \frac{1}{k!} \left(\frac{m_{SE}}{\Omega_{SE}(M_j-1)}\right)^k \sum_{p=0}^{k} \binom{k}{p} \Omega_{JR'}^p \Omega_{R'E}^p \gamma^k \\ \times \exp\left(-\frac{m_{SE}\gamma}{\Omega_{SE}(M_j-1)}\right) G_{1,1}^{1,1}\left[\frac{m_{SE}\Omega_{JR'}\Omega_{R'E}\gamma}{\Omega_{SE}(M_j-1)} \middle| \begin{matrix} -M_j - p + 2 \\ 0 \end{matrix}\right] G_{1,2}^{1,1}\left[\frac{\sqrt{\gamma}}{b\sqrt{\overline{\gamma}}} \middle| \begin{matrix} 1 \\ 1+a, 0 \end{matrix}\right] \end{aligned} \tag{11}$$

The corresponding PDF of the instantaneous SNR can be obtained by derivation and simplification of Equation (11) as:

$$\begin{aligned} f_{\gamma_{SJR'E}}(\gamma) = \frac{1}{\Gamma(m_{SE})\Gamma(M_j-1)\Gamma(a+1)} \left(\frac{m_{SE}}{\Omega_{SE}(M_j-1)}\right)^{m_{SE}} \sum_{p=0}^{m_{SE}} \binom{m_{SE}}{p} \Omega_{JR'}^p \Omega_{R'E}^p \gamma^{m_{SE}-1} \exp\left(-\frac{m_{SE}\gamma}{\Omega_{SE}(M_j-1)}\right) \\ \times G_{1,2}^{1,1}\left[\frac{\sqrt{\gamma}}{b\sqrt{\overline{\gamma}}} \middle| \begin{matrix} 1 \\ a+1, 0 \end{matrix}\right] G_{1,1}^{1,1}\left[\frac{m_{SE}\Omega_{JR'}\Omega_{R'E}\gamma}{\Omega_{SE}(M_j-1)} \middle| \begin{matrix} -M_j - p + 2 \\ 0 \end{matrix}\right] - \frac{2^a}{\sqrt{\pi}\gamma} \sum_{k=0}^{m_{SE}-1} \frac{1}{k!} \left(\frac{m_{SE}}{\Omega_{SE}(M_j-1)}\right)^k \sum_{p=0}^{k} \binom{k}{p} \\ \times \Omega_{JR'}^p \Omega_{R'E}^p \gamma^k \exp\left(-\frac{m_{SE}\gamma}{\Omega_{SE}(M_j-1)}\right) G_{3,5}^{2,3}\left[\frac{\gamma}{4b^2\overline{\gamma}} \middle| \begin{matrix} 0, 1, 0, \frac{1}{2}, 1 \\ \frac{a+1}{2}, \frac{a+2}{2}, 0, \frac{1}{2}, 1 \end{matrix}\right] G_{1,1}^{1,1}\left[\frac{m_{SE}\Omega_{JR'}\Omega_{R'E}\gamma}{\Omega_{SE}(M_j-1)} \middle| \begin{matrix} -M_j - p + 2 \\ 0 \end{matrix}\right] \end{aligned} \tag{12}$$

2.3. FSO Channel Model

As Figure 1 shows, R to D indicates that FSO links and adopts an M distribution. Atmospheric fading and pointing errors are compromising factors for the FSO communication link performance [24–26]. The M distribution channel PDF and CDF expressions are as follows [27]:

$$f_{RD}(\gamma) = \frac{\xi^2 A}{2\gamma} \sum_{m'=1}^{\beta} b_{m'} G_{1,3}^{3,0}\left[\frac{B\gamma_{RD}}{\overline{\gamma}_{RD}} \middle| \begin{matrix} \xi^2+1 \\ \xi^2, \alpha, m' \end{matrix}\right] \tag{13}$$

$$F_{RD}(\gamma) = \frac{\xi^2 A}{2} \sum_{m'=1}^{\beta} b_{m'} G_{2,4}^{3,1}\left[\frac{B\gamma_{RD}}{\overline{\gamma}_{RD}} \middle| \begin{matrix} 1, 1+\xi^2 \\ \xi^2, \alpha, m', 0 \end{matrix}\right] \tag{14}$$

where:

$$A = \frac{2\alpha^{\alpha/2}}{g^{1+\frac{\alpha}{2}}\Gamma(\alpha)} \left(\frac{g\beta}{g\beta + \Omega_0'}\right)^{\beta+\frac{\alpha}{2}} \tag{15}$$

$$B = \frac{\xi^2 \alpha \beta \left(g + \Omega_0'\right)}{\left(\xi^2+1\right)\left(g\beta + \Omega_0'\right)} \tag{16}$$

$$b_{m'} = \binom{\beta-1}{m'-1} \frac{\left(g\beta + \Omega_0'\right)^{1-\frac{m'}{2}}}{(m'-1)!} \left(\frac{\Omega_0'}{g}\right)^{m'-1} \left(\frac{\alpha}{\beta}\right)^{\frac{m'}{2}} \left(\frac{\alpha\beta}{g\beta + \Omega_0'}\right)^{-\frac{\alpha+m'}{2}} \tag{17}$$

$\overline{\gamma}_{RD}$ is the FSO link average SNR, and α and β denote positive parameters related to the effective number of large-scale cells of the scattering process, and a natural number

for the fading parameter, respectively. The ratio of the equivalent beam width to the pointing error displacement standard deviation at the receiver is represented by ξ, g is the average power of the scattering component, $\Omega_0^{'}$ represents the average power of the coherent contribution, and $G_{p,q}^{m,n}[\cdot]$ is the Meijer's G function.

3. End-to-End SNR Statistics

The end-to-end instantaneous SNR under the DF relay is given by:

$$\gamma_{SRD} = \frac{\gamma_{SR}\gamma_{RD}}{\gamma_{SR} + \gamma_{RD} + 1} \approx \min(\gamma_{SR}, \gamma_{RD}) \tag{18}$$

The joint channel end-to-end CDF is as follows:

$$F_{\gamma_{SRD}}(\gamma) = \Pr\{\min(\gamma_{SR}, \gamma_{RD}) < \gamma\} = F_{\gamma_{SR}}(\gamma) + F_{\gamma_{RD}}(\gamma) - F_{\gamma_{SR}}(\gamma)F_{\gamma_{RD}}(\gamma) \tag{19}$$

Substituting Equations (6) and (14) into (17) yields:

$$F_{\gamma_{SRD}}(\gamma) = 1 - \exp\left(-\frac{m_{SR}}{\Omega_{SR}}\gamma\right)\sum_{t=0}^{m_{SR}N_{SR}-1}\frac{1}{t!}\left(\frac{m_{SR}}{\Omega_{SR}}\gamma\right)^t\left(1 - \frac{\xi^2 A}{2}\sum_{m'=1}^{\beta} b_{m'}G_{2,4}^{3,1}\left[\frac{B\gamma}{\overline{\gamma}_{RD}}\middle|\begin{matrix}1, 1+\xi^2\\ \xi^2, \alpha, m', 0\end{matrix}\right]\right) \tag{20}$$

4. Secrecy Outage Probability Analysis

The SOP event occurs when the instantaneous secrecy capability falls below the security threshold R_s.Therefore, the SOP lower bound expression for the mixed system is as follows [7]:

$$P_{out}(R_s) = \int_0^{\infty} F_{\gamma_{SRD}}(\theta\gamma) f_{\gamma_{SJR'E}}(\gamma) d\gamma \tag{21}$$

where $\theta = \exp(R_s)$, substituting (20) and (12) into (21) and using the relevant formula in [28] (Equation (07.34.21.0081.01)) and the Laguerre polynomial to calculate the end-to-end SOP, we obtain the following expression:

$$\begin{aligned}
P_{out}(R_s) = {} & \frac{1}{\Gamma(m_{SE})\Gamma\left(M_j-1\right)\Gamma(a+1)}\left(\frac{m_{SE}}{\Omega_{SE}\left(M_j-1\right)}\right)^{m_{SE}}\sum_{p=0}^{m_{SE}}\binom{m_{SE}}{p}\Omega_{JR'}^{p}\Omega_{R'E}^{p}\left\{\sum_{j=1}^{e}H_j\left(\gamma_j^{m_{SE}-0.5}\exp\left(-\frac{m_{SE}\gamma_j}{\Omega_{SE}\left(M_j-1\right)}+\gamma_j\right)-\sum_{t=0}^{m_{SR}N_{SR}-1}\frac{1}{t!}\left(\frac{m_{SR}\theta}{\Omega_{SR}}\right)^t\gamma_j^{m_{SE}+t-0.5}\right.\right.\\
& \times\exp\left(-\frac{m_{SE}\gamma_j}{\Omega_{SE}\left(M_j-1\right)}-\frac{m_{SR}\theta\gamma_j}{\Omega_{SR}}+\gamma_j\right)\left(1-\frac{\xi^2A}{2}\sum_{m'=1}^{\beta}b_{m'}G_{2,4}^{3,1}\left[\frac{B\gamma_j}{\overline{\gamma}_{RD}}\middle|\begin{matrix}1, 1+\xi^2\\ \xi^2, \alpha, m', 0\end{matrix}\right]\right)G_{1,2}^{1,1}\left[\frac{\sqrt{\gamma_j}}{b\sqrt{\overline{\gamma}}}\middle|\begin{matrix}1\\ a+1, 0\end{matrix}\right]G_{1,1}^{1,1}\left[\frac{m_{SE}\Omega_{JR'}\Omega_{R'E}\gamma_j}{\Omega_{SE}\left(M_j-1\right)}\middle|\begin{matrix}-M_j-p+2\\ 0\end{matrix}\right]\left.\right\}\\
& -\frac{2^a}{\sqrt{\pi}}\sum_{k=0}^{m_{SE}-1}\frac{1}{k!}\sum_{p=0}^{k}\Omega_{JR'}^{p}\Omega_{R'E}^{p}\left\{G_{1,0:3,5:1,1}^{0,1:2,3:1,1}\left[\begin{matrix}1-k\\ -\end{matrix}\middle|\begin{matrix}0,1,0,\frac{1}{2},1\\ \frac{a+1}{2},\frac{a+2}{2},0,\frac{1}{2},1\end{matrix}\middle|\begin{matrix}-M_j-p+2\\ 0\end{matrix}\middle|\frac{\Omega_{SE}\left(M_j-1\right)}{4b^2m_{SE}\overline{\gamma}},\Omega_{JR'}^{p},\Omega_{R'E}^{p}\right]-\left(\frac{m_{SE}}{\Omega_{SE}\left(M_j-1\right)}\right)^{m_{SR}N_{SR}-1}\frac{1}{t!}\left(\frac{m_{SR}\theta}{\Omega_{SR}}\right)^t\right.\\
& \times\left(\left(\Omega_{SE}\left(M_j-1\right)\Psi\right)^{k+t}G_{1,0:3,5:1,1}^{0,1:2,3:1,1}\left[\begin{matrix}1-k-t\\ -\end{matrix}\middle|\begin{matrix}0,1,0,\frac{1}{2},1\\ \frac{a+1}{2},\frac{a+2}{2},0,\frac{1}{2},1\end{matrix}\middle|\begin{matrix}-M_j-p+2\\ 0\end{matrix}\middle|\frac{\Omega_{SE}\left(M_j-1\right)\Psi}{4b^2m_{SE}\overline{\gamma}},m_{SE}\Omega_{JR'}\Omega_{R'E}\Psi\right]-\frac{\xi^2A}{2}\sum_{m'=1}^{\beta}b_{m'}\sum_{j=1}^{e}H_j\gamma^{k+t-0.5}\right.\\
& \left.\left.\times\exp\left(-\frac{m_{SE}\gamma_j}{\Omega_{SE}\left(M_j-1\right)}-\frac{m_{SR}\theta\gamma_j}{\Omega_{SR}}+\gamma_j\right)G_{1,1}^{1,1}\left[\frac{m_{SE}\Omega_{JR'}\Omega_{R'E}\gamma_j}{\Omega_{SE}\left(M_j-1\right)}\middle|\begin{matrix}-M_j-p+2\\ 0\end{matrix}\right]G_{1,2}^{1,1}\left[\frac{\sqrt{\gamma_j}}{b\sqrt{\overline{\gamma}}}\middle|\begin{matrix}1\\ a+1,0\end{matrix}\right]G_{2,4}^{3,1}\left[\frac{B\gamma_j}{\overline{\gamma}_{RD}}\middle|\begin{matrix}1,1+\xi^2\\ \xi^2,\alpha,m',0\end{matrix}\right]\right)\right\}
\end{aligned} \tag{22}$$

What needs illustration is that $H_j = \frac{\Gamma(n+0.5)x_j}{n!(n+1)^2\left[L_n^{(-1/2)}(x_j)\right]^2}$ and $\Psi = \Omega_{SR}/\left(m_{SE}\Omega_{SR} + m_{SR}\theta\Omega_{SE}\left(M_j-1\right)\right)$ in (22), where $L_n^{(-1/2)}(x)$ denoted the generalized Laguerre polynomial, and x_j is the jth root of this polynomial.

5. Average Secrecy Capacity Analysis

Another crucial indicator for evaluating the active eavesdropping secrecy performance is the ASC, whose expression is as follows [18]:

$$ASC = \int_0^{\infty}\frac{1}{1+\gamma}F_{\gamma_{SJR'E}}(\gamma)(1 - F_{\gamma_{SRD}}(\gamma))d\gamma \tag{23}$$

Substituting (11) and (20) into (23), and using the Meijer's G function provided in ([28] Equations (07,34,21,0011,01) and (07.34.21.0081.01)) to first simplify and then calculate using the Laguerre polynomial yields the following expression:

$$
\begin{aligned}
ASC = & \sum_{t=0}^{m_{SR}N_{SR}-1} \frac{1}{t!}\left(\frac{m_{SR}}{\Omega_{SR}}\right)^{t}\left\{G_{2.1}^{1.2}\left[\frac{m_{SR}}{\Omega_{SR}}\middle| \begin{matrix} -t \\ 0,-t \end{matrix}\right] - \frac{\xi^2 A}{2}\sum_{m'=1}^{\beta} b_{m'} G_{1,1:0,1:2,4}^{1,1:1,0:3,1}\left[\begin{matrix} -t \\ -t \end{matrix} \middle| \begin{matrix} - \\ 0 \end{matrix} \middle| \begin{matrix} 1, 1+\xi^2 \\ \xi^2, \alpha, m', 0 \end{matrix} \middle| \frac{m_{SR}}{\Omega_{SR}}, \frac{B}{\overline{\gamma}_{RD}}\right]\right. \\
& - \frac{1}{\Gamma(1+a)\Gamma(M_j-1)} \sum_{k=0}^{m_{SE}-1} \frac{1}{k!}\left(\frac{m_{SE}}{\Omega_{SE}(M_j-1)}\right)^{k} \sum_{p=0}^{k}\binom{k}{p} \Omega_{JR'}^{p}\Omega_{R'E}^{p}\left\{\sum_{j=1}^{e} H_j \frac{\gamma_j{}^{t+k+0.5}}{1+\gamma_j}\left(1-\frac{\xi^2 A}{2}\sum_{m'=1}^{\beta} b_{m'}\right)\right. \\
& \left.\left. \times \exp\left(-\frac{m_{SR}}{\Omega_{SR}}\gamma_j - \frac{m_{SE}\gamma_j}{\Omega_{SE}(M_j-1)} + \gamma_j\right) G_{1,1}^{1,1}\left[\frac{m_{SE}\Omega_{JR'}\Omega_{R'E}\gamma_j}{\Omega_{SE}(M_j-1)}\middle| \begin{matrix} -M_j-p+2 \\ 0 \end{matrix}\right] G_{1,2}^{1,1}\left[\frac{\sqrt{\gamma_j}}{b\sqrt{\overline{\gamma}}}\middle| \begin{matrix} 1 \\ 1+a, 0 \end{matrix}\right]\right\}\right\}
\end{aligned} \tag{24}
$$

6. Simulation Results and Analysis

In this section, the simulation results of the RIS-aided mixed RF/FSO-based system under the influence of various parameters are provided. Subsequently, Monte Carlo simulations are performed to further verify the accuracy of the simulated numerical results. The following parameters are assumed in the RF link: $d_{SJ} = d_{SR} = d_{SE} = 10$ m, $m_{SR} = m_{SE} = 2$. The instantaneous SNR of this link is $\gamma_{SR} = 15$ dB. In the interference link, the number of reflecting elements is N = 3, and the average interference noise ratio is 1 dB, m = 3, $\Omega = 1$, $\lambda = \rho = 0.4$, and $d_{JR'} = d_{R'E} = 10$ m. Following are the parameters of the FSO link: the FSO link distance is 1 km, the wavelength is 758 nm, the refractive index structure constant is $C_n^2 = 2.1 \times 10^{-14}$, the instantaneous SNR of the FSO link is $\gamma_{RD} = 20$ dB, and the optical wave number is $k = 2\pi/\lambda_1$. Additional parameters include the instantaneous SNR of the eavesdropping link $\lambda_{SE} = -10$ dB, $\overline{\gamma}_{RD} = 20$ dB, $\xi = 6.7$, $\tau = 1$, $M_j = 4$, and the target secrecy rate $R_s = 0.01$ nat/s. In the following simulations, the above values are used without additional explanation. In the calculations of the generalized Laguerre orthogonal numerical integration method, j is set to 30 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 are closely aligned with the simulation results, which verifies the accuracy of the expression.

Figure 2 shows the correlation between the RF link instantaneous SNR λ_{SR} and SOP under the influence of different time-switching factors with or without the RIS assistance. The results show that the system SOP decreases as λ_{SR} increases. The value of SOP when $\lambda = 0.7$ is lower than that when $\lambda = 0.3$, irrespective of whether the RIS is introduced or not. This is because as the time switching factor increases, the energy storage time becomes longer and the jamming effect of the transmitted jamming signal is better. Consequently, the system SOP was reduced significantly. Next, keeping the time switching factor of the system fixed and $\lambda_{SR} = 35$ dB, $\lambda = 0.3$, RIS is introduced in the mixed system and compared with the SOP of the system before its introduction. The SOP values before and after the introduction of RIS are about 5.02×10^{-6} and 7.24×10^{-7}, respectively. They differ by an order of magnitude, indicating that incorporating RIS can decrease SOP to improve security performance. Similarly, when $\lambda_{SR} = 35$ dB, $\lambda = 0.7$, the SOP values before and after the introduction of RIS are about 2.38×10^{-6} and 8.45×10^{-8}, respectively. Thus, they differ by two orders of magnitude. Therefore, as λ increases, the addition of RIS noticeably enhances the mixed system secrecy performance.

Figure 3 shows the correlation between λ_{SR} and the RF/FSO system SOP under the influence of different energy conversion efficiency values with or without the RIS assistance. As Figure 3 shows, the RF/FSO system SOP gradually diminishes with the λ_{SR} rises. Regardless of whether the RIS is introduced in the mixed system, the SOP of the system is obviously lower for $\rho = 0.9$ compared to that with $\rho = 0.5$. This is because as the energy conversion efficiency increases, the jammer stores more energy, the quality of the jamming signal is higher, the rate limit on the receiver side of the eavesdropper is enhanced, and the secrecy performance is better. When $\lambda_{SR} = 35$ dB, $\rho = 0.5$, the SOP values before and after the introduction of RIS are about 4.86×10^{-6} and 1.42×10^{-6}, respectively, which indicates that incorporating RIS can decrease the SOP to improve the security performance. Similarly, when $\lambda_{SR} = 35$ dB, $\rho = 0.9$, the SOP values before and after the introduction of RIS are about 2.15×10^{-6} and 8.00×10^{-8}, respectively, they differ by two orders of

magnitude. Therefore, it is further demonstrated that the addition of RIS in mixed systems proves especially potent in effectively decreasing SOP as ρ increases.

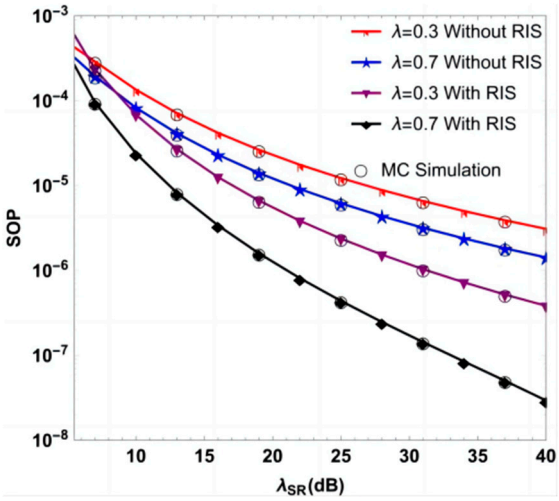

Figure 2. Simulation diagram of SOP under different time switching factors λ with or without RIS.

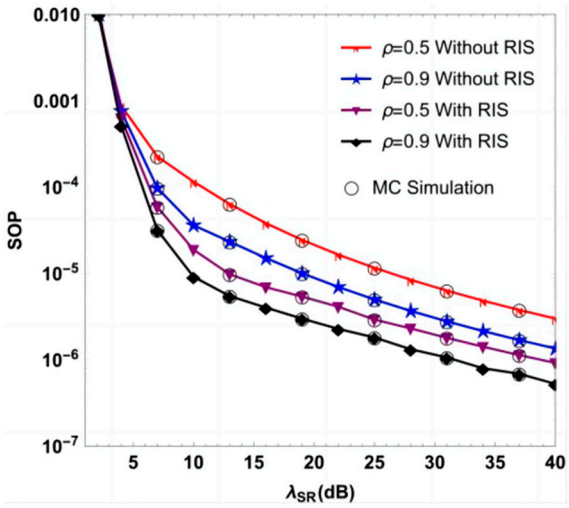

Figure 3. Simulation diagram of SOP under different energy conversion efficiency ρ with or without RIS.

Figure 4 shows how λ_{SR} and the system SOP are related before and after RIS was introduced with different values of average interference noise ratio in the mixed RF/FSO system. The simulation results show that the SOP of the system decreases monotonically as λ_{SR} increases. Regardless of the presence or absence of RIS, with an increase in the average interference noise ratio, there is a concurrent decrease in the SOP. Furthermore, the RIS can significantly reduce the SOP when the average interference noise ratio remains constant. When $\lambda_{SR} = 35$ dB and the average interference noise ratio is 2 dB, the system SOP before and after the introduction of RIS in the system is about 9.12×10^{-7} and 8.14×10^{-8}, respectively. Similarly, when $\lambda_{SR} = 35$ dB, the average interference noise ratio is 4 dB, the system SOP values before and after the introduction of RIS in the system are about 2.85×10^{-7} and 2.25×10^{-8}, respectively. Therefore, when the RIS is employed in the mixed RF/FSO system, the SOP is obviously lower and the system has better secrecy performance.

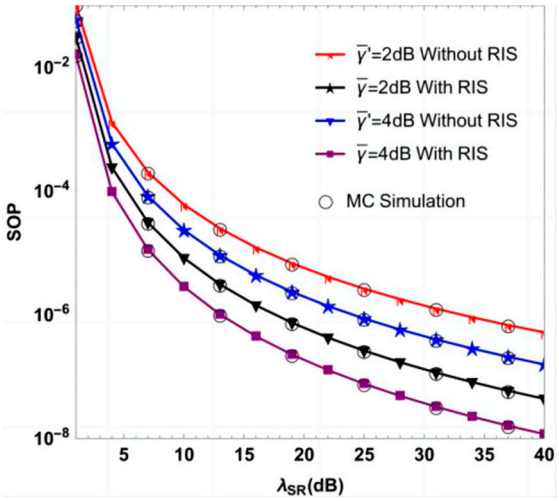

Figure 4. Simulation diagram of SOP with different average interference noise ratio with or without RIS.

Figure 5 presents the correlation between λ_{SR} and in the RIS-aided mixed RF/FSO system SOP under the influence of different reflecting elements N. Figure 5 shows that the system SOP decreases gradually as λ_{SR} increases. When $\lambda_{SR} = 35$ dB, and the number of reflecting elements N is varied as 4, 6, and 8, respectively, the corresponding system SOP values are about 1.07×10^{-7}, 2.75×10^{-8}, and 7.05×10^{-9}, respectively. The SOP value of the system at N = 8 is significantly lower than those at N = 4 and 6. This is because a higher number of reflecting elements indicates that more reflecting elements are jointly involved in receiving and reflecting the interfering signals, which can reduce the quality of the eavesdropper communication to a greater extent and increase the effectiveness of interference. Therefore, an appropriate increase in N in the RIS-aided mixed RF/FSO system can improve its security performance.

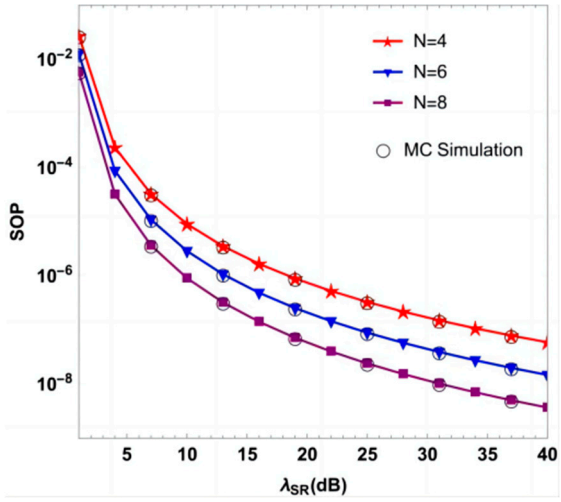

Figure 5. Simulation diagram of SOP under different number of RIS reflecting elements N in the RIS-aided mixed RF/FSO system.

Figure 6 shows the correlation between λ_{SR} and the RIS-aided mixed RF/FSO system SOP for different distances of $J - R'$ as well as $R' - E$. As λ_{SR} increases, the mixed system SOP decreases with decreasing $d_{JR'}$ and $d_{R'E}$. When $\lambda_{SR} = 35$ dB, the SOP values of the system are about 5.01×10^{-6} and 3.31×10^{-6} for $d_{JR'} = 10$ m, $d_{R'E} = 10$ m and $d_{JR'} = 5$ m, $d_{R'E} = 5$ m, respectively. When the link distances are increased simultaneously, the greater the loss of interference signal in the link, and the worse the interference effect.

When the distances between the two sections are relatively small, the interference signal transmission loss is small which enhances the interference effect, consequently reducing the SOP. Therefore, a proper reduction of the link distances before and after reflection in the RIS-aided mixed RF/FSO system can effectively improve the system's secrecy performance.

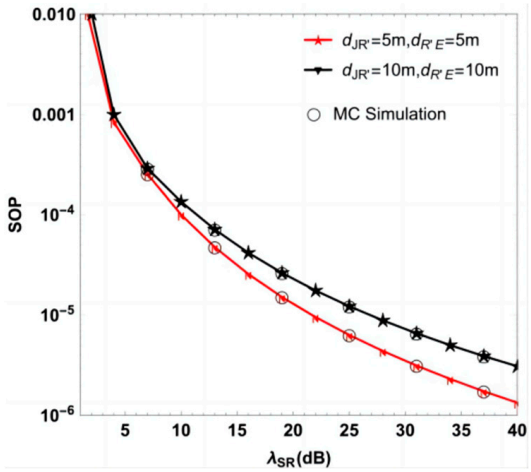

Figure 6. Simulation diagram of the SOP with different RIS reflection before and after link distances $d_{JR'}, d_{R'E}$ in the RIS-aided mixed RF/FSO system.

Figure 7 presents the correlation between λ_{SR} and the RIS-aided mixed RF/FSO system SOP under the influence of different fading severity parameter values. Figure 7 shows that the system SOP decreases continuously as λ_{SR} increases. The number of reflecting elements N is fixed, and the mixed system SOP is significantly decreased by increasing m from 2 to 6. When $\lambda_{SR} = 35$ dB and N = 2, the system SOP is about 9.85×10^{-7} and 1.05×10^{-7} for m equal to 2 and 6, respectively. It is shown that increasing the fading severity parameter value improves the quality of the interfering link fading, providing better secrecy performance for the mixed system. Similarly, for $\lambda_{SR} = 35$ dB and N = 4, the values of SOP corresponding to m equal to 2 and 6 are about 2.82×10^{-7} and 6.47×10^{-9}, respectively; they differ by two orders of magnitude. As m varies, the mixed system SOP with N = 4 is better than that of the mixed system with N = 2 in terms of security performance, indicating that the increase of m improves the system security performance more significantly with a higher N compared to the system with a lower N.

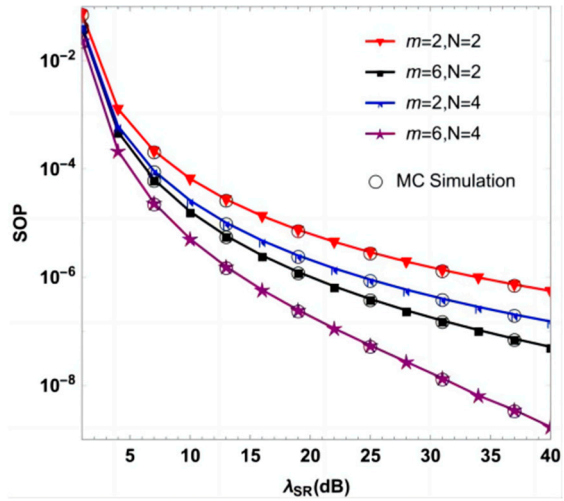

Figure 7. Simulation diagram of SOP under different fading severity parameters m of RIS in the RIS-aided mixed RF/FSO system.

Figure 8 shows the correlation between λ_{SR} and the RIS-aided mixed RF/FSO system ASC with the effect of a varying number of RIS-reflecting elements. As the simulation diagram shows, as λ_{SR} increases, there is a corresponding increase in ASC. When $\lambda_{SR} = 35$ dB, the ASC values are about 3.26, 3.44, and 3.75 for 4, 6, and 8 reflecting elements, respectively. The results show that the ASC is maximum at N = 8. This is because the RIS can reflect more interference signals with the increase of N that can greatly limit the receiver side rate of the eavesdropper, consequently increasing the ASC. Therefore, in the RIS-aided mixed RF/FSO system, an appropriate increase in N can effectively increase the ASC of the entire communication system.

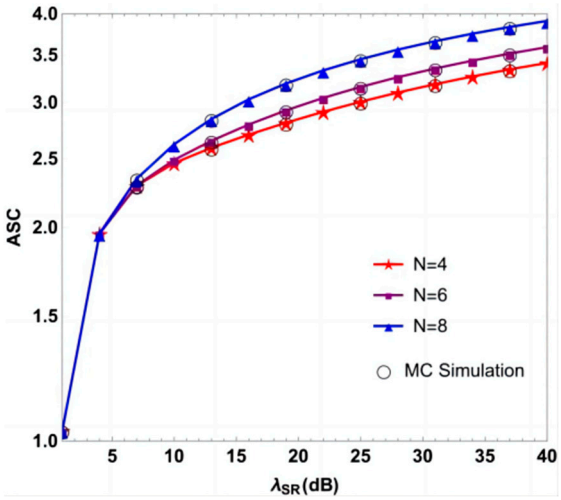

Figure 8. Simulation diagram of ASC under different numbers of RIS reflecting elements N in the RIS-aided mixed RF/FSO system.

Figure 9 investigates the correlation between λ_{SR} and the RIS-aided mixed RF/FSO system ASC for different link distances before and after the RIS reflection. As the instantaneous SNR λ_{SR} increases, the system ASC increases as $d_{JR'}, d_{R'E}$ decreases. When $\lambda_{SR} = 35$ dB, the ASC values of the system are about 2.86 and 3.26 for $d_{JR'} = 10$ m, $d_{R'E} = 10$ m and $d_{JR'} = 5$ m, $d_{R'E} = 5$ m, respectively. When $d_{JR'}$ and $d_{R'E}$ increase simultaneously, the interference signal loss in the link becomes higher, the effect of interference becomes worse, and the ASC decreases. On the other hand, when both distances are relatively small, the interference signal loss is low, the interference signal is received with high quality by the RIS, the interference effect is enhanced, and thus, the ASC increases. Therefore, a proper reduction of the link distances before and after reflection in the RIS-aided mixed RF/FSO system can effectively improve the physical layer security performance.

Figure 10 shows the correlation between λ_{SR} and the RIS-aided mixed RF/FSO system ASC for different fading severity parameters of the RIS. It can be concluded based on the figure that the system ASC gradually increases as λ_{SR} increases. Considering that N is fixed, the mixed system ASC shows a prominent increase when m increases. When $\lambda_{SR} = 35$ dB, $N = 2$, the ASC values are about 2.72, and 3.55 for m equal to 2 and 6, respectively. Similarly, when $\lambda_{SR} = 35$ dB, $N = 4$, the ASC values are about 3.00, and 3.77 corresponding to m equal to 2 and 6, respectively. It is obvious that as m increases, the fading quality of the interference link improves, the rate limit at the receiver end of the eavesdropper is enhanced, and the ASC rises. Therefore, an appropriate increase in the fading severity parameter m allows the RIS-aided mixed RF/FSO system to achieve better security performance.

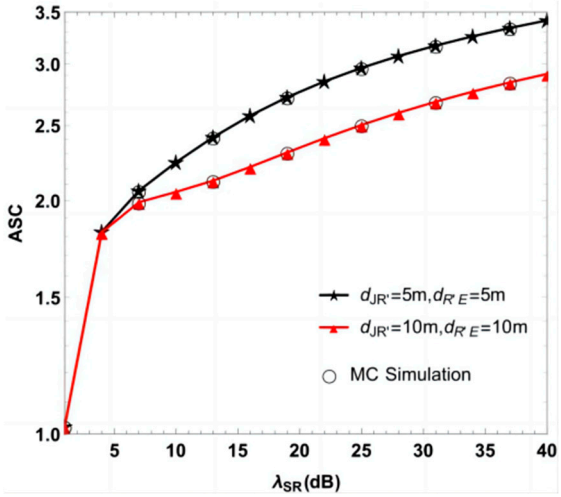

Figure 9. Simulation diagram of ASC with different RIS reflections before and after of link distances $d_{JR'}, d_{R'E}$ in the RIS-aided mixed RF/FSO system.

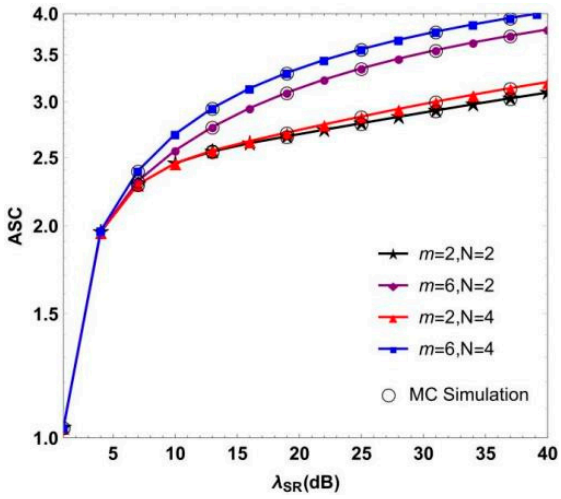

Figure 10. Simulation diagram of the ASC under different fading severity parameters m of RIS in the RIS-aided mixed RF/FSO system.

7. Conclusions

This paper investigated how integrating RIS into the mixed RF/FSO system's interference link affects its physical layer security performance. We analyzed the system's security outage probability (SOP) and the average secrecy capacity (ASC) theoretically, and then Monte Carlo simulations were employed to verify the correctness of the theoretical expressions. The time switching factor, energy conversion efficiency, and average interference noise ratio, as well as the number of reflecting elements, fading severity parameter, and link distances before and after RIS reflection were mainly studied, and an analysis of their effects on the secrecy performance was conducted.

The findings indicate that the system's SOP decreased when the time switching factor, energy conversion efficiency, and average interference noise ratio were increased with or without RIS assistance. When the time switching factor, energy conversion efficiency, and average interference noise ratio were fixed, the RIS-aided mixed system's SOP was significantly lower than that of the mixed system without RIS assistance. The improvement of secrecy performance achieved by introducing RIS in the mixed system was more significant as the time switching factor and energy conversion efficiency increased. Therefore, using RIS to assist reflection interference against eavesdropping in a mixed RF/FSO

system could considerably decrease the SOP and improve the system's physical layer security performance.

Furthermore, there was an impact of RIS-related parameters on system secrecy performance. With the increase in the number of RIS-reflecting elements, a higher intensity of interference signals could be reflected, which reduced the eavesdropper receiver side rate to a greater extent and decreased the SOP. The increase in the fading severity parameter improved the fading quality of the interfering link, thus providing better system secrecy performance. With an increase in the number of reflecting elements, the reduction in the SOP of the mixed system became more pronounced with an increase in the fading severity parameter. To reduce the interference signal transmission loss to improve the interference effect, the link distances before and after the reflection could be reduced properly, which would decrease the SOP of the system. Similarly, increasing the number of reflecting elements and fading severity parameters, as well as decreasing the link distances before and after reflection, would also increase the ASC of the system. In engineering applications, the appropriate number of reflecting elements, fading severity parameter, and link distances before and after reflection could be selected based on the actual performance requirements and flexible implementation cost considerations. In summary, the quality of eavesdropper communication was degraded and the mixed RF/FSO system physical layer security performance was considerably improved under the effect of RIS-assisted reflected interference signals. This provides a feasible solution for future research on physical layer security to improve security performance, and actively explores the breakthroughs of RIS in hardware as well as application so that it can be adapted to more application scenarios and have a greater function and effect.

Author Contributions: Conceptualization, Y.W. (Yong Wang) and Y.W. (Yi Wang); methodology, Y.W. (Yong Wang); software, Y.W. (Yong Wang); validation, Y.W. (Yong Wang), Y.W. (Yi Wang), and W.L.; formal analysis, Y.W. (Yong Wang); investigation, W.L.; resources, Y.W. (Yi Wang); data curation, Y.W. (Yong Wang); writing—original draft preparation, Y.W. (Yong Wang); writing—review and editing, Y.W. (Yong Wang); visualization, Y.W. (Yi Wang); supervision, Y.W. (Yi Wang); project administration, Y.W. (Yi Wang); funding acquisition, Y.W. (Yi Wang). All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by The Open Project of Guangxi Key Laboratory of Nuclear Physics and Nuclear Technology, China (No. NLK2022-09), the Central Government Guidance Funds for Local Scientific and Technological Development, China (No. Guike ZY22096024) and the National Natural Science Foundation of China (Grant No. 51704267).

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Mansour, A.; Mesleh, R.; Abaza, M. New challenges in wireless and free space optical communications. *Opt. Lasers Eng.* **2017**, *89*, 95–108. [CrossRef]
2. Ghassemlooy, Z.; Arnon, S.; Uysal, M.; Xu, Z.; Cheng, J. Emerging Optical Wireless Communications-Advances and Challenges. *IEEE J. Sel. Areas Commun.* **2015**, *33*, 1738–1749. [CrossRef]
3. Yang, N.; Wang, L.; Geraci, G.; Elkashlan, M.; Renzo, M.D. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Commun. Mag.* **2015**, *53*, 20–27. [CrossRef]
4. Pattanayak, D.R.; Dwivedi, V.K.; Karwal, V.; Ansari, I.S.; Lei, H.; Alouini, M.S. On the Physical Layer Security of a Decode and Forward Based Mixed FSO/RF Co-Operative System. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 1031–1035. [CrossRef]
5. Yang, L.; Liu, T.; Chen, J.; Alouini, M.S. Physical-Layer Security for Mixed eta-mu and M-Distribution Dual-Hop RF/FSO Systems. *IEEE Trans. Veh. Technol.* **2018**, *67*, 12427–12431. [CrossRef]
6. Lei, H.; Dai, Z.; Ansari, I.S.; Park, K.H.; Pan, G.; Alouini, M.S. On Secrecy Performance of Mixed RF-FSO Systems. *IEEE Photonics J.* **2017**, *9*, 1–14. [CrossRef]
7. Hongjiang, L.; Haolun, L.; Ki-Hong, P.; Zhi, R.; Gaofeng, P.; Mohamed-Slim, A. Secrecy Outage Analysis of Mixed RF-FSO Systems with Channel Imperfection. *IEEE Photonics J.* **2018**, *10*, 1–13.
8. Lei, H.; Luo, H.; Park, K.H.; Ansari, I.S.; Lei, W.; Pan, G.; Alouini, M.S. On Secure Mixed RF-FSO Systems with TAS and Imperfect CSI. *IEEE Trans. Commun.* **2020**, *68*, 4461–4475. [CrossRef]

9. Wang, Y.; Zhan, Z.; Shen, Z. On Secrecy Performance of SWIPT Energy-Harvesting Relay Jamming Based Mixed RF-FSO Systems. *Photonics* **2022**, *9*, 374. [CrossRef]
10. Wang, Y.; Tong, Y.; Zhan, Z. On Secrecy Performance of Mixed RF-FSO Systems with a Wireless-Powered Friendly Jammer. *IEEE Photonics J.* **2022**, *14*, 1–8. [CrossRef]
11. Basar, E.; Renzo, M.D.; Rosny, J.D.; Debbah, M.; Zhang, R. Wireless Communications Through Reconfigurable Intelligent Surfaces. *IEEE Access* **2019**, *7*, 116753–116773. [CrossRef]
12. Alnwaimi, G.; Boujemaa, H. Hybrid RF/FSO communications through Reconfigurable Intelligent Surfaces in the presence of pointing errors. *Telecommun. Syst.* **2021**, *78*, 155–162. [CrossRef]
13. Odeyemi, K.O.; Aiyetoro, G.; Owolawi, P.A.; Olakanmi, O.O. Performance analysis of reconfigurable intelligent surface in a dual-hop DF relay empowered asymmetric RF/FSO networks. *Opt. Quantum Electron.* **2021**, *53*, 621. [CrossRef]
14. Han, L.; Hao, X. Performance analysis of mixed IRS-aided RF-FSO system with pointing errors and link blockage. *Optik* **2023**, *291*, 171386. [CrossRef]
15. Sikri, A.; Mathur, A.; Kaddoum, G. Signal Space Diversity-Based Distributed RIS-Aided Dual-Hop Mixed RF-FSO Systems. *IEEE Commun. Lett.* **2022**, *26*, 1066–1070. [CrossRef]
16. Wang, H.; Zhang, Z.; Zhu, B.; Zhang, Y. Performance Analysis of Hybrid RF-Reconfigurable Intelligent Surfaces Assisted FSO Communication. *IEEE Trans. Veh. Technol.* **2022**, *71*, 1–7. [CrossRef]
17. Wu, H.; Kang, D.; Ding, J.; Yang, J.; Wang, Q.; Wu, J.; Ma, J. Secrecy performance analysis in the FSO communication system considering different eavesdropping scenarios. *Opt. Express* **2022**, *30*, 41028–41047. [CrossRef]
18. Yuan, J.; Wang, X.; Jin, M.; Liu, W.; Wu, R.; Wei, Z.; Deng, D.; Liu, H. A Novel System of Mixed RF/FSO UAV Communication Based on MRR and RIS by Adopting Hybrid Modulation. *Photonics* **2022**, *9*, 379. [CrossRef]
19. Salhab, A.M.; Yang, L. Mixed RF/FSO Relay Networks: RIS-Equipped RF Source vs RIS-Aided RF Source. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 1712–1716. [CrossRef]
20. Saber, M.J.; Keshavarz, A.; Mazloum, J.; Sazdar, A.M.; Piran, M.J. Physical-Layer Security Analysis of Mixed SIMO SWIPT RF and FSO Fixed-Gain Relaying Systems. *IEEE Syst. J.* **2019**, *13*, 2851–2858. [CrossRef]
21. Wu, Q.; Zhang, R. Intelligent Reflecting Surface Enhanced Wireless Network via Joint Active and Passive Beamforming. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 5394–5409. [CrossRef]
22. Kumar, L.B.; Naik, R.P.; Krishnan, P.; Raj, A.A.B.; Majumdar, A.K.; Chung, W.-Y. RIS Assisted Triple-Hop RF-FSO Convergent with UWOC System. *IEEE Access* **2022**, *10*, 66564–66575. [CrossRef]
23. Liang, H.; Li, Y.; Miao, M.; Gao, C.; Li, X. Analysis of selection combining hybrid FSO/RF systems considering physical layer security and interference. *Opt. Commun.* **2021**, *497*, 127146. [CrossRef]
24. Yang, F.; Cheng, J.; Tsiftsis, T.A. Free-space optical communication with nonzero boresight pointing errors. *IEEE Trans. Commun.* **2014**, *62*, 713–725. [CrossRef]
25. Yousif, B.B.; Elsayed, E.E.; Alzalabani, M.M. Atmospheric turbulence mitigation using spatial mode multiplexing and modified pulse position modulation in hybrid RF/FSO orbital-angular-momentum multiplexed based on MIMO wireless communications system. *Opt. Commun.* **2019**, *436*, 197–208. [CrossRef]
26. Yousif, B.B.; Elsayed, E.E. Performance Enhancement of an Orbital-Angular-Momentum-Multiplexed Free-Space Optical Link Under Atmospheric Turbulence Effects Using Spatial-Mode Multiplexing and Hybrid Diversity Based on Adaptive MIMO Equalization. *IEEE Access* **2019**, *7*, 84401–84412. [CrossRef]
27. Xu, G.; Song, Z. Performance Analysis for Mixed—Fading and M-Distribution Dual-Hop Radio Frequency/Free Space Optical Communication Systems. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 1517–1528. [CrossRef]
28. The Wolfram Functions Site. 2015. Available online: https://functions.wolfram.com/HypergeometricFunctions/MeijerG/ (accessed on 1 August 2022).