On the Physical Layer Security of Mixed FSO-RF SWIPT System With Non-Ideal Power Amplifier

Rupender Singh, *Student Member, IEEE*, Meenakshi Rawat, *Member, IEEE*, and Anshul Jaiswal, *Member, IEEE*

***Abstract*—Free-space optical (FSO) links are contemplated as a potential paradigm to yield efficient point-to-point communication in wireless systems. Notably, these links are used to provide the proficient wireless connectivity between the radio frequency (RF) wireless network and the fiber optic-based network. To this end, more attention has been paid to mixed FSO-RF systems where single-hop FSO transmission and single-hop RF transmission configuration is used. In this paper, we propose a mixed FSO-RF dual-hop simultaneous wireless information and power transfer (SWIPT) relaying system in the presence of power amplifier (PA). It is assumed that FSO links suffer from Málaga (*M*)-turbulence with pointing errors and RF links experience the double shadowed Rician fading. Particularly, the physical layer security is analyzed by deriving the closed-form expressions for secrecy metrics such as secure outage probability, strictly positive secrecy capacity, and secrecy throughput. We consider the three scenarios: 1) FSO-side eavesdropping attack 2) RF-side eavesdropping attack 3) Simultaneous FSO- and RF-side eavesdropping attacks. The asymptotic approximations for the final results are also derived to obtain secrecy diversity order. The effect of SWIPT parameters and PA efficiency on the secrecy performance are then further investigated in detail. In summary, the results show that the reliability and security of the proposed system can be enhanced by utilizing efficient PAs at the RF front end depending on the eavesdropper's location and can also be controlled by the SWIPT parameters.**

***Index Terms*—Double shadowed Rician (DSR) fading, physical layer security (PLS), Málaga (*M*)-turbulence, mixed FSO-RF systems, power amplifier (PA), secrecy outage probability (SOP), strictly positive secrecy capacity (SPSC), secrecy throughput (ST).**

I. Introduction

A. Background

COMPARED with radio frequency (RF) wireless systems, free-space optical (FSO) communication has several advantages such as high bandwidth, high security at physical layer, short deployment time, large transmission capacity, immutability to RF interferences, and flexibility. Due to wide range of FSO applications in wireless back-haul networks and fiber backup, FSO communication has received significant attention over the decade. FSO communication utilizes the unlicensed optical spectrum for high security transmission through line-of-sight (LOS) at low cost [1]. In addition, FSO is also contemplated as a promising technology for the last mile problem in wireless systems. However, the applications of FSO communication on a broad scale are restricted due to many limiting factors, including strong path-loss, atmospheric turbulence and pointing error. Therefore, a dual-hop configuration for so-called mixed FSO-RF systems has been proposed in [2] to amalgamate the benefits of both FSO and RF technologies. The proposed system can be applied in a downlink environment where the high-speed FSO stream is demultiplexed to serve multiple RF users [2]–[8]. In a typical mixed FSO-RF system, the signals are propagated to the relay node (which serves as a base station) via the FSO link. Then, the converted and demultiplexed RF signals are imparted to the destination through an RF link.

Cooperative communication assists terminal nodes to communicate through relay nodes by exploiting the broadcast nature of wireless communication [9]. The relay-based approach can find its applications in green communication networks and 5G systems by improving transmission reliability, power efficiency, network connectivity, and service availability [7]–[9]. It also has rewarding merits such as hardware feasibility and deployment flexibility. However, the main bottleneck of power-constrained relay-based system is that it consists of low cost high power consuming elements such as power amplifiers (PAs). Particularly, when analyzing the performance of the system, the effects of hardware impairments including PA efficiency should be considered [9], [10]. This problem must be paid immediate attention because 70%-90% of the total power is consumed by the radio transmitters, especially at RF PA stage. Therefore, it is necessary to design PA aware data transmission schemes [11]. It is worth noting that a few studies in [9]–[11] analyzed the performance of single-and multi-relay networks by considering the effects of PAs. Although plenty of studies revealed that PA inefficiency is having a substantial impact on the performance of single- and multi-relay systems in the recent past. In the realistic scenario, the relays are non-ideal hardware, and they create non-linear distortions during the signal amplification due to its low quality. The previous studies in [12]–[16] investigated the performance of PA-based systems in terms of symbol error rate, power spectral density, the optimal power allocation, and the power efficiency for different relaying techniques. The studies adopted different PA non-linearity models to obtain the results; for instance, for instance, a few of them considered Bussgang linearization

Manuscript received April 21, 2021; revised June 29, 2021; accepted July 1, 2021. Date of publication July 7, 2021; date of current version August 13, 2021. This work was supported in part by the "Visvesvaraya Ph.D. Scheme," Digital India Corporation and Ministry of Electronics and Information Technology (MEITY), under Grant VISPHD-MEITY-2495, and in part by Science and Engineering Research Board, Government of India under Grant SRG/2020/000902. *(Corresponding author: Meenakshi Rawat.)*

The authors are with the Department of Electronics and Communication Engineering, Indian Institute of Technology Roorkee, Roorkee 247667, India (e-mail: rsingh1@ec.iitr.ac.in; meenakshi.rawat@ece.iitr.ac.in; anshul.jaiswal@ece.iitr.ac.in).

Digital Object Identifier 10.1109/JPHOT.2021.3095084

theory, which is different from our adopted non-ideal PA model. In contrast to these studies, we consider the mixed FSO-RF SWIPT system in the presence of FSO- and RF-side eavesdroppers. Moreover, the obtained analytical/numerical results on the PLS secrecy metrics such as SOP, SPSC, and ST, as well as our investigations on the effect of non-ideal PA on security, have not been presented before. In fact, the problem formulation in this study is completely different from the ones in the previous studies, e.g., [12]–[16], and also our analytical/numerical results and conclusion make this study unique. The numerical and the analytical results show that:

1) Secure transmission is largely affected by various parameters, including atmospheric turbulence conditions, pointing errors, and SWIPT parameters.
2) The PA efficiency affects the secrecy performance considerably. Depending on the location of the adversary, the system security and reliability can be controlled by the PA inefficiencies.
3) As long as the double shadowing becomes more severe, the proposed system is more susceptible to eavesdropping attacks.
4) The secrecy of the system can be enhanced by reducing the energy at the harvester, which costs the battery life of the RF receiver node.
5) While eavesdropping attacks can occur on any link but RF-side eavesdropping is always stronger compare to FSO-side eavesdropping.

On the other hand, next generation wireless sensor networks will incorporate the battery-operated sensor nodes. Due to limited energy budget, replacing or recharging the batteries is infeasible in many difficult-to-access scenarios (e.g., sensor nodes inserted into the human body or fixed in typical building structures, underground installed sensor nodes). To overcome such challenges, the concept of simultaneous wireless information and power transfer (SWIPT) technology was proposed to vanquish such challenges [17]–[21]. SWIPT allows both the processes of information decoding and energy harvesting at the sensor node simultaneously. Therefore, SWIPT presents tremendous potential to prolong the lifetime of sensor nodes. Since the batteries at receivers are charged from a part of signal energy, the power of information signal is reduced, which will lead to the compromise in the performance of the system [22]. Thus a few studies focused on secrecy performance of the SWIPT systems [23]–[25].

B. Related Work

Recently, by exploiting the random nature of time-varying wireless channels, the physical layer security (PLS) techniques are propounded as a potential solution to counteract the eavesdropping by the adversaries [26]–[30]. Therefore, several researchers considered the secure mixed RF-FSO (uplink) and mixed FSO-RF (downlink) communication systems and investigated the secure outage probability (SOP), strictly positive secrecy capacity (SPSC), and average secrecy capacity (ASC). For instance, the numerical studies of PLS for mixed RF-FSO systems were performed under various fading environments, including Rayleigh-$\mathcal{GG}$ [26], Nakagami-m-$\mathcal{GG}$ [32], [33], η-μ-M-turbulence [34], SWIPT mixed RF-FSO system [35] and SWIPT mixed RF-FSO systems with multiple antennas [36]. Subsequently, in these works, it was assumed that an adversary is located near the RF receiver, and the full channel state information (CSI) of the adversary channel is known to the information source. Moreover, many researchers have recently devoted their efforts to conduct the performance analysis under various fading scenarios for mixed FSO-RF systems. In these studies, the authors have analyzed the performance of mixed FSO-RF for various fading scenarios, including Gamma-Gamma ($\mathcal{GG}$)-Nakagami-m [2], [3], $\mathcal{GG}$-generalized-K [4], double generalized Gamma-Nakagami-m [5], Málaga(M)-turbulence-κ-μ [6], $\mathcal{GG}$-Rician [7], exponentiated-Weibull-Nakagami-m [8] and SWIPT mixed FSO-RF systems [32] under either the decode-and-forward (DF) or amplify-and-forward (AF) relaying schemes.

More recently, the PLS of Wyner's Model over optical links was introduced in [38]. Inherently, FSO links are considered more protected from unauthorized access than RF links due to the high directionality of the laser beam. However, in few scenarios, eavesdropping may occur due to optical beam divergence, atmospheric turbulence, pointing errors, and channel scattering. Therefore, in [39] and [40], it is pointed out that the adversaries can access the information through scattering over a non-line-of-sight (NLOS) channel and scattering over LOS channel (due to aerosol particles), respectively. In [38], it is highlighted that if both the adversary and the legitimate receiver are placed close to each other, then eavesdropping may be possible through FSO links. Then, in [1], the authors have shown that beam reflection due to the dust particles or blocked by solid objects may result in eavesdropping. Thereafter, the PLS secrecy of the FSO link was investigated over M-turbulence in [1]. Similarly, the PLS security metrics such as SOP, SPSC, and ASC were derived into unified form in the context of FSO communication in [38] and [41], respectively. In [42], secrecy analysis was conducted for a mixed RF-FSO system in which an adversary is accessing the secure information through the FSO link by collecting a fraction of optical power because of beam scattering. Hitherto, the performance of PLS for mixed FSO-RF systems has been investigated by a few studies. The authors in [43] have conducted the PLS secrecy analysis for the mixed FSO-RF system over $\mathcal{GG}$-Rayleigh fading scenario. In [44], the secrecy performance of the mixed FSO-RF SWIPT system was analyzed under DF relaying scheme. These reported works have considered the FSO side eavesdropping under full CSI of eavesdropper's channel. It is noteworthy that reported studies in [1]–[8], [31]–[36], [43], [44] are limited to the PLS secrecy analysis under the assumption of ideal PA deployment at the RF front end. However, in the practical scenario, the secrecy performance is highly impacted due to the non-negligible power consumption by PA. Hence, the effects of PA efficiency cannot be neglected in PLS secrecy analysis. Although the impact of hardware imperfections on the performance of mixed RF-FSO systems were investigated in a very few studies in [10], [45]. To model these hardware imperfections, the soft envelope limiter (SEL) PA non-linearities were considered in [45], while in [10] degradation PA model was used to characterize the hardware impairments. A recent

study in [46] analyzed the secrecy performance of hybrid RF-FSO system under hardware impairments by considering the degradation PA model. They considered the scenario where only RF eavesdropper intercepted the secure information. Unlike these studies, we propose a different system structure for a mixed FSO-RF system under hardware imperfections in which all RF receivers explore the SWIPT technique to collect energy from the received wireless signals sent by the relay. Moreover, it is assumed that both FSO- and RF-side eavesdroppers can overhear the intended information separately and simultaneously. However, the consideration of non-ideal PA poses the major challenge on obtaining the novel closed-form expressions for PLS metrics which is hugely improved in our work. To the best of the author's knowledge, no study has considered the effect of PA efficiency on the secrecy performance of mixed FSO-RF or mixed RF-FSO systems. In addition, the previous works have studied the secrecy performance of only SWIPT mixed RF-FSO systems, and the secrecy performance of SWIPT mixed FSO-RF systems is still an open issue.

C. Contribution

The studies, as mentioned earlier, motivate exploring the effects of non-ideal (realistic) PA inefficiencies on PLS secrecy of SWIPT mixed FSO-RF system in which information is wiretapped either from the FSO side or RF side eavesdroppers. In particular, the SWIPT mixed FSO-RF system is proposed in which a non-ideal PA is deployed at the RF front end. Specifically, we focus on the trade-off between the consumed (or processed) and transmitted power directly by using the effective efficiencies of PA. The efficiency degradation model is adopted to characterize the different PA classes (i.e., class A, B, C). This model signifies that the reduction in consumed power cannot be translated into transmitted power because of PA nonlinearities. The RF link is subject to double shadowed Rician (DSR) fading whereas FSO link experiences M-turbulence. Recently introduced DSR fading has the ability to characterize the double shadowing effects of RF channels that may arise due to varying levels of shadowing and moving obstacles [47]. The physical model of DSR fading can illustrate the environment in which the blockages (e.g., buildings, trees, cars, people, and mountains) between transmitter and receiver path may cause primary shadowing followed by secondary shadowing due to obstacles in the vicinity of the transmitter/receiver. It is worth remarking that well-known fading conditions such as shadowed Rician, shadowed Rayleigh Nakagami-q, Rician, and Rayleigh can be obtained as special cases of DSR fading. On the other hand, M-distribution is regarded because of its generality to model the conventional turbulence models (i.e., both generalized-K and lognormal) and its ability to characterize the irradiance for a wide range (weak to strong) turbulence conditions. It is noteworthy that the applications of the proposed system can be seen in future technologies (i.e., loon by Google), satellite-aerial-terrestrial networks, and cooperative satellite-terrestrial systems to provide wireless connectivity in rural and remote areas. The main contribution of our study are summarized as follows:

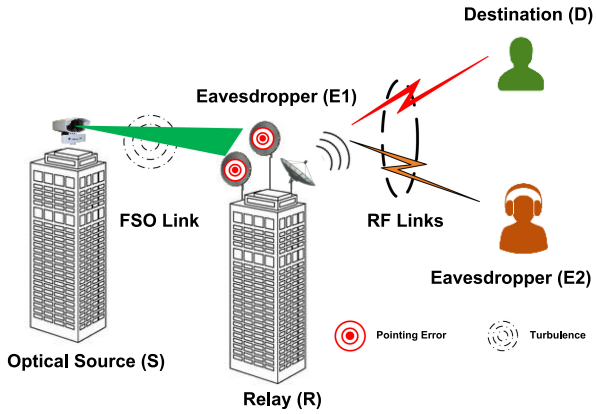

Fig. 1. Wireless relay network model for the proposed system.

1) We propose a mixed FSO-RF SWIPT system for three different scenarios; in the first scenario, it is assumed that only the FSO link is under eavesdropping attack. Secondly, it is assumed that the eavesdropper is overhearing only the RF link. Finally, in the last scenario, it is assumed that two active eavesdroppers are wiretapping both FSO and RF links simultaneously.
2) We derive the probability density function (PDF) and cumulative distribution function (CDF) of the signal-to-noise ratio (SNR) of the RF links with energy harvesting technology in the case with non-ideal PA at the relay.
3) We evaluate the PLS secrecy of the proposed relaying system with non-ideal PA at RF front end. In particular, we derive the expressions of PLS secrecy metrics such as SOP, SPSC, and secrecy throughput (ST) into closed-form. Furthermore, we also investigate the effects of FSO link parameters, RF SWIPT parameters, and PA efficiency on the secrecy performance.
4) Afterwards, the asymptotic expressions of the derived results are determined to obtain the secrecy diversity order of the proposed system. Moreover, the obtained results are compared with the previous works to validate the usefulness of the proposed system. Additionally, as a special case, the M-turbulence/Rayleigh fading scenario is illustrated.

II. System and Channel Model

As illustrated in Fig. 1, a downlink mixed FSO-RF SWIPT system is proposed where an optical source (S) transmits secure information to DF relaying based relay (R) over M-turbulence channel ($S \rightarrow R$) in the presence of pointing errors under the heterodyne (HD) detection and the intensity modulation with direct detection (IM-DD). The relay R consists of an optical filter, a photo-detector (PD), a demodulator, a modulator with a local oscillator (LO), and an RF antenna and forwards the secure information to the RF receiver (D) over an independent and identical DSR fading channel ($R \rightarrow D$). It is also assumed that a non-ideal PA is deployed at R as shown in Fig. 2(a). During transmission, the eavesdroppers ($E1$ and $E2$) are intercepting

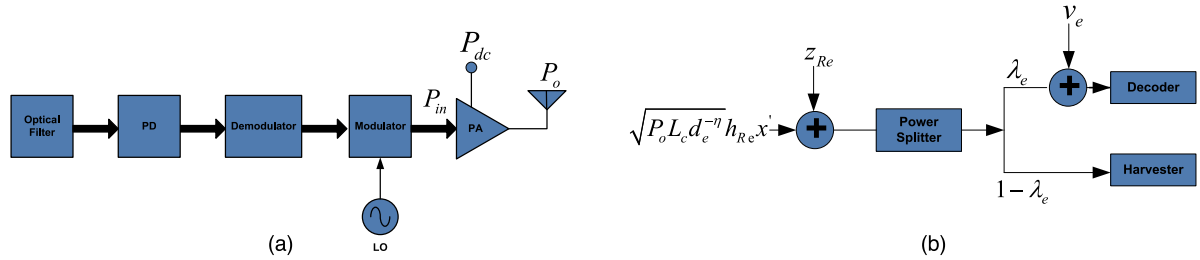

Fig. 2. (a) Relay model with non-ideal PA at RF end (b) Power splitting model at energy harvester.

the secure information through the LOS scattering FSO link ($S \rightarrow E1$) and RF links ($R \rightarrow E2$), respectively. The transmission bandwidth is restricted by the bandwidth of the RF link. All the RF receivers (*D* and *E1*) are accoutred with rechargeable batteries and adopt the power splitting (PS) method to proportionate the energy harvesting and information decoding from the received RF signal. In other words, the received RF signal is split into two portions, out of which $\lambda_e (0 \leq \lambda_e \leq 1; e \in \{D, E2\})$ proportion is utilized to decode the secure information, and the rest of the signal power is used by the energy harvester. The illustration of PS approach is shown in Fig. 2(b). The system parameters of the proposed system with definitions are provided in Table I.

A. Power Amplifier Model

To take the non-ideal PA effects into account, we assume that the relay *R* is equipped with a non-ideal PA as shown in the Fig. 2(a). The PA is responsible for the majority of the power losses. Several studies derive the generic expression for the losses and efficiency of PA [9], [11]. For instance, the maximum theoretical effi ciency of ideal class B amplifier at $P_o = P_{\max}$ can be obtained as [50]

$$\frac{P_o}{P_c} = \frac{\pi}{4} \tag{1}$$

For the low values of P_o, the PA efficiency is related to the square root of P_o as [10]

$$\varepsilon_{PA} = \frac{P_o}{P_c} = \varepsilon_{\max} \sqrt{\frac{P_o}{P_{\max}}} \tag{2}$$

where $\varepsilon_{\max} \in [0, 1]$ is denoting the maximum PA efficiency which is achieved only when $P_o = P_{\max}$. The maximum PA efficiencies for different classes of PA are provided in the Table II. If we want to change efficiency we have to change the hardware [51]. Another approach to control the PA efficiency is removing higher order harmonics which are responsible for heat dissipation. At $\varepsilon_{\max} = 0$, the PA provides zero output power (i.e., $P_o = 0$ dBm) and all the power is dissipated. In [50], the authors have expressed the effective PA efficiency as

$$\varepsilon_{eff} = \frac{P_o}{P_c} = \varepsilon_{\max} \left(\frac{P_o}{P_{\max}} \right)^{\ell}, \quad P_o \leq P_{\max} \tag{3}$$

where ℓ is related to the PA classes that can vary between $[0, 1]$. In [52, Eq. (2.14)], and [53, Eq. (6) and Table I], it is shown that at $\ell = 0.5$, the measurements of efficiency for different classes are accurate as the PA output power linearly increases with P_c at $\ell = 0.5$. Therefore, in harmony with the previous studies, we adopt the PA model of (3) in this study. In Fig. 3(a), the ε_{eff} is illustrated in percentage as a function of P_c. It can be noted that at $P_o = P_{\max}$, ε_{eff} attained its maximum value $\varepsilon_{\max}$; further increment in P_c may result in a reduction in ε_{eff}, which may damage the PA. It can also be seen that the P_o is reached at its peak at lower P_c for higher $\varepsilon_{\max}$with comparing to lower $\varepsilon_{\max}$. In (3), P_c can also be written in terms of P_{dc} and P_{in} as $P_c = P_{dc} + P_{in}$. Usually, P_{dc} remains constant for a particular PA class, while increasing P_{in} may result in increasing P_c. It is worth noting that $P_{\max}$ provides power constraint $P_o \leq P_{\max}$ at the relay and also affects the ε_{eff}. As illustrated in Fig. 3(b), the low PA output power is obtained at small values of PA input power due to the low efficiency. Moreover, high values of PA input power may improve the PA output power up to saturation point under power constraint $P_o \leq P_{\max}$. Finally, with an ideal PA, we have $\varepsilon_{\max} = 1, \ell = 0$, and $P_{\max} \rightarrow \infty$ in (3).

B. FSO Links

The effects of pointing errors, path-loss and atmospheric turbulence are considered and received optical information by *R* and *E1* can be expressed as [44]

$$y_{Sj} = \varepsilon^{r/2} x I_{Sj}^{r/2} + z_{Sj} \tag{4}$$

where $j \in \{R, E1\}$, x is the message symbol with $E[|x|^2] = 1$, z_{Sj} denotes zero mean complex valued additive white Gaussian noise (AWGN) with variance N_0 and I_{Sj} represents the coefficients of FSO link, which is described as the joint effects of pointing errors (I_p), path-loss (I_l), and atmospheric turbulence (I_a). Mathematically, it can be given by $I_{Sj} = I_a I_l I_p$. Here, it is assumed that the path-loss I_l remains unchanged for a given link distance and the provided weather conditions. Also, the zero-boresight pointing errors are considered that can be expressed as $I_p \simeq A_0 \exp(-2D^2/w_{z_{eq}}^2)$ where $A_0 = [erf(v)]^2$, $erf(\bullet)$ is denoting error function, $w_{z_{eq}}^2 = w_z^2[\sqrt{\pi} erf(v)/2v \exp(-v^2)]$, $v = \sqrt{\pi}\theta/(\sqrt{2} w_z)$[29]. The PDF of I_p is given as $f_{I_p}(I_p) = (\xi^2/A_0^{\xi^2}) I_p^{\xi^2 - 1}$; $0 \leq I_p \leq A_0$ [1], where $\xi = w_{z_{eq}}^2 / 2\sigma_s^2$. The *M*-distribution is adopted to characterize the atmospheric turbulence I_a and its PDF can be written as [6]

$$f_{I_a}(I_a) = A \sum_{q=1}^{\beta} \partial_q I_a K_{\alpha - q} \left(2 \sqrt{\frac{\alpha \beta I_a}{g\beta + \Omega'}} \right), \quad I_a > 0 \tag{5}$$

TABLE I
DEFINITIONS OF SYSTEM AND CHANNEL PARAMETERS

Parameters	Definitions
h_{Re}	RF channel coefficient
r	Parameter related to the type of detection scheme ($r=1$ for HD and $r=2$ for IM-DD)
ξ	Ratio between beam radius and jitter at receiver
ε	Photoelectric conversion ratio
α	FSO link parameter related to the effective number of large-scale cells of the scattering process ($\alpha>0$)
β	Amount of fading of FSO link
ρ	Amount of scattering power coupled to the LOS component $\rho\in[0,1]$
ϕ_A	Phase of the LOS term
ϕ_B	Phase of the coupled-to-LOS scatter
w_z	Beam waist
θ	Radius of the detection aperture
D	Radial displacement
$w_{z_{eq}}^2$	Equivalent beam width
σ_s	Jitter standard derivation
Ω	Average power of the LOS term
$\mu_{I_{SR}}, \mu_{I_{SE1}}$	Electrical SNRs of *S-R* and *S-E1* links
λ_D, λ_{E2}	Power used to decode the information at *D* and *E2,* respectively
$\bar{\gamma}_{RD}, \bar{\gamma}_{RE2}$	Average SNRs of the *R-D* and *R-E2* link, respectively
d_D, d_{E2}	Distance between {*R, D*} and {*R, E2*} in meters, respectively
m_s	Inverse Nakagami-*m* parameter
m_d	Nakagami-*m* parameter
k	Rician parameter
η	Path-loss exponent $\eta\in[2.7,3.1]$
L_c	Propagation loss constant of RF link
P_o	PA output power at *R*
$P_{\max}$	Maximum PA output power
P_c	PA consumed power
P_{dc}	PA bias power
P_{in}	PA input power
$G_{p,q}^{m,n}(\bullet)$	Meijer-G function [48, Eq. (07.34.02.0001.01)]
$G_{p,q;t,s;w,x}^{m,n;r,s;w,x}[\bullet]$	Extended generalized bivariate Meijer-G function [49, Eq. (1)]
${}_2F_1(\bullet,\bullet;\bullet;)$	Gaussian hypergeometric function [48, Eq. (07.23.02.0001.01)]
$(a)_n$	Pochhamer symbol [48, Eq. (06.10.02.0001.01)]

where

$$A \triangleq \frac{2\alpha^{\alpha/2}}{g^{1+\alpha/2}\Gamma(\alpha)}\left(\frac{g\beta}{g\beta+\Omega'}\right)^{\beta+\alpha/2} \tag{6}$$

$$\partial_q \triangleq \binom{\beta-1}{q-1}\frac{(g\beta+\Omega')^{1-q/2}}{\Gamma(q)}\left(\frac{\Omega'}{g}\right)^{q-1}\left(\frac{\alpha}{\beta}\right)^{q/2}, \tag{7}$$

$g=2\Im_0(1-\rho)$ describes the average power received by off-axis eddies due to scattered component, $\Omega'=\Omega+2\Im_0\rho+2\sqrt{2\rho\,\Omega}\cos(\phi_A-\phi_B)$, and $2\Im_0$ represent the average power of total scatter components.

The corresponding SNR can be written from (4) as $\gamma_{Sj}=(\varepsilon I_{Sj})^{r_{Sj}}/N_0$. Under the assumption of *M*-distributed turbulence, the CDF of γ_{Sj} can be obtained as

$$F_{\gamma_{Sj}}(\gamma)=D_{Sj}\sum_{q=1}^{\beta_{Sj}}c_{q_{Sj}}G_{r+1,3r+1}^{3r,1}\left[\frac{E_{Sj}\gamma}{\mu_{r_{Sj}}}\middle|\begin{matrix}1,\Upsilon_1^{Sj}\\ \Upsilon_2^{Sj},0\end{matrix}\right] \tag{8}$$

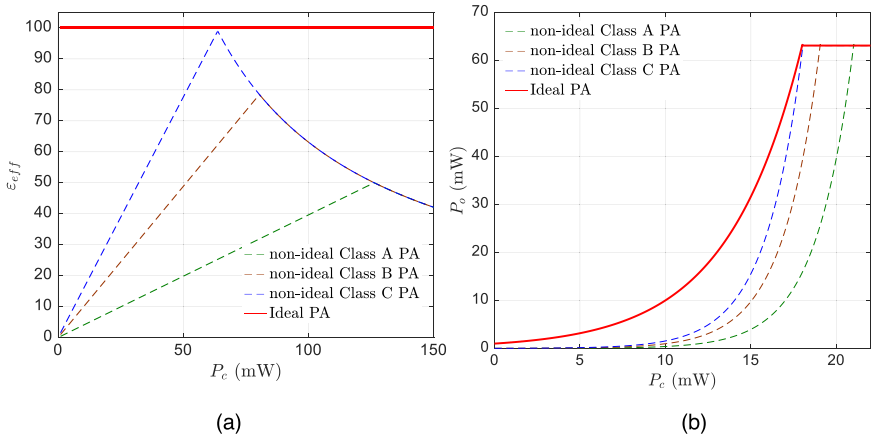

Fig. 3. (a) Effective PA efficiency for different PA classes (b) PA output power for different PA classes.

TABLE II
MAXIMUM PA EFFICIENCIES [52]

PA Class	$\varepsilon_{\max}$
Non-ideal class A PA	0.50
Non-ideal class B PA	0.785
Non-ideal class C PA	0.90
Ideal PA	1

where $c_q = b_q r^{\alpha+q-1}$, $D = \xi^2 A/2^r(2\pi)^{r-1}$, $b_q = \partial_q[\alpha\beta/(g\beta+\Omega')]^{-(\alpha+q)/2}$, $E = B^r/r^{2r}$, $B = \xi^2\alpha\beta(g+\Omega')/[(\xi^2+1)(g\beta+\Omega')]$, $\Upsilon_1 = [\Delta(r,\xi^2+1)]$, $\Upsilon_2 = [\Delta(r,\xi^2), \Delta(r,\alpha), \Delta(r,q)]$, where $\Delta(x,y)$ is defined as $\Delta(x,y) = [\frac{y}{x}, \frac{y+1}{x}, \ldots \frac{x+y-1}{x}]$.

With the help of [48, Eq. (07.34.21.0084.01)] and (8), the PDF of γ_{Sj} can be determined as

$$f_{\gamma_{Sj}}(\gamma) = \frac{D_{Sj}E_{Sj}}{\mu_{r_{Sj}}} \sum_{q=1}^{\beta_{Sj}} c_{q_{Sj}} G_{r+2,3r+2}^{3r,2}\left[\frac{E_{Sj}\gamma}{\mu_{r_{Sj}}}\middle| \begin{matrix} -1, 0, \Upsilon_1^{Sj}-1 \\ \Upsilon_2^{Sj}-1, 0, -1 \end{matrix}\right] \tag{9}$$

Note that as a special case, when $\{\rho = 1, g = 0, \Omega' = 1\}$, the *M*-turbulence model can be transformed into $\mathcal{I}\mathcal{I}$ turbulence model.

C. RF Links

The received signal by *D* and *E2* under short-term RF fading and path-loss effects can be expressed as [26]

$$y_{Re} = \sqrt{\lambda_e}\left(\sqrt{P_o L_c d_e^{-\eta}} h_{Re} x' + z_{Re}\right) + v_e \tag{10}$$

where x' is the retrieved message symbol at *R* and z_{Re} and v_e denote zero mean AWGN noise with variance N_0 and σ_e^2, respectively. The corresponding SNR of y_{Re} is then written as [44]

$$\gamma_{Re} = \frac{\lambda_e L_c (\varepsilon_{\max} P_c)^{1/1-\ell} |h_{Re}|^2}{d_e^{\eta} P_{\max}^{\ell/1-\ell}(\lambda_e N_0 + \sigma_e^2)} \tag{11}$$

It is recalled that RF link is subject to DSR fading, the PDF of $|h_{Re}|^2$ for DSR distributed fading channel can be enunciated by using [45] as

$$f_{|h_{Re}|^2}(\gamma) = \frac{\overline{\gamma}_{Re}^{m_{s_{Re}}} m_{s_{\mathrm{Re}}} (m_{s_{Re}}-1)^{m_{s_{Re}}} (1+k_{Re})}{(\gamma(1+k_{Re}) + (m_{s_{Re}}-1)\overline{\gamma}_{Re})^{m_{s_{Re}}+1}} \left(\frac{m_{d_{Re}}}{m_{d_{Re}}+k_{Re}}\right)^{m_{d_{Re}}}$$
$$ {}_2F_1\left(m_{d_{Re}}, m_{s_{Re}}+1; 1; \frac{k_{Re}(1+k_{Re})\gamma}{(m_{d_{Re}}+k_{Re})(\gamma(1+k_{Re}) + (m_{s_{Re}}-1)\overline{\gamma}_{Re})}\right) \tag{12}$$

which can also be expressed in terms of Meijer's G function by utilizing [48, Eq. (07.23.02.0001.01)] and [54, Eq. (8.4.2.5)] as follows

$$f_{|h_{Re}|^2}(\gamma) = \tau_{Re} \sum_{i=0}^{\infty} H_{Rei} G_{1,1}^{1,1}\left[\tau_{Re}\gamma \middle| \begin{matrix} -m_{s_{Re}} \\ i \end{matrix}\right] \tag{13}$$

where $\tau_{Re} = \frac{(1+k_{Re})}{(m_{s_{Re}}-1)\overline{\gamma}_{Re}}$ and $H_{Re_i} = \frac{m_{s_{Re}} k_{Re}^i (m_{d_{Re}})_i (m_{s_{Re}}+1)_i}{(m_{d_{Re}}+k_{Re})^i i!(1)_i \Gamma(m_{s_{Re}}+1+i)} (\frac{m_{d_{Re}}}{m_{d_{Re}}+k_{Re}})^{m_{d_{Re}}}$.

The corresponding CDF of $|h_{Re}|^2$ can be derived, using (13) and [55, Eq. (26)], to be

$$F_{|h_{Re}|^2}(\gamma) = \sum_{i=0}^{\infty} H_{Re_i} G_{2,2}^{1,2}\left[\tau_{Re}\gamma \middle| \begin{matrix} 1-m_{s_{Re}}, 1 \\ i+1, 0 \end{matrix}\right] \tag{14}$$

Note that the considered DSR distribution is advantageous to characterize the RF link as it includes other well-known traditional fading distributions for fixed values of fading parameters, i.e., Shadowed Rician distribution ($m_s \to \infty, m_d, k$), Shadowed Rayleigh distribution ($m_s \to \infty, m_d \to 0, k$), Nakagami-$q$ distribution ($m_s \to \infty, m_d \to 0.5, k$), Rician distribution ($m_s \to \infty, m_d \to \infty, k$), and Rayleigh distribution ($m_s \to \infty, m_d \to \infty, k \to 0$).

After performing necessary algebraic manipulations, the PDF and CDF of γ_{Re} can be obtained, respectively, as

$$f_{\gamma_{Re}}(\gamma) = \tau_{Re} \sum_{i=0}^{\infty} H_{Re_i} \Xi_e G_{1,1}^{1,1}\left[\Xi_e \tau_{Re}\gamma \middle| \begin{matrix} -m_{s_{Re}} \\ i \end{matrix}\right] \tag{15}$$

$$F_{\gamma_{Re}}(\gamma) = \sum_{i=0}^{\infty} H_{Re_i} G_{2,2}^{1,2}\left[\Xi_e \tau_{Re}\gamma \,\middle|\, \begin{matrix} 1-m_{s_{Re}}, 1 \\ i+1, 0 \end{matrix}\right] \tag{16}$$

where $\Xi_e = \frac{d_e^{\eta}(\lambda_e N_0 + \sigma_e^2) P_{\max}^{\ell/1-\ell}}{\lambda_e L_c (\varepsilon_{\max} P_c)^{1/1-\ell}}$.

Note that the derived PDF and CDF given by (15) and (16), respectively, are convergent with increasing number of terms i. The test of convergence is carried out using d'Alembert's ratio test for the infinite series of (15) and (16). Accordingly, under the following condition, the convergence of infinite series can be testified.

$$\lim_{i\to\infty}\left|\frac{a_{i+1}}{a_i}\right| < 1 \tag{17}$$

where a_i is denoting the i^{th} term in the infinite series.

The i^{th} term in the series expansion of CDF in (16) is

$$a_i = \frac{m_{s_{\mathrm{Re}}} k_{Re}^i (m_{d_{Re}})_i \left(m_{s_{\mathrm{Re}}}+1\right)_i}{(m_{d_{Re}}+k_{Re})^i i! (1)_i \Gamma\left(m_{s_{\mathrm{Re}}}+1+i\right)} \times \left(\frac{m_{d_{Re}}}{m_{d_{Re}}+k_{Re}}\right)^{m_{d_{Re}}} G_{2,2}^{1,2}\left[\Xi_e \tau_{Re}\gamma \,\middle|\, \begin{matrix} 1-m_{s_{Re}}, 1 \\ i+1, 0 \end{matrix}\right] \tag{18}$$

Therefore,

$$\frac{a_{i+1}}{a_i} = \frac{k_{Re}\left(m_{d_{Re}}+i+1\right)}{\left(m_{d_{Re}}+k_{Re}\right)(i+1)(i+2)} \frac{G_{2,2}^{1,2}\left[\Xi_e \tau_{Re}\gamma \,\middle|\, \begin{matrix} 1-m_{s_{Re}}, 1 \\ i+2, 0 \end{matrix}\right]}{G_{2,2}^{1,2}\left[\Xi_e \tau_{Re}\gamma \,\middle|\, \begin{matrix} 1-m_{s_{Re}}, 1 \\ i+1, 0 \end{matrix}\right]} \tag{19}$$

From (19), it is pronounced that infinite series in (15) and (16) are convergent, considering the fact that the order of i in the numerator is lesser than the order of i in the denominator, and also, for all values of i, the ratio of two Meijer's G function results in a non-zero real number.

Remark 1: The proposed mixed FSO-RF SWIPT system can be seen as a generalized version of the system models considered in previous studies [5], [6], [37]. For instance, the proposed system is similar to the system model presented in [5] for $m_s \to \infty$ with the assumption of no energy harvesting at the receiver. The system considered in [6] can be obtained from the proposed system by setting $\{m_s \to \infty, m_d \to \infty, k\}$ and $\{\rho = 1, g = 0, \Omega' = 1\}$ in the absence of the SWIPT concept. Furthermore, our model leads to the system model discussed in [37] when $\{m_s \to \infty, m_d \to \infty, k \to 0\}$ and $\{\rho = 1, g = 0, \Omega' = 1\}$.

D. End-to-End SNR

When a DF relaying scheme is utilized at *R*, the end-to-end SNR i.e., $\gamma_{eq,D}$ received by *D* can be enunciated as[1]

$$\gamma_{eq,D} = \min\left(\gamma_{SR}, \gamma_{RD}\right) \tag{20}$$

From (20), the CDF of $\gamma_{eq,D}$ can be obtained as

$$F_{\gamma_{eq,D}}(\gamma) = \Pr\left\{\min\left(\gamma_{SR}, \gamma_{RD}\right) < \gamma_{eq,D}\right\} = F_{\gamma_{SR}}(\gamma) + F_{\gamma_{RD}}(\gamma) - F_{\gamma_{SR}}(\gamma) F_{\gamma_{RD}}(\gamma) \tag{21}$$

After placing (8) and (16) into (21), the CDF of $\gamma_{eq,D}$ can be written as

$$\begin{aligned} F_{\gamma_{eq,D}}(\gamma) = {} & D_{SR} \sum_{q=1}^{\beta_{SR}} c_{q_{SR}} G_{r+1,3r+1}^{3r,1}\left[\frac{E_{SR}\gamma}{\mu_{r_{SR}}} \,\middle|\, \begin{matrix} 1, \Upsilon_1^{SR} \\ \Upsilon_2^{SR}, 0 \end{matrix}\right] \\ & + \sum_{i=0}^{\infty} H_{RD_i} G_{2,2}^{1,2}\left[\Xi_D \tau_{RD}\gamma \,\middle|\, \begin{matrix} 1-m_{s_{RD}}, 1 \\ i+1, 0 \end{matrix}\right] \\ & - D_{SR} \sum_{q=1}^{\beta_{SR}} \sum_{i=0}^{\infty} H_{RD_i} c_{q_{SR}} G_{r+1,3r+1}^{3r,1}\left[\frac{E_{SR}\gamma}{\mu_{r_{SR}}} \,\middle|\, \begin{matrix} 1, \Upsilon_1^{SR} \\ \Upsilon_2^{SR}, 0 \end{matrix}\right] \\ & G_{2,2}^{1,2}\left[\Xi_D \tau_{RD}\gamma \,\middle|\, \begin{matrix} 1-m_{s_{RD}}, 1 \\ i+1, 0 \end{matrix}\right] \end{aligned} \tag{22}$$

Upon expanding Meijer's G function at high SNR by using [48, Eq. (07.34.06.0006.01)] and after some algebraic manipulations, the asymptotic CDF of $\gamma_{eq,D}$ is obtained as

$$F_{\gamma_{eq,D}}^{\infty}(\gamma) \underset{\mu_{r_{SR}} >> 1}{\cong} F_{\gamma_{SR}}^{\infty}(\gamma) + F_{\gamma_{RD}}^{\infty}(\gamma) - F_{\gamma_{SR}}^{\infty}(\gamma) F_{\gamma_{RD}}^{\infty}(\gamma) \tag{23}$$

where

$$F_{\gamma_{SR}}^{\infty}(\gamma) = D_{SR} \sum_{q=1}^{\beta_{SR}} c_{q_{SR}} \sum_{l=1}^{3r} \left(\frac{\mu_{r_{SR}}}{E_{SR}\gamma}\right)^{-\Upsilon_{2_l}^{SR}} \frac{\prod_{p=1, p\neq l}^{3r} \Gamma\left(\Upsilon_{2_p}^{SR} - \Upsilon_{2_l}^{SR}\right)}{\left(1+\Upsilon_{2_l}^{SR}\right) \prod_{p=2}^{r+1} \Gamma\left(\Upsilon_{1_p}^{SR} - \Upsilon_{2_l}^{SR}\right)} \tag{24}$$

$$F_{\gamma_{RD}}^{\infty}(\gamma) = \sum_{i=0}^{\infty} H_{RD_i} (\Xi_D \tau_{RD}\gamma)^{i+1} \frac{\Gamma(-i-1)\Gamma\left(m_{s_{RD}}+i+1\right)}{\Gamma(i+2)} \tag{25}$$

In (24), $\Upsilon_{u_v}^{SR}$ is representing the v^{th}term of Υ_u^{SR}.

III. Physical Layer Secrecy Analysis

In what follows, the secrecy capacity is firstly described as the maximum rate of transfer of secure information over the reliable link between transmitter and receiver. At the same

[1]The approximated end-to-end SNR with variable gain AF relaying scheme is similar to (21), as testified in literature [2], [3], and [33].

time, the eavesdropper is unable to intercept the link. Therefore, achievable secrecy rate can be mathematically written as

$$C_o = [C_{eq,D} - C_Z]^+ = \begin{cases} [C_{eq,D} - C_Z], & \text{for } \gamma_{eq,D} > \gamma_Z \\ 0, & \text{otherwise} \end{cases} \tag{26}$$

where $Z \in \{E1, E2\}$, $[\Delta]^+ \triangleq \max(0, \Delta)$, $\max(.)$ describes the maximum of the arguments, $C_{eq,D} = \log_2(1 + \gamma_{eq,D})$ and $C_Z = \log_2(1 + \gamma_Z)$ are denoting the channel capacities of legitimate link and eavesdropper's link, respectively and γ_Z is representing the SNR at *E1* (or *E2*), respectively. Next, we define the PLS performance metric i.e., SOP which is elucidated as the probability that C_o falls below the target secrecy rate R_o. Usually, the SOP analysis allows determining the probability that the transmitted information is secretly overheard by the eavesdropper. Mathematically, for the considered scenario, the SOP can be expressed as

$$P_{out}(R_o) = \Pr[C_o \le R_o | \gamma_{eq,D} > \gamma_Z] \Pr[\gamma_{eq,D} > \gamma_Z] + \Pr[\gamma_{eq,D} \le \gamma_Z] \tag{27}$$

In the following, we perform the SOP analysis and also derive the expressions for SPSC and ST. We consider three scenarios: 1) First in which it is assumed that only the FSO link encounters eavesdropping attacks 2) Second in which the information is leaked to the RF eavesdropper only 3) Third in which both eavesdroppers *E1* and *E2* can intercept the secure information simultaneously.

A. Scenario 1: Eavesdropping on FSO Link Only

Here we perform secrecy analysis for the case where a passive eavesdropper *E1* is intercepting the confidential information through FSO link. In this case, the transmitters (*S* and *R*) has no choice but to adopt constant target secrecy rate as R_o. As long as $C_o > R_o$, the perfect secure link is established between *S* and *D*, otherwise the secrecy is compromised and information is leaked to *E1*.

1) SOP: After performing some mathematical manipulation, (27) can be further obtained as [36]

$$P_{out}(R_o) = \Pr\left(\gamma_{eq,D} \le 2^{R_o}(1 + \gamma_{SE1}) - 1 | \gamma_{eq,D} > \gamma_{SE1}\right) \Pr(\gamma_{eq,D} > \gamma_{SE1}) + \Pr(\gamma_{eq,D} \le \gamma_{SE1}) \tag{28}$$

which can also be expressed as

$$P_{out}(R_o) = \int_0^\infty \int_{\gamma_{SE1}}^{2^{R_o}(1+\gamma_{SE1})-1} f_{\gamma_{eq,D}}(\gamma_{eq,D}) f_{\gamma_{SE1}}(\gamma_{SE1})\, d\gamma_{eq,D} d\gamma_{SE1} + \int_0^\infty \int_0^{\gamma_{SE1}} f_{\gamma_{eq,D}}(\gamma_{eq,D}) f_{\gamma_{SE1}}(\gamma_{SE1})\, d\gamma_{eq,D} d\gamma_{SE1} \tag{29}$$

Due to intractability in obtaining the (29) into closed-form, the lower bound of the SOP for $\gamma_{SE1} >> 1$ is derived as follows [24]

$$P_{out}^L(R_o) = \int_0^\infty F_{\gamma_{eq,D}}\left(2^{R_o}\gamma_{SE1}\right) f_{\gamma_{SE1}}(\gamma_{SE1})\, d\gamma_{SE1} \tag{30}$$

On plugging (9) and (22) into (30) and applying [48, Eq. (07.34.21.0011.01), the resulting SOP is obtained as (31), shown at the bottom of the page, where $\Re_1 = \Xi_D \frac{2^{R_o}\tau_{RD}\mu_{r_{SE1}}}{E_{SE1}}$ and $\Re_2 = \frac{2^{R_o}E_{SR}\mu_{r_{SE1}}}{E_{SE1}\mu_{r_{SR}}}$.

Substituting (9) and (23) into (30) and using [48, Eq. (07.34.21.0009.01)], we have the asymptotic lower bound of SOP at high SNR in (32), shown at the bottom of the next page, where $H_t = \frac{\prod_{p=1,p\neq t}^{3r}\Gamma(\Upsilon_{2_p}^{SR} - \Upsilon_{2_t}^{SR})}{(1+\Upsilon_{2_t}^{SR})\prod_{p=2}^{r+1}\Gamma(\Upsilon_{1_p}^{SR} - \Upsilon_{2_t}^{SR})}$ and $M_i = \frac{\Gamma(-i-1)\Gamma(m_{s_{RD}}+i+1)}{\Gamma(i+2)}$.

Next, we evaluate the secrecy diversity order of the proposed system to obtain useful insights. For this purpose, the secrecy diversity order can be defined as asymptotic ratio of the logarithmic $P_{out}^L(R_o)$ to the logarithmic SNR (i.e., $G_d^o = -\lim_{\text{SNR}\to\infty} \log(P_{out}^L)/\log(\text{SNR})$) [32], [44]. The G_d^o is usually described as the slope of SOP at high SNR. From (32), the G_d^o can be evaluated as

$$G_d^o = \min\left(\frac{\xi_{SR}^2}{r}, \frac{\alpha_{SR}}{r}, \frac{q}{r}, 0\right) = 0 \tag{33}$$

Here, it is assumed that the average SNR of the FSO link $\mu_{r_{SR}}$ is varied while $\overline{\gamma}_{RD}$ is kept fixed. The diversity order of zero implies the presence of zero-floor in SOP performance. Further,

$$P_{out}^L(R_o) = D_{SE1}\sum_{q=1}^{\beta}\sum_{i=0}^{\infty} c_{q_{SE1}} H_{RD_i} G_{3r+4,r+4}^{3,3r+2}\left[\Re_1 \middle| \begin{matrix} 1-m_{s_{RD}}, 1, 1-\Upsilon_2^{SE1}, 0, 1 \\ i+1, 1, 0, 1-\Upsilon_1^{SE1}, 0 \end{matrix}\right] + D_{SR}D_{SE1}\sum_{l=1}^{\beta_{SR}}\sum_{q=1}^{\beta_{SE1}} c_{l_{SR}} c_{q_{SE1}} G_{4r+3,4r+3}^{3r+2,3r+1}\left[\Re_2 \middle| \begin{matrix} 1, 1-\Upsilon_2^{SE1}, 0, 1, \Upsilon_1^{SR} \\ \Upsilon_2^{SR}, 1, 0, 1-\Upsilon_1^{SE1}, 0 \end{matrix}\right] - D_{SR}D_{SE1}\sum_{l=1}^{\beta_{SR}}\sum_{q=1}^{\beta_{SR}}\sum_{i=0}^{\infty} c_{l_{SR}} c_{q_{SE1}} H_{RD_i} G_{3r+2,r+2;2,2;r+1,3r+1}^{2,3r;1,2;3r,1}\left[\begin{matrix} 1-\Upsilon_2^{SE1}, 0, 1 \\ 1, 0, 1-\Upsilon_1^{SE1} \end{matrix}\middle| \begin{matrix} 1-m_{s_{RD}}, 1 \\ i+1, 0 \end{matrix}\middle| \begin{matrix} 1, \Upsilon_1^{SR} \\ \Upsilon_2^{SR}, 0, \end{matrix}\middle| \Re_1, \Re_2\right] \tag{31}$$

the obtained G_d^o is applicable for both the detection techniques (i.e., HD and IM-DD).

Remark 2: The derived lower bound of SOP is considerably affected by $\mu_{r_{SR}}$, $\mu_{r_{SE1}}$, and R_o while slightly affected by $\overline{\gamma}_{RD}$. This unfolds the fact that the increasing $\mu_{r_{SE1}}$ has adverse impacts on the secrecy of the system, which cannot be controlled. To improve the security, *S* is required to increase $\mu_{r_{SR}}$which may result in higher pointing accuracy as $\mu_{r_{SR}}$ is direct related to the ξ_{SR}. Moreover, PA with high $\varepsilon_{\max}$ can help to improve the security of the system. The designer can adopt various digital pre-distortion algorithms to boost PA efficiency and also compensate the power losses, which enhance the secrecy of the system [56]. Additionally, the SWIPT parameter Ξ_D can also improve reliability by adjusting the harvested RF energy.

2) SPSC: From (26) and using the non-negativity nature of channel capacity, it is revealed that the C_o is positive when $\gamma_{eq,D} > \gamma_Z$ and is zero when $\gamma_{eq,D} < \gamma_Z$. Therefore, the SPSC is defined as the probability of attaining positive secrecy rate (i.e., $C_o > 0$) and can be expressed as [30]

$$P_{SPSC} = \Pr(C_o > 0) = \Pr\left(\gamma_{eq,D} > \gamma_Z\right) \tag{34}$$

From (28), (34) can also be written in terms of SOP as

$$P_{SPSC} = 1 - P_{out}^{L}\left(0\right) \tag{35}$$

The SPSC can be determined straighforwardly by substituting $R_o = 0$ in (31), then using $1 - P_{out}^{L}\left(0\right)$ as (36), shown at the bottom of the page, where $\Re_3 = \Xi_D \frac{\tau_{RD}\mu_{r_{SE1}}}{E_{SE1}}$ and $\Re_4 = \frac{E_{SR}\mu_{r_{SE1}}}{E_{SE1}\mu_{r_{SR}}}$.

Similar to (36), the asymptotic SPSC can be obtained by substituting (32) into (35) at $R_o = 0$. Then, asymptotic SPSC can be written as (37), shown at the bottom of the next page.

Remark 3: Interestingly, it is observed that the SPSC depends on SWIPT parameters including λ_D, η, and d_D and is independent of R_o. Particularly, the SPSC is a monotonically increasing function of λ_D, which implies that an energy-efficient system provides better secrecy.

3) Secrecy Throughput: In this study, it is assumed that the transmission between all the transmitters (i.e., *S* and *R*) and legitimate receivers (i.e., *R* and *D*) is delay intolerant. In this case, the transmitters transfer the secure information at a fixed rate R_o regardless of the wiretap code rates. Particularly, due to fix value of R_o, the trade-off between system reliability and R_o can be utilized. Moreover, the transmitters can use the higher R_o for information transmission at the cost of reliability of the system if it is acceptable. In this context, we adopt another PLS metric i.e., ST to investigate the secrecy performance which contribute in analysing both secure and reliable system. It quantifies the average rate, of secure information decoded correctly by the legitimate user when perfect secrecy is achieved. Mathematically,

$$\begin{aligned}
P_{out_\infty}^{L}\left(R_o\right) \underset{\mu_{r_{SR}}>>1}{\cong} & D_{SR}D_{SE1}\sum_{l=1}^{\beta_{SR}}\sum_{q=1}^{\beta_{SE1}} c_{l_{SR}}c_{q_{SE1}}\sum_{t=1}^{3r} H_t\left(\frac{\mu_{r_{SR}}}{2^{R_o}E_{SR}}\right)^{-\Upsilon_{2_t}^{SR}}\left(\frac{\mu_{r_{SE1}}}{E_{SE1}}\right)^{\left(\Upsilon_{2_t}^{SR}+1\right)}\frac{\prod_{j=1}^{3r}\Gamma\left(\Upsilon_{2_t}^{SR}+\Upsilon_{2_j}^{SE1}\right)}{\prod_{j=3}^{r+2}\Gamma\left(\Upsilon_{2_t}^{SR}+\Upsilon_{1_j}^{SE1}\right)} \\
& + D_{SE1}\left[\sum_{q=1}^{\beta_{SE1}}\sum_{i=0}^{\infty} c_{q_{SE1}}H_{RD_i}M_i\left(2^{R_o}\Xi_D\tau_{RD}\right)^{i+1}\left(\frac{\mu_{r_{SE1}}}{E_{SE1}}\right)^{i+2}\frac{\prod_{j=1}^{3r}\Gamma\left(i+1+\Upsilon_{2_j}^{SE1}\right)}{\prod_{j=3}^{r+2}\Gamma\left(i+1+\Upsilon_{1_j}^{SE1}\right)}\right] \\
& - D_{SR}D_{SE1}\left[\sum_{l=1}^{\beta_{SR}}\sum_{q=1}^{\beta_{SE1}}\sum_{i=0}^{\infty} H_{RD_i}M_i\left(2^{R_o}\Xi_D\tau_{RD}\right)^{i+1}c_{l_{SR}}c_{q_{SE1}}\sum_{t=1}^{3r} H_t\left(\frac{\mu_{r_{SR}}}{2^{R_o}E_{SR}}\right)^{-\Upsilon_{2_t}^{SR}}\left(\frac{\mu_{r_{SE1}}}{E_{SE1}}\right)^{i+2+\Upsilon_{2_t}^{SR}}\right. \\
& \left. \times \frac{\prod_{j=1}^{3r}\Gamma\left(i+1+\Upsilon_{2_t}^{SR}+\Upsilon_{2_j}^{SE1}\right)}{\prod_{j=3}^{r+2}\Gamma\left(i+1+\Upsilon_{2_t}^{SR}+\Upsilon_{1_j}^{SE1}\right)}\right]
\end{aligned} \tag{32}$$

$$\begin{aligned}
P_{SPSC} &= 1 - \left[\begin{array}{l}
D_{SE1}\sum_{q=1}^{\beta}\sum_{i=0}^{\infty} c_{q_{SE1}}H_{RD_i}G_{3r+4,r+4}^{3,3r+2}\left[\Re_3\left|\begin{matrix}1-m_{s_{RD}},1,1-\Upsilon_2^{SE1},0,1\\ i+1,1,0,1-\Upsilon_1^{SE1},0\end{matrix}\right.\right] \\
\quad +D_{SR}D_{SE1}\sum_{l=1}^{\beta_{SR}}\sum_{q=1}^{\beta_{SE1}} c_{l_{SR}}c_{q_{SE1}}G_{4r+3,4r+3}^{3r+2,3r+1}\left[\Re_4\left|\begin{matrix}1,1-\Upsilon_2^{SE1},0,1,\Upsilon_1^{SR}\\ \Upsilon_2^{SR},1,0,1-\Upsilon_1^{SE1},0\end{matrix}\right.\right] \\
-D_{SR}D_{SE1}\sum_{l=1}^{\beta_{SR}}\sum_{q=1}^{\beta_{SR}}\sum_{i=0}^{\infty} c_{l_{SR}}c_{q_{SE1}}H_{RD_i}G_{3r+2,r+2;2,2;r+1,3r+1}^{2,3r;1,2;3r,1}\left[\begin{matrix}1-\Upsilon_2^{SE1},0,1\\ 1,0,1-\Upsilon_1^{SE1}\end{matrix}\left|\begin{matrix}1-m_{s_{RD}},1\\ i+1,0\end{matrix}\right|\begin{matrix}1,\Upsilon_1^{SR}\\ \Upsilon_2^{SR},0,\end{matrix}\right|\Re_3,\Re_4\right]
\end{array}\right] \\
&= 1 - \left[\begin{array}{l}
D_{SE1}\sum_{q=1}^{\beta}\sum_{i=0}^{\infty} c_{q_{SE1}}H_{RD_i}G_{3r+4,r+4}^{3,3r+2}\left[\Re_3\left|\begin{matrix}1-m_{s_{RD}},1,1-\Upsilon_2^{SE1},0,1\\ i+1,1,0,1-\Upsilon_1^{SE1},0\end{matrix}\right.\right] \\
\quad +D_{SR}D_{SE1}\sum_{l=1}^{\beta_{SR}}\sum_{q=1}^{\beta_{SE1}} c_{l_{SR}}c_{q_{SE1}}G_{4r+3,4r+3}^{3r+2,3r+1}\left[\Re_4\left|\begin{matrix}1,1-\Upsilon_2^{SE1},0,1,\Upsilon_1^{SR}\\ \Upsilon_2^{SR},1,0,1-\Upsilon_1^{SE1},0\end{matrix}\right.\right] \\
-D_{SR}D_{SE1}\sum_{l=1}^{\beta_{SR}}\sum_{q=1}^{\beta_{SR}}\sum_{i=0}^{\infty} c_{l_{SR}}c_{q_{SE1}}H_{RD_i}G_{3r+2,r+2;2,2;r+1,3r+1}^{2,3r;1,2;3r,1}\left[\begin{matrix}1-\Upsilon_2^{SE1},0,1\\ 1,0,1-\Upsilon_1^{SE1}\end{matrix}\left|\begin{matrix}1-m_{s_{RD}},1\\ i+1,0\end{matrix}\right|\begin{matrix}1,\Upsilon_1^{SR}\\ \Upsilon_2^{SR},0,\end{matrix}\right|\Re_3,\Re_4\right]
\end{array}\right]
\end{aligned} \tag{36}$$

the ST can be written as [57]

$$\tau = R_o \left(1 - P_{out}^{L}\left(R_o\right)\right) \tag{38}$$

Remark 4: It is noteworthy that R_o can take any value between in interval $\{0, \infty\}$, which affects both ST and SOP. At low R_o, both SOP and ST are small. Moreover, at large R_o, a secure and reliable transmission cannot be established, which also provides a reduction in ST. This means that there must be an optimal R_o (i.e., R_o^*) exist to achieve the maximum ST. Based on the derived ST in (38), the maximum ST can be obtained for R_o^* by utilizing the gradient based search method [58].

B. Scenario 2: Eavesdropping on RF Link Only

Here we compute the PLS metrics, including SOP, SPSC, and ST, for the system under consideration where an RF eavesdropper *E2* is present on the RF link. *E2* processes the wiretapped RF energy for information decoding as well as for energy harvesting.

1) SOP: Utilizing (27) and (30), the lower bound of the SOP can be written as

$$P_{out}^{L}\left(R_o\right) = \int_0^{\infty} F_{\gamma_{eq,D}}\left(2^{R_o}\gamma_{SE2}\right) f_{\gamma_{SE2}}\left(\gamma_{SE2}\right) d\gamma_{SE2} \tag{39}$$

On plugging (15) and (22) into (39) and applying [48, Eq. (07.34.21.0011.01) and Eq. (07.34.21.0081.01)], the resulting SOP is obtained as (40), shown at the bottom of the page.

On placing (15) and (23) into (40) and using [48, Eq. (07.34.21.0009.01)], the asymptotic lower bound of SOP at high SNR can be achieved as (41), shown at the bottom of the next page.

It should be noted that only the dominant terms are required to represent the expression in (41). Here, we define a ratio of SNRs at destination and eavesdropper, i.e., $\overline{\gamma}_{D/E2} = \overline{\gamma}_{RD}/\overline{\gamma}_{RE2}$. For fixed $\mu_{r_{SR}}$, the secrecy diversity order at $\overline{\gamma}_{D/E2} \to \infty$ can be obtained as

$$G_d^S = \min\left(\frac{\xi_{SR}^2}{r}, \frac{\alpha_{SR}}{r}, \frac{q}{r}, i+1\right) \underset{\alpha_{SR}>\beta_{SR}}{=} \min\left(\frac{\xi_{SR}^2}{r}, \frac{q}{r}\right) \tag{42}$$

Remark 5: From (41), it is observed that the SOP is proportional to the $\overline{\gamma}_{RE2}$. Hence, the secrecy of the system is compromised with increasing $\overline{\gamma}_{RE2}$. To mitigate the impacts of $\overline{\gamma}_{RE2}$ on secrecy performance, S has to adjust the R_o accordingly. In addition, we observe that the increasing P_o increases the ergodic capacity of the eavesdropper's link which improves the intercept probability (i.e., $\Pr[C_{E2} > R_o]$) and also degrades the secrecy performance. On the other hand, system reliability is compromised with decreasing P_o. Therefore, the relay choose optimal P_o (i.e., P_o^{opt}) to maintain secrecy of the system without affecting the system reliability (i.e., $\Pr[C_{eq,D} > R_o]$). Since the relay operates under DF protocol, the transmission with $P_{\max}$ would be inefficient and wastage of power resources in the case of FSO dominant because no improvement can be achieved in secrecy performance. Whereas, in case of RF dominant, the transmission with $P_{\max}$ enhances the system reliability but reduces the secrecy performance.

$$\begin{aligned}
&P_{SPSC}^{\infty} \underset{\mu_{r_{SR}}>>1}{\cong} \\
&-\Bigg[D_{SR}D_{SE1} \sum_{l=1}^{\beta_{SR}} \sum_{q=1}^{\beta_{SE1}} c_{l_{SR}} c_{q_{SE1}} \sum_{t=1}^{3r} H_t \left(\frac{\mu_{r_{SR}}}{E_{SR}}\right)^{-\Upsilon_{2_t}^{SR}} \left(\frac{\mu_{r_{SE1}}}{E_{SE1}}\right)^{\left(\Upsilon_{2_t}^{SR}+1\right)} \frac{\prod_{j=1}^{3r} \Gamma\left(\Upsilon_{2_t}^{SR}+\Upsilon_{2_j}^{SE1}\right)}{\prod_{j=3}^{r+2} \Gamma\left(\Upsilon_{2_t}^{SR}+\Upsilon_{1_j}^{SE1}\right)} \\
&\qquad + D_{SE1}\left[\sum_{q=1}^{\beta_{SE1}} \sum_{i=0}^{\infty} c_{q_{SE1}} H_{RD_i} M_i (\Xi_D \tau_{RD})^{i+1} \left(\frac{\mu_{r_{SE1}}}{E_{SE1}}\right)^{i+2} \frac{\prod_{j=1}^{3r} \Gamma\left(i+1+\Upsilon_{2_j}^{SE1}\right)}{\prod_{j=3}^{r+2} \Gamma\left(i+1+\Upsilon_{1_j}^{SE1}\right)}\right]_{i+2+\Upsilon_{2_t}^{SR}} \\
&\qquad - D_{SR}D_{SE1}\left[\sum_{l=1}^{\beta_{SR}} \sum_{q=1}^{\beta_{SE1}} \sum_{i=0}^{\infty} H_{RD_i} M_i \left(2^{R_o}\Xi_D \tau_{RD}\right)^{i+1} c_{l_{SR}} c_{q_{SE1}} \sum_{t=1}^{3r} H_t \left(\frac{\mu_{r_{SR}}}{E_{SR}}\right)^{-\Upsilon_{2_t}^{SR}} \left(\frac{\mu_{r_{SE1}}}{E_{SE1}}\right) \right. \\
&\left. \times \frac{\prod_{j=1}^{3r} \Gamma\left(i+1+\Upsilon_{2_t}^{SR}+\Upsilon_{2_j}^{SE1}\right)}{\prod_{j=3}^{r+2} \Gamma\left(i+1+\Upsilon_{2_t}^{SR}+\Upsilon_{1_j}^{SE1}\right)}\right] \Bigg]
\end{aligned} \tag{37}$$

$$\begin{aligned}
P_{out}^{L}\left(R_o\right) &= D_{SR} \sum_{q=1}^{\beta_{SR}} \sum_{i=0}^{\infty} c_{q_{SR}} H_{RE2_i} G_{r+2,3r+2}^{3r+1,2}\left[\frac{2^{R_o}E_{SR}}{\mu_{r_{SR}}\tau_{RE2}\Xi_{E2}} \middle| \begin{matrix} 1, -i, \Upsilon_1^{SR} \\ \Upsilon_2^{SR}, m_{s_{RE2}}, 0 \end{matrix}\right] \\
&+ \sum_{i=0}^{\infty} \sum_{p=0}^{\infty} H_{RD_i} H_{RE2_p} G_{3,3}^{2,3}\left[\frac{2^{R_o}\tau_{RD}\Xi_D}{\tau_{RE2}\Xi_{E2}} \middle| \begin{matrix} 1-m_{s_{RD}}, 1, -p \\ i+1, m_{s_{RE2}}, 0 \end{matrix}\right] \\
&- D_{SR} \sum_{q=1}^{\beta_{SR}} \sum_{i=0}^{\infty} \sum_{p=0}^{\infty} c_{q_{SR}} H_{RD_i} H_{RE2_p} G_{1,1;r+1,3r+1;2,2}^{1,1;3r,1;1,2}\left[\begin{matrix} -p \\ m_{s_{RE2}} \end{matrix} \middle| \begin{matrix} 1, \Upsilon_1^{SR} \\ \Upsilon_2^{SR}, 0 \end{matrix} \middle| \begin{matrix} 1-m_{s_{RD}}, 1 \\ i+1, 0 \end{matrix} \middle| \frac{2^{R_o}E_{SR}}{\mu_{r_{SR}}\tau_{RE2}\Xi_{E2}}, \frac{2^{R_o}\tau_{RD}\Xi_D}{\tau_{RE2}\Xi_{E2}}\right]
\end{aligned} \tag{40}$$

2) SPSC: Similar to (35), the SPSC can be derived in (43), shown at the bottom of the page, using (40).

C. Scenario 3: Simultaneous eavesdropping on Both FSO and RF Links

In this scenario, it is assumed that both eavesdroppers *E1* and *E2* are active simultaneously and can intercept secure information through FSO and RF links, respectively. Similar to previous scenario 2, *E2* has the ability to utilize received wireless energy for both information decoding and energy harvesting.

1) SOP: Following (27), the SOP for independent two hops under DF scheme can be written as [59]

$$P_{out}\left(R_o\right) = \Pr\left[C_o < R_o\right] = \Pr\left[\min\left(C_{SR}, C_{RD}\right) < R_o\right] \tag{44}$$

By using basic probability theory, (44) can be rewritten as

$$\begin{aligned} P_{out}\left(R_o\right) &= 1 - \Pr\left[\min\left(C_{SR}, C_{RD}\right) > R_o\right] \\ &= 1 - \Pr\left[C_{SR} > R_o\right]\Pr\left[C_{RD} > R_o\right] \end{aligned} \tag{45}$$

With the help of (30) and (39), the lower bound on SOP can be obtained from (45) as

$$\begin{aligned} P^{L}_{out}\left(R_o\right) &= 1 \\ &- \left(1 - \int_0^{\infty} f_{\gamma_{SE1}}\left(\gamma_{SE1}\right) F_{\gamma_{SR}}\left(2^{R_o}\gamma_{SE1}\right) d\gamma_{SE1}\right) \\ &\times \left(1 - \int_0^{\infty} f_{\gamma_{RE2}}\left(\gamma_{RE2}\right) F_{\gamma_{RD}}\left(2^{R_o}\gamma_{RE2}\right) d\gamma_{RE2}\right) \end{aligned} \tag{46}$$

Using (8), (9), (13) and (14) in (46) and by utilizing the integral identities from [48, Eq. (07.34.21.0011.01)], the solution of (46) is given in (47), shown at the bottom of the next page.

Substituting (9), (15), (24) and (25) into (46) and using [48, Eq. (07.34.21.0009.01)], we have the asymptotic lower bound of SOP at high SNR in (48), shown at the bottom of the next page.

Remark 6: Interestingly, it is revealed numerically from (48) that the SOP is independent of PA output power. This means that the security and reliability of the proposed system cannot be controlled by varying P_o. Therefore, the system designer can be provided the flexibility to choose some optimum value of P_o (i.e., P_o^{opt}) to reduce the cost of the power budget. Moreover, both the eavesdroppers *E1* and *E2* can dominantly affect the secrecy of the system by intercepting both the links. It is due to that the SOP is proportional to both μ_{SE1} and $\overline{\gamma}_{RE2}$. Therefore, similar to the previous scenario, *S* has to adjust the R_o to keep information secure from eavesdropping attacks.

IV. Numerical Results & Discussions

In this section, the derived results are illustrated using figures to elucidate the PLS secrecy performance of the proposed system. Particularly, we investigate the effects of the following parameters on SOP, SPSC and ST: FSO turbulence parameters, RF fading parameters, power splitting factor, non-linearity of the power amplifier, and detection techniques. Additionally, the simulations are performed to validate the derived results. For simplification, it is assumed that $\alpha_{SR} = \alpha_{SE1} = \alpha$, $\beta_{SR} = \beta_{SE1} = \beta$, $m_{s_{RD}} = m_{s_{RE2}} = m_s$, $m_{d_{RD}} = m_{d_{RE2}} = m_d$, and $k_{RD} = k_{RE2} = k$. Unless otherwise stated, the values of the

$$\begin{aligned} P^{L}_{out_{\infty}}\left(R_o\right) \underset{\overline{\gamma}_{RD} >> 1}{\cong} & D_{SR}\sum_{q=1}^{\beta_{SR}}\sum_{i=0}^{\infty} H_{RE2_i} c_{q_{SR}} \sum_{t=1}^{3r}\left(\frac{\mu_{r_{SR}}}{2^{R_o}E_{SR}}\right)^{-\Upsilon_{2_t}^{SR}} H_t(\Xi_{E2}\tau_{RE2})^{-\Upsilon_{2_t}^{SR}}\Gamma\left(\Upsilon_{2_t}^{SR}+1+i\right)\Gamma\left(-\Upsilon_{2_t}^{SR}+m_{s_{RE2}}\right) \\ &+ \sum_{i=0}^{\infty}\sum_{p=0}^{\infty} H_{RE2_p} H_{RD_i}\left(\Xi_D 2^{R_o}\tau_{RD}\right)^{i+1} M_i(\Xi_{E2}\tau_{RE2})^{-i-1}\Gamma\left(i+2+p\right)\Gamma\left(-i-1+m_{s_{RE2}}\right) \\ &- D_{SR}\left[\sum_{q=1}^{\beta_{SR}}\sum_{i=0}^{\infty}\sum_{p=0}^{\infty} H_{RD_i} H_{RE2_p} c_{q_{SR}} M_i\left(\Xi_D 2^{R_o}\tau_{RD}\right)^{i+1}\sum_{t=1}^{3r}\left(\frac{\mu_{r_{SR}}}{2^{R_o}E_{SR}}\right)^{-\Upsilon_{2_t}^{SR}} H_t(\Xi_{E2}\tau_{RE2})^{-\Upsilon_{2_t}^{SR}-i-1}\right. \\ &\left.\times\,\Gamma\left(\Upsilon_{2_t}^{SR}+i+2+p\right)\Gamma\left(-\Upsilon_{2_t}^{SR}-i-1+m_{s_{RE2}}\right)\right] \end{aligned} \tag{41}$$

$$\begin{aligned} P_{SPSC} &= 1 - \left[\begin{array}{l} D_{SR}\sum_{q=1}^{\beta_{SR}}\sum_{i=0}^{\infty} c_{q_{SR}} H_{RE2_i} G^{3r+1,2}_{r+2,3r+2}\left[\frac{E_{SR}}{\mu_{r_{SR}}\tau_{RE2}\Xi_{E2}}\middle|\begin{matrix}1,-i,\Upsilon_1^{SR}\\ \Upsilon_2^{SR},m_{s_{RE2}},0\end{matrix}\right] \\ \qquad + \sum_{i=0}^{\infty}\sum_{p=0}^{\infty} H_{RD_i} H_{RE2_p} G^{2,3}_{3,3}\left[\frac{\tau_{RD}\Xi_D}{\tau_{RE2}\Xi_{E2}}\middle|\begin{matrix}1-m_{s_{RD}},1,-p\\ i+1,m_{s_{RE2}},0\end{matrix}\right] \\ -D_{SR}\sum_{q=1}^{\beta_{SR}}\sum_{i=0}^{\infty}\sum_{p=0}^{\infty} c_{q_{SR}} H_{RD_i} H_{RE2_p} G^{1,1;3r,1;1,2}_{1,1;r+1,3r+1;2,2}\left[\begin{matrix}-p\\ m_{s_{RE2}}\end{matrix}\middle|\begin{matrix}1,\Upsilon_1^{SR}\\ \Upsilon_2^{SR},0\end{matrix}\middle|\begin{matrix}1-m_{s_{RD}},1\\ i+1,0\end{matrix}\middle|\frac{E_{SR}}{\mu_{r_{SR}}\tau_{RE2}\Xi_{E2}},\frac{\tau_{RD}\Xi_D}{\tau_{RE2}\Xi_{E2}}\right] \end{array}\right] \end{aligned} \tag{43}$$

TABLE III
THE VALUES OF THE SYSTEM PARAMETERS

Parameters	Values
Optical link length	1 km
Wavelength	785 nm
C_n^2 and $\{\alpha,\beta\}$ (weak turbulence)	1.2×10^{-13} m$^{-2/3}$ and $\{8,4\}$
C_n^2 and $\{\alpha,\beta\}$ (moderate turbulence)	10^{-11} m$^{-2/3}$ and $\{4.2,3\}$
C_n^2 and $\{\alpha,\beta\}$ (strong turbulence)	2.8×10^{-14} m$^{-2/3}$ and $\{2.296,2\}$
R_o	1 bits/s/Hz
$d_D = d_{E2} = d$	10 m
P_c	15 dBm
$P_{\max}$	18 dBm
ℓ	0.5
$\Im_0$	0.1079
Ω	1.3265
ρ	0.596
$\phi_A - \phi_B$	$\pi/2$
L_c	3.597×10^{-2}
$N_0 = \sigma_D^2 = \sigma_{E2}^2$	1

FSO and RF links parameters used in our work are set according to [1], [5], [10], [36], [44], [60], [61] and provided in Table III.

A. Scenario 1: Eavesdropping on FSO Link Only

Fig. 4(a) illustrates the significant impact of PA non-linearity on the security of the proposed system. As expected, the SOP follows water filling with increasing $\mu_{r_{SR}}$. This is because high $\mu_{r_{SR}}$ improves the channel capacity of the legitimate link. It is seen that our asymptotic curves perfectly match with the SOP at the high SNR regime and also predict the secrecy gain and secrecy diversity order. It is observed that lower SOP is obtained for the relaying system with ideal PA compared with the imperfect PAs. The reason is that SOP depends on the difference between the channel capacities of the legitimate and eavesdropper's links. The ideal PA delivers the maximum output power which leads to increase in channel capacity of the legitimate link while the channel capacity of the eavesdropper's link remains same as eavesdropper is receiving information through the FSO link only. This implies that increasing PA output power enhances the security of the overall system. It is also important to mention that with same PA input power, the larger PA output power can be delivered by the efficient PAs. Thus, the SOP will be lower for ideal PA with the same P_c. Furthermore, the SOP is higher with low PA input power than that with high PA input power. It can also be revealed from Fig. 4(a) that inefficient PAs have significant adverse effects on the secrecy performance of the proposed system. The similar effects of PA efficiency and PA output power on the system performance are exhibited in [10], [61]. Furthermore, the SOP performance of the mixed FSO-RF SWIPT system with non-ideal class C PA in [44] under $\mathcal{IT}$-Nakagami-*m* fading scenario is compared with the SOP performance of the proposed system. It is revealed that the behavioural pattern of the SOP of the proposed system is similar as exhibited in [44]. Finally, the SOP stays stagnant with increasing $\mu_{r_{SR}}$ at high SNR as the DF becomes independent of $\mu_{r_{SR}}$ at higher values. Consequently, the RF link becomes dominating in this region, as testified in [44].

To evaluate the effect of detection techniques on the SOP performance, Fig. 4(b) represent the SOP as a function of $\mu_{r_{SR}}$ under varying pointing error. It is worth mentioning that PLS secrecy can be enhanced by utilizing the physical characteristics of the transmission link such as turbulence, pointing error, and fading etc. It can be clearly observed that the secrecy of the proposed system can be enhanced with the HD technique ($r = 1$) compared to IM-DD technique ($r = 2$).This result is expected as limited modulation schemes are permitted in the IM-DD technique due to reduced cost and complexity. Contrarily, the relay can improve the received SNR by utilizing the HD technique, which enhances the security against eavesdropping. Furthermore, the result also shows the impact of strong and

$$P_{out}^{L}(R_o) = \left[1 - \left\{\left(1 - D_{SR}D_{SE1}\sum_{l=1}^{\beta_{SR}}\sum_{q=1}^{\beta_{SE1}} c_{l_{SR}}c_{q_{SE1}}G_{4r+3,4r+3}^{3r+2,3r+1}\left[\frac{2^{R_o}E_{SR}\mu_{r_{SE1}}}{E_{SE1}\mu_{r_{SR}}}\middle|\begin{matrix}1,1-\Upsilon_2^{SE1},0,1,\Upsilon_1^{SR}\\ \Upsilon_2^{SR},1,0,1-\Upsilon_1^{SE1},0\end{matrix}\right]\right)\right.\right.$$
$$\left.\left.\times\left(1 - \sum_{i=0}^{\infty}\sum_{p=0}^{\infty} H_{RD_i}H_{RE2_p}G_{3,3}^{2,3}\left[\frac{2^{R_o}\tau_{RD}\Xi_D}{\tau_{RE2}\Xi_{E2}}\middle|\begin{matrix}1-m_{s_{RD}},1,-p\\ i+1,m_{s_{RE2}},0\end{matrix}\right]\right)\right\}\right] \tag{47}$$

$$P_{out_\infty}^{L}(R_o) \underset{\mu_{r_{SR}}>>1}{\cong} \left[1 - \left\{\left(1 - D_{SR}D_{SE1}\sum_{l=1}^{\beta_{SR}}\sum_{q=1}^{\beta_{SE1}} c_{l_{SR}}c_{q_{SE1}}\sum_{t=1}^{3r} H_t\left(\frac{\mu_{r_{SR}}}{2^{R_o}E_{SR}}\right)^{-\Upsilon_{2_t}^{SR}}\left(\frac{\mu_{r_{SE1}}}{E_{SE1}}\right)^{(\Upsilon_{2_t}^{SR}+1)}\frac{\prod_{j=1}^{3r}\Gamma\left(\Upsilon_{2_t}^{SR}+\Upsilon_{2_j}^{SE1}\right)}{\prod_{j=3}^{r+2}\Gamma\left(\Upsilon_{2_t}^{SR}+\Upsilon_{1_j}^{SE1}\right)}\right)\right.\right.$$
$$\left.\left.\times\left(1 - \sum_{i=0}^{\infty}\sum_{p=0}^{\infty} H_{RE2_p}H_{RD_i}\left(\Xi_D 2^{R_o}\tau_{RD}\right)^{i+1}M_i\left(\Xi_{E2}\tau_{RE2}\right)^{-i-1}\Gamma\left(i+2+p\right)\Gamma\left(-i-1+m_{s_{RE2}}\right)\right)\right\}\right] \tag{48}$$

negligible pointing error. Due to improved pointing accuracy with negligible pointing error ($\xi = 6$), a better secure link is established between the transmitter and the receiver.

Fig. 4(c) demonstrates the influence of target secrecy rate on the security of the proposed system with varying $\mu_{r_{SE1}}$. It can be observed that the SOP with higher $\mu_{r_{SE1}}$ is higher than that with the lower $\mu_{r_{SE1}}$. This is because the channel capacity of the eavesdropper's link improves with higher $\mu_{r_{SE1}}$, leading to a decrease in the secrecy capacity. Besides the impacts of SNR of the eavesdropper's link, the dominance of target secrecy rate on the SOP performance is also shown in Fig. 4(c). Since the probability of C_o being less than R_o is enhanced with increasing R_o, the secrecy of the proposed system is reduced for higher R_o. Similar to Fig. 4(a), a zero floor can also be observed in high SNR regime due to the dominance of RF link.

To examine the impact of double shadowing on the secrecy performance, Fig. 5(a) shows the SOP versus $\mu_{r_{SR}}$ for different values of $\{m_{s_{RD}}, m_{d_{RD}}\}$. We can see that at low SNR regime, the double shadowing has negligible effect on the SOP performance. This is because DF depends only on FSO link in low SNR regime. Therefore, the varying RF link parameters have insignificant impacts on SOP performance. One can also observe that severe multiplicative shadowing (i.e., low $m_{s_{RD}}$) has destructive effect on the secure transmission between transmitter and receiver, when compared to the LOS shadowing (i.e., low $m_{d_{RD}}$). This is the case where the received signal (both through multipath and LOS) is highly impacted due to a number of moving obstacles present in the vicinity of the legitimate receiver. By considering the impact of fading severity on secrecy performance, our observation is consistent with the results in [44], [57].

In Fig. 5(b), the SPSC performance is demonstrated with respect to $\mu_{r_{SR}}$ for different detection techniques with varying pointing error conditions. It can be observed that as long as $\mu_{r_{SR}} < \mu_{r_{SE1}}$, the SPSC with IM-DD tends to be better compared to SPSC with HD. The enhancement in secrecy is obtained because the SNR received at *R* with HD is higher than the SNR received with IM-DD but lower than the SNR of the eavesdropper's link, which always provides zero secrecy capacity. Similarly, despite the high pointing accuracy, the SPSC with higher ξ is lower than that with lower ξ. Another important observation can be noted that as $\mu_{r_{SR}}$ surpasses the $\mu_{r_{SE1}}$, the HD technique contributes to improved secrecy performance compared to IM-DD technique. The reason for this trend is already discussed in Fig. 4(b). From the pointing accuracy point of view, the high value of ξ leads to secure transmission as the eavesdropper has fewer chances to receive the optical signal.

Fig. 5(c) plots the secrecy throughput versus the target secrecy rate for varying power splitting factor. We can observe the bell shaped behavioural pattern of secrecy throughput with increasing R_o. The secrecy throughput first increases and reach a certain value at optimum R_o and then it decreases with further increase in R_o. The reason for this behaviour is that secrecy throughput depends on R_o as given in (38) and thus relatively low values of R_o provides increment in secrecy throughput. However, at large values of R_o, the security and reliability of the system are compromised and hence SOP increases then the secrecy throughput decreases. It can also be observed that power splitting factor λ_D has favourable impact on optimal R_o. This is because secrecy capacity ameliorates at higher λ_D as a large portion of received power is utilized to decode the secure information. Our results trends are also supported by [57], [58], [62].

In Fig. 6(a), the secrecy throughput is presented as a function of $\mu_{r_{SR}}$ for different turbulence conditions and $\mu_{r_{SE1}}$. The secrecy throughput significantly improves with increasing $\mu_{r_{SR}}$ in the low SNR regime. There is a ceiling in the high SNR regime since the received SNR at *D* becomes equal to $\overline{\gamma}_{RD}$. The adverse effect of high $\mu_{r_{SE1}}$ on secrecy throughput can be observed from the result. This is because secrecy capacity reduces with higher $\mu_{r_{SE1}}$ and hence the SOP increases which results in decrement in ST. As another important observation, it can be noted that severe atmospheric turbulence conditions have favourable impacts on secrecy throughput for the case when $\mu_{r_{SE1}} > \mu_{r_{SR}}$. Under such condition, the secrecy capacity becomes zero, which upper-bounded the SOP, and the resultant secrecy throughput increases.

B. Scenario 2: Eavesdropping on RF Link Only

To demonstrate the non-linear effects of PA on the secrecy performance, Fig. 6(b) plots the SOP versus the ratio of SNRs at destination and eavesdropper $\overline{\gamma}_{D/E2}$ for different detection techniques. It is clear from the result that the secrecy performance improves while increasing the $\overline{\gamma}_{D/E2}$. This is because increasing $\overline{\gamma}_{D/E2}$ leads to weakening the eavesdropper link. Interestingly, the SOP for the case with efficient PA is highly deteriorated compared to cases with inefficient PA. This occurs because the transmitted power increases with efficient PA, which makes the eavesdropper link (i.e., $R \rightarrow E2$) better. This can be seen from (11) that the SNR at *E2* increases with increasing $\varepsilon_{\max}$ and P_c. Since the received SNR at *D* is dominated by $\min(\gamma_{SR}, \gamma_{RD})$, the SNR at *D* stays stagnant with efficient PA, but the SNR at *E2* improves. As a result, the difference between the ergodic capacities of legitimate link and eavesdropper's link is reduced and the probability of C_o being less than R_o is increased. This observation trend is supported by the previous study presented in [63]. Furthermore, the security of the system is enhanced for the scenario where the relay utilizes the HD technique for signal detection. The explanation for this behavior is already discussed in Fig. 5(a). Additionally, by determining the secrecy diversity order, the asymptotic analysis of the proposed system can be verified. For instance, SOP with HD for non-ideal class A PA at 70 dB and 80 dB are 1.418×10^{-5} and 1.509×10^{-6}, respectively. Then, the slope can be evaluated at high SNR as $\log_{10}(\frac{1.418\times10^{-5}}{1.509\times10^{-6}}) = 0.97 \approx \min(\xi^2, q) = 1$. Furthermore, the obtained result is compared with the SOP performance of the mixed FSO-RF SWIPT system proposed in [44]. It is evident that our observation is consistent with the result in [44].

Fig. 6(c) plots the SOP versus $\overline{\gamma}_{D/E2}$ for different turbulence conditions with varying path-loss exponent. The lowest SOP is achieved for weak turbulence while comparing to the moderate and strong turbulence conditions that also agree well with [35], [36], [57], [60].This is due to the fact that with increasing level of turbulence, the SNR at *D* is highly deteriorated, resulting in a

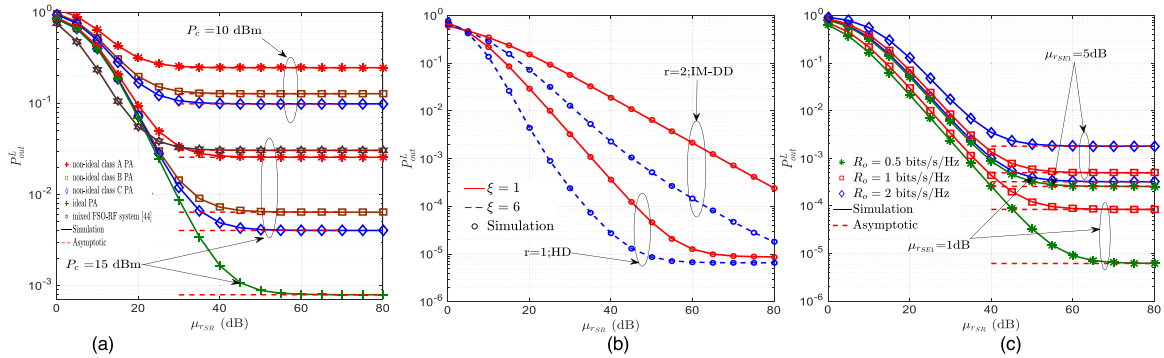

Fig. 4. (a) SOP versus $\mu_{r_{SR}}$ with $\overline{\gamma}_{RD} = 5\,dB$, $\{m_d = 1.3, m_s = 2.7, k = 1.2\}$, $\lambda_D = 0.5$, $\eta = 3.1$, $\mu_{r_{SE1}} = 5\,dB$, $\xi = 1$, $r = 1$, $\{\alpha = 4.2, \beta = 3\}$. (b) SOP versus $\mu_{r_{SR}}$ with $\overline{\gamma}_{RD} = 15\,dB$, $\{m_d = 1.3, m_s = 2.7, k = 1.2\}$, $\lambda_D = 0.5$, $\eta = 3.1$, $\varepsilon_{\max} = 0.9$, $\mu_{r_{SE1}} = 1\,dB$, $\{\alpha = 4.2, \beta = 3\}$. (c) SOP versus $\mu_{r_{SR}}$ with $\overline{\gamma}_{RD} = 10\,dB$, $\{m_d = 1.3, m_s = 2.7, k = 1.2\}$, $\lambda_D = 0.5$, $\eta = 3.1$, $\varepsilon_{\max} = 0.9$, $r = 1$, $\{\alpha = 4.2, \beta = 3\}$.

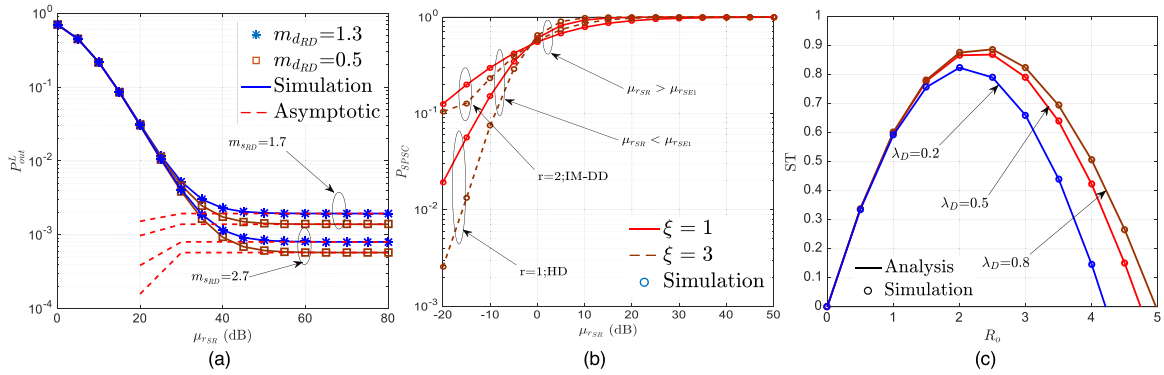

Fig. 5. (a) SOP versus $\mu_{r_{SR}}$ with $\overline{\gamma}_{RD} = 10\,dB$,$k = 1.2$,$\lambda_D = 0.5$,$\eta = 3.1$,$\varepsilon_{\max} = 0.9$,$\mu_{r_{SE1}} = 1\,dB$,$\xi = 1$,$r = 1$,$\{\alpha = 4.2, \beta = 3\}$. (b) SPSC versus $\mu_{r_{SR}}$ with $\overline{\gamma}_{RD} = 10\,dB$, $\{m_d = 1.3, m_s = 1.7, k = 1.2\}$, $\lambda_D = 0.5$, $\eta = 3.1$, $\varepsilon_{\max} = 0.9$, $\mu_{r_{SE1}} = -2dB$, $\{\alpha = 4.2, \beta = 3\}$. (c) Secrecy throughput versus R_o with $\overline{\gamma}_{RD} = 10\,dB$,$\{m_d = 1.3, m_s = 2.7, k = 1.2\}$, $\eta = 3.1$, $\varepsilon_{\max} = 0.9$, $\mu_{r_{SR}} = 15\,dB$, $\mu_{r_{SE1}} = 10\,dB$, $\xi = 1$, $r = 1$, $\{\alpha = 4.2, \beta = 3\}$.

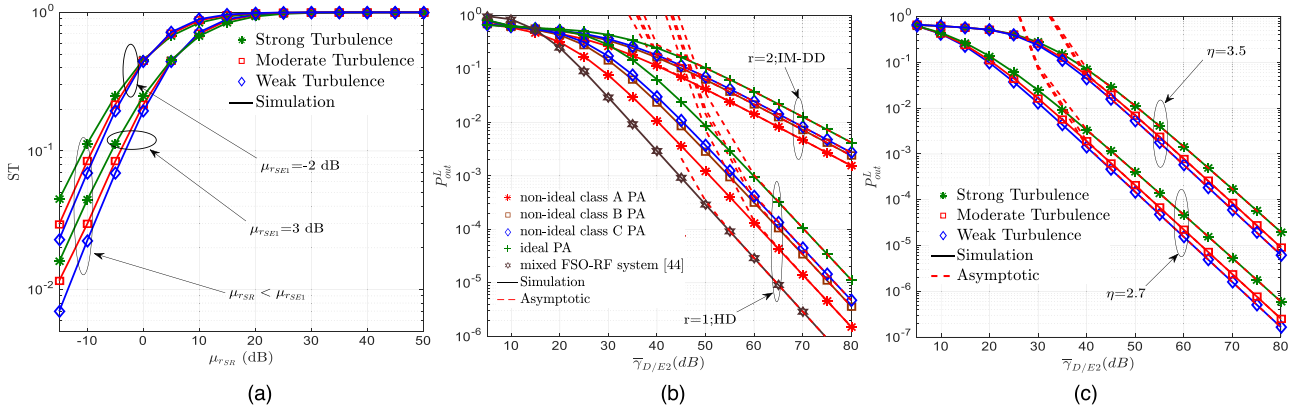

Fig. 6. (a) Secrecy throughput versus $\mu_{r_{SR}}$ with $\overline{\gamma}_{RD} = 10\,dB$,$\{m_d = 1.3, m_s = 2.7, k = 1.2\}$, $\eta = 3.1$, $\varepsilon_{\max} = 0.5$, $\xi = 1$, $r = 1$. (b) SOP versus $\overline{\gamma}_{D/E2}$ with $\overline{\gamma}_{RD} = 15\,dB$, $\{m_d = 1.3, m_s = 1.7, k = 1.2\}$, $\lambda_D = \lambda_{E2} = 0.5$, $\eta = 3.1$, $\mu_{r_{SR}} = 10\,dB$, $\xi = 1$, $\{\alpha = 4.2, \beta = 3\}$. (c) SOP versus $\overline{\gamma}_{D/E2}$ with $\overline{\gamma}_{RD} = 15\,dB$, $\{m_d = 1.3, m_s = 1.7, k = 1.2\}$, $\lambda_D = \lambda_{E2} = 0.5$, $\varepsilon_{\max} = 0.5$, $\mu_{r_{SR}} = 10\,dB$, $\xi = 1$, $r = 1$.

reduction in ergodic capacity of the legitimate link. Furthermore, it can also be seen that a higher value of η has an adverse effect on the SOP performance, where η represents the stronger path-loss for RF links.

In Fig. 7(a), the SOP versus $\overline{\gamma}_{D/E2}$ is presented for various values of power splitting factor λ_D at destination with varying distance between relay and destination. Since λ_D signifies the fraction of power allocated to decoding the information, it can be seen that secrecy performance improves with increasing λ_D. This is because the level of power is increased at the information decoder for higher values of λ_D, resulting in a small amount of power being utilized at the energy harvester. This leads to a higher received SNR at D which results in a higher ergodic capacity of the legitimate link and a reduction in the SOP. On the other hand, as the destination moves away from the relay, the secrecy performance deteriorates, which is

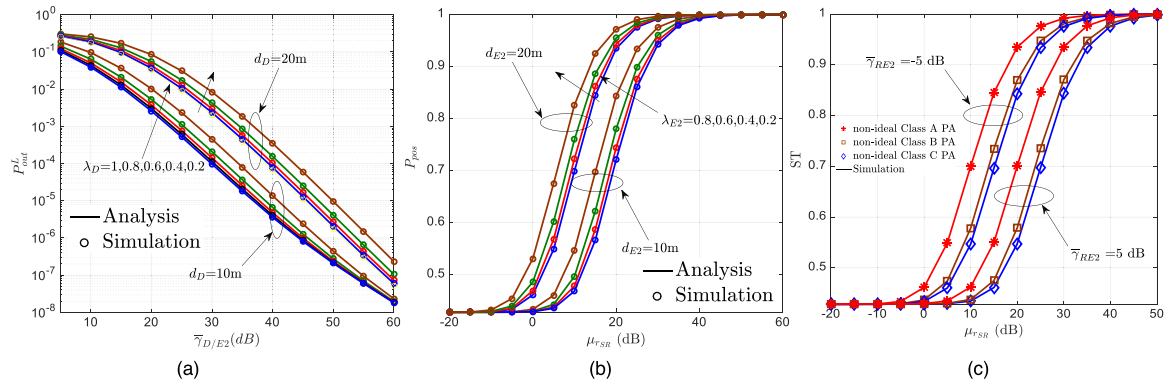

Fig. 7. (a) SOP versus $\overline{\gamma}_{D/E2}$ with $\overline{\gamma}_{RD} = 10\,dB$, $\{m_d = 1.3, m_s = 1.7, k = 1.2\}$, $\lambda_{E2} = 0.5$, $\varepsilon_{\max} = 0.9$, $\mu_{r_{SR}} = 50\,dB$, $\xi = 1$, $r = 1$, $\{\alpha = 4.2, \beta = 3\}$. (b) SPSC versus $\mu_{r_{SR}}$ with $\overline{\gamma}_{RD} = 30\,dB$, $\overline{\gamma}_{RE2} = 1\,dB$, $\{m_d = 1.3, m_s = 1.7, k = 1.2\}$, $\lambda_D = 0.5$, $\varepsilon_{\max} = 0.9$, $\xi = 1$, $r = 1$, $\{\alpha = 8, \beta = 4\}$. (c) Secrecy throughput versus $\mu_{r_{SR}}$ with $\overline{\gamma}_{RD} = 30\,dB$, $\{m_d = 1.3, m_s = 1.7, k = 1.2\}$, $\lambda_D = \lambda_{E2} = 0.5$, $\xi = 1$, $r = 1$, $\{\alpha = 8, \beta = 4\}$.

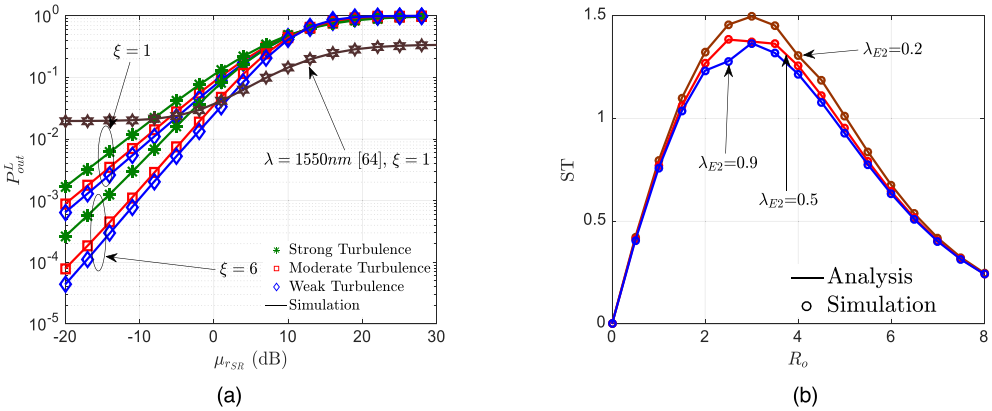

Fig. 8. (a) SOP versus $\overline{\gamma}_E$ with $\mu_{SR} = \overline{\gamma}_{RD} = 15\,dB$, $\{m_d = 1.3, m_s = 1.7, k = 1.2\}$, $\lambda_D = \lambda_{E2} = 0.5$, $\varepsilon_{\max} = 0.9$, $\eta = 2.7$, $r = 1$. (b) Secrecy throughput versus R_o with $\mu_{SR} = \overline{\gamma}_{RD} = 15\,dB$, $\mu_{SE1} = \overline{\gamma}_{RE2} = 5\,dB$, $\{m_d = 1.3, m_s = 1.7, k = 1.2\}$, $\lambda_D = 0.5$, $\varepsilon_{\max} = 0.9$, $\eta = 3.1$, $r = 1$, $\{\alpha = 4.2, \beta = 3\}$.

evident because the RF signal suffers stronger path-loss with increasing d_D.

Fig. 7(b) demonstrate the SPSC versus $\mu_{r_{SR}}$ for different values of power splitting factor λ_{E2} at the eavesdropper with varying distance between the relay and the eavesdropper. It can be observed that the SPSC with higher d_{E2} outperforms as compared to the SPSC with lower d_{E2}. Since the received SNR at the eavesdropper depends on d_{E2} as given in (11), the eavesdropper's link is degraded with increasing d_{E2}. Therefore, the difference between the ergodic capacities of legitimate link and eavesdropper's link is increased, and the resultant SPSC is enhanced. In addition, it can also be deduced from the result that the secrecy performance suffers destructive effects with increasing λ_{E2}. This performance behavior is inversive if we compare the impact of the power splitting factor on the secrecy of the system in Fig. 7(a). The reason for this trend is discussed in the previous finding in Fig. 7(a).

Fig. 7(c) plots secrecy throughput versus $\mu_{r_{SR}}$ for different values of average SNR of the eavesdropper's link. As expected, higher values of the received SNR at eavesdropper have detrimental effects on the secrecy performance. It is observed that the secrecy throughput with high $\overline{\gamma}_{RE2}$ is lower than that with low $\overline{\gamma}_{RE2}$. This is because the quality of the eavesdropper's link is enhanced with increasing $\overline{\gamma}_{RE2}$, reducing secrecy capacity. As another important observation, the destructive impacts of efficient PA on the secrecy throughput can be noted from the result. The explanation for this trend is similar to that for the previous findings in Fig. 7(a).

C. Scenario 3: Simultaneous eavesdropping on Both FSO and RF Links

Fig. 8(a) represents the SOP derived in (47) for different pointing errors and atmospheric conditions when both eavesdroppers *E1* and *E2* are active. To show the impact of both the eavesdroppers, we set $\mu_{r_{SE1}} = \overline{\gamma}_{E2} = \overline{\gamma}_E$. As expected, the SOP with lower ξ is higher than with the larger ξ. This is because larger values of ξ represents severe pointing errors and creates substantial distortions in optical signals. These distortions weaken the signal received by the relay and result in a reduction in the channel capacity of the legitimate link. Furthermore, one can also see that the SOP with strong turbulence is higher than that with weak turbulence. The reason is the same as that for the previous findings in Fig. 6(a) and Fig. 6(c). These observations are in agreement with the previous study on simultaneous FSO- and RF-side eavesdropping in

[59]. Moreover, the SOP decreases with increasing $\overline{\gamma}_E$, keeping other parameters constant. The reason for this is that increasing $\overline{\gamma}_E$ enhances the channel capacities of illegitimate links (i.e., $S \rightarrow E1$ and $R \rightarrow E2$), which deteriorates the overall secrecy of the system. Finally, the validity of the obtained results is verified by including the SOP at $\lambda = 1550$ nm in Fig. 8(a). The change in wavelength has an influence on the atmospheric turbulence parameters and the values of these parameters can be calculated as $\{\alpha = 4.2, \beta = 5\}$[64]. It is clearly noted that the system can be designed for all other specific values of parameters, and this analysis will also be applicable to these systems.

In Fig. 8(b), the secrecy throughput is illustrated as a function of R_o for varying power splitting factor at the *E2*. Similar to Fig. 5(c), the bell-shaped behavioral pattern can be observed from the results. The reason is the same as discussed in Fig. 5(c). It can also be observed that power splitting factor λ_{E2} has an influence on the optimal R_o. Moreover, the secrecy throughput with lower λ_{E2} is higher than that with larger λ_{E2}. This is because the more the power at *E2* is utilized to decode the information, the channel capacity of illegitimate link (i.e., $R \rightarrow E2$) increases, which results in a reduction in secrecy capacity.

V. Conclusion

In this work, we have proposed a mixed FSO-RF SWIPT system under the effects of atmospheric turbulence and hardware impairments wherein it has been assumed that two eavesdroppers could hear the secure information either through FSO or RF links and also through both links simultaneously. The secrecy performance was analyzed by deriving the closed-form expressions for various PLS performance indicators such as SOP, SPSC, and ST. Furthermore, the asymptotic expressions were derived to highlight the significant insights into the secrecy performance in the high SNR regime and also determined the secrecy diversity order. Our analysis demonstrated that the secure transmission was largely affected by various parameters, including atmospheric turbulence conditions, pointing errors, and SWIPT parameters. Moreover, these parameters can play a crucial role in establishing a secure link between source and destination. Our results also show that the secrecy performance of the proposed system is remarkably affected by the PA inefficiencies and should be carefully considered in the system design. Based on the location of an adversary, it can be noticed that efficient PA can provide enhanced secrecy performance when an eavesdropper is present on the FSO link. Whereas the system reliability improves with efficient PA when an eavesdropper is present on the RF link. Therefore, the networks should be designed in such a way that in case of optical eavesdropping efficient PAs can be used to provide high security while in case of RF eavesdropping the designer has flexibility in compromising with efficiency of PAs to establish a secure link between intended users. However, it is not easy to select the PA properties due to dependency on several other parameters such as infrastructure size, cost of device and circuit complexity. In addition, it was also found that double shadowing had a significant impact on the PLS secrecy of the proposed system.

References

[1] M. J. Saber and S. M. S. Sadough, "On secure free-space optical communications over Málaga turbulence channels," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 274–277, Apr. 2017.

[2] E. Zedini, H. Soury, and M.-S. Alouini, "On the performance of dual hop FSO/RF systems," in *Proc. IEEE Int. Symp. Wireless Commun. Syst. (ISWCS)*, Brussels, Belgium, Aug. 2015, pp. 31–35.

[3] E. Zedini, H. Soury, and M.-S. Alouini, "On the performance analysis of dual-hop mixed FSO/RF systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 5, pp. 3679–3689, May 2016.

[4] N. Zdravkovic, M. I. Petkovic, G. T. Djordjevic, and K. Kansanen, "Outage analysis of mixed FSO/WiMAX link," *IEEE Photon. J.*, vol. 8, no. 1, Feb. 2016, Art. no. 7900814.

[5] B. Asharafzadeh, E. Soleimani-Nasab, and M. Kamandar, "Performance analysis of mixed DGG and generalized Nakagami-*m* dual-hop FSO/RF transmission systems," in *Proc. 24th Telecommun. Forum (TELFOR)*, Belgrade, Serbia, Nov. 2016, pp. 1–4.

[6] I. Trigui, N. Cherif, and S. Affes, "Relay-assisted mixed FSO/RF systems over Málaga-*M* and $\kappa - \mu$ shadowed fading channels," *IEEE Wireless Commun. Lett.*, vol. 6, no. 5, pp. 682–685, Oct. 2017.

[7] T. V. Nguyen, T. V. M. Pham, T. A. Pham, H. T. T. Pham, N. T. Dang, and A. T. Pham, "Performance analysis of network-coded two-way dualhop mixed FSO/RF systems," in *Proc. Int. Conf. Adv. Tech. Commun. (ATC)*, Hanoi, Vietnam, Oct. 2016, pp. 70–75.

[8] Z. Jing, Z. Shang-Hong, Z. Wei-Hu, and C. Ke-Fan, "Performance analysis for mixed FSO/RF Nakagami-*m* and exponentiated weibull dual-hop airborne systems," *Opt. Commun.*, vol. 392, pp. 294–299, Jun. 2017.

[9] B. Makki, T. Svensson, T. Eriksson, and M. Nasiri-Kenari, "On the throughput and outage probability of multi-relay networks with imperfect power amplifiers," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 4994–5008, Sep. 2015.

[10] B. Makki, T. Svensson, M. Brandt-Pearce, and M. Alouini, "On the performance of millimeter wave-based RF-FSO multi-hop and mesh networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 12, pp. 7746–7759, Dec. 2017.

[11] H. Tan and P. Ho, "Multiply-and-forward—A robust transmission scheme for two-way cooperative communication in the presence of nonlinear power amplifier distortion," in *Proc. WCNC*, Apr. 2013, pp. 4026–4031.

[12] I. Ahmad, A. Iyanda Sulyman, A. Alsanie, A. Alasmari, and S. Alshebeili, "Spectral re-growth due to high power amplifier nonlinearities in MIMOOFDM relaying channels," in *Proc. IB2Com*, Nov. 2011, pp. 240–245.

[13] C. Zhang, Y. Zhang, and Z. Gao, "Performances of amplify-and-forward based wireless relay networks with traveling-wave tube amplifiers," in *Proc. WCSP*, Oct. 2013, pp. 1–5.

[14] J. Qi, S. Aissa, and M.-S. Alouini, "Performance analysis of AF cooperative systems with HPA nonlinearity in semi-blind relays," in *Proc. GLOBECOM*, Dec. 2012, pp. 4182–4186.

[15] C. Zhang, Q. Du, Y. Wang, and G. Wei, "Optimal relay power allocation for amplify-and-forward OFDM relay networks with deliberate clipping," in *Proc. WCNC*, Apr. 2012, pp. 381–386.

[16] M. Haenggi, "The impact of power amplifier characteristics on routing in random wireless networks," in *Proc. GLOBECOM*, Dec. 2003, pp. 513–517.

[17] 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, May 2013.

[18] G. Pan, H. Lei, Y. Yuan, and Z. Ding, "Performance analysis and optimization for SWIPT wireless sensor networks," *IEEE Trans. Commun.*, vol. 66, no. 5, pp. 229–2302, May 2017.

[19] N. Zhao, S. Zhang, F. R. Yu, Y. Chen, A. Nallanathan, and V. C. M. Leung, "Exploiting interference for energy harvesting: A survey, research issues, and challenges," *IEEE Access*, vol. 5, pp. 10403–10421, Jun. 2017.

[20] J. Huang, C. C. Xing, and C. Wang, "Simultaneous wireless information and power transfer: Technologies, applications, and research challenges," *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 26–32, Nov. 2017.

[21] D. Wu, J. He, H. Wang, C. Wang, and R. Wang, "A hierarchical packet forwarding mechanism for energy harvesting wireless sensor networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 92–98, Aug. 2015.

[22] I. Krikidis, S. Timotheou, S. Nikolaou, G. Zheng, D. W. K. Ng, and R. Schober, "Simultaneous wireless information and power transfer in modern communication systems," *IEEE Commun. Mag.*, vol. 52, no. 11, pp. 104–110, Nov. 2014.

[23] G. Pan, C. Tang, T. Li, and Y. Chen, "Secrecy performance analysis for SIMO simultaneous wireless information and power transfer systems," *IEEE Trans. Commun.*, vol. 63, no. 9, pp. 3423–3433, Sep. 2015.

[24] G. Pan *et al.*, "On secrecy performance of MISO SWIPT systems with TAS and imperfect CSI," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3831–pp. 3843, Sep. 2016.

[25] H. Lei, M. Xu, I. S. Ansari, G. Pan, K. A. Qaraqe, and M.-S. Alouini, "On secure underlay MIMO cognitive radio networks with energy harvesting and transmit antenna selection," *IEEE Trans. Green Commun. Netw.*, vol. 1, no. 2, pp. 192–203, Jun. 2017.

[26] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, May 2016.

[27] H.-M. Wang and T.-X. Zheng, *Physical Layer Security in Random Cellular Networks*. Singapore: Springer, 2016.

[28] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel interference," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1494–1505, Dec. 2016.

[29] L. S. Fan, X. F. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secrecy cooperative networks with outdated relay selection over correlated fading channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7599–7603, Aug 2017.

[30] H. Lei, H. Zhang, I. S. Ansari, G. Pan, and K. A. Qaraqe, "Secrecy outage analysis for SIMO underlay cognitive radio networks over generalized-K fading channels," *IEEE Signal Process. Lett.*, vol. 23, no. 8, pp. 1106–1110, Aug. 2016.

[31] H. Lei, H. Luo, K. Park, Z. Ren, G. Pan, and M. Alouini, "Secrecy outage analysis of mixed RF-FSO systems with channel imperfection," *IEEE Photon. J.*, vol. 10, no. 3, Jun. 2018, Art. no. 7904113.

[32] 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. 904–5918, May 2016.

[33] H. Lei, Z. Dai, I. S. Ansari, K. Park, G. Pan, and M. Alouini, "On secrecy performance of mixed RF-FSO systems," *IEEE Photon. J.*, vol. 9, no. 4, Jul. 2017, Art. no. 7904814.

[34] L. Yang, T. Liu, J. Chen, and M. Alouini, "Physical-layer security for mixed η-μ and M-Distribution Dual-Hop RF/FSO systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12427–12431, Oct. 2018.

[35] M. J. Saber, J. Mazloum, A. M. Sazdar, A. Keshavarz, and M. J. Piran, "On secure mixed RF-FSO decode-and-forward relaying systems with energy harvesting," *IEEE Syst. J.,* vol. 14, no. 3, pp. 4402–4405, Sep. 2020.

[36] 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, Sep. 2019.

[37] J. Chen *et al.*, "A novel energy harvesting scheme for mixed FSO-RF relaying systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 8259–8263, Aug. 2019.

[38] F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical layer security in free-space optical communications," *IEEE Photon. J.*, vol. 7, no. 2, Apr. 2015, Art. no. 7901014.

[39] D. Zou, and Z. Xu, "Information security risks outside the laser beam in terrestrial free-space optical communication," *IEEE Photon. J.*, vol. 8, no. 5, Oct. 2016, Art. no. 7804809.

[40] V. G. Sidorovich, "Optical countermeasures and security of free-space optical communication links," *Proc. Eur. Symp. Opt. Photon. Defence Secur.*, London, U.K., 2004, pp. 97–108.

[41] R. Boluda-Ruiz, S. C. Tokgoz, A. García-Zambrana, and K. Qaraqe, "Enhancing secrecy capacity in FSO links via MISO systems through turbulence-induced fading channels with misalignment errors," *IEEE Photon. J.*, vol. 12, no. 4, Aug. 2020, Art. no. 7903313.

[42] X. Pan, H. Ran, G. Pan, Y. Xie, and J. Zhang, "On secrecy analysis of DF based dual hop mixed RF-FSO systems," *IEEE Access*, vol. 7, pp. 66725–66730, May 2019.

[43] D. Wang, P. Ren, J. Cheng, Q. Du, Y. Wang, and L. Sun, "Secure transmission for mixed FSO-RF relay networks with physical-layer key encryption and wiretap coding," *Opt. Exp.*, vol. 25, no. 9, pp. 10078–10089, Mar. 2017.

[44] H. Lei, Z. Dai, K. Park, W. Lei, G. Pan, and M. Alouini, "Secrecy outage analysis of mixed RF-FSO downlink SWIPT systems," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6384–6395, Dec. 2018.

[45] E. Balti, M. Guizani, B. Hamdaoui, and B. Khalfi, "Mixed RF/FSO relaying systems with hardware impairments," in *Proc. IEEE Glob. Commun. Conf.*, 2017.

[46] Y. Ai *et al.*, "Secrecy enhancement of RF backhaul system with parallel FSO communication link," *Opt. Commun.*, vol. 475, Nov. 2020.

[47] N. Simmons, C. R. N. da Silva, S. L. Cotton, P. C. Sofotasios, and M. D. Yacoub, "Double shadowing the rician fading model," *IEEE Wireless Commun. Lett.*, vol. 8, no. 2, pp. 344–347, Apr. 2019.

[48] Wolfram. *The Wolfram Functions Site*. [Online]. Available: http://functions.wolfram.com/id

[49] B. L. Sharma and R. F. A. Abiodun, "Generating function for generalized function of two variables," *Amer. Math. Soci.*, vol. 46, no. 1, pp. 69–72, Oct. 1974.

[50] S. Mikami, T. Takeuchi, H. Kawaguchi, C. Ohta, and M. Yoshimoto, "An efficiency degradation model of power amplifier and the impact against transmission power control for wireless sensor networks," *Proc. 2007 IEEE Radio Wireless Symp.*, pp. 447–450.

[51] J. Fu and A. Mortazawi, "Improving power amplifier efficiency and linearity using a dynamically controlled tunable matching network," *IEEE Trans. Microw. Theory Techn.*, vol. 56, no. 12, pp. 3239–3244, Dec. 2008.

[52] E. Björnemo, "Energy constrained wireless sensor networks: Communication principles and sensing aspects," Ph.D. dissertation, Dept. Eng. Sci, Signals Syst. Uppsala Univ., Uppsala, Sweden, 2009.

[53] D. Wulich, "Definition of efficient PAPR in OFDM," *IEEE Commun. Lett.*, vol. 9, no. 9, pp. 832–834, Sep. 2005.

[54] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals Ser.: More Special Functions,* vol. 3. New York, NY, USA: CRC Press, 1992.

[55] V. S. Adamchik, and O. I. Marichev, "The algorithm for calculating integrals of hypergeometric type functions and its realization in REDUCE system," in *Proc. Int. Symp. Symb. Algeb. Comput.*, Japan, 1990.

[56] K. Gumber and M. Rawat, "Low-cost $\mathrm{rF_{in}}$–$\mathrm{rf_{out}}$ Predistorter linearizer for high-power amplifiers and ultra-wideband signals," *IEEE Trans. Instr. Meas.*, vol. 67, no. 9, pp. 2069–2081, Sep. 2018.

[57] H. Lei *et al.*, "On secure mixed RF-FSO systems with TAS and imperfect CSI," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4461–4475, Jul. 2020.

[58] D. Chen, Y. Cheng, X. Wang, W. Yang, J. Hu, and Y. Cai, "Energy-efficient secure multiuser scheduling in energy harvesting untrusted relay networks," *J. Commun. Netw.*, vol. 21, no. 4, pp. 365–375, Aug. 2019.

[59] R. Singh, M. Rawat, and A. Jaiswal, "On the performance of mixed FSO/RF SWIPT systems with secrecy analysis," *IEEE Syst. J.*, doi: 10.1109/JSYST.2021.3073098.

[60] R. Singh, M. Rawat, and A. Jaiswal, "Mixed FSO/RF SIMO SWIPT Decode-and-Forward relaying systems," in *Proc. 2020 Int. Conf. Signal Proc. Commun. (SPCOM)*, Bangalore, India, 2020.

[61] D. Persson, T. Eriksson, and E. G. Larsson, "Amplifier-aware multiple-input multiple-output power allocation," *IEEE Commun, Lett.,* vol. 17, no. 6, pp. 1112–1115, Jun. 2013.

[62] S. H. Islam *et al.*, "Impact of correlation and pointing error on secure outage performance over arbitrary correlated Nakagami-m and M-Turbulent fading mixed RF-FSO channel," *IEEE Photon. J.*, vol. 13, no. 2, Apr. 2021, Art. no. 7900117.

[63] A. H. A. El-Malek, A. M. Salhab, S. A. Zummo, and M. Alouini, "Effect of RF interference on the security-reliability tradeoff analysis of multiuser mixed RF/FSO relay networks with power allocation," *J. Lightw. Technol.*, vol. 35, no. 9, pp. 1490–1505, May 2017

[64] E. Balti, M. Guizani, B. Hamdaoui, and B. Khalfi, "Aggregate hardware impairments over mixed RF/FSO relaying systems with outdated CSI," *IEEE Trans. Commun.*, vol. 66, no. 3, pp. 1110–1123, Mar. 2018.