Security-Reliability Tradeoff Analysis for Multiuser FSO Communications over a Generalized Channel

Wafaa Mohammed Ridha Shakir, Jinan Charafeddine, Hani Hamdan, Israa Alshabeeb, Nidaa Ali, Israa Abed

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 8 May 2023, accepted 21 May 2023, date of publication 29 May 2023, date of current version 5 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3280908

RESEARCH ARTICLE

Security-Reliability Tradeoff Analysis for Multiuser FSO Communications Over a Generalized Channel

WAFAA MOHAMMED RIDHA SHAKIR[1], (Member, IEEE), JINAN CHARAFEDDINE[2], (Student Member, IEEE), HANI HAMDAN[3], ISRAA ALI ALSHABEEB[1], NIDAA GHALIB ALI[1], AND ISRAA E. ABED[1]

[1]Department of Computer Systems, Technical Institute of Babylon, Al-Furat Al-Awsat Technical University, Babil 51015, Iraq
[2]Pôle scientifique et technologique de Vélizy, Laboratoire d'Ingénierie des Systèmes de Versailles, Université Paris-Saclay, 78140 Vélizy, France
[3]CentraleSupélec, CNRS, Laboratoire des Signaux et Systèmes (L2S UMR CNRS 8506), Université Paris-Saclay, 91190 Gif-sur-Yvette, France

Corresponding author: Wafaa Mohammed Ridha Shakir (inb.wfa@atu.edu.iq)

This work was supported in part by the Ministry of Higher Education and Scientific Research, Iraq, under Grant IQ-123456.

ABSTRACT The security-reliability tradeoff (SRT) in free-space optical (FSO) communications is the most critical property to highlight, especially with respect to the development of wireless optical communications. In this paper, opportunistic scheduling selection techniques are used to improve the SRT of multiuser FSO systems under the combined influence of atmospheric turbulence with Fisher-Snedecor $\mathcal{F}$ distribution, generalized pointing error, and path losses due to foggy weather. Due to the broadcast nature of wireless optical propagation, the optical transmission from the transmitting users to the legitimate receiver can be easily intercepted by eavesdroppers. Therefore, an optimal user scheduling (OUS) scheme is proposed in this work to protect the legitimate wireless transmission from eavesdroppers, where a user with the highest secrecy capacity is scheduled to transmit his confidential information to the receiver. Closed-form expressions for the outage probability, interception probability, and SRT are derived for the conventional round-robin scheduling (RRS) and the proposed OUS. In addition, an asymptotic analysis for the outage probability, interception probability, and SRT is performed to provide insight into the impact of user scheduling on the system performance. We also propose the use of ''friendly jamming'' techniques, where the user with the lowest secrecy capacity is selected by the authorized receiver to jam the existing interceptor. Finally, another SRT is formulated to determine the impact of a friendly jammer on the secrecy performance of the system. The results show that the proposed OUS outperforms the RRS in terms of intercept probability and SRT performance. The obtained exact and asymptotic results are validated by Monte-Carlo simulations.

INDEX TERMS Free-space optical, security, reliability, security-reliability tradeoff, opportunistic scheduling, Fisher–Snedecor, $\mathcal{F}$ distribution, atmospheric turbulence, non-zero boresight pointing error, fog.

I. INTRODUCTION

Global mobile data traffic is expected to be 5016 exabytes per month in 2030, compared to only 7.462 exabytes per month in 2010 [1]. This statistic clearly shows the importance of improving the security of wireless communication networks, especially with the advent of fifth-generation (5G) and beyond 5G (B5G) networks. Preventing eavesdropping of useful information in such high-traffic environments is as much a challenge as eliminating eavesdroppers from the network [2], [3]. Compared to radio frequency (RF), whose spectrum is becoming scarce, free-space optical (FSO) technology, with its license-free spectrum, wide spectrum, very high data rate, very low latency, low cost, and lower power consumption, is widely accepted as an extent efficient solution to mitigate the conventional RF spectrum scarcity [4], [5]. A narrow beam of laser diodes (LD) is used to establish high-speed communication links, while a photodetector (PD) is used as an optical receiver in FSO systems. Due to the coherent nature of laser technology, the FSO signal can be

The associate editor coordinating the review of this manuscript and approving it for publication was Zijian Zhang.

transmitted for several kilometers, although the performance of the FSO link degrades significantly when the transmission distance exceeds one kilometer due to environmental effects [6]. In general, FSO communication is more secure than RF communication because the laser beam has a line-of-sight (LOS) nature and high directivity [2]. However, since the laser beam experiences divergence at the receiving end due to light diffraction, the relatively close location of the eavesdropper with respect to the legitimate receiver in the divergence area can cause serious security flaws [7], [8], [9], [10], [11]. An alternative scenario would be that the eavesdropper approaches the legitimate transmitter and attempts to block the laser beam in order to collect a larger amount of power [8], [10]. The first case is more reasonable as a real-world threat scenario because the eavesdropper near the transmitter is unable to interrupt the beam without blocking the line of sight, which could allow the transmitter to detect its presence visually or based on variations in the power received by the legitimate receiver [10]. Locating the eavesdropper near the legitimate receiver represents the worst-case scenario for eavesdropping, which has been reported in several works [7], [8], [9], [10]. In this framework, physical layer security (PLS) solutions emerge as competitive candidates for low complexity, low delay, adaptability, and flexibility, with an inherent ability to adapt to the characteristics of the transmission medium, in contrast to the highly complex encryption methods of the higher layer [3]. In addition, FSO communication is highly susceptible to atmospheric conditions such as turbulence and weather conditions. Another notable parameter of FSO systems is the pointing error caused by a misalignment between transceiver peers [12]. The pointing error has two components: jitter and boresight. Jitter is the random displacement of the beam and the detector plane caused mainly by dynamic wind loads, weak earthquakes, and swaying buildings. While the non-zero boresight (NZB); which is the more general model of pointing error, refers to the fixed displacement between the beam center and the detector center caused by thermal expansion [12]. Another important limiting factor is fog, which leads to the reflection of the light beam and causes attenuation and scattering of the laser beam as it passes through the medium [13].

A number of research efforts on FSO-based systems are being conducted worldwide to address the aforementioned issues. For example, to evaluate the efficiency and availability of FSO links under different weather conditions, a four-channel dense wavelength division multiplexing (DWDM) scheme is proposed in [14], while return to zero (RZ) and non-return to zero (NRZ) modulation formats are used for the single FSO link in [15]. In addition, several securing approaches have been proposed for FSO systems inspired by the recent advances in PLS in the RF counterparts, including diversity methods [16], [17], transmit aperture selection (TAS) [18], artificial noise injection [19], and chaotic waveform modulation [20]. In another study [21], the PLS performance of the FSO system was analyzed considering the effects of correlated Malaga-M FSO links. The authors assumed that the main and wiretap channels are correlated due to the spatial proximity of the eavesdropper and legitimate receiver [21]. Other research groups analyzed the combined effect of NZB pointing error and atmospheric turbulence on the secrecy performance of single-input single-output (SISO) FSO systems in [13], [22], and [23]. However, the approximation of the Beckmann distribution into a modified Rayleigh distribution described in [24] and [25] is used in [13], [22], and [23] to model the generalized NZB pointing error. On the other hand, opportunistic scheduling selection is a potential technique to address the security and reliability issues of FSO communications, which allows the system to allocate the available channel resources to the user with the best channel quality to maximize the overall throughput of the system [26]. In such a technique, the transmitter needs accurate information about the channel quality of each user to make efficient scheduling decisions. Feedback techniques are used to obtain accurate channel state information (CSI) about the channel quality for each user. Feedback is important because it allows the transmitter to decide which user should transmit and when. In FSO systems, several feedback techniques can be used to obtain accurate CSI. For example, the acknowledgment/ negative acknowledgment (ACK/NACK) protocol provides feedback to the sender about the successful or failed delivery of a transmitted message. Another type of feedback mechanism is signal-to-noise ratio (SNR) feedback, which informs the transmitter about the SNR of the received signal [27]. Moreover, it has been shown in several studies that when the intercept probability (P_{int}) requirements (which considers the security metric of a system) are relaxed, the outage probability (P_{out}) performance (which is considered as a reliability metric) increases and vice versa [28], [29]. This implies a tradeoff between the security and reliability of wireless transmission in the presence of eavesdropping attacks, which is referred to as the security-reliability tradeoff (SRT). Although the notion of SRT has been studied in the context of FSO transmission [30], [31], these contributions mainly focused on the use of encryption algorithms to defend against eavesdropping attacks on such systems. In contrast, our work uses PLS instead of encryption techniques to characterize SRT achieved in multiple-input single-output (MISO) environments using opportunistic scheduling to improve the performance of the multiuser FSO system.

A. RELATED WORK

Studies have been conducted in the literature on the use of opportunistic selection scheduling to improve the diversity gain of FSO systems and mitigate the effects of channel variation. In this context, greedy scheduling (GS) and proportional fair scheduling (PFS) schemes are employed in [32] over weak turbulence with log-normal (LN) distribution for multiple-input multiple-output (MIMO) FSO system assuming equal user distance. Best user selection (BUS) scheduling is used in [33] to evaluate the performance of a multiuser single-input multiple-output (SIMO) FSO system over LN

and Gamma-Gamma (G-G) turbulence channels. However, the authors assume a constant SNR for all users, which means that path loss effects are either neglected or that each user is positioned at the same distance from the receiver, resulting in identical path losses. Such an assumption is unrealistic since users in a real system are likely to be distributed over a large area. Moreover, unlike RF systems, the fading variance in FSO systems is distance dependent [18], so the placement of users has a significant impact on the performance of such systems. In [34] and [35], the outage capacity and outage throughput of the MIMO FSO system is evaluated using different scheduling schemes over a weak turbulence channel. However, the effects of path loss and pointing error impacts are ignored in [32], [33], [34], and [35].

Another group of studies investigated opportunistic scheduling to improve the reliability of FSO systems [36], [37], [38], [39], [40], [41], [42], [43], [44]. In particular, the analysis has been conducted for strong turbulence with G-G distribution using repetition coding (RC) and transmit laser selection (TLS) scheduling to evaluate the outage probability of the MIMO FSO system in [36]. However, the approximation introduced in [45] for the MIMO FSO channel model was applied in [36] due to the complexity of the exact analysis of the MIMO FSO transmission over G-G turbulence channel. In [37], [38], [39], [40], [41], [42], and [43], the authors studied the reliability of mixed FSO/RF relay systems considering Malaga-M/Nakagami-m distributions in [37] while Rayleigh/G-G distributions are used in [38], [39], and [40]. Transmit aperture selection (TAS) and BUS schemes were used in FSO and RF links respectively to select between signals that transmitted over these links [37]. However, the pointing error and path loss were not considered in [37], [38], and [45]. In [38], [39], [40], [41], [42], and [43], the BUS scheme is used in multiuser RF links to improve the reliability of the mixed RF/FSO relay system over the Rayleigh fading channel. It is worth noting that the Malaga-M distribution was chosen to represent the multiple-input single-output (MISO) FSO links with asymptotic analysis in [37], while the G-G distribution characterizes the SISO FSO channel in [38], [39], [40], [41], [42], and [43]. Recently, there has been a growing research interest in the use of FSO in unmanned aerial vehicle (UAV) technology. For example, in [44], a hovering UAV is presented that serves as a decode and forward relay (DF) between the ground central unit (CU) and multiple ground users (GU) for a mixed FSO/RF system over LN/Nakagmi-IG fading channels. For the FSO, TAS is applied for opportunistic selection, while opportunistic GU scheduling (GUS) is used in the RF links to improve the outage probability of the system [44].

Another group of studies investigated opportunistic scheduling to improve the security of mixed RF/FSO [46], [47], [48] and MISO FSO [18] systems against eavesdropping attacks. For example, the authors studied the security of the mixed RF/FSO relay system, by using the BUS scheme in the multiuser RF link [46]. They also studied the impact of eavesdropping attacks in RF links on the security system performance. Later, another study investigated the impact of RF co-channel interference (CCI) on SRT for the same system [47]. However, the SISO FSO link with G-G distribution is considered an extension of the RF link with multiple users in [46], [47], and [48]. Finally, the security performance of the MISO FSO system with the BUS scheme is examined in [18]. However, in [18], the combined effect of Malaga-M turbulence and zero boresight (ZB) pointing error is used with the same approximation method for the channel model used in [37].

In the above and related literature, we find several research gaps in examining the tradeoff between the security and reliability of the FSO system that needs to be addressed. First, FSO transmission was limited to zero boresight pointing error and random jitter. Although the statistical analysis of NZB pointing error for the FSO system has been extensively studied in the literature using a limited model (i.e., modified Rayleigh model [24]), it has never been addressed for the SRT of the FSO system considering a more general pointing error model (i.e., Rician distribution [49]).

Second, for moderate to strong atmospheric turbulence, the G-G and Malaga-M distributions were mainly chosen. These models are mathematically complicated because they incorporate Bessel and Meijer G-functions in their probability density functions (PDF). The Fisher-Snedecor $\mathcal{F}$ distribution was recently introduced to characterize atmospheric turbulence over FSO links [50]. In [50], the authors showed that the proposed distribution can provide better agreement with experimental and computer results than the well-known G-G and LN distributions and various practical propagation scenarios. Moreover, the PDF and the cumulative distribution function (CDF) of the $\mathcal{F}$ distribution are presented in a simplified form in comparison with other known distributions such as the G-G, the M-Malaga and the inverse Gaussian-Gamma distributions [50]. Due to their generality, several well-known fading models such as the Nakagami-m, the Rayleigh, and the one-sided Gaussian distributions can be derived as special cases of the $\mathcal{F}$ distribution. Moreover, it has been shown that the $\mathcal{F}$ distribution is a good approximation, both theoretically and experimentally, to other composite fading distributions such as the generalized K-model with lower computational complexity [51]. It is worth mentioning that there is an increasing interest in the analysis of FSO performance in $\mathcal{F}$ turbulence [52], [53], [54], [55], [56], [57]. Third, signal attenuation in FSO transmissions is assumed to be deterministic and quantified using a visibility range, e.g., lower attenuation in a clear sky and greater loss of signal power in fog [58]. As far as the authors are aware, there are no analyses for the SRT of the FSO system under the influence of random fog, generalized pointing error, and atmospheric turbulence. Fourth, the user scheduling studied in this paper has some advantages over conventional user selection [33], [34], [35], [36] because it avoids using an approximation to express the end-to-end SNR PDF for the MISO FSO system over

TABLE 1. Related literature on SRT based on opportunistic schedule selection of the multiuser FSO systems.

Reference	System Model	Channel model	Pointing error	Fog's path loss	Scheduling Scheme	Objective
[18]	MISO FSO	Malaga-M	ZB	No	BUS	System security enhancement
[26]	MIMO FSO	Malaga-M	NZB	No	TAS	SRT improvement
[32]	MIMO FSO	LN	No	No	PFS, GS	Exploring the multiuser diversity gain
[33]	SIMO FSO	LN, G-G	No	No	BUS	Exploring the multiuser diversity gain
[34]	MIMO FSO	LN	No	No	RRS, BUS	Exploring the multiuser diversity gain
[35]	SIMO FSO	LN	No	No	BUS	Exploring the multiuser diversity gain
[36]	MIMO FSO	G-G	No	No	RC, TLS	System reliability improving
[37]	SIMO mixed FSO/RF	Malaga-M/ Nakagami-m	No	No	TLS, BUS	System reliability improving
[38]	MISO mixed RF/FSO	Rayleigh/G-G	Jitter	No	BUS	System reliability improvement
[39]	MISO mixed RF/FSO	Rayleigh/G-G	Jitter	No	BUS	System reliability improvement
[40]	MISO mixed RF/FSO	Rayleigh/G-G	No	No	BUS	System reliability improvement
[41]	MIMO mixed FSO/RF	G-G/shadowed κ-μ	Jitter	No	TAS/BUS	System reliability improvement
[43]	SIMO mixed FSO/RF	G-G/Nakagami-m	Jitter	No	BUS	System reliability improvement
[44]	MIMO mixed FSO/RF	LN/Nakagmi-IG	Jitter	No	TAS/GUS	System reliability improvement
[46]	SIMO mixed RF/FSO	Nakagami-m/G-G	Jitter	No	BUS	System security enhancement
[47]	SIMO mixed RF/FSO	Nakagami-m/G-G	Jitter	No	BUS	System security enhancement
[48]	SIMO mixed RF/FSO	Nakagami-m/G-G	ZB	No	TAS	System security enhancement
[This paper]	MISO FSO	Fisher-Sendecor $\mathcal{F}$	NZB, and jitter	Yes	RRS, proposed OUS	Security, reliability, and SRT improvement

weak to strong turbulence channels. In this paper, an optimal user scheduling (OUS) scheme is proposed to protect the multiuser FSO transmission against the eavesdropping attack, where a user with the highest secrecy capacity is selected to transmit his confidential message to the legitimate receiver in this case. Fifth, although the friendly jamming (FJ) technique has been studied to improve the secrecy performance of the multiuser RF link of the mixed RF/FSO system [46], this technique has never been used in multiuser FSO systems. We employ the FJ technique in which the worst user serves as a friendly jammer by transmitting a jamming signal known to the authorized receiver to jam the eavesdropper and improve the secrecy performance of the FSO system.

B. MOTIVATION AND CONTRIBUTIONS

Despite their considerable potential as excellent candidates for future backhaul networks and a variety of other applications, the SRT of multiuser FSO systems has not been studied in depth in the open literature, using opportunistic schedule selection to improve the security and reliability of these systems. To the authors' knowledge, there are no analyses for the SRT of multiuser FSO systems under the influence of random fog, generalized pointing error, and atmospheric turbulence with $\mathcal{F}$ distribution. Table 1 provides a summary of the current state-of-the-art research on the SRT of FSO systems. The main contributions of this work can be summarized as follows:

1) An optimal user scheduling scheme is proposed for improving the security of the multiuser FSO transmission contrary to [26], where only a conventional TAS scheme is used. The conventional RRS is also considered a benchmark.
2) Exact and asymptotic closed-form expressions of the intercept probability, outage probability, and security-reliability tradeoff for the RRS and the proposed OUS schemes are derived under the combined effect of fog-induced fading, generalized pointing error, and atmospheric turbulence with $\mathcal{F}$ distribution contrary to [26], where only the Malaga-M turbulence and pointing error effect is considered.
3) A friendly jamming technique has been introduced for improving the secrecy performance of the considered system and the SRT has been found for this case. Moreover, Monte-Carlo simulations verify the accuracy of the analytical results.

The following is the outline for this paper: Section II presents models of the multiuser FSO system and channel in consideration, while Section III develops an exact analytical

expression for the intercept probability of the proposed OUS and RRS schemes for the considered systems. The asymptotic analysis of the intercept probability of the OUS and RRS schemes is introduced in Section IV. Section V considers the outage probability analysis. The SRT of the considered multiuser FSO system is presented in Section VI. The FJ model for enhancing the SRT of the considered system is presented in Section VII. Section VIII has several interesting numerical examples as well as instructive discussions. Finally, Section IX brings the paper to a conclusion.

II. SYSTEM AND CHANNEL MODELS

We consider a multiuser FSO communication system consisting of a transmitter T with M users, where each user is equipped with a single aperture and communicates with a single receiver r equipped with a photodetector via legitimate $T \rightarrow r$ links. For each transmitting device in T, a DC bias is added to the intensity-modulated signal by the laser diode to avoid a negative value of the modulated signal. Then, the laser diode of each device transmits the user's message through the $T \rightarrow r$ links. Since the laser beam emitted by T suffers divergence due to optical diffraction, we assume that a single eavesdropper e is located in the divergence region, which means that e is close to r and is able to obtain part of the laser beam that is not captured by r as shown in Fig. 1. Just as the legitimate transmitters and receivers in the multiuser FSO system model are static devices placed on buildings in common scenarios, we also assume that a physically feasible device that can eavesdrop is static. The transmit aperture of the ith user, $i \in \{1, 2, \ldots, M\}$, on the transmitting side is directed to the aperture of the receiver r, whose receive aperture is also directed to the transmit aperture of the ith user. In this work, M transmitting users at T are alternatively selected for transmission in time-division multiplexing (TDM), and only one transmitting user has access to the channel in each time slot. To ensure independence between the main channel and the eavesdropping channel, the spacing between the legitimate receiver and the eavesdropper is larger than the fading correlation length [59]. The values of the atmospheric refractive index structure parameter, C_n^2 for weak, moderate, and strong turbulence, are given as 5×10^{-15} $m^{-2/3}$, 1.25×10^{-14} $m^{-2/3}$, and 5×10^{-14} $m^{-2/3}$, respectively [57], for an FSO transmission with an optical wavelength of $\lambda = 1550$ nm. Contrary to other optical transmission wavelengths, the 1550 nm band is well suited for free-space transmission due to its low attenuation and the proliferation of high-quality transmitter and detector components. In addition, laser beams with a wavelength of 1550 nm are more eye safety since the laser beam is absorbed by the lens and cornea at a wavelength of more than 1400 nm and thus does not form a destructive focus that could cause damage to the retina [6].

Assuming that the noncoherent intensity modulation/direct detection IM/DD technique and the on-off keying (OOK) modulation with $x \in \{0, P_i\}$ and P_i is the average transmitted optical power in this work. For signal transmission between

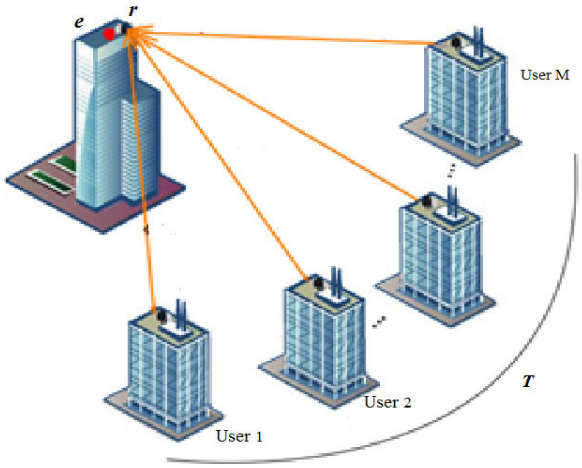

FIGURE 1. Multiuser FSO communication system model showing the transmitting users, the receiver, and the eavesdropping device.

the ith transmitting user and the receiving aperture at r or e, the PD converts the incident optical power into an electrical signal by direct detection. After filtering out the DC bias, the electrical signal is demodulated to obtain the original information stream. The received signal y_{il} at l, $(l \in \{r, e\})$ can be written as follows

$$y_{il} = I_{il} x_i + w_{il} \tag{1}$$

where x_i is the optical signal of the ith transmitted user received in r or e, w_{il} is the additive white Gaussian noise with mean zero and variance N_o, and $I_{il} = I_{f_{il}} I_{p_{il}} I_{t_{il}}$ is the channel coefficient of the ith link. Here, $I_{f_{il}}$ denotes the path loss due to fog-induced fading, $I_{p_{il}}$ represents the generalized pointing error, and $I_{t_{il}}$ signifies the atmospheric turbulence. The instantaneous received electrical SNR for the ith user is given by

$$\gamma_l = \frac{2P_i^2 I_{il}^2}{N_0} = \bar{\gamma}_{il} I_{il}^2 \tag{2}$$

where $\bar{\gamma}_{il}$ denotes the average SNR of the ith user received from either r or e via $T \rightarrow r$ or $T \rightarrow e$ link, respectively.

To analyze the statistical performance of the FSO system in (1), we need density functions of path loss, generalized pointing error, and atmospheric turbulence, which are presented below.

The PDF of the path loss due to fog-induced fading is given as [57]

$$f_{I_{f_{il}}}(x) = \frac{z_{il}^{k_{il}}}{\Gamma(k_{il})} \left(log \frac{1}{x}\right)^{k_{il}-1} x^{z_{il}-1}, \quad 0 < x \leq 1 \tag{3}$$

where $z_{il} = 4.343/\beta_{il} d_{il}$, d_{il} is the distance between the transmitter and the receiver of the ith user, $k_{il} > 0$, $\beta_{il} > 0$ is the shape parameter and the scale parameter of the fog, receptively, $\Gamma(\cdot)$, and gamma function. Next, we consider the Rician distribution to model the non-zero

boresight and random jitter of the pointing error $I_{p_{il}}$ [49]

$$f_{I_{p_{il}}}(x) = \frac{\rho_{il}^2 exp\left(\frac{-s_{il}^2}{2\sigma_{il}^2}\right)}{A_{il}^{\rho_{il}^2}} x^{\rho_{il}^2-1} I_o\left(\frac{s_{il}}{\sigma_{il}^2}\sqrt{\frac{w_{zeq_{il}}^2 \ln\frac{A_{il}}{x}}{2}}\right)^{k_{il}-1} \tag{4}$$

where $0 < x \leq A_{il}$, $w_{zeq_{il}}^2 = \frac{w_{z_{il}}^2}{2v_{il}exp(-v_{il}^2)}$, $A_{il} = [erf\ (v_{il})]^2$ with $v_{il} = \sqrt{\frac{r_{il}^2\pi}{2w_{z_{il}}^2}}$ as the ratio of aperture radius r_{il} and beamwidth $w_{z_{il}}$, and $\rho_{il} = \frac{w_{zeq_{il}}}{2\sigma_{il}}$ with σ_{il} as the standard deviation of the jitter and the equivalent beamwidth $w_{zeq_{il}}$. Here, $s_{il} = \sqrt{\mu_{x_{il}}^2 + \mu_{y_{il}}^2} \neq 0$ models the NZB, where $\mu_{x_{il}} \neq 0$ and $\mu_{y_{il}} \neq 0$ denote the horizontal and vertical displacement, respectively, between the center of the beam and the center of the detector. $I_o(\cdot)$ is a modified Bessel function [49].

According to the $\mathcal{F}$ distribution model, the PDF of irradiance I_{til} is given by [52]

$$f_{I_{t_{il}}}(x) = \frac{a_{il}^{a_{il}}\ (b_{il}-1)^{b_{il}}\ x^{\alpha_{il}-1}}{\beta\ (\alpha_{il}, b_{il})\ (b_{il}-1)^{\alpha_{il}+b_{il}}\ (B_{il}x+1)^{\alpha_{il}+b_{il}}} \tag{5}$$

where $0 < I_{t_{il}} < \infty$, $B_{il} = \frac{a_{il}}{(b_{il}-1)}$, $\beta\ (\cdot)$ is denotes the Beta function. The parameters, $a_{il} = \frac{1}{exp\left(\sigma_{In\mathcal{S}}^{2_{il}}\right)-1}$ and $b_{il} = \frac{1}{exp\left(\sigma_{In\mathcal{L}_{il}}^2\right)-1} + 2$ are two key parameters describing the atmospheric refractive-index structure parameter, the propagation path length, and the inner and outer scale of turbulence, respectively, which depend on the small-scale $\sigma_{In\mathcal{S}}^{2_{il}}$ and large-scale $\sigma_{In\mathcal{L}_{il}}^2$ log-irradiance variances.

Assuming spherical wave propagation, the small-scale log-irradiance variance, $\sigma_{In\mathcal{S}}^{2_{il}}$, is given by [3]

$$\sigma_{In\mathcal{S}}^{2_{il}} = \frac{0.51\delta_{SPil}^2\left(1+0.69\delta_{SPil}^{12/5}\right)^{-5/6}}{1+0.90d_{il}^2(\sigma_{il}/\delta_{SPil})^{12/5}+0.62d_{il}^2\sigma_{il}^{12/5}} \tag{6}$$

where δ_{SPil}^2 represents the spherical wave scintillation index assuming weak irradiance fluctuations, which is given by [3]

$$\begin{aligned}\delta_{SPil}^2 = 9.65\sigma_{il}^2 \Bigg\{0.4(1+9/Q_{il}^2)^{11/12}\Bigg[\sin\left(\frac{11}{6}\arctan\frac{Q_{il}}{3}\right) \\ + \frac{2.61}{(9+Q_{il}^2)^{1/4}}\sin\left(\frac{4}{3}\arctan\frac{Q_{il}}{3}\right) - \frac{0.52}{(9+Q_{il}^2)^{7/24}} \\ \times \sin\left(\frac{5}{4}\arctan\frac{Q_{il}}{3}\right) - 3.5/Q_{il}^{5/6}\Bigg\},\end{aligned} \tag{7}$$

where $Q_{il} = 10.89d_{il}/(\mathcal{B}_{il}l_{0il}^2)$ with l_{0il} denoting the inner scale of turbulence in mm, and $\mathcal{B}_{il} = 2\pi/\lambda$ is the optical wave number. Furthermore, $\sigma_{il}^2 = 0.5C_n^2\mathcal{B}_{il}^{7/6}d_{il}^{11/6}$ is the Rytov variance. The large-scale log-irradiance variance $\sigma_{In\mathcal{L}_{il}}^2$ can be expressed as [3]

$$\sigma_{In\mathcal{L}_{il}}^2 = \sigma_{In\mathcal{L}_{il}}^2(l_{0il}) - \sigma_{In\mathcal{L}_{il}}^2(L_{0il}) \tag{8}$$

where $\sigma_{In\mathcal{L}_{il}}^2(l_{0il})$ and $\sigma_{In\mathcal{L}_{il}}^2(L_{0il})$ denote the large-scale log-irradiance variances, that take into account inner- and outer-scale effects as defined in [52] with L_{0il} being the outer scale. The PDF and CDF of the $\mathcal{F}$ turbulence channel combined with the generalized pointing error and fog-induced fading are given as follows [57]

$$\begin{aligned}&f_{\gamma_{il}}(\gamma) \\ &= \frac{a_{il}^{a_{il}} z_{il}^{k_{il}} \rho_{il}^2 exp\left(\frac{-s_{il}^2}{2\sigma_{il}^2}\right)}{2A_{il}^{a_{il}}\beta\ (a_{il}, b_{il})\ (b_{il}-1)^{a_{il}}\sqrt{\gamma\bar{\gamma}_{il}}} \sum_{j=0}^{\infty}\frac{1}{j!} \\ &\times\left(\frac{s_{il}^2 w_{zeq_{il}}^2}{8\sigma_{il}^4}\right)^j\left(\sqrt{\frac{\gamma}{\bar{\gamma}_{il}}}\right)^{a_{il}-1} G_{2+j+k_{il},2+j+k_{il}}^{2+j+k_{il},1}\left(\frac{B_{il}}{A_{il}}\sqrt{\frac{\gamma}{\bar{\gamma}_{il}}}\middle| \begin{matrix} 1-a_{il}-b_{il}, \{1+\rho_{il}^2-a_{il}\}_0^{j+1}, \{1+z_{il}-a_{il}\}_0^{k_{il}} \\ 0, \{\rho_{il}^2-a_{il}\}_0^{j+1}, \{z_{il}-a_{il}\}_0^{k_{il}} \end{matrix}\right)\end{aligned} \tag{9}$$

$$\begin{aligned}&F_{\gamma_{il}}(\gamma) \\ &= \frac{a_{il}^{a_{il}} z_{il}^{k_{il}} \rho_{il}^2 exp\left(\frac{-s_{il}^2}{2\sigma_{il}^2}\right)}{2A_{il}^{a_{il}}\beta\ (a_{il}, b_{il})\ (b_{il}-1)^{a_{il}}} \sum_{j=0}^{\infty}\frac{1}{j!} \\ &\times\left(\frac{s_{il}^2 w_{zeq_{il}}^2}{8\sigma_{il}^4}\right)^j\left(\sqrt{\frac{\gamma}{\bar{\gamma}_{il}}}\right)^{a_{il}} G_{3+j+k_{il},3+j+k_{il}}^{2+j+k_{il},2}\left(\frac{B_{il}}{A_{il}}\sqrt{\frac{\gamma}{\bar{\gamma}_{il}}}\middle| \begin{matrix} 1-a_{il}-b_{il}, 1-a_{il}, \{1+\rho_{il}^2-a_{il}\}_0^{j+1}, \{1+z_{il}-a_{il}\}_0^{k_{il}} \\ 0, \{\rho_{il}^2-a_{il}\}_0^{j+1}, \{z_{il}-a_{il}\}_0^{k_{il}}, -a_{il} \end{matrix}\right)\end{aligned} \tag{10}$$

Next, for performance compression, we analyze the security and reliability performances of the multiuser FSO system with the conventional RRS and the proposed optimal user scheduling scheme under the combined effect of the three channel impairments for better performance evaluation.

A. ROUND-ROBIN SCHEDULING

Let us first consider conventional round-robin scheduling as a benchmark, where M users take turns accessing a given channel, and thus each user has an equal chance to deliver his confidential message to the receiver. Without loss of generality, we assume that the ith user is scheduled to transmit its signal x_i with power P_i and rate $\mathcal{R}$, where $\mathcal{R}$ is the maximum secrecy rate from the ith user to the receiver that guarantees that the ergodic capacity is achieved by legitimate transmission. Using the Shannon capacity formula [60] and (1), the channel capacity of the main channel can be calculated as follows

$$C_{ir} = log_2\left(1+\frac{|I_{ir}|^2 P_i}{N_0}\right) \tag{11}$$

Due to the open nature of the free-space optical transmission, the eavesdropper can overhear the signal sent by the ith user and attempt to decode x_i from the intercepted signal. Therefore, from (1), the channel capacity of the eavesdropping channel between ith user and the eavesdropper e can be

calculated as follows

$$C_{ie} = log_2\left(1 + \frac{|I_{ie}|^2 P_i}{N_0}\right) \tag{12}$$

where I_{ie} denotes the atmospheric turbulence over the interception channel. The secrecy capacity, C, which characterizes the transmission from the ith specified user to the r, is the difference between the channel capacity of the legitimate and the eavesdropping channel as in [3]

$$C = C_{ir} - C_{ie} \tag{13}$$

B. PROPOSED OPTIMAL USER SCHEDULING

In this subsection, we present an optimal user scheduling scheme to maximize the secrecy capacity of legitimate transmission. In this case, a user with the highest secrecy capacity should be selected and scheduled to transmit its data to the legitimate receiver. Therefore, from (13), the OUS criterion U_o is as follows

$$\begin{aligned} U_o &= arg\max_{i\in\mathcal{M}} C \\ &= arg\max_{i\in\mathcal{M}} \frac{\left(1 + \frac{|I_{ir}|^2 P_i}{N_0}\right)}{\left(1 + \frac{|I_{ie}|^2 P_i}{N_0}\right)} \end{aligned} \tag{14}$$

where $\mathcal{M}$ represents the set of M users. From (14), it can be seen that the channel state information of each user is required to find the optimal user and then send the estimated CSI to the receiver. After collecting the CSI of all users, it can easily determine the optimal user and notify the entire network. The feedback signaling described in [61] is utilized for accurate CSI estimation. Feedback of $(log_2 M)$ bits is required to estimate the CSI of each user, and an additional 1-bit feedback is required to activate the optimal user for the next transmission. Thus, the proposed OUS method requires a total of $(1 + log_2 M)$ feedback bits. Therefore, the secrecy capacity of legitimate transmissions based on the proposed OUS scheme can be calculated from (14) in the presence of e as follows

$$C^O = arg\max_{i\in\mathcal{M}} \frac{\left(1 + \frac{|I_{ir}|^2 P_i}{N_0}\right)}{\left(1 + \frac{|I_{ie}|^2 P_i}{N_0}\right)} \tag{15}$$

III. INTERCEPT PROBABILITY BASED ON MULTIUSER SCHEDULING

In this section, we investigate the secrecy performance of the considered multiuser FSO system in the presence of an eavesdropper e trying to intercept the signal of the transmitting user through the eavesdropping channel. The intercept probability is the probability that the secrecy capacity of the legitimate link becomes non-positive. In other words, the intercept probability is the probability that the capacity of the interception channel exceeds $\mathcal{R}$, as [3]

$$P_{int} = P_r\left[C_{ir} < C_{ie}\right] = P_r\left[C_{ie} > \mathcal{R}\right] \tag{16}$$

Substituting (11) and (12) in (16), yields

$$\begin{aligned} P_{int} &= P_r\left[|I_{ir}|^2 < |I_{ie}|^2\right] \\ &= \int_0^\infty \int_0^{\gamma_{ie}} f_{\gamma_{ir}}(\gamma_{ie}) f_{\gamma_{ie}}(\gamma_{ie})\, d\gamma_{ir} d\gamma_{ie} \\ &= \int_0^\infty F_{\gamma_{ir}}(\gamma_{ie}) f_{\gamma_{ie}}(\gamma_{ie})\, d\gamma_{ie} \end{aligned} \tag{17}$$

The integral in (17) can be solved using [62, Eq. (07.34.21.0011.01)], so that the intercept probability of the system under consideration can be calculated as follows

$$\begin{aligned} P_{int} = \Psi_1 \sum_{j=0}^{\infty} \frac{1}{j!}\left(\frac{s_{ir}^2 w_{z_{eq_{ir}}}^2}{8\sigma_{ir}^4}\right)^j \sum_{\acute{j}=0}^{\infty} \frac{1}{\acute{j}!}\left(\frac{s_{ir}^2 w_{z_{eq_{ir}}}^2}{8\sigma_{ir}^4}\right)^{\acute{j}} \\ \times G_{5+2j+k_{ir}+k_{ie},5+2j+k_{ir}+k_{ie}}^{4+j+k_{ie},3+2j+k_{ir}}\left(\frac{A_{ir}B_{ie}}{A_{ie}B_{ir}}\sqrt{\lambda}_{re}\,\middle|\, \begin{matrix} k_1 \\ k_2 \end{matrix}\right) \end{aligned} \tag{18}$$

where $\lambda_{re} = \frac{\bar{\gamma}_{ir}}{\bar{\gamma}_{ie}}$, being the average main to eavesdropper's signal ratio (MER) throughout this work,

$$\begin{aligned} &\Psi_1 \\ &= \frac{a_{ir}^{a_{ir}} a_{ie}^{a_{ie}} z_{ir}^{k_{ir}} z_{ie}^{k_{ie}} \rho_{ir}^2 \rho_{ie}^2 exp\left(\frac{-s_{ir}^2}{\sigma_{ir}^2}\right) exp\left(\frac{-s_{ie}^2}{\sigma_{ie}^2}\right)\left(\frac{B_{ir}}{A_{ie}\sqrt{\bar{\gamma}_{ir}}}\right)^{\frac{a_{ie}-a_{ir}}{2}-1}}{2A_{ir}^{a_{ir}} A_{ir}^{a_{ir}} \beta(a_{ir}, b_{ir})\beta(a_{ie}, b_{ie})(b_{ir}-1)^{a_{ir}}(b_{ie}-1)^{a_{ie}}\sqrt{\bar{\gamma}_{ie}}}, \\ &k_1 \\ &= 1 - a_{ie} - b_{ie}, \quad \left\{1 + \rho_{ie}^2 - a_{ie}\right\}_0^{j+1}, \quad \frac{a_{ie}-a_{ir}}{2}, \\ &\frac{a_{ie}-a_{ir}}{2} - \left\{\rho_{ir}^2 - a_{ir}\right\}_0^{j+1}, \quad \frac{a_{ie}-a_{ir}}{2} - \{1 + z_{ir} - a_{ir}\}_0^{k_{ir}}, \\ &\{1 + z_{ie} - a_{ie}\}_0^{k_e}, \quad \text{and } k_2 = 0, \quad \left\{\rho_{ie}^2 - a_{ie}\right\}_0^{j+1}, \\ &\frac{a_{ie}-a_{ir}}{2}, \quad -(1 - a_{ir} - b_{ir}), \quad \frac{a_{ie}-a_{ir}}{2} - (1 - a_{ir}), \\ &\frac{a_{ie}-a_{ir}}{2}, \quad -\left\{1 + \rho_{ir}^2 - a_{ir}\right\}_0^{j+1}, \\ &\frac{a_{ie}-a_{ir}}{2} - \{1 + z_{ir} - a_{ir}\}_0^{k_{ir}}, \quad \{z_{ie} - a_{ie}\}_0^{k_{ie}}. \end{aligned}$$

In the RRS scheme, M users take turns transmitting to r so the intercept probability of the RRS is the mean of the intercept probabilities of the M users, resulting in the following

$$P_{int}^R = \frac{1}{M}\sum_{i=1}^{M} P_{int} \tag{19}$$

where P_{int} is given by (18).

Next, we will obtain an exact intercept probability of the proposed OUS scheme considering the combined channel effects. Using (15), we obtain the intercept probability of the OUS scheme as

$$\begin{aligned} P_{int}^O &= P_r\left[C^O < 0\right] \\ &= P_r\left[\max_{i\in\mathcal{M}} log_2\left(\frac{1 + \frac{|I_{ir}|^2 P_i}{N_0}}{1 + \frac{|I_{ie}|^2 P_i}{N_0}}\right) < 0\right] \\ &= P_r\left[\max_{i\in\mathcal{M}}\left(\frac{(N_0 + |I_{ir}|^2 P_i)}{(N_0 + |I_{ie}|^2 P_i)}\right) < 1\right], \end{aligned} \tag{20}$$

Considering that for different users $i \in \mathcal{M}$, the random variables $|I_{ir}|^2$ and $|I_{ie}|^2$ are independent, we can simplify (20) as given by

$$\begin{aligned} P_{int}^{O} &= \prod_{i=1}^{M} P_r\left[C < 0\right] \\ &= \prod_{i=1}^{M} P_r\left[|I_{ir}|^2 < |I_{ie}|^2\right] \\ &= \prod_{i=1}^{M} P_{int} \end{aligned} \tag{21}$$

where P_{int} is given by (18). So far, we have derived the closed-form intercept probability for both the RRS and the proposed OUS methods under the influence of the combined channel effect. It is worth noting that the intercept probability expressions given by (19) and (21) can be used for numerical performance evaluation, but they do not provide insight into the effect of the number of users on the intercept probability. Therefore, an asymptotic analysis of the intercept probability is presented in the following section to characterize the performance of the diversity order of the considered system.

IV. ASYMPTOTIC INTERCEPT PROBABILITY ANALYSIS OF USER SCHEDULING

In this section, we analyze the asymptotic intercept probability of both the RRS and the proposed OUS methods. We will examine the asymptotic intercept probability in the range of high MER values as $\lambda_{re} \to \infty$. The asymptotic analysis of (18) can be obtained via the expansion of Meijer's G-function [63, Eq. (26)] as follows

$$\begin{aligned} &P_{int}^{Asy} \\ &= \Psi_1 \sum_{j=0}^{\infty} \frac{1}{j!}\left(\frac{s_{ir}^2 w_{z_{eq_{ir}}}^2}{8\sigma_{ir}^4}\right)^j \sum_{J=0}^{\infty} \frac{1}{J!}\left(\frac{s_{ie}^2 w_{z_{eq_{ie}}}^2}{8\sigma_{ie}^4}\right)^{\mathcal{J}} \\ &\times \sum_{v=1}^{4+j+k_{ie}} \left(\frac{A_{ir}B_{ie}}{A_{ie}B_{ir}}\sqrt{\lambda}_{re}\right)^{\grave{V}_{\grave{u}}} \frac{\prod_{\grave{u}=1,\grave{u}\neq\grave{v}}^{4+j+k_e} \Gamma(\grave{V}_{\grave{v}} - \grave{V}_{\grave{u}})}{\prod_{\grave{u}=4}^{5+2j+k_{ir}+k_{ie}} \Gamma(\grave{U}_{\grave{v}} - \grave{V}_{\grave{u}})} \\ &\times \frac{\Gamma(a_{ie} + b_{ie} + \grave{V}_{\grave{u}})\Gamma(\frac{2+a_{ir}-a_{ie}}{2} + \grave{V}_{\grave{u}})}{\Gamma(\frac{2-a_{ie}-a_{ir}+2\grave{V}_{\grave{u}}}{2})\Gamma(\frac{a_{ie}+a_{ir}-2+2\grave{V}_{\grave{u}}}{2})\Gamma(\frac{3a_{ir}-a_{ie}+\grave{V}_{\grave{u}}+2\grave{V}_{\grave{u}}}{2})} \end{aligned} \tag{22}$$

where $\grave{U}_{\grave{v}} = \grave{U}_{\grave{u}} = k_1$, $\grave{V}_{\grave{v}} = \grave{V}_{\grave{u}} = k_2$. Moreover, it is straightforward to compute the asymptotic intercept probability when using RRS or OUS scheduling by substituting (22) into (19) and (21), respectively.

Moreover, the derived asymptotic forms can be used to determine the secrecy diversity performance of multiuser FSO systems to intuitively determine the impact of the number of active users in the system or other system parameters on secrecy. Using (22) and computing the exponent of $\bar{\gamma}_{ir} = \bar{\gamma}_{ie} = \bar{\gamma}$, the diversity order is derived as $\Lambda = min\left\{\frac{z_i}{2}, \frac{\rho_i^2}{2}, \frac{a_i}{2}\right\}$. Note that the diversity order is independent of the parameters of the pointing error. It can now be concluded from (22) that the RRS secrecy diversity order can be determined as $\Lambda^R = min\left\{\frac{z_i}{2}, \frac{\rho_i^2}{2}, \frac{a_i}{2}\right\}$. While the OUS secrecy diversity order has the following form: $\Lambda^O = \sum_{i=1}^{M} min\left\{\frac{z_i}{2}, \frac{\rho_i^2}{2}, \frac{a_i}{2}\right\}$.

V. OUTAGE PROBABILITY ANALYSIS

The outage probability, which is an important measure of the system's transmission reliability, can be defined as the probability that the SNR at the receiver falls below a certain outage threshold γ_{th}. Mathematically, $P_{out} = P_r[\gamma_{sel} \leq \gamma_{th}]$, where $P_r[\cdot]$ denotes the probability operation, γ_{sel} is the SNR that r receives from the selected user, and $\gamma_{th} = 2^{\mathcal{R}} - 1$, where $\mathcal{R}$ is the expected secrecy rate. Using opportunistic RRS and OUS methods, the outage probability can be obtained by replacing γ with γ_{th} in the CDF expression of (10) as follows

$$P_{out}^{R} = P_r\left[\gamma_{sel} \leq \gamma_{th}\right] = \frac{1}{M}\sum_{i=1}^{M} F_{\gamma_{sel}}\left(\gamma_{th}\right) \tag{23}$$

$$P_{out}^{O} = \prod_{i=1}^{M} F_{\gamma_{sel}}\left(\gamma_{th}\right) \tag{24}$$

To gain further insight into the regime with high SNR, we have analyzed the asymptotic behavior of P_{out} and present it in an easy-to-follow form with good accuracy. To analyze the asymptotic behavior of the outage probability for the scheduling schemes in the range of high SNR values, we recall the series expansion of Meijer's G-function from [63, Eq. (26)] and after some algebraic manipulations, we obtain

$$\begin{aligned} P_{out}^{Asy} &= \Psi_2 \sum_{j=0}^{\infty} \frac{1}{j!}\left(\frac{s_{ir}^2 w_{z_{eq_{ir}}}^2}{8\sigma_{ir}^4}\right)^j \left(\sqrt{\frac{\gamma_{th}}{\bar{\gamma}_{ir}}}\right)^{a_{ir}} \\ &\times \sum_{v=1}^{2+j+k_{ir}} \left(\frac{B_{ir}}{A_{ir}}\sqrt{\frac{\gamma_{th}}{\bar{\gamma}_{ir}}}\right)^{V_u} \frac{\prod_{v=1,v\neq u}^{2+j+k_{ir}} \Gamma(V_v - V_u)}{\prod_{v=3}^{3+j+k_{ir}} \Gamma(U_v - V_u)} \\ &\times \frac{\Gamma(a_{ir} + b_{ir} + V_u)\Gamma(a_{ir} + V_u)}{\Gamma(1 + a_{ir} + V_u)} \end{aligned} \tag{25}$$

where $\Psi_2 = \frac{a_{ir}^{a_{ir}} z_{ir}^{k_{ir}} \rho_{ir}^2 exp\left(\frac{-s_{ir}^2}{2\sigma_{ir}^2}\right)}{2A_{ir}^{a_{ir}} \beta(a_{ir}, b_{ir})(b_{ir}-1)^{a_{i,r}}}$, $U_v = U_u = k_3$, $V_v = V_u = k_4$, $k_3 = 1 - a_{ir} - b_{ir}, 1 - a_{ir}, \left\{1 + \rho_{ir}^2 - a_{ir}\right\}_0^{j+1}, \{1 + z_{ir} - a_{ir}\}_0^{k_{ir}}$, and $k_4 = 0, \left\{\rho_{ir}^2 - a_{ir}\right\}_0^{j+1}, \{z_{ir} - a_{ir}\}_0^{k_{ir}}, -a_{ir}$.

In the same way, the asymptotic outage probability of RRS and OUS can be easily found by applying (25) in the user selection criteria of both schemes.

VI. SECURITY–RELIABILITY TRADEOFF

In this section, we develop an expression for the SRT for the multiuser FSO system that takes into account the given outage threshold of the system. The outage threshold corresponds to the threshold SNR, γ_{th}, below which detection is very unlikely at the given data rate. An interception occurs when the eavesdropper detects the signal with an SNR above this threshold. In the meantime, the SRT can be represented as follows [11]

$$\begin{aligned} P_{int}^{th} &= P_r\left(\gamma_{ir} \leq \gamma_{ie}, \gamma_{ie} > \gamma_{th}\right) \\ &= P_r\left(\gamma_{ir} \leq \gamma_{ie}\right) P_r\left(\gamma_{ie} > \gamma_{th}\right) \end{aligned} \tag{26}$$

where $P_r(\gamma_{ir} \le \gamma_{ie})$ and $P_r(\gamma_{ie} > \gamma_{th})$ represent the intercept probability, and the outage probability of the legitimate $T \to r$ link, respectively, noting that γ_{ir} and γ_{ie} are statistically independent. Now, Eq. (26) can be rewritten as follows

$$\begin{aligned} P_{int}^{th} &= P_r(\gamma_{ir} \le \gamma_{ie}, \gamma_{ie} > \gamma_{th}) \\ &= P_{int} \times F_{\gamma_{sel}}(\gamma_{th}). \end{aligned} \tag{27}$$

Thus, by substituting (10) and (18), and applying [62, Eq. (07.34.16.0003.01)] we have

$$P_{int}^{th} = \Psi_3 G_{0,0:5+2j+k_{ir}+k_{ie},5+2j+k_{ir}+k_{ie}:3+j+k_{ir},3+j+k_{ir}}^{0,0:4+j+k_{ie},3+2j+k_{ir}:2+j+k_{ir},2} \times \left[- \left| \frac{k_1}{k_2} \right| \left| \frac{k_3}{k_4} \right| \frac{A_{ir}B_{ie}}{A_{ie}B_{ir}} \sqrt{\bar{\lambda}_{re}}, \frac{B_{ir}}{A_{ir}} \sqrt{\frac{\gamma_{th}}{\bar{\gamma}_{ir}}} \right] \tag{28}$$

where,

$$\Psi_3 = \Psi_1 \sum_{j=0}^{\infty} \frac{1}{j!} \left(\frac{s_{ir}^2 w_{z_{eq_{ir}}}^2}{8\sigma_{ir}^4} \right)^{2j} \sum_{\acute{j}=0}^{\infty} \frac{1}{\acute{j}!} \left(\frac{s_{ir}^2 w_{z_{eq_{ir}}}^2}{8\sigma_{ir}^4} \right)^{\acute{j}} \times \frac{a_{ir}^{a_{ir}} z_{ir}^{k_{ir}} \rho_{ir}^2 exp\left(\frac{-s_{ir}^2}{2\sigma_{ir}^2} \right)}{2A_{ir}^{a_{ir}} \beta(a_{ir}, b_{ir})(b_{ir}-1)^{a_{ir}}} \times \left(\sqrt{\frac{\gamma_{th}}{\bar{\gamma}_{ir}}} \right)^{a_{ir}},$$

where $G_{0,0:p_1,q_1:p_2,q_2}^{0,0:m_1,n_1:m_2,n_2}$ is the extended generalized bivariate Meijer's G-function (EGBMGF) [3].

Moreover, an asymptotic expression of the SRT can be obtained in a simplified formula by solving (27) but using the asymptotic P_{int} and P_{out} in (22) and (25), respectively, to reach the following result

$$\begin{aligned} P_{int}^{th,Asy} = \Psi_4 & \sum_{v=1}^{2+j+k_{ir}} \sum_{\grave{v}=1}^{4+j+k_{ie}} \left(\frac{A_{ir}B_{ie}}{A_{ie}B_{ir}} \sqrt{\bar{\lambda}_{re}} \right)^{\grave{V}_{\grave{u}}} \left(\frac{B_{ir}}{A_{ir}} \sqrt{\frac{\gamma_{th}}{\bar{\gamma}_{ir}}} \right)^{V_u} \\ & \times \frac{\prod_{\grave{u}=1,\grave{u}\neq\grave{v}}^{4+j+k_e} \Gamma(\grave{V}_{\grave{v}} - \grave{V}_{\grave{u}}) \prod_{v=1,v\neq u}^{2+j+k_{ir}} \Gamma(V_v - V_u)}{\prod_{\grave{u}=4}^{5+2j+k_{ir}+k_{ie}} \Gamma(\grave{U}_{\grave{v}} - \grave{V}_{\grave{u}}) \prod_{v=3}^{3+j+k_{ir}} \Gamma(U_v - V_u)} \\ & \times \frac{\Gamma(a_{ie} + b_{ie} + \grave{V}_{\grave{u}}) \Gamma(\frac{2+a_{ir}-a_{ie}+2\grave{V}_{\grave{u}}}{2})}{\Gamma(\frac{2-a_{ie}-a_{ir}+2\grave{V}_{\grave{u}}}{2}) \Gamma(\frac{a_{ie}+a_{ir}-2+2\grave{V}_{\grave{u}}}{2})} \\ & \times \frac{\Gamma(a_{ir} + b_{ir} + V_u) \Gamma(a_{ir} + V_u)}{\Gamma(\frac{3a_{ir}-a_{ie}+2\grave{V}_{\grave{u}}}{2}) \Gamma(1 + a_{ir} + V_u)} \end{aligned} \tag{29}$$

where

$$\Psi_4 = \Psi_1 \Psi_2 \sum_{j=0}^{\infty} \frac{1}{j!} \left(\frac{s_{ir}^2 w_{z_{eq_{ir}}}^2}{8\sigma_{ir}^4} \right)^{j} \left(\sqrt{\frac{\gamma_{th}}{\bar{\gamma}_{ir}}} \right)^{a_{ir}} \times \sum_{\jmath=0}^{\infty} \frac{1}{\jmath!} \left(\frac{s_{ir}^2 w_{z_{eq_{ir}}}^2}{8\sigma_{ir}^4} \right)^{\jmath} \sum_{\mathcal{L}=0}^{\infty} \frac{1}{\mathcal{L}!} \left(\frac{s_{ie}^2 w_{z_{eq_{ie}}}^2}{8\sigma_{ie}^4} \right)^{\mathcal{L}}$$

VII. FRIENDLY JAMMING MODEL FOR ENHANCING THE SRT OF THE MULTIUSER FSO SYSTEM

In this section, a friendly jamming technique is employed to improve the secrecy performance of the considered multiuser FSO system. Friendly jamming is a PLS solution originally used in RF communications and later extended to mixed RF-FSO systems to enhance security by using a jamming signal with prior knowledge to assist legitimate users of the system [46], [64]. To this end, a friendly jamming signal is used that is known in r and can be canceled by subtraction at r. Since the system under consideration selects the user with the highest secrecy capacity among M users, the remaining $J = M - 1$ users are idle during the transmission of the selected user. Therefore, a user with the lowest secrecy capacity J is chosen here as the FJ to enhance the security of the physical layer of the system under consideration. The FJ reduces the intercept probability in r by increasing the interference signal caused by the jammer in e. Therefore, the received signal at e from the ith user in this case is given by

$$y_{ie} = P_i I_{ie} x_i + P_J I_{Je} x_J + w_e, \tag{30}$$

where I_{Je} is the channel coefficient between the jamming user J and e and x_J is the jamming signal transmitted by J with $E[x_J]^2 = 1$. P_J is the available power for friendly jamming that would be transmitted by a single jammer user J. Using (30), the SNR observed at e can be expressed as

$$\gamma_{ie} = \frac{P_i |I_{ie}|^2}{P_J |I_{Je}|^2 + N_0} \tag{31}$$

According to Shannon's theorem, in this case, the capacity of the wiretap channel is given by

$$C_{ie} = log_2 \left(1 + \frac{P_i |I_{ie}|^2}{P_J |I_{Je}|^2 + N_0} \right) \tag{32}$$

Similarly, the substitution of C_{ie} from (32) to (16) leads to

$$P_{int}^{FJ} = P_r \left[log_2 \left(1 + \frac{P_i |I_{ie}|^2}{P_J |I_{Je}|^2 + N_0} \right) > \Re \right] \tag{33}$$

Using the FJ, e will be suffering from a jamming signal transmitted by the user with the lowest secrecy capacity J, hence, the intercept probability can be expressed as

$$P_{int}^{th,FJ} = P_r(\gamma_{ir} \le \gamma_{ie}) P_r(T_t = T_J) P_r(\gamma_{ie} > \gamma_{th}) \tag{34}$$

The result in (34) is similar to (26) with the new term $P_r(T_t = T_J)$ denotes the event that the tth ($i.e., t = 1, 2, \ldots, i-1$), the user is the jamming user J by the unauthorized receiver e. Hence, $P_r(T_t = T_J)$ in (34) is given by

$$\begin{aligned} P_r(T_t = T_J) &= P_r \left[\frac{P_i |I_{ie}|^2}{P_J |I_{Je}|^2 + N_0} > \Re \right] \\ &= P_r \left[\max_{\substack{1 \le p \le M \\ p \notin \{i,t\}}} |I_{pr}|^2 > |I_{te}|^2 \right] \\ &= 1 - \int_0^{\infty} \prod_{\substack{1 \le p \le M \\ p \notin \{i,t\}}} \left[1 - F_{I_{pr}}(x) \right] f_{I_{te}}(x) \, dx \end{aligned} \tag{35}$$

By applying the following identity [65]

$$\prod_{i=1}^{M} (1 - \Omega_i) = \sum_{i=0}^{M} \frac{(-1)^i}{i!} \sum_{n_1,\ldots,n_i}^{M} \prod_{t=1}^{i} \Omega_{n_t} \tag{36}$$

where Ω_k denotes any arbitrary function with $\sum_{n_1,\ldots,n_i}^{M}$ being a short-hand notation for $\sum_{\substack{n_1=\ldots=n_i=1 \\ n_1\neq\ldots\neq n_i}}\ldots\sum$, then with the help of [62, Eq. (07.34.21.0011.01)], the integral of (35) can be solved as the following,

$$\begin{aligned}
&P_r\left(T_t = T_J\right) \\
&= 1 - \int_0^{\infty} \prod_{\substack{1\le p\le M \\ p\notin\{i,t\}}} \left[1 - \Psi_5 x^{\frac{a_{pr}}{2}} G_{3+p+k_{pl},3+p+k_{pr}}^{2+p+k_{pr},2}\right. \\
&\quad \left. \times \frac{B_{pr}x^{\frac{1}{2}}}{A_{pr}}\middle| \begin{matrix} k_5 \\ k_6 \end{matrix}\right)\Bigg] \times \Psi_6 x^{\frac{a_{te}}{2}-1} G_{2+t+k_{te},2+t+k_{te}}^{2+t+k_{te},1} \\
&\quad \times \left(\frac{B_{te}x^{\frac{1}{2}}}{A_{te}}\middle| \begin{matrix} k_7 \\ k_8 \end{matrix}\right) dx \\
&= \sum_{p=0}^{M-1} \frac{(-1)^p}{p!} \sum_{\substack{n_1,\ldots,n_M \\ n_p\neq n_i,n_t}}^{M-1} \left(\frac{B_{pr}}{A_{pr}}\right)^{\frac{a_{te}-a_{pr}}{2}} \Psi_5\Psi_6 \\
&\quad \times G_{5+2p+k_{pr}+k_{te},5+2p+k_{pr}+k_{te}}^{4+p+k_{pr},3+j+k_{te}} \left(\frac{A_{ir}B_{tr}\sqrt{\bar{\gamma}_{ir}}}{A_{tr}B_{ir}\sqrt{\bar{\gamma}_{tr}}}\middle| \begin{matrix} k_9 \\ k_{10} \end{matrix}\right) \quad (37)
\end{aligned}$$

where

$$\begin{aligned}
\Psi_5 &= \frac{a_{pr}^{a_{pr}} z_{pr}^{k_{pr}} \rho_{pr}^2 exp\left(\frac{-s_{pr}^2}{2\sigma_{pr}^2}\right)\left(\sqrt{\frac{1}{\bar{\gamma}_{pr}}}\right)^{a_{pr}-1}}{2A_{pr}^{\frac{a_{tr}}{2}}\beta\left(a_{pr},b_{pr}\right)\left(b_{pr}-1\right)^{a_{pr}}\sqrt{\bar{\gamma}_{pr}}} \sum_{j=0}^{\infty}\frac{1}{j!} \\
&\quad \times \left(\frac{s_{pr}^2 w_{z_{eq_{pr}}}^2}{8\sigma_{pr}^4}\right)^j \left(\sqrt{\frac{1}{\bar{\gamma}_{pr}}}\right)^{a_{pr}} \quad (38) \\
\Psi_6 &= \frac{a_{te}^{a_{te}} z_{te}^{k_{te}} \rho_{te}^2 exp\left(\frac{-s_{te}^2}{2\sigma_{te}^2}\right)}{2A_{te}^{\frac{a_{te}}{2}}\beta\left(a_{te},b_{te}\right)\left(b_{te}-1\right)^{a_{te}}\sqrt{\bar{\gamma}_{te}}} \sum_{j=0}^{\infty}\frac{1}{j!} \\
&\quad \times \left(\frac{s_{te}^2 w_{z_{eq_{te}}}^2}{8\sigma_{te}^4}\right)^j \left(\sqrt{\frac{1}{\bar{\gamma}_{te}}}\right)^{a_{te}-1} \quad (39)
\end{aligned}$$

$k_5 = 1-a_{pr}-b_{pr}, 1-a_{pr}, \left\{1+\rho_{pr}^2-a_{pr}\right\}_0^{j+1}, \left\{1+z_{pr}-a_{pr}\right\}_0^{k_{pr}}, k_6 = 0, \left\{\rho_{pr}^2-a_{pr}\right\}_0^{j+1}, \left\{z_{pr}-a_{pr}\right\}_0^{k_{pr}}, -a_{pr}, k_7 = 1-a_{te}, 1-a_{te}, \frac{1-a_{te}-b_{te}}{2}, \frac{2-a_{te}-b_{te}}{2}, \frac{\left\{1+\rho_{te}^2-a_{te}\right\}_0^{j+1}}{2}, \frac{\left\{1+\rho_{te}^2-a_{te}\right\}_0^{j+1}+1}{2}, \frac{\left\{1+z_{te}-a_{te}\right\}_0^{k_{te}}}{2}, \frac{\left\{1+z_{te}-a_{te}\right\}_0^{k_{te}}+1}{2}, k_8 = 0, \frac{1}{2}, \frac{\left\{\rho_{te}^2-a_{te}\right\}_0^{j+1}}{2}, \frac{\left\{\rho_{te}^2-a_{te}\right\}_0^{j+1}+1}{2}, \frac{\left\{z_{te}-a_{te}\right\}_0^{k_{te}}}{2}, \frac{\left\{z_{te}-a_{te}\right\}_0^{k_{te}}+1}{2}, 1-a_{te}.$
$k_9 = 1-a_{te}-b_{te}, \left\{1+\rho_{te}^2-a_{te}\right\}_0^{j+1}, 1-\frac{a_{ir}+b_{te}}{2}, 1-\frac{a_{ir}+b_{te}}{2}-\left\{\rho_{ir}^2-a_{ir}\right\}_2^{j+1}, 1-\frac{a_{ir}+b_{te}}{2}-\left\{z_{ir}-a_{ir}\right\}_0^{z_{ir}}, \left\{z_{te}-a_{te}\right\}_0^{k_{te}}, 1+a_{te}-\frac{a_{ir}+b_{te}}{2}, \left\{1+z_{te}-a_{te}\right\}_0^{k_{te}}. k_{10} = 0, \left\{\rho_{ir}^2-a_{ir}\right\}_2^{j+1}, \frac{a_{ir}+b_{te}+2b_{ir}}{2}, \frac{a_{ir}+b_{te}}{2}, \frac{2-2a_{ir}2a_{te}}{2}-\left\{1+\rho_{ir}^2-a_{ir}\right\}_0^{j+1}, \frac{2-2a_{ir}2a_{te}}{2}-\left\{1+z_{ir}-a_{ir}\right\}_0^{k_{ir}}, \left\{z_{te}-a_{te}\right\}_0^{k_{te}}.$

VIII. NUMERICAL RESULTS

Selected simulation results of opportunistic scheduling schemes for multiuser FSO systems are provided and analyzed in this section, using the above analytical expressions.

TABLE 2. Simulation parameters.

Quantity	Symbol	Value
AWGN variance	N_o	10^{-14} A^2/GHz
Link distance	d_{il}	1 km
Inner-scale turbulence	l_0	0.8 m
Outer-scale turbulence	L_0	5.98 mm
Threshold SNR	γ_{th}	5 dB
The shape parameter of fog	k_{il}	{2.32, 5.49, 6.00}
Number of users	M	5
Average SNR of the $T \to e$ link	$\bar{\gamma}_{ie}$	5 dB
Scale parameter of fog	β_{il}	{13.12, 12.06, 23.00}
Aperture radius	r_{il}	5 cm
Normalized beam-width	$w_{z_{il}}/r_{il}$	{3,6}
Pointing error	$\{\frac{w_{z_{il}}}{r_{il}}, \sigma_{il}\}$	{3, 0.05}, {6, 0.05}, {6, 0.2}
Jitter standard deviation	σ_{il}	{5-20} cm
Horizontal and vertical displacement	$\mu_{x_{il}}, \mu_{y_{il}}$	{0.1, 0.1} m
Optical wavelength	λ	1550 nm
Expected secrecy rate	$\mathcal{R}$	1 bits/s/Hz
Atmospheric turbulence (AT) parameters	$\{a_{il}, b_{il}\}$	{4.5916, 2.3378, 1.4321}, {7.0941, 4.5323, 3.4948}

We investigate the reliability, security, and SRT performance of multiuser FSO systems in the presence of atmospheric turbulence with $\mathcal{F}$ distribution, fog and generalized pointing error using both numerical and Monte- Carlo simulation approaches (averaged over 10^6 channel realizations). For simplicity, we assume independent, identically distributed main and wiretap channels. We validate our derived analytical expressions with numerical and simulation results. In addition, we demonstrate the significance of the proposed OUS scheme compared to the traditional RRS for various system and channel impairments. Unless stated otherwise, the considered system simulation parameters are listed in Table 2 [13], [50], [52], [53].

Fig. 2 shows the outage probability of the RRS and OUS schemes by plotting (23), (24), and (25) with respect to the average electrical SNR of the legitimate $T \to r$ links, with light fog, moderate pointing error $\{\frac{w_{z_{il}}}{r_{il}}, \sigma_{il}\} = (6, 0.05)$ and different turbulence conditions. From Fig. 2, it can be seen that as the turbulence increases (from weak to strong), P_{out} decreases for both schemes, although P_{out} is significantly better with OUS scheme, showing the reliability advantage of the proposed scheduling approach over the RRS.

Fig. 3 shows the outage probability performance comparison of the OUS and RRS schemes as a function of the number of users, M, to illustrate the effects of the generalized pointing error in weak turbulence and light fog. Fig. 3 shows that the outage probability values for both schemes decrease linearly as M increases, implying that the diversity order has a linear relationship with M. This is due to the fact that the diversity order of the system increases as the power received by r increases. Moreover, the best performance is obtained when

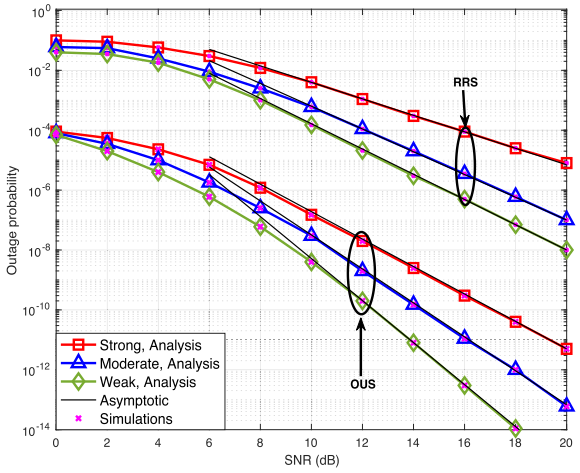

FIGURE 2. Outage probability versus $\bar{\gamma}_{ir}$ for different turbulence conditions over the light fog.

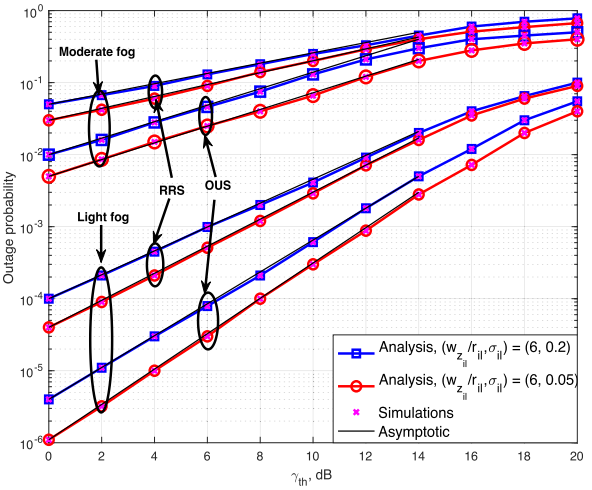

FIGURE 4. Outage probability versus γ_{th} over varying fog densities with different pointing error conditions values.

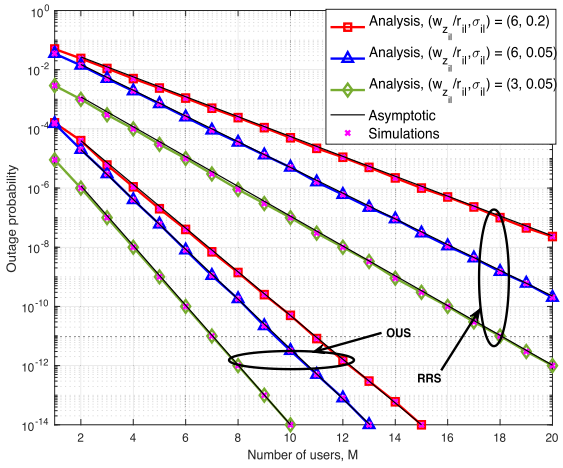

FIGURE 3. Outage probability versus M for different pointing error conditions.

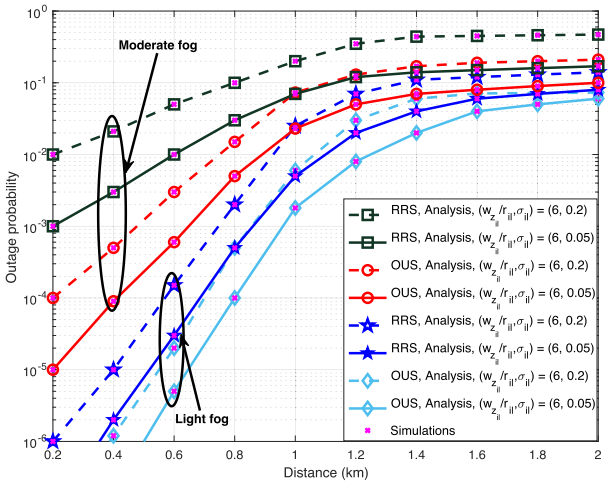

FIGURE 5. Outage probability versus link distance, d_{il} over varying fog densities with different pointing error conditions.

the value of the pointing error is small, i.e., $\{\frac{w_{z_{il}}}{r_{il}}, \sigma_{il}\} = (3, 0.05)$, since the receiver is better positioned in this case.

In the following, we discuss how the reliability of the system is affected by the SNR threshold. Fig. 4 depicts the outage probability of the system as a function of the SNR threshold γ_{th} under the combined effect of fog and pointing error with weak atmospheric turbulence. From the results, it can be inferred that the increase in γ_{th} and pointing error significantly degrade the P_{out} of the system for both fog densities, especially for higher values of γ_{th}. This figure also shows that the OUS scheme significantly outperforms the RRS in terms of P_{out} for all values of γ_{th}. The analytical results agree well with the simulation and asymptotic results, confirming the validity of the derived expressions.

Fig. 5 shows the outage probability of the RRS and OUS schemes as a function of the link distance d_{il} for the combined effect of fog, pointing error, and weak turbulence. The outage probability obviously increases with the longest link length, high values of pointing error, and high fog density. Nevertheless, the OUS scheme shows better performance over all link lengths, regardless of the channel impurities. The results of the Monte-Carlo simulations agree well with the exact results, showing the accuracy of the obtained expressions (23)-(25). Moreover, the analytical results agree very well with the asymptotic results and agree well with the exact results at high SNR values, as shown in Figs. 2-5.

In Fig. 6, we show the intercept probability as a function of MER of the RRS and the OUS schemes by plotting (19), (21), and (22) for different turbulence and pointing error conditions. One can see from Fig. 6 that as the turbulence conditions increase from moderate to strong, the intercept probabilities of both scheduling schemes decrease significantly. Fig. 6 also shows that for both pointing error values of $\{\frac{w_{z_{il}}}{r_{il}}, \sigma_{il}\} = (6, 0.2)$, and $(6, 0.05)$, the intercept probability performance of the proposed OUS is better than that of the RRS.

Fig. 7 shows the intercept probability of the RRS and the OUS schemes as a function of MER for the combined effect of fog, pointing error, and weak turbulence. The intercept

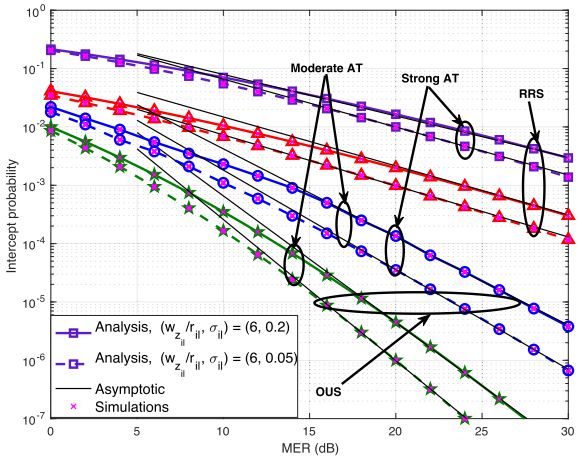

FIGURE 6. Intercept probability versus MER, over different turbulence and pointing error conditions, with light fog.

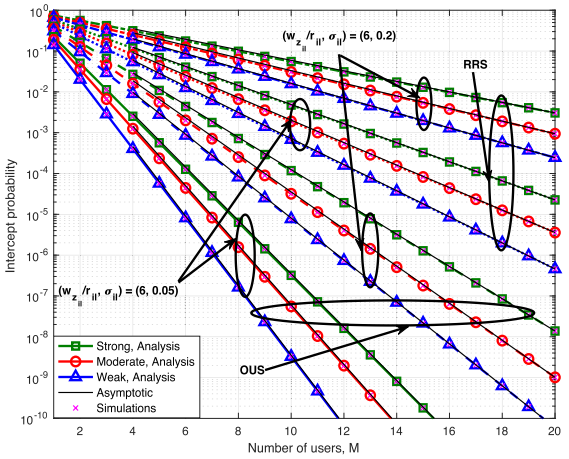

FIGURE 8. Intercept probability versus the number of users, M over different turbulence and pointing error conditions, with the light fog.

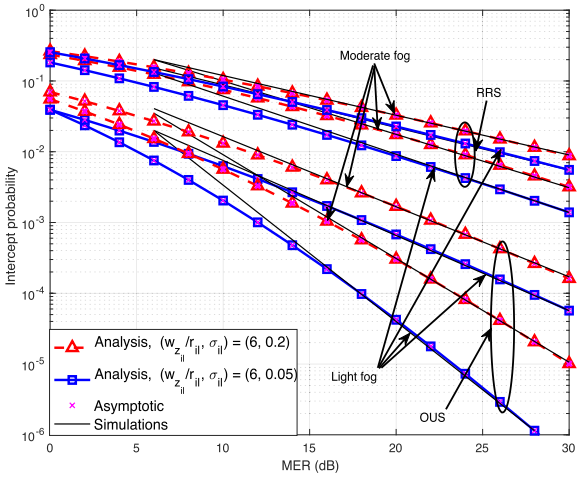

FIGURE 7. Intercept probability versus MER over varying fog densities with different pointing error conditions.

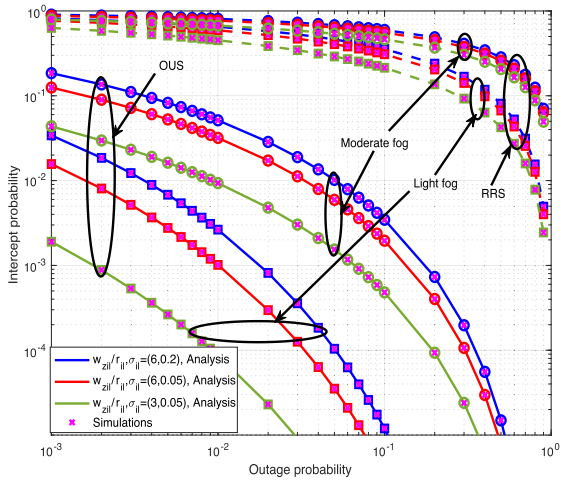

FIGURE 9. SRT analysis with RRS and OUS schemes over the different fog and pointing error conditions, with light fog.

probability decreases with the increase of the MER, low pointing error, and light fog density. This is because decreasing pointing error decreases the required transmission power which enhances the system secrecy performance by decreasing the intercept probability. Although, the OUS scheme shows better performance overall MER values regardless of channel conditions.

Fig. 8 presents the security performance represented by the intercept probability of the RRS and the OUS schemes as a function of M with different turbulence and pointing error conditions. First, we observe that the intercept probability decreases with increasing of M under all turbulence and pointing error conditions, although better performance is achieved with OUS schemes. This is because increasing M increases the number of links between the T and the legitimate receiver r, which improves the receiver's total SNR value and thus decreases the intercept probability. For instance, when $M = 10$, the system with an OUS scheme under weak turbulence and a low value of pointing error achieves an intercept probability of 4×10^{-9}, which rises to 7×10^{-4} in the case of the RRS scheme under the same conditions, showing the security benefit achieved by the OUS with the improvement of channel conditions. It can be seen that there is an excellent match between the analytical and simulation results for the previous figures.

The SRT analysis of the considered system is presented in Figs. 9-11 where the tradeoff relationship between the system outage probability and intercept probability is investigated. Fig. 9 depicts the SRT's performance comparison of the RRS and OUS schemes considering the combined effect of pointing error and fog with low atmospheric turbulence. Results show that decreasing fog density and pointing error improves the system security performance against the eavesdropper attack. This is because of less attenuation achieved under light fog condition which means more power received by r. Based on (28) and the discussion of Fig. 7, decreasing pointing error enhances the system secrecy performance by decreasing the intercept probability since the receiver is better positioned in this case.

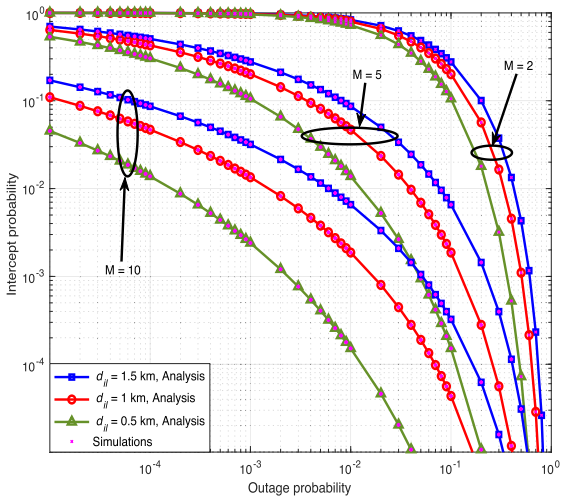

FIGURE 10. SRT analysis of multiuser FSO system with OUS scheme over moderate turbulence and light fog, with a different number of users, M and different link distance, d_{il}.

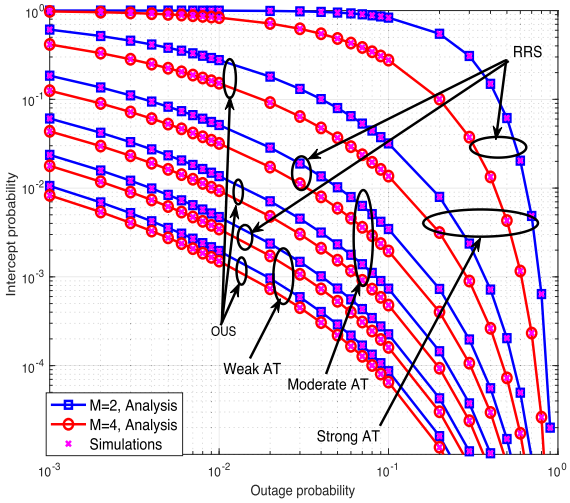

FIGURE 11. The impact of FJ on the SRT analysis for OUS scheme of multiuser FSO system over different atmospheric turbulence conditions, with light fog.

In Fig. 10, we illustrate the SRT analysis for the considered system over the moderate turbulence, and light foggy weather with moderate pointing error of $\{\frac{w_{z_{il}}}{r_{il}}, \sigma_{il}\} = (6, 0.05)$. We demonstrate the effect of the number of users, M and link distance, d_{il} on the SRT performance of the system with the OUS scheme. The figure shows that the intercept probability is too high for practical practices in a long-distance transmission for a small number of users. However, the transmission with a higher number of users (i.e., $M = 5$, and $M = 10$ users) significantly decreases the intercept probability and enhances the security performance due to increases in the diversity gain in this case.

Fig. 11 studies the impact of the friendly jamming scheme in (34) on the SRT analysis of the considered system for different atmospheric turbulence conditions with light fog. The results show that increasing the required outage probability values decreases the interception probability of the system and improves the secrecy performance. This result can be explained as follows: a high outage probability requires a lower transmit power of the transmitted user, which reduces the interception probability of the system. Second, this reduction in required transmit power increases P_J, which further improves the secrecy performance of the system. The Monte-Carlo simulations agree well with the exact results and show the accuracy of the obtained expressions (28), and (34), as shown in Figs. 9-11.

IX. CONCLUSION

In this paper, the SRT of a multiuser FSO system was investigated using an opportunistic scheduling technique. An OUS scheme is proposed to improve the security of the considered system, and the conventional RRS is considered as a benchmark. The outage probability, intercept probability, and SRT were determined using exact and asymptotic closed form expressions assuming an $\mathcal{F}$ distribution for the FSO links and the combined effect of generalized pointing error and fog path losses. Moreover, a friendly jamming model was introduced, where the user with the lowest secrecy capacity is used a*-s a friendly jammer to improve the secrecy performance of the considered system. As a concluding remark, we can say that significant improvement in outage probability, interception probability, and SRT is achieved by fully exploiting the potential of opportunistic scheduling techniques for multiuser FSO systems. In other words, combining the OUS scheme with the FJ technique leads to significant improvements in achievable SRT when atmospheric turbulence and foggy weather are encountered. The main results of this work show that increasing the number of users improves the security of the system regardless of the channel conditions. More pecifically, the best performance is obtained in weak turbulence, low pointing error, and light fog. The results also show that increasing the required outage probability values improves the secrecy performance of the system. In summary, the proposed OUS significantly improves the security, reliability, and SRT performance compared to the RRS scheme. Finally, the results of this work can be extended to other channel models, including the Nakagami-m, Rayleigh, and one-sided Gaussian distributions, since these distributions are considered as special cases of the $\mathcal{F}$ distribution. The important findings of this paper can help telecommunication engineers in designing PLS schemes for multiuser FSO systems that consider various opportunistic scheduling schemes.

REFERENCES

[1] *IMT Traffic Estimates for the Years 2020 to 2030*, document ITU 2083, International Telecommunication Union, 2015.

[2] W. Shakir and R. Abdulkareem, "A survey on physical layer security for FSO communication systems," in *Proc. 2nd Int. Multi-Disciplinary Conf., Theme, Integr. Sci. Technol. (IMDC-IST)*, Sakarya, Turkey, Sep. 2022, pp. 7–9.

[3] W. M. R. Shakir and M. Alouini, "Secrecy performance analysis of parallel FSO/mm-wave system over unified Fisher–Snedecor channels," *IEEE Photon. J.*, vol. 14, no. 2, pp. 1–13, Apr. 2022.

[4] W. M. R. Shakir, "Performance analysis of the hybrid MMW RF/FSO transmission system," *Wireless Pers. Commun.*, vol. 109, pp. 2199–2211, Aug. 2019.

[5] A. Jahid, M. H. Alsharif, and T. J. Hall, "A contemporary survey on free space optical communication: Potentials, technical challenges, recent advances and research direction," *J. Netw. Comput.*, vol. 200, Apr. 2022, Art. no. 103311.

[6] A. K. Majumdar, Z. Ghassemlooy, and A. A. B. Raj, *Principles and Applications of Free Space Optical Communications*. London, U.K.: IET, 2019.

[7] R. Boluda-Ruiz, A. García-Zambrana, B. Castillo-Vázquez, and K. Qaraqe, "Secure communication for FSO links in the presence of eavesdropper with generic location and orientation," *Opt. Exp.*, vol. 27, no. 23, pp. 34211–34229, Nov. 2019.

[8] Y. Ai, A. Mathur, G. D. Verma, L. Kong, and M. Cheffena, "Open access comprehensive physical layer security analysis of FSO communications over Málaga channels," *IEEE Photon. J.*, vol. 12, no. 6, pp. 1–17, Dec. 2020.

[9] P. V. Trinh, A. Carrasco-Casado, A. T. Pham, and M. Toyoshima, "Secrecy analysis of FSO systems considering misalignments and eavesdropper's location," *IEEE Trans. Commun.*, vol. 68, no. 12, pp. 7810–7823, Dec. 2020.

[10] H. Wu, D. Kang, J. Ding, J. Yang, Q. Wang, J. Wu, and J. Ma, "Secrecy performance analysis in the FSO communication system considering different eavesdropping scenarios," *Opt. Exp.*, vol. 30, no. 23, pp. 41028–41047, 2022.

[11] W. M. R. Shakir and S. A. A. Mohammed, "Free space optical communications security and reliability trade-off: A survey," in *Proc. Int. Conf. Natural Appl. Sci. (ICNAS)*, Baghdad, Iraq, 2022, pp. 114–119.

[12] R. Boluda-Ruiz, A. García-Zambrana, B. Castillo-Vázquez, C. Castillo-Vázquez, and K. Qaraqe, "Outage capacity of rate-adaptive relaying for FSO links with nonzero boresight pointing errors," *IEEE Photon. Technol. Lett.*, vol. 31, no. 9, pp. 717–720, May 1, 2019.

[13] W. M. R. Shakir and R. A. A. A. Kareem, "On secure communications for FSO systems over generalized turbulence channels," in *Proc. IEEE Int. Symp. Meas. Netw. (M&N)*, Padua, Italy, Jul. 2022, pp. 1–6.

[14] M. F. N. Khan, H. Khalil, F. Qamar, M. Ali, R. Shahzadi, and N. Qamar, "FSO communication: Benefits, challenges and its analysis in DWDM communication system," *Sir Syed Univ. Res. J. Eng. Technol.*, vol. 9, no. 2, pp. 45–53, Jun. 2020.

[15] N. Sadiq, A. Hussain, F. Qamar, R. Shahzadi, M. Ali, N. Qamar, M. Nadeem, and U. Masud, "Performance analysis of NRZ and RZ variants for FSO communication system under different weather conditions," *J. Opt. Commun.*, vol. 8, pp. 1–8, Aug. 2020, doi: 10.1515/joc-2019-0294.

[16] M. E. P. Monteiro, J. L. Rebelatto, R. D. Souza, and G. Brante, "Effective secrecy throughput analysis of relay-assisted free-space optical communications," *Phys. Commun.*, vol. 35, Aug. 2019, Art. no. 100731.

[17] 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, pp. 1–13, Aug. 2020.

[18] W. M. R. Shakir, "On secrecy performance of multiuser FSO networks with opportunistic user scheduling," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Dubai, UAE, Oct./Nov. 2021, hboxpp. 1–6.

[19] A. Sikri, A. Mathur, and G. Verma, "Secrecy performance enhancement of artificial noise injection scheme-based FSO systems," in *Proc. IEEE 94th Veh. Technol. Conf. (VTC-Fall)*, Norman, OK, USA, Sep. 2021, pp. 1–5.

[20] A. Niaz, F. Qamar, M. Ali, R. Farhan, and M. K. Islam, "Performance analysis of chaotic FSO communication system under different weather conditions," *Trans. Emerg. Telecommun. Technol.*, vol. 30, no. 2, Feb. 2019, p. e3486.

[21] Y. Ai, A. Mathur, L. Kong, and M. Cheffena, "Secure outage analysis of FSO communications over arbitrarily correlated Málaga turbulence channels," *IEEE Trans. Veh. Technol.*, vol. 70, no. 4, pp. 3961–3965, Apr. 2021.

[22] R. Boluda-Ruiz, C. Castillo-Vázquez, B. Castillo-Vázquez, A. García-Zambrana, and K. Qaraqe, "On the average secrecy capacity for FSO wiretap channels with nonzero boresight pointing errors," in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Chicago, IL, USA, Aug. 2018, pp. 1–5.

[23] G. D. Verma, A. Mathur, Y. Ai, and M. Cheffena, "Secrecy performance of FSO communication systems with non-zero boresight pointing errors," *IET Commun.*, vol. 15, no. 1, pp. 155–162, Jan. 2021.

[24] R. Boluda-Ruiz, A. García-Zambrana, C. Castillo-Vázquez, and B. Castillo-Vázquez, "Novel approximation of misalignment fading modeled by Beckmann distribution on free space optical links," *Opt. Exp.*, vol. 24, no. 20, pp. 22635–22649, 2016.

[25] G. K. Varotsos, H. E. Nistazakis, M. I. Petkovic, G. T. Djordjevic, and G. S. Tombras, "SIMO optical wireless links with nonzero boresight pointing errors over M modeled turbulence channels," *Opt. Commun. Opt. Commun.*, vol. 403, pp. 391–400, Nov. 2017.

[26] W. M. R. Shakir, J. Charafeddine, H. A. Satai, H. Hamdan, S. Haddad, and J. Sayah, "Opportunistic schedule selection for multiuser MIMO FSO communications: A security-reliability trade-off perspective," *IEEE Photon. J.*, vol. 15, no. 3, pp. 1–15, Jun. 2023.

[27] M. A. Khalighi and M. Uysal, "Survey on free space optical communication: A communication theory perspective," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 2231–2258, 4th Quart., 2014.

[28] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2653–2661, Jul. 2014.

[29] X. Ding, Y. Zou, F. Ding, D. Zhang, and G. Zhang, "Opportunistic relaying against eavesdropping for Internet-of-Things: A security-reliability trade-off perspective," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8727–8738, Oct. 2019.

[30] J. Ji, B. Wu, J. Zhang, M. Xu, and K. Wang, "Enhancement of reliability and security in a time-diversity FSO/CDMA wiretap channel," *OSA Continuum*, vol. 2, no. 5, pp. 1524–1538, 2019.

[31] N. Alshaer, A. Moawad, and T. Ismail, "Reliability and security analysis of an entanglement-based QKD protocol in a dynamic ground-to-UAV FSO communications system," *IEEE Access*, vol. 9, pp. 168052–168067, 2021.

[32] J. Abouei and K. N. Plataniotis, "Multiuser diversity scheduling in free-space optical communications," *J. Lightw. Technol.*, vol. 30, no. 9, pp. 1351–1358, May 1, 2012.

[33] L. Yang, X. Gao, and M.-S. Alouini, "Performance analysis of free-space optical communication systems with multiuser diversity over atmospheric turbulence channels," *IEEE Photon. J.*, vol. 6, no. 2, pp. 1–17, Apr. 2014.

[34] S. Zhalehpour and M. Uysal, "Performance of multiuser scheduling in free space optical systems over atmospheric turbulence channels," *IET Optoelectron.*, vol. 9, no. 5, pp. 275–281, Oct. 2015.

[35] S. Zhalehpour, M. Uysal, O. A. Dobre, and T. Ngatched, "Outage capacity and throughput analysis of multiuser FSO systems," in *Proc. IEEE 14th Can. Workshop Inf. Theory (CWIT)*, St. John's, NL, Canada, Jul. 2015, pp. 143–146.

[36] M. Qin, L. Chen, and W. Wang, "Generalized selection multiuser scheduling for the MIMO FSO communication system and its performance analysis," *IEEE Photon. J.*, vol. 8, no. 5, pp. 1–9, Oct. 2016.

[37] N. Cherif, I. Trigui, and S. Affes, "On the performance analysis of mixed multi-aperture FSO/multiuser RF relay systems with interference," in *Proc. IEEE 18th Int. Workshop Signal Process. Adv. Wireless Commun.* Sapporo, Japan, Jul. 2017, pp. 1–5.

[38] A. M. Salhab, F. S. Al-Qahtani, R. M. Radaydeh, S. A. Zummo, and H. Alnuweiri, "Power allocation and performance of multiuser mixed RF/FSO relay networks with opportunistic scheduling and outdated channel information," *J. Lightw. Technol.*, vol. 34, no. 13, pp. 3259–3272, Jul. 1, 2016.

[39] Y. F. Al-Eryani, A. M. Salhab, S. A. Zummo, and M. Alouini, "Performance analysis and power allocation for two-way multi-user mixed RF/FSO relay networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Barcelona, Spain, Apr. 2018, pp. 1–6.

[40] M. A. Amer and S. Al-Dharrab, "Performance of two-way relaying over α-μ fading channels in hybrid RF/FSO wireless networks," 2019, *arXiv:1911.05959*.

[41] I. Trigui, S. Affes, A. M. Salhab, and M.-S. Alouini, "Transmit diversity for FSO/RF-based multiuser networks," in *Proc. Int. Wir. Commun. Mobile Comput. (IWCMC)*, Limassol, Cyprus, Jun. 2020, pp. 1118–1123.

[42] J. Zhang, H. Ran, G. Pan, and Y. Xie, "Outage probability of multi-aperture and multi-antenna wireless-powered relaying assisted FSO-RF systems with a nonlinear energy harvester," *Appl. Opt.*, vol. 59, no. 33, hboxpp. 10269–10277, 2020.

[43] P. K. Singya and M.-S. Alouini, "Performance of UAV-assisted multiuser terrestrial-satellite communication system over mixed FSO/RF channels," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 2, pp. 781–796, Apr. 2022.

[44] E. T. Michailidis, P. S. Bithas, N. Nomikos, D. Vouyioukas, and A. G. Kanatas, "Outage probability analysis in multi-user FSO/RF and UAV-enabled MIMO communication networks," *Phys. Commun.*, vol. 49, pp. 101475–101511, Dec. 2021.

[45] C. Abou-Rjeily, "Performance analysis of FSO communications with diversity methods: Add more relays or more apertures?" *IEEE J. Sel. Areas Commun.*, vol. 33, no. 9, pp. 1890–1902, Sep. 2015.

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

[47] A. H. A. El-Malek, A. M. Salhab, S. A. Zummo, and M.-S. Alouini, "Physical layer security enhancement in multiuser mixed RF/FSO relay networks under RF interference," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, San Francisco, CA, USA, Mar. 2017, pp. 1–6.

[48] H. Lei, H. Luo, K.-H. Park, I. S. Ansari, W. Lei, G. Pan, and M.-S. Alouini, "On secure mixed RF-FSO systems with TAS and imperfect CSI," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4461–4475, Jul. 2020.

[49] K.-J. Jung, S. S. Nam, M.-S. Alouini, and Y.-C. Ko, "Unified finite series approximation of FSO performance over strong turbulence combined with various pointing error conditions," *IEEE Trans. Commun.*, vol. 68, no. 10, pp. 6413–6425, Oct. 2020.

[50] K. Peppas, G. Alexandropoulos, E. D. Xenos, and A. Maras, "The Fischer–Snedecor F-distribution model for turbulence-induced fading in free-space optical systems," *J. Lightw. Technol.*, vol. 38, no. 6, pp. 1286–1295, Mar. 15, 2020.

[51] S. K. Yoo, S. L. Cotton, P. C. Sofotasios, M. Matthaiou, M. Valkama, and G. K. Karagiannidis, "The Fisher–Snedecor F distribution: A simple and accurate composite fading model," *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1661–1664, Jul. 2017.

[52] O. S. Badarneh and R. Mesleh, "Diversity analysis of simultaneous mmWave and free-space-optical transmission over F-distribution channel models," *J. Opt. Commun. Netw.*, vol. 12, no. 11, pp. 324–334, 2020.

[53] O. S. Badarneh, R. Derbas, F. S. Almehmadi, F. E. Bouanani, and S. Muhaidat, "Performance analysis of FSO communications over F turbulence channels with pointing errors," *IEEE Commun. Lett.*, vol. 25, no. 3, pp. 926–930, Mar. 2021.

[54] L. Han, Y. Wang, X. Liu, and B. Li, "Secrecy performance of FSO using HD and IM/DD detection technique over F-distribution turbulence channel with pointing error," *IEEE Wireless Commun. Lett.*, vol. 10, no. 10, pp. 2245–2248, Oct. 2021.

[55] C. Stefanovic, M. Morales-Céspedes, R. Róka, and A. G. Armada, "Performance analysis of N-Fisher–Snedecor F fading and its application to N-hop FSO communications," in *Proc. 17th Int. Symp. Wireless Commun. Syst. (ISWCS)*, Berlin, Germany, Sep. 2021, pp. 1–6.

[56] L. Han, X. Liu, Y. Wang, and X. Hao, "Analysis of RIS-assisted FSO systems over F turbulence channel with pointing errors and imperfect CSI," *IEEE Wireless Commun. Lett.*, vol. 11, no. 9, pp. 1940–1944, Sep. 2022.

[57] Z. Rahman, M. Z. Syed, and V. K. Chaubey, "Multihop optical wireless communication over F-turbulence channels and generalized pointing errors with fog-induced fading," *IEEE Photon. J.*, vol. 14, no. 5, pp. 1–14, Oct. 2022.

[58] W. M. R. Shakir and A. S. Mahdi, "Errors rate analysis of the hybrid FSO/RF systems over foggy-weather fading-induced channel," in *Proc. 4th Sci. Int. Conf. Najaf (SICN)*, Al-Najef, Iraq, Apr. 2019, pp. 156–160.

[59] S. M. Navidpour, M. Uysal, and M. Kavehrad, "BER performance of free-space optical transmission with spatial diversity," *IEEE Trans. Wireless Commun.*, vol. 6, no. 8, pp. 2813–2819, Aug. 2007.

[60] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[61] M. R. Bhatnagar, "A one bit feedback based beamforming scheme for FSO MISO system over Gamma-Gamma fading," *IEEE Trans. Commun.*, vol. 63, no. 4, pp. 1306–1318, Apr. 2015.

[62] (Feb. 2023). *The Mathematical Functions Site*. [Online]. Available: http://functions.wolfram.com

[63] I. S. Ansari, F. Yilmaz, and M.-S. Alouini, "A unified performance analysis of free-space optical links over Gamma-Gamma turbulence channels with pointing errors," in *Proc. IEEE 81st Veh. Technol. Conf. (VTC Spring)*, Glasgow, U.K., May 2015, pp. 1–9.

[64] Y. Wang, Y. Tong, and Z. Zhan, "On secrecy performance of mixed RF-FSO systems with a wireless-powered friendly jammer," *IEEE Photon. J.*, vol. 14, no. 2, pp. 1–8, Apr. 2022.

[65] P. S. Bithas, G. K. Karagiannidis, N. C. Sagias, P. T. Mathiopoulos, S. A. Kotsopoulos, and G. E. Corazza, "Performance analysis of a class of GSC receivers over nonidentical Weibull fading channels," *IEEE Trans. Veh. Technol.*, vol. 54, no. 6, pp. 1963–1970, Nov. 2005.

WAFAA MOHAMMED RIDHA SHAKIR (Member, IEEE) received the Ph.D. degree in communications and electronics engineering from the University of Technology, Baghdad, Iraq, in 2011. She has been a Faculty Member with the Technical Institute of Babylon, Al-Furat Al-Awsat Technical University, Babil, Iraq, since 2005. She was a Research Fellow with The Pennsylvania State University, PA, USA; a Postdoctoral Fellow with The University of Queen*-sland, QA, Australia; and a Research Fellow with Université de Versailles Saint-Quentin-en-Yvelines, France. She has been an Associate Professor of wireless communications engineering with the Department of Computer Systems, Al-Furat Al-Awsat Technical University, since 2011. Her current research interests include the modeling, design, and performance analysis of wireless communication systems.

JINAN CHARAFEDDINE (Student Member, IEEE) received the master's degree in biomedical engineering and instrumentation and industrial computing from the Faculty of Engineering, Lebanese University, Beirut, Lebanon, in 2013, and the Ph.D. degree in motion science and control of mechatronic systems from Paris-Saclay University, Orsay, France, in 2021. Since 2020, she has been a Lecturer with the Department of Mechatronics and Digital Systems of Engineering, Université Paris Saclay, and a Researcher with Laboratoire d'Ingénierie des Systèmes of Versailles (LISV), Engineering School, Institut des Sciences et Techniques des Yvelines (ISTY).

HANI HAMDAN received the Diploma degree in electricity and electronics option computer science and telecommunication from Faculté de Génie, Université Libanaise, Beirut, Lebanon, in 2000, the M.Sc. degree in industrial control from Faculté de Génie, Université Libanaise in collaboration with Université de Technologie de Compiègne (UTC), France, in 2001, and the Ph.D. degree in systems and information technologies from UTC, in 2005. From 2006 to 2008, he was an Assistant Professor with Université Sorbonne-Paris-Nord. He was a Professor with École Supérieure d'Électricité (Supélec), from 2008 to 2014. He is currently a Professor of electrical engineering and computer science with CentraleSupélec, L2S UMR CNRS 8506, Paris-Saclay University, Paris, France. His current research interests include machine learning, signal processing, automatic control, and data analysis.

ISRAA ALI ALSHABEEB was born in Iraq, in 1987. She received the B.S. degree in computer science from Babylon University, Babil, Iraq, in 2009, and the M.S. degree in computer and information science from Gannon University, PA, USA, in 2014. She has been a Lecturer with Al-Furat Al-Awsat Technical University, Iraq, since 2016. She is the author of several articles. Her research interests include data mining, image processing, machine learning, and AI.

NIDAA GHALIB ALI received the B.S. degree in computer sciences from the University of Babylon, Iraq, in 2004, and the M.S. degree in information technology from Universiti Kebangsaan Malaysia, in 2015. From 2015 to 2018, she was a Lecturer with the Department of Computer Systems, Technical Institute of Babylon, Al-Furat Al-Awsat Technical University, Babil, Iraq, where she has been an Assistant Professor, since 2018. She is the author of several articles. Her research interests include machine learning, information security, and AI.

ISRAA E. ABED received the B.S. degree in mathematical applied sciences from the University of Technology, Baghdad, Iraq, in 2007, and the M.S. degree in mathematical sciences from Universiti Kebangsaan Malaysia, in 2015. She is currently with the Department of Computer Systems, Technical Institute of Babylon, Al-Furat Al-Awsat Technical University, Babil, Iraq, as a Lecturer of mathematical sciences. Her research interest includes computer algorithms for information security.