

Artificial Noise Injection–Based Secrecy Improvement for FSO Systems

Volume 13, Number 2, April 2021

Aman Sikri

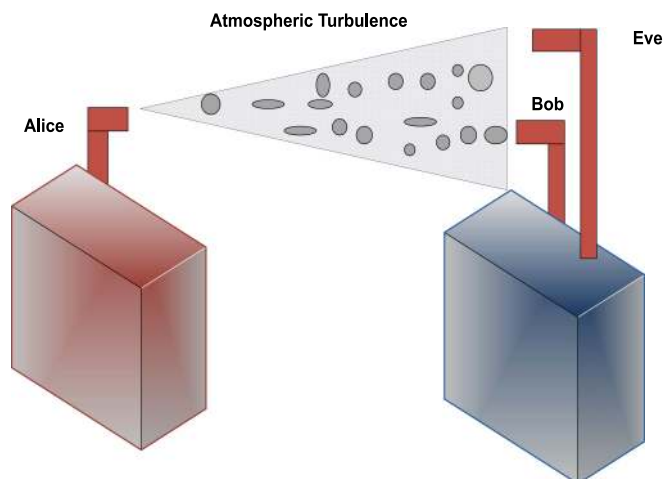
Aashish Mathur, *Member, IEEE*

Manav Bhatnagar, *Senior Member, IEEE*

Georges Kaddoum, *Senior Member, IEEE*







Prakriti Saxena, *Member, IEEE*

Jamel Nebhen



DOI: 10.1109/JPHOT.2021.3060974

Artificial Noise Injection–Based Secrecy Improvement for FSO Systems

Aman Sikri ¹, Aashish Mathur ², *Member, IEEE*,
Manav Bhatnagar ³, *Senior Member, IEEE*,
Georges Kaddoum ⁴, *Senior Member, IEEE*,
Prakriti Saxena ³, *Member, IEEE*, and Jamel Nebhen ⁵

¹Department of Computer Science and Engineering, Indian Institute of Technology, Delhi 110016, India

²Department of Electrical Engineering, Indian Institute of Technology, Jodhpur 342037, India

³Department of Electrical Engineering, Indian Institute of Technology, Delhi 110016, India

⁴University of Quebec, ETS, LaCIME Laboratory, Montreal, Quebec H3C 1K3, Canada

⁵Prince Sattam bin Abdulaziz University, College of Computer Engineering and Sciences, Alkharj 11942, Saudi Arabia

DOI:10.1109/JPHOT.2021.3060974

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see <https://creativecommons.org/licenses/by/4.0/>

Manuscript received January 30, 2021; revised February 15, 2021; accepted February 17, 2021. Date of publication February 22, 2021; date of current version March 10, 2021. This work was supported in part by Ministry of Communication and Information Technology (MCIT) for the Project “Building end to end 5G Test Bed (RP03521G)” and in part by the Science and Education Research Board (SERB), Department of Science and Technology, Government of India for the Project “Experimental Investigation and Performance Evaluation of HARQ Technique for Free-Space Optical Communication Systems” under Project ECR/2018/000797. Corresponding author: Aashish Mathur (e-mail: aashish-mathur@iitj.ac.in).

Abstract: In this paper, an artificial noise (AN) injection technique is incorporated in a free-space optical (FSO) communication system with the aim of enhancing the secrecy performance of the system. An intensity modulated direct detection (IM/DD) FSO link which is subjected to Malaga (\mathcal{M}) distributed turbulence with pointing errors is considered in this paper. The performance of FSO systems is evaluated by deriving novel closed-form expressions for the secrecy outage probability (SOP), strictly positive secrecy capacity (SPSC), and throughput of the system. By formulating a constrained optimization problem, we discuss an optimal power allocation strategy for throughput maximization in the considered system. It is shown through the results that the proposed technique is very effective in improving the secrecy performance of FSO systems.

Index Terms: \mathcal{M} turbulence model, artificial noise (AN), free-space optical communication (FSO), physical layer security, pointing errors.

1. Introduction

Free-Space optical (FSO) communication systems offer higher bandwidth and capacity in comparison to traditional radio frequency (RF) communication systems. In addition, FSO links are license-free and cost-effective compared to expensive and scarce RF spectrum. Due to the directional nature of optical beams, FSO communication systems are inherently more secure than traditional RF communications [1]–[3]. However, it has been shown in [4], [5] that the secure communication between the legitimate transmitter and receiver over FSO links can be intercepted by an eavesdropper at the physical layer. It is reported in [6] that if the eavesdropper is able to

locate itself either close to the transmitter or the legitimate receiver, it will be able to intercept the information. This is depicted by areas 1 and 2 shown in [6, Fig. 1]. Otherwise, the FSO link is secure. A comprehensive physical layer security analysis of an FSO system based on different eavesdropper locations was recently presented in [7]. In [8], [9], the authors analysed the bit error rate (BER) performance of FSO systems in presence of a jammer disrupting the communication between the legitimate transmitter and receiver. However, the secrecy performance of FSO systems was not investigated in this work. Hence, the physical layer security of FSO communication systems is an important open research problem that should be given consideration in order to reap the benefits of high speed FSO links. The authors in [10] analysed BER performance of underwater wireless optical communication system. In [11], the authors analysed the secrecy performance of FSO links in the presence of eavesdropper over Malaga (\mathcal{M}) channels. The authors in [12] discussed about micro optical sensors based on avalanching silicon light-emitting devices monolithically integrated on chips. Orbital angular momentum (OAM) multiplexing was proposed in [13] and [14] to improve the security of FSO systems. In [15], the authors proposed to improve the secrecy performance of FSO systems by fragmenting the transmitted data and simultaneously distributing the data fragments across the different atmospheric channels.

Artificial noise (AN) injection is a powerful technique that was proposed in the context of wireless communication in order to secure the communication between the legitimate transmitter and receiver in the presence of an eavesdropper [16]. In [16], considering multiple antennas at the transmitter, intended receiver, and eavesdropper, AN that lies in the null space of the receiver's channel while simultaneously degrading the eavesdropper's channel, was introduced in the transmitter. In case of a single antenna at each node, [16] considered a collaboration between the transmitter and several relays to generate AN at the transmitter. Recently, a simple system incorporating AN injection scheme and employing a single antenna at each node without considering any external relays was proposed in [17], where the authors showed that perfect secrecy can be achieved in the presence of a passive eavesdropper. Despite the advantages of using AN injection schemes to improve the secrecy performance, this approach has not been explored in the FSO literature, to the best of the authors' knowledge.

Contributions: Motivated by the latest advances in physical layer security analysis of FSO systems and the necessity for improving the security of such systems, we study the secrecy performance of FSO systems under the combined influence of generalized \mathcal{M} turbulence and pointing errors (PEs) using AN injection technique by considering single aperture at each node. The generalized Malaga turbulence model with PEs is considered in this paper as this turbulence model incorporates the well known distributions for different turbulence regimes (strong, moderate, and weak) as its special cases. The derivations are not straightforward as they involve dealing with the Meijer's G-function. In addition, we present an optimization problem to minimize the connection outage probability, P_{co} , with respect to the AN injection parameter, ϵ , considering the security constraint, which is also an important contribution of this paper. Solving the considered optimization problem is indeed mathematically challenging as the mathematical expressions involve the Meijer's G-function. Apart from that, useful insights into FSO secrecy performance are obtained through the numerical results. It is observed that the proposed AN injection scheme plays an important role in improving the secrecy performance of FSO systems. Moreover, it is inferred that the proposed AN injection scheme results in perfect secrecy of FSO systems for certain values of ϵ . However, it is also revealed that allocating more power to AN results in poorer P_{co} , subsequently resulting in lower throughput achieved by the considered FSO communication system. Thus, a trade-off between the secrecy performance and throughput of the considered FSO communication system can be observed which is explained in detail in the Numerical Results section of our work. The main contributions of our research work are summarised as follows:

- We derive novel closed-form expressions of the secrecy outage probability (SOP), strictly positive secrecy capacity (SPSC), and throughput of FSO system utilizing the AN injection scheme under the combined influence of generalized \mathcal{M} turbulence and PEs. The derived results can be mapped to different turbulence (AT) regimes (strong, moderate, and weak).

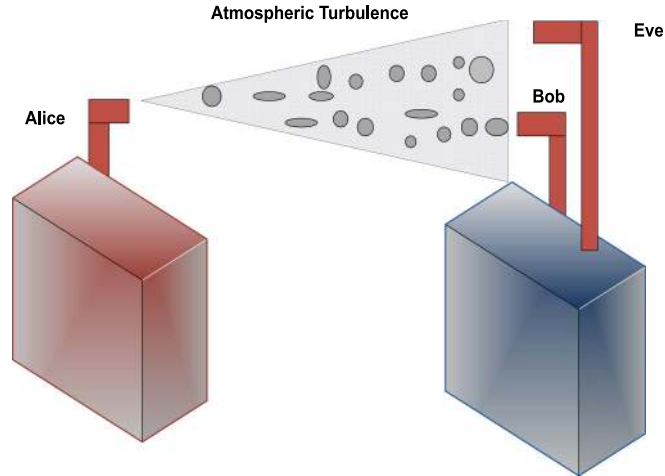


Fig. 1. System model showing communication between Alice and Bob over FSO link in the presence of an eavesdropper, Eve.

- By formulating a constrained optimization problem, we compute the optimal power allocation factor between the information signal and AN that minimizes the connection outage probability of FSO system subject to security constraint.
- It is shown through simulation and analytical results that the proposed AN injection scheme plays a crucial role in improving the secrecy performance of FSO systems.
- The trade-off between the SOP and the throughput of the considered FSO system is also highlighted through the numerical results.

2. System Model

We consider an FSO communication system with intensity modulation direct detection (IM/DD) in which the legitimate transmitter, Alice, wants to send confidential messages to the legitimate receiver, Bob, in the presence of a passive eavesdropper, Eve as shown in Fig. 1. The FSO links are subjected to the combined impact of \mathcal{M} turbulence and PEs. It is assumed that Eve is very close to Bob and can intercept the confidential messages transmitted by Alice. The FSO links are subjected to the combined impact of \mathcal{M} turbulence and PEs. The atmospheric turbulence is a result of random temperature fluctuations caused by the mixing of the rising warm air with cooler air at higher altitudes which leads to inhomogeneities in the medium, thereby resulting in the formation of discrete cells or eddies of different sizes and refractive indices. This phenomenon causes random intensity fluctuations in the received signal, thereby degrading the system performance [18], [19]. PEs are generated due to the misalignment between the transmitter and receiver apertures. Such misalignment is mainly caused by swaying buildings, vibrations, and thermal expansion of the building [20]. The \mathcal{M} turbulence model is based on a physical model that involves a line of sight (LOS) contribution, U_L , a component that is quasi-forward scattered by the eddies on the propagation axis and coupled to the LOS contribution, U_S^C , and another component, U_S^G , due to energy that is scattered to the receiver by off-axis eddies [21], [22]. U_S^C and U_S^G are statistically independent random processes. One of the main motivations behind studying \mathcal{M} turbulence model is that it incorporates various other turbulence models as the special cases [21], [22]. The probability density function (PDF) of the receiver irradiance l from i to j experiencing \mathcal{M} turbulence in the presence of PE impairments is given by [22]

$$f_{l_{i-j}}(l_{i-j}) = \frac{\zeta_j^2 A_j}{2l_{i-j}} \sum_{m=1}^{\beta_j} b_m G_{1,3}^{3,0} \left[\frac{\phi_j l_{i-j}}{l_j A_{oj}} \middle| \frac{1 + \zeta_j^2}{\zeta_j^2, \alpha_j, m} \right], \quad (1)$$

where the subscripts ($i, j \in \{a, b, e\}$), respectively, denote Alice, Bob, and Eve, α_j is a positive parameter related to the effective number of large-scale cells of the scattering process, β_j represents the amount of turbulence-induced fading which is a natural number, ζ_j is the ratio between the equivalent beam radius at the receiver and the PE displacement standard deviation (jitter) at the receiver, l_{ij} is the path loss that is a constant in a given weather condition and link distance, A_{oj} is a constant term that defines the pointing loss, and $G_{p,q}^{m,n}(\cdot)$ is the Meijer's G-function. Further, the parameters, A_j and b_m in (1) are expressed as

$$A_j = \frac{2\alpha_j^{\frac{\alpha_j}{2}}}{g^{1+\frac{\alpha_j}{2}} \Gamma(\alpha_j)} \left(\frac{g\beta_j}{g\beta_j + \Omega'} \right)^{\beta_j + \frac{\alpha_j}{2}}, \quad (2)$$

$$b_m = \left(\frac{\beta_j - 1}{m - 1} \right) \frac{(g\beta_j + \Omega')^{1-\frac{m}{2}} (\Omega')}{(m - 1)!} \left(\frac{\Omega'}{g} \right) \left(\frac{\alpha_j}{\beta_j} \right)^{\frac{m}{2}} \phi_j^{-\frac{\alpha_j+m}{2}}, \quad (3)$$

where $\phi_j = \left(\frac{\alpha_j \beta_j}{g\beta_j + \Omega'} \right)$, $g = 2b_0(1 - \rho)$ denotes the average power of the scattering component received by off-axis eddies, $2b_0$ is the average power of the total scatter components, the parameter $\rho \in (0, 1)$ represents the scattering power coupled to the LOS component and $\Omega' = \Omega + 2b_0\rho + 2\sqrt{2b_0\rho\Omega} \cos(\phi_A - \phi_B)$ represents the average power from the coherent contributions. The parameter Ω is the average power of the LOS component, and ϕ_A and ϕ_B are the deterministic phases of LOS and coupled-to-LOS scatter terms, respectively. The function $\Gamma(\cdot)$ in (2) denotes the Gamma function. We further assume block fading in this work. In addition to that, at the start of each block, Alice transmits pilot symbols to enable channel estimation at the receiver. Assuming channel reciprocity between the transmitter and receiver, we consider that Bob knows the instantaneous channel state information (CSI) $l_{a-b} = l_{b-a}$ [17]. In the following subsections, we propose an AN injection scheme which degrades the received signal-to-noise ratio (SNR) at the eavesdropper, subsequently improving the secrecy performance of the considered FSO communication system:

2.1 Phase 1

During Phase 1, Bob transmits pseudo random AN to Alice. The received signal at Alice is given by

$$r_{a,1} = \eta l_{b-a} z + n_a, \quad (4)$$

where l_{b-a} is the channel gain from Bob to Alice, η is the optical-to-electrical conversion coefficient, $z \sim \mathcal{N}(0, 1)$ denotes AN from Bob, and $n_a \sim \mathcal{N}(0, \sigma_a^2)$ denotes additive white Gaussian noise (AWGN) at Alice with zero mean and variance σ_a^2 .

2.2 Phase 2

During Phase 2, Alice forwards the received signal along with the information-bearing signal to Bob. The signal transmitted by Alice during Phase 2 is given by

$$x_a = \sqrt{\epsilon} x + \sqrt{1 - \epsilon} \frac{r_{a,1}}{|r_{a,1}|}, \quad (5)$$

where x denotes the information-bearing signal and $0 < \epsilon \leq 1$ denotes the power allocation factor between information-bearing signal and AN. The received signal at Bob or Eve during Phase 2 is expressed as

$$r_{i,2} = \eta l_{a-i} x_a + n_i, \quad i \in \{b, e\}. \quad (6)$$

On substituting x_a from (5) into (6) and utilizing (4), we get

$$r_{i,2} = \eta l_{a-i} \left(\sqrt{\epsilon} x + \sqrt{1-\epsilon} \frac{(\eta l_{b-a} z + n_a)}{\sqrt{\eta^2 l_{b-a}^2 + \sigma_a^2}} \right) + n_i, \quad (7)$$

where $n_i \sim \mathcal{N}(0, \sigma_i^2)$ denotes AWGN at the i^{th} node with zero mean and variance σ_i^2 . As discussed earlier, Bob knows the instantaneous CSI $l_{a-b} = l_{b-a}$ and artificial noise z , which was generated during Phase 1. Further, it is also assumed that Alice has shared the values of ϵ and σ_a^2 to Bob before the transmission. Thus, Bob can successfully cancel the received artificial noise z . From (7), the received SNR at Bob is expressed as

$$\begin{aligned} \gamma_b &= \frac{\eta^2 \epsilon l_{a-b}^2 \mathbb{E}[X^2]}{\eta^2 (1-\epsilon) l_{a-b}^2 \frac{\mathbb{E}[n_a^2]}{\eta^2 l_{b-a}^2 + \sigma_a^2} + \mathbb{E}[n_b^2]}, \\ &= \frac{\bar{\gamma}_{a-b} l_{a-b}^2 \epsilon}{1 + \frac{\bar{\gamma}_{a-b} (1-\epsilon) l_{a-b}^2 \sigma_a^2}{(\eta^2 l_{b-a}^2 + \sigma_a^2)}}, \end{aligned} \quad (8)$$

where $\bar{\gamma}_{a-b} = \frac{\eta^2}{\sigma_b^2}$, $\mathbb{E}[X^2] = 1$, $\mathbb{E}[n_a^2] = \sigma_a^2$, and $\mathbb{E}[n_b^2] = \sigma_b^2$. Here, $\mathbb{E}[\cdot]$ denotes the expectation operator. It is assumed that Alice has a more sensitive receiver than Bob, i.e., $\sigma_a^2 \ll \sigma_b^2$. Thus, the received SNR at Bob is approximated as

$$\gamma_b \approx \bar{\gamma}_{a-b} l_{a-b}^2 \epsilon. \quad (9)$$

Similarly, using (7), the received SNR at Eve is written as

$$\gamma_e = \frac{\epsilon l_{a-e}^2}{(1-\epsilon) l_{a-e}^2 + \frac{1}{\bar{\gamma}_{a-e}}}, \quad (10)$$

where $\bar{\gamma}_{a-e} = \frac{\eta^2}{\sigma_e^2}$.

3. Performance Analysis

In this section, we derive the PDFs of the received SNRs at Bob and Eve. We further discuss the SOP, SPSC, and throughput in order to quantify the performance of the considered FSO system. Using the transformation of random variables [23], the PDF of the received SNR at Bob is expressed as

$$f(\gamma_b) = \frac{D_b}{\gamma_b} \sum_{p=1}^{\beta_b} d_p G_{2,6}^{6,0} \left[\frac{E_b \gamma_b}{\mu_b} \middle| \begin{matrix} \kappa_{1b} \\ \kappa_{2b} \end{matrix} \right], \quad (11)$$

where $D_b = \frac{\zeta_b^2 A_b}{8\pi}$, $E_b = \frac{\phi_b^2}{16(l_b A_{ob})^2}$, $d_p = b_p 2^{\alpha_b + p - 1}$, $\mu_b = \epsilon \bar{\gamma}_{a-b}$, $\kappa_{1b} = \{\frac{\zeta_b^2 + 1}{2}, \frac{\zeta_b^2 + 2}{2}\}$, $\kappa_{2b} = \{\frac{\zeta_b^2}{2}, \frac{\zeta_b^2 + 1}{2}, \frac{\alpha_b}{2}, \frac{\alpha_b + 1}{2}, \frac{p}{2}, \frac{p+1}{2}\}$. Similarly, the PDF of the instantaneous SNR at Eve is given by

$$f(\gamma_e) = \frac{\zeta_e^2 A_e \epsilon}{4 \gamma_e (\epsilon - (1-\epsilon)\gamma_e)} \sum_{q=1}^{\beta_e} b_q G_{1,3}^{3,0} \left[\frac{\phi_e}{l_e A_{oe}} \sqrt{\frac{\gamma_e}{\bar{\gamma}_{a-e} (\epsilon - (1-\epsilon)\gamma_e)}} \middle| \begin{matrix} \zeta_e^2 + 1 \\ \zeta_e^2, \alpha_e, q \end{matrix} \right]. \quad (12)$$

3.1 Secrecy Outage Probability

In this section, we formulate the SOP as a direct measure of the probability that a transmitted message fails to achieve perfect secrecy. The encoder chooses two rates, i.e., the codeword transmission rate R_b and the confidential information rate R_s , while designing the encoding scheme [24].

The cost of securing the message transmission against eavesdropping is measured by the rate difference $R_e = R_b - R_s$. Perfect secrecy will not be achieved when $C_e > R_e$. Thus, the SOP is defined as [17]

$$P_{so} = \Pr(C_e > R_b - R_s), \quad (13)$$

where $C_e = \log_2(1 + \gamma_e)$ is Eve's instantaneous channel capacity. Thus, using (12), the SOP is expressed as

$$P_{so}(\epsilon) = \int_{2^{R_b - R_s - 1}}^{\infty} \left(\frac{\zeta_e^2 A_e \epsilon}{4 \gamma_e (\epsilon - (1 - \epsilon)\gamma_e)} \right) \sum_{q=1}^{\beta_e} b_q G_{1,3}^{3,0} \left[\frac{\phi_e}{l_e A_{oe}} \sqrt{\frac{\gamma_e}{\bar{\gamma}_{a-e} (\epsilon - (1 - \epsilon)\gamma_e)}} \middle| \zeta_e^2 + 1, \alpha_e, q \right] d\gamma_e. \quad (14)$$

On substituting $\frac{\gamma_e}{(\epsilon - (1 - \epsilon)\gamma_e)} = t$ in (14), using [29, Eq. (2.24.2.3)], and after some mathematical manipulations, the closed-form SOP expression is written as

$$P_{so}(\epsilon) = \frac{\zeta_e^2 A_e}{8\pi} \sum_{q=1}^{\beta_e} b_q 2^{\alpha_e + q - 1} G_{3,7}^{7,0} \left[\frac{\phi_e^2}{(l_e A_{oe})^2} \frac{1}{\bar{\gamma}_{a-e}} \frac{\Delta}{16} \middle| \kappa_{1e}, 1 \right], \quad (15)$$

where $\kappa_{1e} = \left\{ \frac{\zeta_e^2 + 1}{2}, \frac{\zeta_e^2 + 2}{2} \right\}$, $\kappa_{2e} = \left\{ \frac{\zeta_e^2}{2}, \frac{\zeta_e^2 + 1}{2}, \frac{\alpha_e}{2}, \frac{\alpha_e + 1}{2}, \frac{q}{2}, \frac{q + 1}{2} \right\}$ and $\Delta = \frac{2^{R_b - R_s} - 1}{(\epsilon - (1 - \epsilon)(2^{R_b - R_s} - 1))}$. It should be noted here that $P_{so} = 0$ for $\epsilon \leq 1 - 2^{R_s - R_b}$.

3.2 Throughput

The reliability performance of the system is usually measured by the connection outage probability (COP) which is given by

$$P_{co} = \Pr(R_b > C_b), \quad (16)$$

where $C_b = \log_2(1 + \gamma_b)$ is Bob's instantaneous channel capacity. Thus, the COP is alternately expressed as

$$P_{co} = \Pr(\gamma_b < 2^{R_b} - 1) = \int_0^{2^{R_b} - 1} f(\gamma_b) d\gamma_b. \quad (17)$$

On substituting $f(\gamma_b)$ in (17) and after some mathematical simplifications, the closed-form expression for P_{co} is obtained as

$$P_{co}(\epsilon) = D_b \sum_{p=1}^{\beta_b} d_p G_{3,7}^{6,1} \left[\frac{E_b (2^{R_b} - 1)}{\mu_b} \middle| 1, \kappa_{1b}, \kappa_{2b}, 0 \right]. \quad (18)$$

Now, the throughput of the system (in Gbps) is defined as the average confidential data transmission rate subjected to a given secrecy outage constraint. This is related to the connection outage probability $P_{co}(\epsilon)$ [17]

$$v(\epsilon) = \frac{(1 - P_{co}(\epsilon))R_s}{2}. \quad (19)$$

Substituting (18) into (19), we get the throughput of the considered FSO system as follows:

$$v(\epsilon) = \left(1 - D_b \sum_{p=1}^{\beta_b} d_p G_{3,7}^{6,1} \left[\frac{E_b (2^{R_b} - 1)}{\mu_b} \middle| 1, \kappa_{1b}, \kappa_{2b}, 0 \right] \right) \frac{R_s}{2}. \quad (20)$$

3.3 Strictly Positive Secrecy Capacity

The SPSC is defined as the probability of existence of secrecy capacity and serves as a fundamental benchmark for secrecy performance. The SPSC of the FSO system is thus equivalent to

the probability that the instantaneous secrecy capacity (C_s) is a positive quantity, yielding

$$SPSC = \Pr(C_s > 0),$$

$$\text{where } C_s = \begin{cases} \log(1 + \gamma_b) - \log(1 + \gamma_e), & \gamma_b > \gamma_e. \\ 0, & \text{otherwise.} \end{cases}$$

Substituting the definition of C_s and after some mathematical simplifications, the SPSC is re-written as

$$\begin{aligned} SPSC &= \Pr(\gamma_b > \gamma_e). \\ &= 1 - \Pr(\gamma_b \leq \gamma_e). \\ &= 1 - \int_0^\infty \int_0^{\gamma_e} f(\gamma_b) f(\gamma_e) d\gamma_b d\gamma_e. \end{aligned} \quad (21)$$

From (11) and (12) and substituting $\frac{\gamma_e}{(\epsilon - (1-\epsilon)\gamma_e)} = t$, and after some mathematical calculations, (21) is re-written as

$$\begin{aligned} SPSC &= 1 - \frac{\zeta_e^2 \zeta_b^2 A_e A_b D_e}{(8\pi)^2} \sum_{q=1}^{\beta_e} \sum_{p=1}^{\beta_b} b_p b_q 2^{\alpha_e+q-1} \\ &\quad \times 2^{\alpha_b+p-1} \int_0^\infty G_{3,7}^{6,1} \left[\frac{D_b t \epsilon}{1 + (1-\epsilon)t} \middle| \begin{matrix} 1, \kappa_{1b} \\ \kappa_{2b}, 0 \end{matrix} \right] \\ &\quad \times G_{2,6}^{6,0} \left[D_e t \middle| \begin{matrix} \kappa_{1e} - 1 \\ \kappa_{2e} - 1 \end{matrix} \right] dt, \end{aligned} \quad (22)$$

where $D_e = \frac{\phi_e^2 \sigma_e^2}{16(\eta_e A_{oe})^2 \eta^2}$. The integral in (22) can be expressed using Gauss-Laguerre approximation [25], and hence the SPSC is evaluated as

$$\begin{aligned} SPSC &\approx 1 - \frac{\zeta_e^2 \zeta_b^2 A_e A_b D_e}{(8\pi)^2} \sum_{q=1}^{\beta_e} \sum_{p=1}^{\beta_b} \sum_{n=1}^N b_i b_j 2^{\alpha_e+q-1} \\ &\quad \times 2^{\alpha_b+p-1} w_n e^{t_n} G_{3,7}^{6,1} \left[\frac{D_b t_n \epsilon}{1 + (1-\epsilon)t_n} \middle| \begin{matrix} 1, \kappa_{1b} \\ \kappa_{2b}, 0 \end{matrix} \right] \\ &\quad \times G_{2,6}^{6,0} \left[D_e t_n \middle| \begin{matrix} \kappa_{1e} - 1 \\ \kappa_{2e} - 1 \end{matrix} \right], \end{aligned} \quad (23)$$

where w_n and t_n denote the weight factor and the n^{th} zero of the Laguerre polynomial, respectively.

Remark 1: For finite values of N , the Gauss-Laguerre approximation used in (23) converges to the exact integral value in (22). We consider $N = 60$ for an accurate approximation.

Discussion: Based on aforementioned performance parameters, i.e., SOP, SPSC, and throughput, it can be easily inferred that for the better throughput and secrecy performance of FSO communication system, it is desirable that C_b should be as high as possible while on the contrary C_e should be as low as possible. It should be noted here that the parameter ϵ in (5) plays a crucial role in controlling C_b and C_e , subsequently effecting the overall performance of the AN injection scheme based FSO communication system. It is observed that allocating more power to the AN signal would enhances the secrecy performance (SOP and SPSC) of FSO communication systems. However, such secrecy performance is achieved at the cost of reduction in the throughput of the considered system. Useful insights into the FSO secrecy performance are obtained by analyzing this trade-off between the secrecy performance and throughput for the considered FSO communication system as detailed in the following sections.

4. Optimal Power Allocation

In this section, we discuss the optimal power allocation parameter ϵ that maximizes the throughput, $\nu(\epsilon)$ or equivalently minimizes the connection outage probability, $P_{co}(\epsilon)$ of FSO systems subject to security constraints. We assume that the optimal value is computed for fixed values of R_b and R_s . Thus, the optimization problem is formulated as

$$\min_{\epsilon} P_{co}(\epsilon) \quad (24)$$

$$\text{s.t. } P_{so}(\epsilon) \leq \rho, \quad 0 < \epsilon \leq 1, \quad (25)$$

where $\rho \in [0, 1]$ represents the maximum allowed SOP. Utilizing Slater's theorem [26] to express the Meijer's G-function in terms of the generalized hypergeometric function and then using its series expansion [27, Eq. 9.14.1], it can be shown that the double derivative of the objective function $P_{co}(\epsilon)$ w.r.t. ϵ is positive. Therefore, the objective function is a convex function of ϵ . Hence, the considered optimization problem is convex and the optimal solution must satisfy the Karush-Kuhn-Tucker (KKT) conditions [28] as follows:

$$(a) \quad \frac{\partial P_{co}(\epsilon)}{\partial \epsilon} + \lambda_1 \frac{\partial P_{so}(\epsilon)}{\partial \epsilon} = 0.$$

$$(b) \quad \lambda_1 (P_{so}(\epsilon) - \rho) = 0.$$

$$(c) \quad P_{so}(\epsilon) - \rho \leq 0.$$

$$(d) \quad \lambda_1 \geq 0.$$

Let us observe condition (a) above. Now, using (18) and [29, Eq. (8.2.2.41)], $\frac{\partial P_{co}(\epsilon)}{\partial \epsilon}$ is expressed as

$$\frac{\partial P_{co}(\epsilon)}{\partial \epsilon} = D_b \epsilon^{-1} \sum_{p=1}^{\beta_b} d_p G_{4,8}^{7,1} \left[\frac{E_b (2^{R_b} - 1)}{\epsilon \bar{\gamma}_{a-b}} \middle| \begin{matrix} 1, 0, \kappa_{1b} \\ 1, \kappa_{2b}, 0 \end{matrix} \right]. \quad (26)$$

The quantity $\frac{\partial P_{so}(\epsilon)}{\partial \epsilon}$ in (a) is re-written as follows:

$$\frac{\partial P_{so}(\epsilon)}{\partial \epsilon} = \frac{\partial z}{\partial \epsilon} \frac{\partial P_{so}(\epsilon)}{\partial z}, \quad (27)$$

where $z = (\epsilon - (1 - \epsilon)(2^{R_b - R_s} - 1))$. Now, using [29, Eq. (8.2.2.41)], $\frac{\partial P_{so}(\epsilon)}{\partial \epsilon}$ is written as

$$\begin{aligned} \frac{\partial P_{so}(\epsilon)}{\partial \epsilon} &= \frac{\zeta_e^2 A_e}{8\pi (\epsilon - (1 - \epsilon)(2^{R_b - R_s} - 1))} \sum_{q=1}^{\beta_e} b_q 2^{\alpha_e + q - 1} \\ &\times 2^{R_b - R_s} G_{4,8}^{8,0} \left[\frac{\phi_e^2}{(h_e A_{oe})^2} \frac{1}{\bar{\gamma}_{a-e}} \frac{\Delta}{16} \middle| \begin{matrix} 0, \kappa_{1e}, 1 \\ 1, 0, \kappa_{2e} \end{matrix} \right]. \end{aligned} \quad (28)$$

Now, from (a) and (d), we have two different cases as follows:

- *Case 1* ($\lambda_1 = 0$): In this case, condition (a) becomes

$$\frac{\partial P_{co}(\epsilon)}{\partial \epsilon} = D_b \epsilon^{-1} \sum_{p=1}^{\beta_b} d_p G_{4,8}^{7,1} \left[\frac{E_b (2^{R_b} - 1)}{\epsilon \bar{\gamma}_{a-b}} \middle| \begin{matrix} 1, 0, \kappa_{1b} \\ 1, \kappa_{2b}, 0 \end{matrix} \right] = 0.$$

This condition is valid only when $\epsilon \rightarrow \infty$, which is not a feasible solution as $\epsilon \in [0, 1]$. Hence, we discard this case.

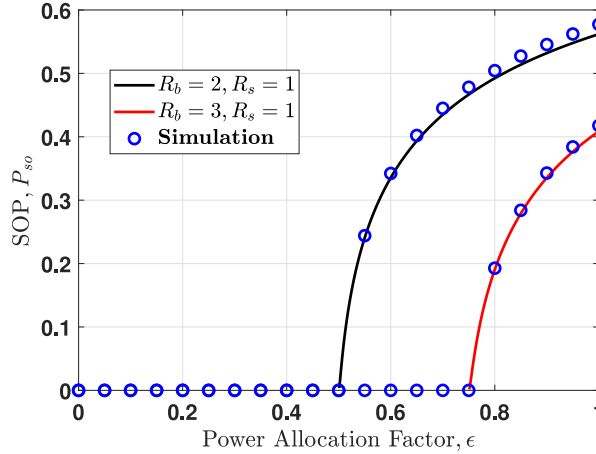


Fig. 2. SOP versus AN power allocation factor ϵ for strong turbulence and $\bar{\gamma}_{a-e} = 10$ dB.

- *Case 2* ($\lambda_1 \neq 0$): For this condition, we have $P_{so}(\epsilon) = \rho$. Thus, (a) is written as

$$\frac{\partial P_{co}(\epsilon)}{\partial \epsilon} + \lambda_1 \frac{\partial P_{so}(\epsilon)}{\partial \epsilon} = 0.$$

Using Mathematica software, it is found that $\lambda_1 > 0$. The value of ϵ obtained by solving $P_{so}(\epsilon) = \rho$ satisfies the constraint $P_{so}(\epsilon) \leq \rho$. Thus, the optimum value of ϵ that minimizes the objective function $P_{co}(\epsilon)$ while satisfying the constraint is obtained by solving

$$P_{so}(\epsilon) = \rho. \quad (29)$$

Remark 2: It will be shown in Fig. 1 in Section 5 that $P_{so} = 0$ for $\epsilon \leq 1 - 2^{R_s - R_b}$. Thus, (29) holds for $\epsilon \geq 1 - 2^{R_s - R_b}$, which satisfies all the constraints in (25). Thus, it can be said that the secrecy performance of the considered FSO system is compromised when achieving the maximum throughput.

5. Numerical Results

In this section, the analytical as well as simulated results of the considered FSO system for different performance metrics such as SOP, SPSC, and throughput are presented. We consider various turbulence conditions such as strong turbulence ($\alpha_b = \alpha_e = 2.296$; $\beta_b = \beta_e = 2$), moderate turbulence ($\alpha_b = \alpha_e = 4.2$; $\beta_b = \beta_e = 3$), and weak turbulence ($\alpha_b = \alpha_e = 8$; $\beta_b = \beta_e = 4$). Unless otherwise stated, the other parameters that are considered in our study are set to $\Omega = 1.3256$, $b_0 = 0.1079$, $\rho = 0.596$, $\phi_A - \phi_B = \pi/2$, $\zeta_b = \zeta_e = 1$, and $l_{eA_{oe}} = l_{bA_{ob}} = 1$.

Fig. 2 shows the SOP behavior as a function of the AN power allocation factor for strong turbulence considering $\bar{\gamma}_{a-e} = 10$ dB and different values of R_b and R_s . It can be inferred from the figure that the SOP increases with the increase in the value of ϵ . It is interesting to note that the SOP is zero for $\epsilon \leq 1 - 2^{R_s - R_b}$, i.e., the considered FSO system attains the perfect secrecy. Since ϵ can take a maximum value of unity indicating the scenario with no AN injection, the SOP will be maximum for this case while other parameters are constant. Hence, the SOP saturates to this maximum value as the value of ϵ is increased. Thus, it can be said that the AN injection scheme is very effective in improving the secrecy performance of FSO systems.

In Fig. 3, the SOP of the considered FSO system is plotted as a function of the average eavesdropper's SNR, $\bar{\gamma}_{a-e}$ for $R_b = 2$ and $R_s = 1$ and different ϵ values. The factor $\frac{1}{\bar{\gamma}_{a-e}}$ in the denominator of (10) decreases with increasing $\bar{\gamma}_{a-e}$ leading to the increments in the value of γ_e and C_e . Hence, a logarithmic growth in the value of P_{so} can be observed with increasing $\bar{\gamma}_{a-e}$. It can be inferred from the figure that strong turbulence conditions are beneficial for the secrecy performance of FSO systems. At lower turbulence, C_e is large due to lower spreading of the optical signals, and

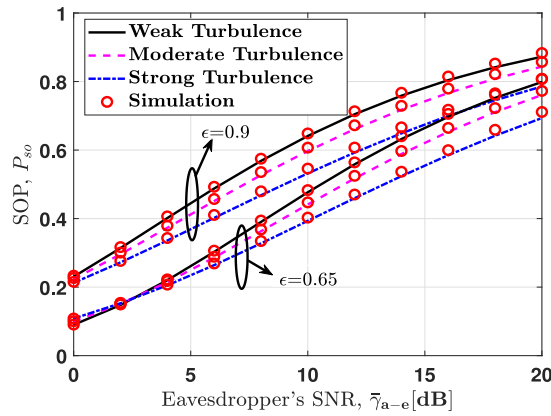


Fig. 3. SOP versus $\bar{\gamma}_{a-e}$ for $R_b = 2$ and $R_s = 1$.

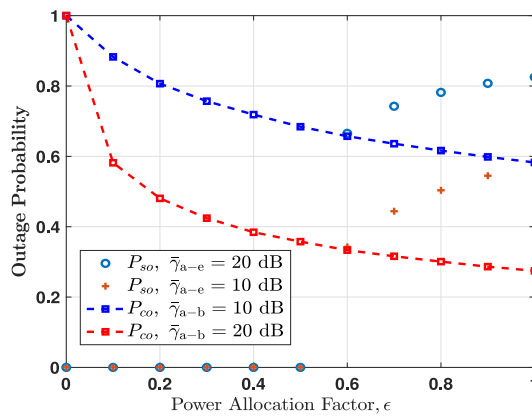


Fig. 4. Outage probability versus AN power allocation factor ϵ for strong turbulence considering $R_b = 2$, and $R_s = 1$.

hence the secrecy performance of FSO systems is poor. It is also quite intuitive to observe that the SOP performance deteriorates with increasing values of ϵ .

Fig. 4 shows the outage probability as a function of the AN power allocation factor for strong turbulence with $R_b = 2$, $R_s = 1$, and different values of $\bar{\gamma}_{a-b}$ and $\bar{\gamma}_{a-e}$. For $\epsilon \leq 0.5$, the considered FSO system is perfectly secure and exhibits a relatively large P_{co} . However, for $\epsilon > 0.5$, i.e., by allocating more power to the information signal and less power to the AN, it can be observed from the figure that the considered FSO system attains a lower P_{co} at the cost of a reduction in the secrecy performance. It can also be inferred from the figure that the secrecy performance of the considered FSO system degrades with the increase in $\bar{\gamma}_{a-e}$. Moreover, the P_{co} of the considered FSO system decreases, i.e., the system becomes more reliable, with the increase in $\bar{\gamma}_{a-b}$. Thus, Fig. 4 is instrumental in highlighting the trade-off between the SOP and throughput of the considered FSO system.

The variation of throughput of the FSO system as a function of the average SNR of Bob, i.e., $\bar{\gamma}_{a-b}$, for different values of AN power allocation factor and PE parameters $\zeta_b = \zeta_e$ is captured in Fig. 5. It is observed from the plots that the throughput of the FSO system improves on increasing the values of ϵ and ζ_b . It is also evident from the figure that the throughput attains the maximum value for $\epsilon = 1$. However, as mentioned earlier, in this case, the system becomes highly insecure.

In Fig. 6, we compare the SPSC performance of the considered FSO system as a function of $\bar{\gamma}_{a-b}$ for different values of AN power allocation factor and PE parameters $\zeta_b = \zeta_e$, under strong turbulence. It can be seen from the figure that the SPSC of FSO systems deteriorates on increasing the value of ϵ . This is due to the fact that more power is allocated to the information bearing signal

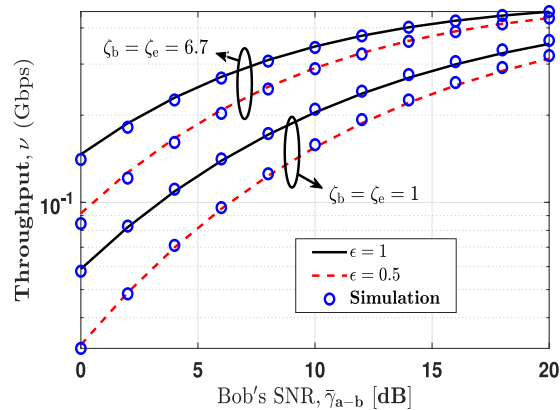


Fig. 5. Throughput versus $\bar{\gamma}_{a-b}$ for different values of AN power allocation factor ϵ and PE parameter ($\zeta_b = \zeta_e$) considering strong turbulence.

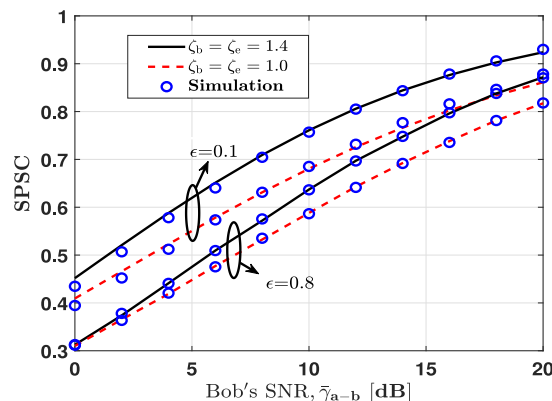


Fig. 6. SPSC versus $\bar{\gamma}_{a-b}$ for $\bar{\gamma}_{a-e} = 10$ dB and different values of AN power allocation factor ϵ and PE parameter considering strong turbulence.

and less to the AN. In addition, it can be observed from the figure that the SPSC of FSO systems improves with an increase in the values of ζ_b and ζ_e .

Discussion: It can be inferred from the aforementioned numerical results that the choice of the power allocation factor ϵ , received SNR at Bob as well as at Eve, the AT regimes, and PEs play an important role in the performance of AN-based FSO communication systems. The secrecy performance of the considered FSO system deteriorates with the increase in ϵ and the eavesdropper's SNR. Additionally, a poor secrecy performance can also be observed for weak AT and lower value of PEs. Moreover, it is also found that the reliability and throughput of the considered FSO system improves with the increase in ϵ , increase in received SNR at Bob, and decrease in PEs. For instance, $\epsilon = 1$ represents the absence of AN in the considered FSO system. Thus, it can be inferred from Fig. 2 that the considered FSO system becomes highly insecure for $\epsilon = 1$. Additionally, it can be observed from Fig. 5 that the considered FSO system attains the maximum throughput for $\epsilon = 1$. Thus, a trade-off between security and throughput can be observed as a function of ϵ .

6. Conclusions

In this paper, an AN injection scheme is proposed to enhance the secrecy performance of FSO systems. Performance metrics such as the SOP, SPSC, and throughput of the FSO system are investigated. Through analysis and simulation, it is shown that the proposed technique is

beneficial in improving the secrecy performance of FSO systems. Useful insights into the FSO system performance are drawn from the simulation results. The experimental implementation of the proposed AN injection-based FSO systems would be considered as our future research work.

References

- [1] 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.
- [2] P. Saxena, A. Mathur, and M. R. Bhatnagar, "BER performance of an optically pre-amplified FSO system under turbulence and pointing errors with ASE noise," *J. Opt. Commun. Netw.*, vol. 9, no. 6, pp. 498–510, Jun. 2017.
- [3] Y. Ai, A. Mathur, M. Cheffena, M. R. Bhatnagar, and H. Lei, "Physical layer security of hybrid satellite-FSO cooperative systems," *IEEE Photon. J.*, vol. 11, no. 1, Feb. 2019, Art. no. 7900814.
- [4] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical-layer security in evolving optical networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 110–117, Aug. 2016.
- [5] K. Guan, J. Cho, and P. J. Winzer, "Physical layer security in fiber-optic MIMO-SDM systems: An overview," *Opt. Commun.*, vol. 408, pp. 31–41, Feb. 2018.
- [6] 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.
- [7] Y. Ai, A. Mathur, G. D. Verma, L. Kong, and M. Cheffena, "Comprehensive physical layer security analysis of FSO communications over Málaga channels," *IEEE Photon. J.*, vol. 12, no. 6, Dec. 2020, Art. no. 7906617.
- [8] P. Paul, M. R. Bhatnagar, and A. Jaiswal, "Jamming in free space optical systems: Mitigation and performance evaluation," *IEEE Trans. Commun.*, vol. 68, no. 3, pp. 1631–1647, Mar. 2020.
- [9] P. Paul, M. R. Bhatnagar, and A. Jaiswal, "Alleviation of jamming in free space optical communication over Gamma-Gamma channel with pointing errors," *IEEE Photon. J.*, vol. 11, no. 5, Oct. 2019, Art. no. 7906418.
- [10] C. Li *et al.*, "A 5 m/25 gbps underwater wireless optical communication system," *IEEE Photon. J.*, vol. 10, no. 3, Jun. 2018, Art. no. 7904909.
- [11] 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.
- [12] K. Xu, Y. Chen, T. Okhai, and L. Snyman, "Micro optical sensors based on avalanching silicon light-emitting devices monolithically integrated on chips," *Opt. Mater. Exp.*, vol. 9, no. 10, pp. 3985–3997, Oct. 2019.
- [13] T. Wang and I. B. Djordjevic, "Physical-layer security in free-space optical communications using Bessel-Gaussian beams," in *Proc. IEEE Photon. Conf.*, Reston, VA, 2018, pp. 1–2.
- [14] X. Sun and I. B. Djordjevic, "Physical-layer security in orbital angular momentum multiplexing free-space optical communications," *IEEE Photon. J.*, vol. 8, no. 1, Feb. 2016, Art. no. 7901110.
- [15] Q. Huang *et al.*, "Secure free-space optical communication system based on data fragmentation multipath transmission technology," *Opt. Exp.*, vol. 26, no. 10, pp. 13536–13542, May 2018.
- [16] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
- [17] B. He, Y. She, and V. K. N. Lau, "Artificial noise injection for securing single-antenna systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9577–9581, Oct. 2017.
- [18] Z. Ghassemloooy, W. Popoola, S. Rajbhandari, *Optical Wireless Communications: System and Channel Modelling With MATLAB*. Amsterdam, Paris, New York: CRC Press, 2012.
- [19] K. Xu, "Monolithically integrated si gate-controlled light-emitting device: Science and properties," *J. Opt.*, vol. 20, no. 2, pp. 1–8, Jan. 2018.
- [20] 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.
- [21] A. Jurado-Navas, J. M. Garrido-Balsells, J. F. Paris, and A. Puerta-Notario, "A unifying statistical model for atmospheric optical scintillation," in *Numerical Simulations of Physical and Engineering Processes*, J. Awrejcewicz, Ed., Intech, 2011, ch. 8.
- [22] I. S. Ansari, F. Yilmaz, and M.-S. Alouini, "Performance analysis of free-space optical links over Málaga (M) turbulence channels with pointing errors," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 91–102, Jan. 2016.
- [23] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*. New York, NY, USA: McGraw-Hill, 2002.
- [24] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [25] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables*. New York, NY, USA: Dover, 1970.
- [26] K. Roach, "Meijer-g function representations," in *Proc. ACM Int. Conf. Symbolic Algebraic Comput.*, Jul. 1997, pp. 205–211.
- [27] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 6th ed. San Diego, CA, USA: Academic Press, 2000.
- [28] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York, NY, USA: Cambridge Univ. Press, 2004.
- [29] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals and Series: Vol. 3: More Special Functions*, New York, NY, USA: CRC Press, 1992.