PHYSICAL LAYER SECURITY OF HYBRID MILLIMETER-WAVE AND FREE-SPACE OPTICAL SYSTEMS FOR 5G AND BEYOND NETWORKS

A Dissertation

by

SEZER CAN TOKGOZ

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Chair of Committee,	Khalid A. Qaraqe
Co-Chair of Committee,	Scott L. Miller
Committee Members,	Erchin Serpedin
	Aydin Karsilayan
	Madhav Erraguntla
Head of Department,	Miroslav M. Begovic

December 2021

Major Subject: Electrical Engineering

ABSTRACT

Wireless communication technologies have evolved significantly over the past decades. The explosive growth of the wireless communications market is predicted to continue in the future, with the increasing demand for all types of wireless services. Besides providing higher data rates in comparison with previous technologies, next-generation wireless networks are expected to have advanced capabilities such as ultra-low latency, high reliability, interoperability, efficient spectrum utilization along with a wide variety of applications over various domains, e.g., public safety and military, aeronautical networks, femtocells, etc.

On the other hand, security flaws have also been serious problems in the community of wireless communications. The information-theoretic security of wireless communications goes long way back to 1949, Shannon's leading work, in which a random secret key is shared to secure the communication between a legitimate pair in the presence of an eavesdropper. After many years, Wyner presented his model, aka the wiretap channel, where the fading channel impairments take place to secure the communication in the physical layer without the need for a secret key. Since then, the interest in wiretap channels has remarkably increased and also extended to other systems.

Therefore, considering the quality of service (QoS) requirements of 5G and beyond networks, hybrid Free-Space Optical (FSO) and millimeter Wave (mmWave) systems have emerged as a promising remedy due to the unique complementary properties against the different channel and environmental conditions. Consequently, in this dissertation, hybrid FSO-mmWave systems are investigated from a physical-layer security point of view in the presence of different types of eavesdroppers, where the communication between two legitimate peers takes place over both FSO and mmWave links simultaneously. Practical scenarios are examined to eavesdrop on the legitimate communication, and the effects of random radio power of mmWave links and optical irradiance of FSO links are discussed on the probability of achieving a secure transmission. The impact of fundamental physical layer parameters on the secrecy performance of the hybrid system is analyzed by obtaining analytical derivations of several performance metrics.

DEDICATION

To my wife for her endless love, support and encouragement.

ACKNOWLEDGMENTS

First of all, I would like to sincerely thank my chair Dr. Khalid A. Qaraqe for his support, guidance, encouragement, valuable feedback, and arranging all facilities throughout my Ph.D. studies both at Texas A&M University (TAMU) and at Texas A&M University at Qatar (TAMUQ).

I also would like to send my special thanks to my co-chair Dr. Scott L. Miller for his guidance, financial support, and the valuable time that he spent in the revision of my studies at TAMU.

I wish to thank individually Dr. Erchin Serpedin, Dr. Aydin Karsilayan, and Dr. Madhav Erraguntla for agreeing to serve in my supervisory committee, and for their valuable recommendations.

I would like to extend my very special thanks to Dr. Serhan Yarkan, who enlightened and supported me starting from my B.Sc. time at Istanbul Commerce University. I can certainly say that I would not be able to go for a Ph.D. without his guidance, directions, and encouragement.

I would like to recognize Dr. Saud Althunibat from Al-Hussein Bin Talal University in a very special way for his solid technical contribution, providing ideas, stimulating suggestions, understanding, and encouragement during the entire period of my Ph.D.

I am also grateful to Dr. Ali Boyaci for his precious help, guidance, substantial advices, and valuable time that he spent during my time at both Istanbul Commerce University and TAMUQ.

I am also very thankful to Dr. Muhammed Ali Aydin from Istanbul University-Cerrahpasa for his significant help and recommendations, and to Dr. Ferkan Yilmaz from Yildiz Technical University for his contributions and suggestions during the last part of my Ph.D. period.

Special thanks go to Tapir Lab. and its very valuable members. I would like to mention my friends Osman Boyaci, Ozgur Alaca, and Halil Said Cankurtaran for their continuous support, hilarious humor, and the great time that we spent in Istanbul, Doha, and College Station.

Last but by no means least, I would like to express my deepest gratitude to my wife to whom this work is dedicated. I will also be forever grateful to my parents, and my sister for their support.

CONTRIBUTORS AND FUNDING SOURCES

Contributors

This work was supported by a dissertation committee consisting of Professor Khalid A. Qaraqe (advisor), Professor Scott L. Miller (co-advisor), Professor Aydin Karsilayan and Professor Erchin Serpedin of the Department of Electrical & Computer Engineering, and Professor Madhav Erraguntla of the Department of Industrial & Systems Engineering.

All work conducted for the dissertation was completed by the student independently.

Funding Sources

Graduate study was supported by a fellowship from the Department of Electrical & Computer Engineering at Texas A&M University.

NOMENCLATURE

AF	amplify-and-forward
AWGN	additive white Gaussian noise
BER	bit-error-rate
BPSK	binary phase shift keying
CDF	cumulative density function
CNN	convolutional neural network
CSI	channel state information
DL	deep learning
EGBMG	extended generalized binary Meijer's G
EST	effective secrecy throughput
FSO	Free-space optical
GG	Gamma-Gamma
IM	index modulation
IM/DD	intensity-modulation/direct-detection
k-NN	k-nearest neighbors
LCR	level crossing rate
LOS	line-of-sight
MGF	moment generating function
MIMO	multiple-input and multiple-output
ML	machine learning
MLi	maximum lilelihood
*mm*Wave	millimeter wave

MRC	maximum ratio combining
NB	naive-Bayes
PDF	probability density function
PSK	phase shift keying
RF	radio frequency
RV	random variable
SIMO	single-input and multiple-output
SNR	signal-to-noise ratio
SOD	secrecy outage duration
SOP	secrecy outage probability
SOR	secrecy outage rate
SPSC	strictly positive secrecy capacity
SVM	support vector machine

TABLE OF CONTENTS

Page

LIST OF FIGURES

FIGURE Page

LIST OF TABLES

TABLE Page

1. INTRODUCTION

Wireless communication technologies have evolved significantly over the past decades. The explosive growth of the wireless communications market is predicted to continue in the future, with the increasing demand for all types of wireless services. Besides providing higher data rates in comparison with previous technologies, next-generation wireless networks are expected to have advanced capabilities such as ultra-low latency, high reliability, interoperability, efficient spectrum utilization along with a wide variety of applications over various domains, e.g., public safety, military, aeronautical networks, femtocells, picocells, microcells, macrocells, etc.

Therefore, due to the ever-increasing demand of wireless data volumes and scarcity concerns of RF spectrum, researchers exploit the higher frequency bands to fulfill the 5G era requirements, in which overall data volume is predicted to be at least a thousand fold greater compared to 4G. FSO communications is a promising candidate for future high-data-rate wireless transmissions because of its inherent advantages such as low energy consumption, a certain immunity to interference, and a high level of security compared to the traditional RF wireless communication systems. However, FSO systems are very susceptible to line-of-sight (LOS) alignments and are heavily affected by several atmospheric conditions including thermal expansion, wind load, and foggy weather. Alternatively, the higher RF band studies demonstrate that *mm*Wave systems pave the way for multi-gigabit wireless transmissions. However, *mm*Wave systems are dramatically affected by oxygen absorption, rainy atmosphere, and have high energy consumption, and are more vulnerable to security attacks. These mentioned complementary properties of both communication links led to the joint deployment of FSO and *mm*Wave systems to provide reliable and high speed transmissions. Moreover, the supported data rates by each system are compatible, which provides the parallel utilization of both systems to improve transmit diversity or spectral efficiency.

1.1 Millimeter Wave Fading Channel Characteristics

The statistics of small-scale fading at *mm*Wave frequencies have not been extensively investigated, compared to the large-scale path loss model parameters, in the open literature [1,2]. Beyond 6 GHz, the *mm*Wave channel model in the 5G standard, provided by the 3GPP organization, is mathematically intractable [3]. The available small-scale fading measurements in millimeter wave bands have shown significant inference for spatial and temporal fading of multipath amplitudes. Therefore, motivated by a comprehensive literature search, it is widely accepted that Weibull [4–9] or Nakagami-m [10–13] channel models are the most widely considered to approximate small-scale propagation effects for the *mm*Wave link.

1.1.1 Weibull Distribution

A random variable (RV) H is considered to represent the instantaneous RF channel power that can be modeled as Weibull distribution with parameters δ and λ, denoted as $H \sim \mathsf{Wbl}(\delta, \lambda)$. Its probability density function (PDF) is expressed as [14, (2.27)]

$$f_H(h) = \frac{\lambda}{\delta} h^{\lambda-1} \exp\left[-\frac{h^\lambda}{\delta}\right], \tag{1.1}$$

where $h \geq 0$, and $\lambda > 0$ is the shape parameter which characterizes the severity of fading. The scale parameter δ is associated with fading power $\mathbb{E}\langle h \rangle$

$$\delta = \left(\frac{\mathbb{E}\langle h \rangle}{\Gamma\left(1 + \frac{1}{\lambda}\right)}\right)^{\frac{1}{\lambda}}, \tag{1.2}$$

where $\mathbb{E}\langle \cdot \rangle$ denotes the expectation operator, and $\Gamma(\cdot)$ is the gamma function, defined as $\Gamma(z) = \int_0^\infty y^{z-1} e^{-y} dy$. Accordingly, the n^{th} positive integer power of H is also a Weibull RV but with different parameters δ^n and λ/n, denoted as $\widetilde{H} = H^n \sim \mathsf{Wbl}(\delta^n, \lambda/n)$. Therefore, the PDF in (1.1)

is re-written as

$$f_{\widetilde{H}}(\tilde{h}) = \frac{\lambda}{n\delta^n}\tilde{h}^{\frac{\lambda}{n}-1}\exp\left[-\frac{\tilde{h}^{\frac{\lambda}{n}}}{\delta^n}\right]. \tag{1.3}$$

Therefore, $\gamma_{x,f} \sim \mathsf{Wbl}(\delta^2, \lambda/2)$, and based on (1.1), the PDF of $\gamma_{x,f}$ is expressed as

$$f_{\gamma_{x,f}}(\gamma_{x,f}) = \frac{\lambda_x}{2\delta_x^2}\gamma_{x,f}^{\frac{\lambda_x}{2}-1}\exp\left[-\frac{\gamma_{x,f}^{\lambda_x/2}}{\delta_x^2}\right], \tag{1.4}$$

and based on (1.2), the scale parameter δ_x^2 is expressed as

$$\delta_x^2 = \left(\frac{\overline{\gamma}_{x,f}}{\Gamma\left(1+\frac{2}{\lambda_x}\right)}\right)^{2/\lambda_x}. \tag{1.5}$$

1.1.2 Nakagami-m Distribution

Thus, a RV H is considered to denote the instantaneous RF channel power that is modeled by a Nakagami-m distribution, and its well-known PDF is expressed as

$$f_H(h) = \frac{2m^m}{\Gamma(m)}h^{2m-1}e^{-mh^2}, \tag{1.6}$$

where m denotes the fading order/severity.

It is well-known, based on (1.6), that the instantaneous SNR over a Nakagami-m fading channel is distributed according to a Gamma distribution expressed as [14, (2.21)]

$$f_{\gamma_f}(\gamma_{x,f}) = \frac{m^m}{\Gamma(m)\overline{\gamma}_{x,f}^m}\gamma_{x,f}^{m-1}\exp\left[-\frac{m}{\overline{\gamma}_{x,f}}\gamma_{x,f}\right], \tag{1.7}$$

accordingly, the cumulative density function (CDF) of SNR can be obtained as

$$F_{\gamma_f}(\gamma_{x,f}) = \frac{1}{\Gamma(m)}\Gamma_{\mathrm{L}}\left(m, \frac{\gamma_{x,f}}{\overline{\gamma}_{x,f}}\right), \tag{1.8}$$

where $\Gamma_{\mathrm{L}}(\cdot,\cdot)$ represents the lower incomplete Gamma function, and alternatively, the CDF of SNR can be re-expressed as

$$F_{\gamma_f}(\gamma_{x,f}) = 1 - \sum_{k=0}^{\infty} \frac{1}{k!} \left(\frac{m_x}{\overline{\gamma}_{x,f}}\right)^k \gamma_{x,f}^k \exp\left[-\frac{m_x}{\overline{\gamma}_{x,f}}\gamma_{x,f}\right], \tag{1.9}$$

$$= \frac{1}{\Gamma(m_x)} G_{1,2}^{1,1}\left(\frac{\gamma_{x,f}}{\overline{\gamma}_{x,f}}\middle| \begin{matrix} 1 \\ m_x, 0 \end{matrix}\right). \tag{1.10}$$

1.2 Free Space Optical Atmospheric Turbulence Characteristics

The statistical behavior of the received optical irradiance is characterized by means of small- and large-scale eddies. Therefore, in the open literature a high number of models are proposed to model the optical irradieance of FSO channels. An exponential model [15–20] is currently used to model the optical irradieance of a FSO system in specific environmental conditions. Also, a Gamma-Gamma [21–27] model has been widely used to model the FSO channel due to its doubly stochastic scintillation model, where the received intensity is expressed as the product of two independent Gamma RVs which represent the irradiance fluctuations caused by large- and small-scale atmospheric-turbulence.

1.2.1 Exponential Distribution

A RV I is considered to represent the instantaneous irradiance of the FSO channel that can be modeled as an exponential distribution with a scale parameter β, denoted as $I \sim \mathsf{Exp}(\beta)$. Its PDF is expressed as

$$f_I(i) = \frac{1}{\beta} \exp\left[-\frac{1}{\beta} i\right], \tag{1.11}$$

where $i \geq 0$, and $\beta > 0$. Furthermore, the m^{th} positive integer power of I is a Weibull RV with parameters β and $1/m$, denoted as $\tilde{I} = I^m \sim \mathsf{Wbl}(\beta^m, 1/m)$. Therefore, the PDF in (1.11) is

re-written as

$$f_{\tilde{I}}(\tilde{i}) = \frac{1}{m\beta^m} \tilde{i}^{\frac{1}{m}-1} \exp\left[-\frac{\tilde{i}^{1/m}}{\beta^m}\right]. \tag{1.12}$$

It is worthy to note that the pointing errors at FSO links are extensively discussed in the literature as a combination of boresight and jitter effects [28–30]. However, due to the mathematical intractability, the pointing errors are not introduced to the FSO system. Therefore, $\gamma_{b,o} \sim \mathsf{Wbl}(\beta^2, 1/2)$, and based on (1.11), the PDF of $\gamma_{b,o}$ is expressed as

$$f_{\gamma_{b,o}}(\gamma_{b,o}) = \frac{1}{2\beta^2\sqrt{\gamma_{b,o}}} \exp\left[-\frac{\sqrt{\gamma_{b,o}}}{\beta^2}\right], \tag{1.13}$$

and based on (1.2), the scale parameter β^2 is expressed as

$$\beta^2 = \left(\frac{\overline{\gamma}_{b,o}}{\Gamma(3)}\right)^2. \tag{1.14}$$

1.2.2 Gamma-Gamma Distribution

We consider a RV I to represent the instantaneous FSO channel power that is modeled as Gamma-Gamma distribution, and its PDF is expressed as [27, (57)]

$$f_I(i) = \frac{2(\alpha\beta)^{(\alpha+\beta)/2}}{\Gamma(\alpha)\Gamma(\beta)} i^{\frac{\alpha+\beta}{2}-1} K_{\alpha-\beta}(2\sqrt{\alpha\beta i}), \tag{1.15}$$

where $i > 0$ due to the non-negativity property of light waves, $\Gamma(\cdot)$ denotes the Gamma function, $K_\nu(\cdot)$ represents the modified Bessel function of the second kind of the ν^{th} order. α and β denote the effective coefficients of small- and large-scale eddies of the atmospheric-turbulence environ-

ment, respectively, which are calculated as [27, (58)-(59)]

$$\alpha = \exp\left\{\exp\left[\frac{0.49\zeta^2}{\left(1+0.65\vartheta^2+1.11\zeta^{12/5}\right)^{7/6}}\right]-1\right\}^{-1}, \tag{1.16}$$

$$\beta = \exp\left\{\exp\left[\frac{0.51\zeta^2\left(1+0.69\zeta^{12/5}\right)^{-5/6}}{1+0.9\vartheta^2+0.62\vartheta^2\zeta^{12/5}}\right]-1\right\}^{-1}, \tag{1.17}$$

where $\zeta^2 = 1.23C_n^2\Lambda^{7/6}d^{11/6}$ is the Rytov variance, and $\vartheta = \sqrt{\Lambda A^2/4d}$. Here, $\Lambda = 2\pi/\lambda_o$ is the optical wave number, λ_o depicts the optical carrier wavelength, d represents the link distance, A denotes the lens aperture diameter of the receiving photodiode, and C_n^2 stands for the weather-altitude depended refractive index (strength of turbulence). The atmospheric profile C_n^2 is most widely defined by the Hufnagel-Valley (HV5/7) model [26].

Furthermore, by making a simple transformation of the RV I in (1.15), the PDF of the electrical SNR is expressed as

$$f_{\gamma_o}(\gamma_{x,o}) = \frac{(\alpha\beta)^{\frac{(\alpha+\beta)}{2}}\gamma_{x,o}^{\frac{\alpha+\beta}{4}-1}}{\Gamma(\alpha)\Gamma(\beta)\overline{\gamma}_{x,o}^{\frac{\alpha+\beta}{4}}} K_{\alpha-\beta}\left(2\sqrt{\alpha\beta}\sqrt[4]{\frac{\gamma_{x,o}}{\overline{\gamma}_{x,o}}}\right), \tag{1.18}$$

accordingly, the CDF of SNR can be obtained as

$$F_{\gamma_o}(\gamma_{x,o}) = \frac{1}{\Gamma(\alpha)\Gamma(\beta)} G_{1,3}^{2,1}\left(\frac{\alpha\beta}{\sqrt{\overline{\gamma}_{x,o}}}\sqrt{\gamma_{x,o}}\,\middle|\,\begin{matrix}1\\ \alpha,\beta,0\end{matrix}\right). \tag{1.19}$$

1.3 Average Signal-to-Noise Ratio Models

1.3.1 mmWave Subsystems

For an RF channel that is modeled by Nakagami-m distribution, the average electrical SNR of the RF link, $\gamma_{x,f}$, is expressed as

$$\gamma_{x,f} = \overline{\gamma}_{x,f}H_x^2, \tag{1.20}$$

where H_x depicts the instantaneous channel gain, and $\overline{\gamma}_{x,f}$ is the average electrical SNR of the RF link, given as

$$\overline{\gamma}_{x,f} = \frac{P_t R_{x,f} L_{x,f}}{\sigma_x^2}, \tag{1.21}$$

where P_t denotes the transmit power from the legitimate transmitter Alice, $R_{x,f} \in [0, 1)$ stands for the collected power, and $L_{x,f}$ represents the path loss between Alice and the receiving side, which is given as [12]

$$L_{x,f} = \frac{G_T G_R \lambda_f^2}{(4\pi d_x)^2 (\varphi_{\mathrm{O}_2} d_x)(\varphi_{\text{rain}} d_x)}, \tag{1.22}$$

where G_T and G_R, in turn, are the gains of transmitting and receiving antennas, λ_f denotes the RF carrier wavelength, and φ_{O_2} and φ_{rain} stands for the attenuation coefficients caused by the oxygen absorption and rainy weather condition, respectively.

1.3.2 FSO Subsystems

For an FSO channel that is modeled by Gamma-Gamma distribution, considering intensity-modulation/direct-detection (IM/DD) technique, $\gamma_{x,o}$ is expressed as

$$\gamma_{x,o} = \overline{\gamma}_{x,o} I_x^2, \tag{1.23}$$

where I_x represents the normalized irradiance turbulence, and $\overline{\gamma}_{x,o}$ is the average electrical SNR of the FSO link, given as

$$\overline{\gamma}_{x,o} = \left(\frac{\eta I_t R_{x,o} L_{x,o}}{\sigma_x} \right)^2, \tag{1.24}$$

η denotes the optical-to-electrical conversion efficiency, I_t is the radiant emittance of the laser from Alice, $R_{x,o}$ depicts the received power ($0 \leq R_{x,o} \leq 1$), and $L_{x,o}$ stands for the intensity attenuation

loss in the path between legitimate transmitter Alice and the receiving side

$$L_{x,o} = \frac{\pi A^2}{4(\psi d_x)^2} \exp\big[-\varphi_o d_x\big], \tag{1.25}$$

where A is the diameter of the photodetector' aperture, ψ represents the beam divergence of the laser, φ_o denotes the attenuation extinction coefficient, and d_x represents the distance between legitimete transmitter Alice and the receiving side.

1.3.3 Simulation Parameters

The results include various cases including different fundamental physical layer parameters such as average SNRs, link distances, weather conditions, correlation coefficients, and eavesdropper types and location. The simulation parameters for the system and channel models are given in Table 1.1 and Table 1.2 [3, 12, 31, 32]. It should be noted that for all results, the average electrical SNR of each link is assumed to be identical, and adjusted by fixing the electrical transmit power at the *mm*Wave link, and computing the corresponding values of the noise power and the optical transmit power for the FSO link.

1.4 Performance Analysis Metrics for Wireless Transmissions

According to the information-theoretic point of view of physical layer security, the secrecy capacity is the maximum transmission rate at which an eavesdropper Eve is able to retrieve no information. Since the term of capacity is by definition a positive-valued metric, the secrecy capacity is set to zero, if the eavesdropper's channel gain is greater than the legitimate receiver's channel gain. Hence, the secrecy capacity is first time computed in [33] for the Gaussian wiretap channel and given by

$$C_S = \big[C_b - C_e\big]^+, \tag{1.26}$$

Table 1.1: Parameters of FSO and *mm*Wave systems

FSO System		
Parameters	*Symbols*	*Values*
Wavelength	λ_o	$1550\,\text{mm}$
Optical Power	I_t	$40\,\text{mW}$
Aperture's Diameter	A	$0.2\,\text{m}$
Beam Divergence	ψ	$10\,\text{mrad}$
Photosensitivity	η	$0.5\,\text{A/W}$
***mm*Wave System**		
Parameters	*Symbols*	*Values*
Wavelength	λ_f	$c/60\,\text{nm}$
Electrical Power	P_t	$10\,\text{mW}$
Transmitter Antenna Gain	G_T	$44\,\text{dBi}$
Receiver Antenna Gain	G_R	$44\,\text{dBi}$
Oxygen Absorption	φ_{O_2}	$15.1\,\text{dB/km}$

*c is the speed of light, $c = 299,792,458\,\text{m/s}$.

Table 1.2: Parameters for different turbulence conditions

Weather-Dependent Parameters			
Weather Conditions	φ_o *(dB/km)*	φ_{rain} *(dB/km)*	C_n^2
Clean Air	0.43	0	5×10^{-14}
Haze	4.2	0	1.7×10^{-14}
Moderate Rain ($12.5\,\text{mm/h}$)	5.8	5.6	5×10^{-15}
Moderate Fog	42.2	0	2×10^{-15}

where $[\,\cdot\,]^+$ denotes the maximum function $\max\{0, \cdot\}$, and the expressions C_b and C_e are the instantaneous capacity of the main and wiretap channels, respectively, and are expressed as

$$C_b = B \log_2 \big(1 + \gamma_b\big), \tag{1.27}$$

$$C_e = B \log_2 \big(1 + \gamma_e\big), \tag{1.28}$$

where γ_b and γ_e depict the instantaneous electrical SNRs of Bob and Eve, respectively. Note that, for the sake of simplicity, the normalized bandwidth of $B = 1$ is assumed in the rest of this dissertation. Additionally, by substituting (1.27) and (1.28) into (1.26), the secrecy capacity can be re-expressed as

$$C_S = \begin{cases} \log_2\left(1+\gamma_b\right) - \log_2\left(1+\gamma_e\right), & \gamma_b > \gamma_e, \\ 0, & \gamma_b \leq \gamma_e. \end{cases} \tag{1.29}$$

1.4.1 Ergodic Secrecy Capacity

The secrecy capacity given in (1.26) is for a single realization of the wireless fading channels. Therefore, by averaging the secrecy capacity over all available fading channel realizations, the ergodic secrecy capacity with full channel state information (CSI) is expressed as

$$\overline{C}_S = \int_0^\infty \int_{\gamma_e}^\infty \big(\log_2(1+\gamma_b) - \log_2(1+\gamma_e)\big) f_{\gamma_b}(\gamma_b) f_{\gamma_e}(\gamma_e) \cdot d\gamma_b d\gamma_e, \tag{1.30}$$

where $f_{\gamma_b}(\gamma_b)$ and $f_{\gamma_e}(\gamma_e)$ denote the PDFs of SNRs of the legitimate receiver and the eavesdropper, respectively. It is worthy to note that having the full CSI of both main and wiretap channels paves the way for perfect secrecy, in which the legitimate transmitter Alice can ensure that the wireless transmission occurs only when the SNR of Bob is greater than the SNR of Eve, i.e., $\gamma_b > \gamma_e$. For the partial CSI case in which the CSI of the main channel is only available, the ergodic secrecy capacity is expressed as

$$\overline{C}_S = \int_0^\infty \int_0^\infty \big[\log_2(1+\gamma_b) - \log_2(1+\gamma_e)\big]^+ f_{\gamma_b}(\gamma_b) f_{\gamma_e}(\gamma_e) \cdot d\gamma_b d\gamma_e. \tag{1.31}$$

1.4.2 Secrecy Outage Probability

To characterize the secure communication between legitimate transmitter Alice and legitimate receiver Bob, the probabilistic metric of the SOP is widely used which is defined as

$$\begin{aligned} P_{SO}(\mathcal{R}_s) &= \text{Prob.}\big(C_S < \mathcal{R}_s\big), \\ &= \text{Prob.}\big(C_b - C_e < \mathcal{R}_s\big), \end{aligned} \tag{1.32}$$

which is the probability that the achievable secrecy rate is less than a target secrecy rate $\mathcal{R}_s > 0$.

1.4.3 Probability of Strictly Positive Secrecy Capacity

A special version of SOP, called the probability of SPSC, which is also known as the probability of existence of secure communications, defined as

$$\begin{aligned} P_S^+ &= 1 - P_{SO}(\mathcal{R}_s = 0), \\ &= 1 - \text{Prob.}\big(C_b - C_e < 0\big). \end{aligned} \tag{1.33}$$

1.4.4 Effective Secrecy Throughput

Based on the definition of SOP, the EST can be obtained by the product of secrecy rate and the probability of successful transmission. According to this definition, the EST can be formulated as

$$E_{ST}(\mathcal{R}_s) = \mathcal{R}_s\big(1 - P_{SO}(\mathcal{R}_s)\big). \tag{1.34}$$

1.4.5 Secrecy Outage Rate

The average secrecy outage rate (SOR), also known as the average secrecy level crossing rate (LCR), is defined by the instantaneous secrecy capacity at a level of $\mathcal{R}_s$. The average SOR provides the expected number of outage, downward crossings the secrecy capacity in terms of seconds. In other words, it provides the statistic at a specific threshold $\mathcal{R}_s$ in time. The average SOR is

expressed based on the generic expression given in [34, (2.90)]

$$R_{SO}(\mathcal{R}_s) = \int_0^\infty \int_0^\infty \dot{\gamma} f_\gamma(\gamma_{\text{th}}) f_{\dot{\gamma}}(\dot{\gamma}) f_{\gamma_e}(y) \cdot d\dot{\gamma} dy, \tag{1.35}$$

where $\gamma_{\text{th}} = \sqrt{2^{\mathcal{R}_s}(1+\gamma_e) - 1}$, and $\dot{\gamma}$ is the time derivative of the signal amplitude process. It is worthy to note that the time derivative of the signal amplitude process $\dot{\gamma}$ is always independent of the signal amplitude γ and is normally distributed with zero mean but different variance depending on the type of fading.

1.4.6 Secrecy Outage Duration

The average secrecy outage duration (SOD) is another secrecy metric, which defines the expected average duration of the secrecy outage status for a wireless communication system. The average SOD is expressed based on the definition of the average outage duration, as given in [34, (2.106)]

$$D_{SO}(\mathcal{R}_s) = \frac{P_{SO}(\mathcal{R}_s)}{R_{SO}(\mathcal{R}_s)}. \tag{1.36}$$

1.5 Dissertation Outline

Here, a detailed outline of the following chapters in this dissertation are briefly introduced.

1.5.1 Chapter 2 – Secrecy Analysis of Single-Hop Hybrid FSO-RF Systems

In this chapter, a detailed investigation on single-hop hybrid FSO-RF systems is established from a physical-layer security point of view in the presence of independent and dependent wiretap channels for different types of eavesdroppers, where the communication between two legitimate peers takes place over both FSO and *mm*Wave links, simultaneously. Practical scenarios to eavesdrop the legitimate communication are examined, and the effects of random radio power of mmWave link and optical irradiance of FSO link are discussed on the probability of achieving a secure transmission. The outcomes of this chapter have been listed below for ease of reference:

J1. S. C. Tokgoz, S. Althunibat, S. L. Miller, and K. A. Qaraqe, "On the Secrecy Capacity of Hybrid FSO-mmWave Wiretap Channels," IEEE Transactions on Vehicular Technology,

2020, under revision.

J2. S. C. Tokgoz, S. Althunibat, S. L. Miller, and K. A. Qaraqe, "On the Secrecy Capacity of Hybrid FSO-mmWave Links with Correlated Wiretap Channels," ELSEVIER Optics Communications, vol. 499, 2021.

C1. S. C. Tokgoz, S. Althunibat, S. Yarkan, and K. A. Qaraqe, "Physical Layer Security of Hybrid FSO-mmWave Commutations in presence of Correlated Wiretap Channels," IEEE International Conference on Communications (ICC), pp. 1–7, Montreal, Canada, 2021.

1.5.2 Chapter 3 – Index Modulation-based Link Selection for Hybrid FSO-RF Systems

In this chapter, a novel link selection mechanism is proposed and investigated in detail for hybrid FSO-*mm*Wave systems based on the IM concept, which is recently introduced as an adaptive and efficient transmission scheme to exploit the index of system entities, e.g., antennas, subcarriers, users, etc. In the proposed IM-based selection mechanism, there is no feedback or CSI required at the transmitter side. Specifically, the first bit of each transmission block is dedicated to select which link is to be activated, while the remaining bits are modulated and transmitted over the activated link, in which activating only one link at a time provides lower power consumption at the transmitter side, and does not require combining or multiplexing methods at the receiver side. The outcomes of this chapter have been listed below for ease of reference:

J3. S. C. Tokgoz, S. Althunibat, S. L. Miller, and K. A. Qaraqe, "Performance Analysis of Index Modulation based Link-Selection Mechanism for Hybrid FSO-mmWave Systems," ELSEVIER Optics Communications, vol. 479, 2020.

C2. S. C. Tokgoz, S. Althunibat, and K. A. Qaraqe, "A Link-Selection Mechanism for Hybrid FSO-mmWave Systems based on Index Modulation," IEEE International Conference on Communications (ICC), pp. 1–7, Dublin, Ireland, 2020.

1.5.3 Chapter 4 – DL-based Secrecy Enhancement of MIMO Hybrid FSO-RF Systems

In this chapter, the transmitter link selection technique is investigated for multiple-input and multiple-output (MIMO) hybrid FSO-*mm*Wave systems from a physical layer security point of view in the presence of different types of eavesdroppers. In particular, a convolutional neural network (CNN)-based link selection scheme is proposed to maximize the secrecy performance by activating the antennas and lasers at the transmitter side based on predefined configurations. The impact of fundamental physical layer parameters on the secrecy performance of a hybrid system is examined by taking the availability of CSI, channel estimation errors, weather conditions, pointing error in FSO system, link distances, SNRs, path loss models into account. The outcomes of this chapter have been listed below for ease of reference:

J4. S. C. Tokgoz, S. Althunibat, S. Miller, and K. A. Qaraqe, "Learning-based Link Selection for MIMO FSO-mmWave Communications in Presence of Multiple Wiretap Channels," ELSEVIER Optics Communications, 2021, under review.

C3. S. C. Tokgoz, S. Althunibat, S. Miller, and K. A. Qaraqe, "Learning-based Link Selection for Secrecy Enhancement of Hybrid FSO-mmWave MIMO Wiretap Channels," IEEE Wireless Communications and Networking Conference (WCNC), Austin, USA, 2021, under review.

1.5.4 Chapter 5 – Secrecy Analysis of Relay-based Dual-Hop Hybrid FSO-RF Systems

In this chapter, dual-hop relaying schemes are combined with hybrid FSO-*mm*Wave systems to extend the communication distance, and to satisfy the reliability, low latency and high capacity requirements of 5G and beyond era. Particularly, two well-known amplify-and-forward (AF) relaying schemes are examined during data transmission, in which the power amplification operation is based on partial and full channel state information of the system, namely, fixed-gain and variable-gain AF relaying methods, respectively, where the communication in each hop takes place over both FSO and *mm*Wave links, simultaneously. The outcomes of this chapter have been listed below for ease of reference:

J5. S. C. Tokgoz, S. Althunibat, S. Yarkan, S. Miller, and K. A. Qaraqe, "Physical Layer Security of Relay-based Dual-Hop Hybrid FSO-mmWave Systems," IEEE Transactions on Communications, 2021, under review.

J6. S. C. Tokgoz, S. Althunibat, S. Miller, and K. A. Qaraqe, "Outage Analysis of Relay-based Dual-Hop Hybrid FSO-mmWave Systems," IEEE Access Journal, 2021, under revision.

1.5.5 Chapter 6 – A Unified MGF-based Framework for Physical Layer Security

In this chapter, a unified moment generating function (MGF)-based framework is proposed for the physical layer security analysis of wireless communication systems over generalized fading channels. To characterize the secure communication between legitimate pairs, the secrecy capacity, SOP, probability of SPSC, EST, SOR, and SOD metrics are derived for SIMO systems over generalized fading channels in the presence of different types of eavesdroppers. The MGF-based approach proposed in this chapter is explicitly generic enough to unify on the direction of generalized fading channels (i.e., there is no need to separately analyze the security metrics of maximum ratio combining (MRC) diversity technique) in addition to the direction of different type eavesdroppers. The outcomes of this chapter have been listed below for ease of reference:

J7. S. C. Tokgoz, F. Yilmaz, S. Yarkan, S. L. Miller, and K. A. Qaraqe, "A Unified MGF-based Framework for Physical Layer Security Analysis of Generalized Fading Channels," IEEE Transactions on Wireless Communications, 2021, under review.

J8. S. C. Tokgoz, F. Yilmaz, S. L. Miller, and K. A. Qaraqe, "On the Investigations of Sum of Weibull Random Variables with Performance Analysis on Diversity Systems," IEEE Wireless Communications Letter, 2021, under review.

1.5.6 Other Works Done

Apart from the works presented above, there are some other works, given in [35–42], that have been excluded from this dissertation. Although most of them are related to the elements of optical wireless communications, in order to keep the integrity of the text and flow, these works are not included in this dissertation.

2. SECRECY ANALYSIS OF SINGLE-HOP HYBRID FSO-RF SYSTEMS*

2.1 Introduction

2.1.1 Motivation

The performance of dual-hop mixed/relaying systems are dramatically decreased in specific atmospheric conditions. Therefore, as explained previously, one possible solution to overcome this problem is to employ parallel/simultaneous transmissions over both FSO and RF links due to their unique complementary properties with respect to different channel and environment conditions. Moreover, the growing demand of very high data rate in 5G and beyond networks require back-haul communications to have extreme reliability, low latency, and high capacity, in comparison with 3G and 4G, where the conventional RF back-haul systems are potentially limited by latency and throughput.

2.2 Related Works

The mixed, dual-hop, and/or relaying schemes for RF and FSO systems are extensively investigated in [45–72] under several scenarios and configurations. The authors in [55–63] consider a mixed RF-FSO dual-hop communication system for both fixed- and variable-gain relaying schemes in the presence of a single eavesdropper which only happens at RF link. A mixed single-input multiple-output simultaneous wireless information and power transfer based RF and FSO systems are investigated in [64–66] with a energy harvesting RF receiver that acts as a potential eavesdropper. The secrecy outage performance of a mixed RF-FSO transmission system with imperfect channel state information is analyzed in [67–72], for the single-input multiple-output wiretap model, where a relay forwards the transmit signal from a source to a destination, while an eavesdropper wiretaps the confidential information by using multiple antennas.

*Reprinted with permission from "On the secrecy capacity of hybrid FSO-mmWave links with correlated wiretap channels" by Sezer C. Tokgoz, Saud Althunibat, Scott L. Miller, and Khalid A. Qaraqe, 2021. Optics Communications, 499, 127252, Copyright [2021] by Elsevier [43], and from "Physical layer security of hybrid FSO-mmWave communications in presence of correlated wiretap channels" by Sezer C. Tokgoz, Saud Althunibat, Serhan Yarkan, and Khalid A. Qaraqe, 2021. International Conference on Communications (ICC), 1–7, Copyright [2021] by IEEE [44].

On the other hand, security analysis of hybrid FSO and RF systems are examined in [73–77], considering a parallel/simultaneous transmission between legitimate pairs over both RF and FSO links. Additionally, considering high security assumption of FSO links, only RF type eavesdropper is investigated in these studies. For example, the authors in [73–75] examine a hybrid FSO-RF system under a modified selection combining scheme considering the pointing errors in the FSO transmission and the power amplifier (PA) inefficiency for the RF transmission. Furthermore, link blockage impairments are discussed in [76] for the secrecy performance of a cognitive underlay hybrid RF-FSO system with primary and secondary users. Power optimization and rate allocation in each link of a hybrid FSO-RF system are investigated in [77] while satisfying a constraint on the security of the communication, represented by the secrecy outage probability, and a constraint on its power budget. As distinct from others, the authors in [78] proposed an enhanced security algorithm for a wireless communication system deploying hybrid FSO-RF links in presence of hybrid eavesdropper, in which the activation of either links, FSO or RF, is determined through IM technique. A comprehensive physical layer security analysis of dual-hop mixed and hybrid parallel FSO-RF systems is investigated in [79] considering both RF and FSO eavesdroppers individually.

2.3 System Model

In this chapter, we consider a scenario where the classic Wyner's wiretap channel takes place [80]. The legitimate transmitter, Alice, wants to send confidential information to the legitimate receiver, Bob, while an eavesdropper, Eve, tries to wiretap confidential information by sniffing the received signals, as illustrated in Fig. 2.1. As explained previously, to take the advantage of the unique complementary properties of FSO and RF transmissions by using diversity against different weather and environmental conditions, the communication between legitimate pairs Alice and Bob are accomplished through two parallel links, namely, an FSO link and an RF link. As such, it is assumed that Alice has a single transmit antenna and a single laser, while Bob has a single receive antenna and a single photodetector. Transmitted data are divided into $\log_2(M)$ bit blocks, where M is the modulation order. For a simultaneous transmission, each block is modulated and emitted via both links. To provide identical bandwidth over the two links, the RF link operates over the *mm*Wave

frequency range.

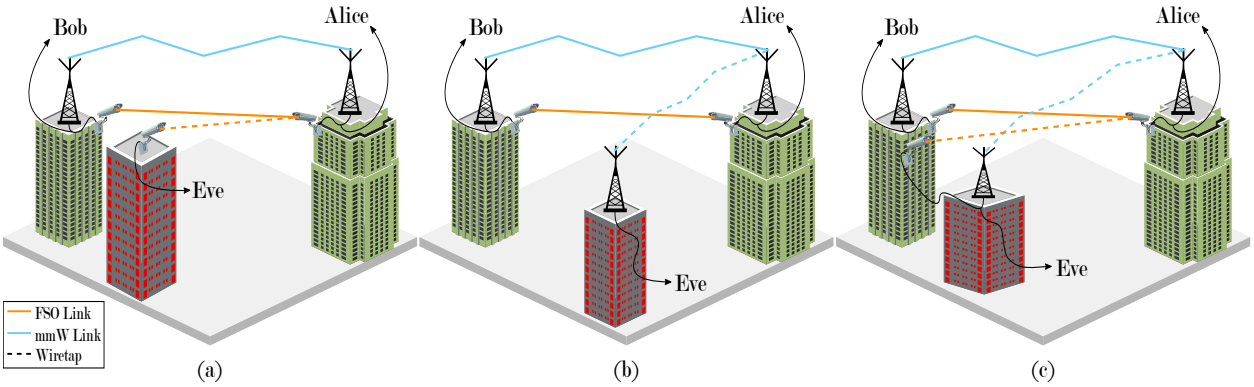


Figure 2.1: System model of hybrid FSO-*mm*Wave communications considering uncorrelated channels, between the legitimate transmitter Alice and receiver Bob in the presence of different types of eavesdroppers: (a) FSO-Eve, (b) RF-Eve, and (c) Hybrid-Eve.

Based on its ability and resources, three different types of Eve are considered, namely, Eve-RF, Eve-FSO and Eve-Hybrid. Eve-RF can eavesdrop only on the RF link using a single receive antenna, while Eve-FSO can eavesdrop only on the FSO link using a single photodetector. On the other hand, Eve-Hybrid is assumed to have a single receive antenna and a single photodetector, and hence, it can eavesdrop both links.

2.3.1 Channel Characteristics

The channel models that are used in this chapter are presented in subsections 1.1 and 1.2 for *mm*Wave and FSO links, respectively. In particular, Weibull and Nakagami-m distributions are considered for *mm*Wave fading channels, while exponential and Gamma-Gamma distributions are used for FSO turbulence channels.

2.3.2 Signal-to-Noise Ratios

Both legitimate receiver Bob and eavesdropper Eve apply the MRC diversity method on the received signals over FSO and RF links, where subscript $x \in \{b, e\}$ denotes the receiving side, i.e., $x = b$ for Bob, and $x = e$ for Eve. Hence, the overall electrical SNR is in fact the sum of the

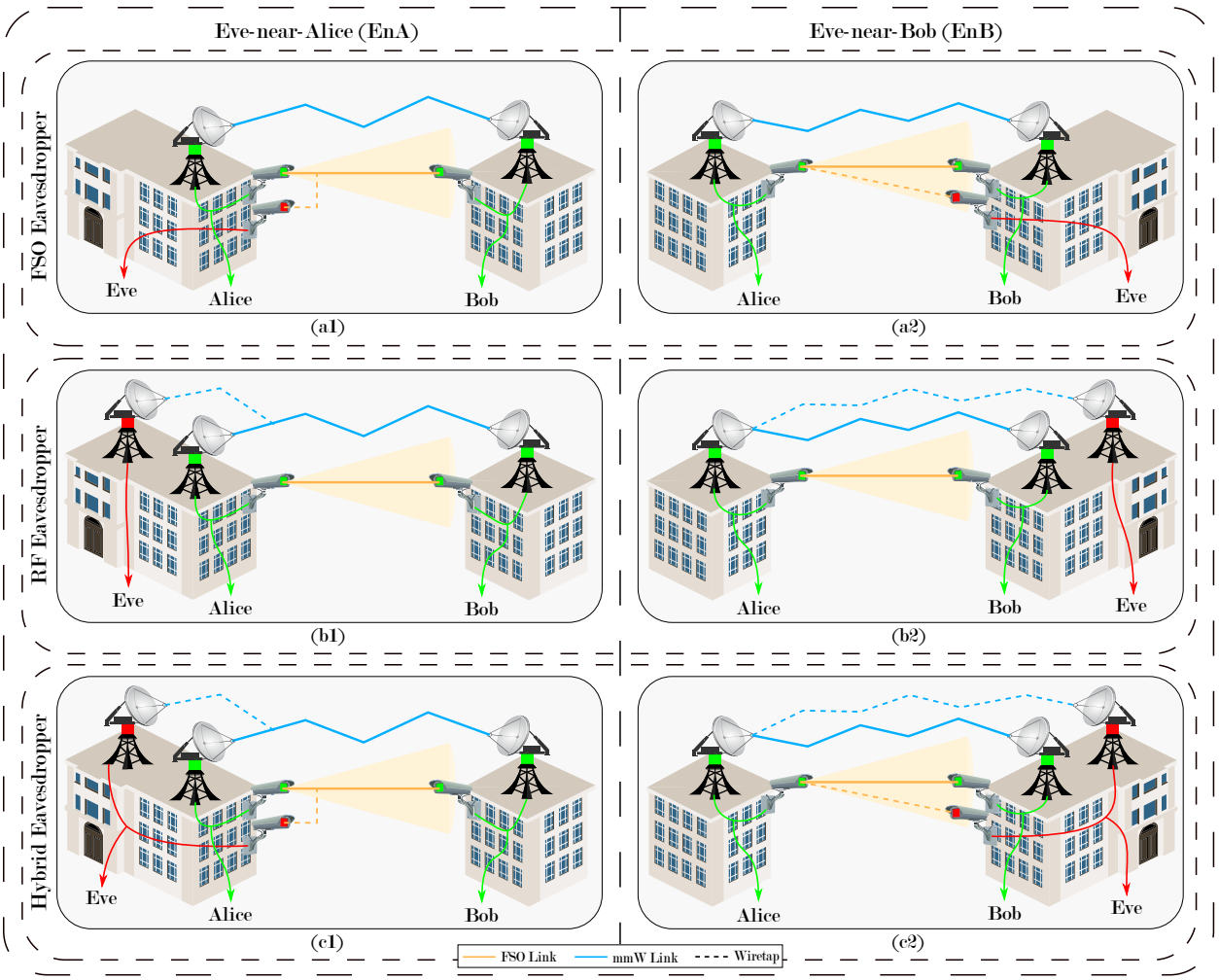


Figure 2.2: System model of hybrid FSO-*mm*Wave communications considering correlated channels, between the legitimate transmitter Alice and receiver Bob in the presence of different type eavesdroppers with different locations: (1) Eve-near-Alice (EnA), (2) Eve-near-Bob (EnB), (a) FSO-Eve, (b) RF-Eve, (c) Hybrid-Eve. Reprinted with permission from [43].

instantaneous electrical SNRs of both links for MRC receiver, and it is expressed as

$$\gamma_x = \gamma_{x,f} + \gamma_{x,o}, \tag{2.1}$$

where $\gamma_{x,o}$ and $\gamma_{x,f}$ denote the instantaneous electrical SNR of the RF and FSO links, respectively.

2.4 Secrecy Capacity Analysis

In this chapter, to characterize the secure communication between legitimate pairs Alice and Bob, the probabilistic metric of SPSC defined in (1.33) is used

$$\begin{aligned} P_S^+ &= 1 - \text{Prob.}\big(C_S < 0\big), \\ &= \text{Prob.}\big(C_b - C_e > 0\big). \end{aligned} \tag{2.2}$$

then by substituting (1.27) and (1.28), the expression in (2.2) is re-expressed as

$$P_S^+ = \text{Prob.}\left(B\log_2\frac{1+\gamma_b}{1+\gamma_e} > 0\right), \tag{2.3}$$

and it can be further simplified as

$$P_S^+ = \text{Prob.}\big(\gamma_f - \gamma_e > 0\big), \tag{2.4}$$

finally, by using (2.1), the probability of secure communication is expressed as

$$P_S^+ = \text{Prob.}\big((\gamma_{b,o} - \gamma_{e,o}) + (\gamma_{b,f} - \gamma_{e,f}) > 0\big). \tag{2.5}$$

In the following, the probability of SPSC, P_S^+, is derived for hybrid FSO-mmWave systems considering uncorrelated and correlated wiretap channels.

2.4.1 Non-Identical Independent Channels

In this subsection, *mm*Wave fading and FSO turbulence channels are modeled by non-identical independent Weibull and exponential RVs, where the PDFs are given in (1.1.1) and (1.2.1), respectively.

2.4.1.1 Considering FSO Eavesdropper

FSO-type Eve can be described as a sensing device that collects a fraction of the optical irradiance sent by Alice. It is worthy noting that the presence of Eve-FSO should not affect the received power at Bob. Actually, blocking the LOS between Alice and Bob or decreasing the amount of received power at Bob makes Bob aware of the attack and, therefore, can terminate the communication for security reasons. Therefore, we consider that Eve-FSO collects a fraction $R_{e,o}$ of the available power from the received laser beam whereas Bob receives a fraction $R_{b,o}$, where $R_{b,o} + R_{e,o} \leq 1$.

As Eve-FSO eavesdrops only on the FSO link, the electrical SNR at its end, $\gamma_{e,o}$, includes only contribution from the optical link, and can be expressed as

$$\gamma_{e,o} = \overline{\gamma}_{e,o} {I_e}^2, \tag{2.6}$$

where $\overline{\gamma}_{e,o}$ is given in (1.24)

$$\gamma_{e,o} = \left(\frac{\eta I_t R_{e,o} L_{e,o} I_e}{\sigma_e} \right)^2, \tag{2.7}$$

Further, letting $\gamma_b = \gamma_{b,o} + \gamma_{b,f}$, and using [81, (4)], the PDF of γ_b can be expressed as

$$f_{\gamma_b}(\gamma_b) = \sum_{l=0}^{\infty} \sum_{k=0}^{l} c_1 \gamma_b^{c_2 - 1} e^{-c_3 \gamma_b}, \tag{2.8}$$

where c_1, c_2, and c_3 are expressed as

$$\begin{aligned} c_1 &= (-1)^k \binom{l}{k} \Omega_l \frac{1}{\Gamma(c_2) \chi^{c_2}}, \\ c_2 &= k + 2, \\ c_3 &= 1/\chi, \end{aligned} \tag{2.9}$$

where χ and Ω_l are defined as

$$\chi = \Gamma\left(1+\frac{1}{\lambda}\right)\delta^{1/\lambda} + 2\beta^2, \tag{2.10}$$

$$\Omega_l = \sum_{k_f+k_o=l}\sum_{k=0}^{k_f}(-1)^k\frac{1}{\chi^k k!}\binom{k_f}{k}\Gamma\left(1+\frac{k}{\lambda}\right)\chi^{k/\lambda}\sum_{k=0}^{k_o}(-1)^k\frac{1}{\chi^k k!}\binom{k_o}{k}\Gamma(1+2k)\chi^{2k}, \tag{2.11}$$

since l and k are non-negative integers, $\binom{l}{k}$ can be re-written as $\Gamma(l+1)/\Gamma(k+1)\Gamma(l-k+1)$ to optimize the running time of program. k_f and k_o are the dummy variables that satisfy the condition of the summation over all possible non-negative integers for $k_f + k_o = l$.

Based on (1.13), the PDF expression of γ_e can be re-written as

$$f_{\gamma_e}(\gamma_e) = d_1\gamma_e^{-1/2}\exp\left[-d_2\gamma_e^{1/2}\right], \tag{2.12}$$

where $d_1 = 1/2\beta_e^2$, and $d_2 = 1/\beta_e^2$.

Accordingly, P_S^+ given in (2.4) can be calculated as

$$P_S^+ = \text{Prob.}\{\gamma_b > \gamma_e\} = \int_0^\infty\int_{\gamma_e}^\infty f_{\gamma_b}(\gamma_b)f_{\gamma_e}(\gamma_e)\cdot d\gamma_b d\gamma_e, \tag{2.13}$$

then, by substituting (2.8) into (2.13), the probability of SPSC is expressed as

$$P_S^+ = \int_0^\infty\sum_{l=0}^\infty\sum_{k=0}^l c_1\Bigg(\underbrace{\int_{\gamma_e}^\infty\gamma_b^{c_2-1}e^{-c_3\gamma_b}\cdot d\gamma_b}_{\mathcal{I}}\Bigg)f_{\gamma_e}(\gamma_e)\cdot d\gamma_e, \tag{2.14}$$

and the interior integral $\mathcal{I}$ can be solved as [82, (3.351-2)]

$$P_S^+ = \int_0^\infty\sum_{l=0}^\infty\sum_{k=0}^l c_1 c_3^{-c_2}\Gamma(c_2, c_3\gamma_e)f_{\gamma_e}(\gamma_e)\cdot d\gamma_e, \tag{2.15}$$

next, by substituting (2.12), the equation (2.15) is expressed as

$$P_S^+ = \sum_{l=0}^{\infty}\sum_{k=0}^{l} c_1 c_3^{-c_2} d_1 \int_0^{\infty} \gamma_e^{-1/2} e^{-d_2\gamma_e^{1/2}} \Gamma(c_2, c_3\gamma_e)\cdot d\gamma_e, \tag{2.16}$$

and the resultant integral can be solved as [83, (2.10.1-5.2)]

$$P_S^+ = \sum_{l=0}^{\infty}\sum_{k=0}^{l} c_1 c_3^{-c_2} d_1 \left[c_3^{-1/2} \left(\sum_{t=0}^{\infty} \frac{\Gamma(c_2+(t+1)/2)}{t!(t+1)/2} \left(-\frac{d_2}{c_3^{1/2}} \right)^t \right) + \frac{2\Gamma(c_2)}{d_2} \right]. \tag{2.17}$$

2.4.1.2 Considering RF Eavesdropper

RF-type Eve can be described as a sensing device that collects a fraction of the power radiated by Alice. It is worthy noting that the presence of Eve-RF should not affect the received power at Bob. Actually, jamming the link between Alice and Bob or decreasing the amount of received power at Bob makes Bob aware of the attack and, therefore, can stop the communication for security reasons. Therefore, we consider that Eve-RF collects a fraction P_e of the available power that is radiated by Alice whereas Bob receives a fraction R_b, where $R_b + R_e \leq 1$.

As RF-Eve eavesdrops only on the RF link, the electrical SNR at its end, $\gamma_{e,f}$, includes only contribution from the RF link, and can be expressed as

$$\gamma_{e,f} = \overline{\gamma}_{e,f} {H_e}^2, \tag{2.18}$$

where $\overline{\gamma}_{e,f}$ is given in (1.21)

$$\gamma_{e,f} = \frac{P_t R_{e,f} L_{e,f} H_e^2}{\sigma_e^2}, \tag{2.19}$$

By letting $\gamma_b = \gamma_{b,o} + \gamma_{b,f}$, the PDF expression of γ_b is expressed in (2.8). Furthermore, based on (1.4), the PDF expression of γ_e can be re-written as

$$f_{\gamma_e}(\gamma_e) = d_1 \gamma_e^{\frac{\lambda_e}{2}-1} \exp\left[-d_2\gamma_e^{\lambda_e/2}\right], \tag{2.20}$$

where $d_1 = \lambda_e/2\delta_e^2$, and $d_2 = 1/\delta_e^2$. Therefore, to obtain P_S^+ in the presence of an RF-type eavesdropper, the integral in (2.15) needs to be re-calculated by using (2.20)

$$P_S^+ = \sum_{l=0}^{\infty}\sum_{k=0}^{l} c_1 c_3^{-c_2} d_1 \int_0^{\infty} \gamma_e^{\frac{\lambda_e}{2}-1} e^{-d_2\gamma_e^{\frac{\lambda_e}{2}}} \Gamma(c_2, c_3\gamma_e)\cdot d\gamma_e, \tag{2.21}$$

and, the resultant integral can be solved as [83, (2.10.1-5.1)]

$$P_S^+ = \sum_{l=0}^{\infty}\sum_{k=0}^{l} c_1 c_3^{-c_2} d_1 \left[\frac{-c_3^{c_2}/2}{\lambda_e d_2^{(2c_2+\lambda_e)/\lambda_e}}\left(\sum_{t=0}^{\infty}\frac{1}{t!(t+c_2)}\Gamma\left(\frac{\lambda_e+2(c_2+t)}{\lambda_e}\right)\left(-\frac{c_3}{d_2^{2/\lambda_e}}\right)^t\right) + \frac{2\Gamma(c_2)}{d_2\lambda_e}\right]. \tag{2.22}$$

2.4.1.3 Considering Hybrid Eavesdropper

Hybrid-type Eve can be described as two sensing devices that collect fractions of the power radiated by Alice in the two links. Alternatively, Eve-Hybrid can be considered as two cooperative eavesdroppers, one Eve-RF and one Eve-FSO.

As hybrid-Eve eavesdrops on both FSO and RF links, the electrical SNR at its end, γ_e, includes contributions from the FSO and RF links, and can be expressed as

$$\gamma_e = \gamma_{e,o} + \gamma_{e,f}, \tag{2.23}$$

where $\gamma_{e,o}$ and $\gamma_{e,f}$ are given in (2.7) and (2.19), respectively.

Likewise, by letting $\gamma_b = \gamma_{b,o} + \gamma_{b,f}$, the PDF expression of γ_b is given in (2.8). Similarly, the PDF of γ_e is also given in (2.8) but with different parameters δ_e and β_e instead of δ_b and β_b, respectively. It is worth noting that the subscript e is used instead of b for all constant of the PDF of γ_e, and d_1, d_2 and d_3 are used instead of c_1, c_2 and c_3, respectively. Therefore, to obtain P_S^+ for hybrid-type eavesdropper, the integral in (2.15) needs to be re-calculated by using (2.8)

$$P_S^+ = \sum_{l=0}^{\infty}\sum_{k=0}^{l} c_1 c_3^{-c_2} d_1 \sum_{l_e=0}^{\infty}\sum_{k_e=0}^{l_e} d_1 \left(\int_0^{\infty} \gamma_e^{d_2-1} e^{-d_3\gamma_e}\Gamma(c_2, c_3\gamma_e)\cdot d\gamma_e\right), \tag{2.24}$$

and the resultant integral can be solved as [83, (2.10.3-2)]

$$P_S^+ = \sum_{l=0}^{\infty}\sum_{k=0}^{l} c_1 c_3^{-c_2} \sum_{l_e=0}^{\infty}\sum_{k_e=0}^{l_e} d_1 \left[\frac{-c_3^{c_2}\Gamma(d_2+c_2)}{c_2 d_3^{c_2+d_2}} {}_2F_1\left(c_2, c_2+d_2; c_2+1; -\frac{c_3}{d_3}\right) + \frac{\Gamma(c_2)\Gamma(d_2)}{d_3^{d_2}}\right]. \tag{2.25}$$

2.4.2 Non-Identical Dependent Channels

In this subsection, *mm*Wave fading and FSO turbulence channels are modeled by non-identical dependent Nakagami-m and Gamma-Gamma RVs, where the PDFs are given in (1.1.2) and (1.2.2), respectively.

2.4.3 Eve-near-Alice Scenarios

In this scenario, the eavesdropper Eve is assumed to locate very near to the legitimate transmitter Alice, $d_e \approx 0$, as shown with the left-column of Fig. 2.2. Accordingly, the intensity attenuation and power loss can be ignored, i.e., $L_{e,o} = L_{e,f} \approx 1$. Moreover, due to the very short distance d_e between Alice and Eve, the turbulence and fading can be ignored, i.e., $I_e = H_e \approx 1$. Consequently, the instantaneous electrical SNRs over FSO and *mm*Wave links at Eve can be assumed constants, and respectively, given as

$$\gamma_{e,o}^0 = \left(\frac{\eta I_t R_{e,o}}{\sigma_e}\right)^2, \tag{2.26}$$

$$\gamma_{e,f}^0 = \frac{P_t R_{e,f}}{\sigma_e^2}, \tag{2.27}$$

can be readily seen, the probability of secrecy given in (2.5) is now characterized by only $\gamma_{b,o}$ and $\gamma_{b,f}$ RVs. Therefore, if we let $\Delta = \gamma_{b,o} + \gamma_{b,f}$, the CDF of Δ can be calculated as

$$\begin{aligned} F_\Delta(\delta) &= \int_{-\infty}^{\infty}\int_{-\infty}^{\delta-\gamma_{b,f}} f_{\gamma_o}(\gamma_{b,o}) f_{\gamma_f}(\gamma_{b,f}) \cdot d\gamma_{b,o} d\gamma_{b,f}, \\ &= \int_0^{\infty} F_{\gamma_o}(\delta-\gamma_{b,f}) f_{\gamma_f}(\gamma_{b,f}) \cdot d\gamma_{b,f}, \end{aligned} \tag{2.28}$$

by substituting (1.7) and (1.19), the integral in (2.28) is re-written as

$$F_{\Delta}(\delta) = \frac{1}{\Gamma(\alpha)\Gamma(\beta)} \frac{m^m}{\Gamma(m)\overline{\gamma}_{b,f}^m} \int_0^{\infty} \gamma_{b,f}^{m-1} e^{-\frac{m}{\overline{\gamma}_{b,f}}\gamma_{b,f}} G_{1,3}^{2,1}\left(\frac{\alpha\beta}{\sqrt{\overline{\gamma}_{b,o}}} \sqrt{\delta - \gamma_{b,f}} \middle| \begin{matrix} 1 \\ \alpha, \beta, 0 \end{matrix} \right) \cdot d\gamma_{b,f}, \tag{2.29}$$

by applying a change of variable $u = \delta - \gamma_{b,f}$, the integral can be re-written as

$$F_{\Delta}(\delta) = -\frac{1}{\Gamma(\alpha)\Gamma(\beta)} \frac{m^m}{\Gamma(m)\overline{\gamma}_{b,f}^m} e^{-\frac{m}{\overline{\gamma}_{b,f}}\delta} \int_0^{\infty} (\delta - u)^{m-1} e^{\frac{m}{\overline{\gamma}_{b,f}}u} G_{1,3}^{2,1}\left(\frac{\alpha\beta}{\sqrt{\overline{\gamma}_{b,o}}} \sqrt{u} \middle| \begin{matrix} 1 \\ \alpha, \beta, 0 \end{matrix} \right) \cdot du, \tag{2.30}$$

where the polynomial term can be re-expressed by the use of binomial theorem

$$(\delta - u)^{m-1} = \sum_{\ell=0}^{m-1} \binom{m-1}{\ell} \delta^{m-\ell-1} (-u)^{\ell}, \tag{2.31}$$

accordingly, the integral can be re-written as

$$\begin{aligned} F_{\Delta}(\delta) = -\frac{1}{\Gamma(\alpha)\Gamma(\beta)} \frac{m^m}{\Gamma(m)\overline{\gamma}_{b,f}^m} e^{-\frac{m}{\overline{\gamma}_{b,f}}\delta} \sum_{\ell=0}^{m-1} \binom{m-1}{\ell} (-1)^{\ell} \delta^{m-\ell-1} \\ \times \int_0^{\infty} u^{\ell} e^{\frac{m}{\overline{\gamma}_{b,f}}u} G_{1,3}^{2,1}\left(\frac{\alpha\beta}{\sqrt{\overline{\gamma}_{b,o}}} \sqrt{u} \middle| \begin{matrix} 1 \\ \alpha, \beta, 0 \end{matrix} \right) \cdot du, \end{aligned} \tag{2.32}$$

and by using [83, (2.24.3-1)], the resultant integral is solved as

$$\begin{aligned} F_{\Delta}(\delta) = -\frac{1}{\Gamma(\alpha)\Gamma(\beta)} \frac{m^m}{\Gamma(m)\overline{\gamma}_{b,f}^m} e^{-\frac{m}{\overline{\gamma}_{b,f}}\delta} \sum_{\ell=0}^{m-1} \binom{m-1}{\ell} (-1)^{\ell} \delta^{m-\ell-1} \frac{2^{\alpha+\beta-1}}{2\pi} \left(-\frac{m}{\overline{\gamma}_{b,f}} \right)^{-(\ell+1)} \\ \times G_{3,6}^{4,3}\left(-\frac{\overline{\gamma}_{b,f}}{\overline{\gamma}_{b,o}} \frac{\alpha^2\beta^2}{16m} \middle| \begin{matrix} -\ell, \frac{1}{2}, 1 \\ \frac{\alpha}{2}, \frac{\alpha+1}{2}, \frac{\beta}{2}, \frac{\beta+1}{2}, 0, \frac{1}{2} \end{matrix} \right). \end{aligned} \tag{2.33}$$

2.4.3.1 FSO Eavesdropper

FSO-type of eavesdropper is described in section 2.4.1.1, where Eve-FSO collects a fraction $R_{e,o}$ of the available power from the received laser beam whereas Bob receives a fraction $R_{b,o}$, where $R_{b,o} + R_{e,o} \leq 1$. Accordingly, the probability of secrecy is calculated by considering only the instantaneous electrical SNR over FSO link at Eve

$$P_S^+ = 1 - F_\Delta(\gamma_{e,o}^0), \tag{2.34}$$

$$= 1 - F_\Delta\left(\left(\frac{\eta I_t R_{e,o} L_{e,o}}{\sigma_e}\right)^2\right). \tag{2.35}$$

2.4.3.2 RF Eavesdropper

RF-type of eavesdropper is described in section 2.4.1.2, where Eve-RF collects a fraction $R_{e,f}$ of the available power that is radiated by Alice whereas Bob receives a fraction $R_{b,f}$, where $R_{b,f} + R_{e,f} \leq 1$. Accordingly, the probability of secrecy is calculated by considering only the instantaneous electrical SNR over RF link at Eve

$$P_S^+ = 1 - F_\Delta(\gamma_{e,f}^0), \tag{2.36}$$

$$= 1 - F_\Delta\left(\frac{P_t R_{e,f} L_{e,f}}{\sigma_e^2}\right). \tag{2.37}$$

2.4.3.3 Hybrid FSO-RF Eavesdropper

As previously mentioned in section 2.4.1.3, Hybrid-type Eve can be considered as two sensing devices that collect fractions of the power radiated by Alice over both links. In another word, Eve-Hybrid can be considered as two cooperative eavesdroppers, i.e one for RF and other one for FSO. It is worthy noting that the presence of Eve should not affect the received power at Bob. Actually, blocking the LOS or jamming the link between Alice and Bob, or decreasing the amount of received power at Bob makes the legitimate pair aware of the attack and, therefore, can terminate the communication for security reasons. Consequently, we consider an Eve that collects

the fractions $R_{e,o}$ and $R_{e,f}$ of the available power from the received laser beam and the radiated by antenna, respectively, whereas Bob receives the fractions $R_{b,o}$ and $R_{b,f}$, where $R_{b,o} + R_{e,o} \leq 1$ and $R_{b,f} + R_{e,f} \leq 1$. We also consider that Bob and Eve equip the same photodetectors and antennas to provide the identical diameter of aperture, conversion efficiency, and antenna gain. Accordingly, the probability of secrecy is calculated by considering both instantaneous electrical SNRs over FSO link at Eve

$$P_S^+ = 1 - F_\Delta(\gamma_{e,o}^0 + \gamma_{e,f}^0), \tag{2.38}$$

$$= 1 - F_\Delta\left(\left(\frac{\eta I_t R_{e,o} L_{e,o}}{\sigma_e}\right)^2 + \frac{P_t R_{e,f} L_{e,f}}{\sigma_e^2}\right). \tag{2.39}$$

2.4.4 Eve-near-Bob Scenarios

In this scenario, the eavesdropper Eve is assumed to locate very close to the legitimate receiver Bob, $d_b \approx d_e$, as shown with the right-column of Fig. 2.2. Due to the fact that this very close location of Eve with respect to Bob, the correlation needs to be introduced into both FSO and RF channels between the main and wiretap parties.

For the FSO links, the large-scale eddies can be assumed to be similar, considering the received signals are to be affected by the same effects [84]. On the other hand, as discussed in [85], the small-scale eddies are considered to be correlated and identically distributed due to the relatively close location of Eve with respect to Bob. Since we only consider the small-scale eddies [86], the FSO links can be modeled with one Gamma random variable [84]. By using the change of variable, we can state the instantaneous SNRs received at Bob and Eve as $\Psi_b = \sqrt{\overline{\gamma}_{b,o}} I_{b,s}$ and $\Psi_e = \sqrt{\overline{\gamma}_{e,o}} I_{e,s}$, respectively, where $I_{.,s}$ denotes the small-scale eddies of the FSO link. Notice that we now have two Gamma RVs denoted by $\Psi_b \sim \mathsf{Gam.}(\beta, \beta/\sqrt{\overline{\gamma}_{b,o}})$ and $\Psi_e \sim \mathsf{Gam.}(\beta, \beta/\sqrt{\overline{\gamma}_{e,o}})$. Then, the joint PDF of $\Psi = \Psi_b - \Psi_e$ can be expressed with the aid of McKay distribution [87,

(22a)], as follows

$$f_{\Psi}(\psi) = C_o|\psi|^{a_o-1}\exp[-b_o\psi]K_{a_o-1}(c_o|\psi|), \tag{2.40}$$

where $\psi \neq 0$, and coefficients C_0, a_o, b_o and c_o are expressed as

$$C_o = \frac{((\beta_1+\beta_2)^2 - 4\beta_1\beta_2\rho_o)^{-(2\beta-1)/4}}{\Gamma(\beta)\sqrt{\pi\beta_1\beta_2(1-\rho_o)}}, \tag{2.41}$$

$$a_o = \beta + 1/2, \tag{2.42}$$

$$b_o = (\beta_2 - \beta_1)/(2\beta_1\beta_2(1-\rho_o)), \tag{2.43}$$

$$c_o = \sqrt{(\beta_1+\beta_2)^2 - 4\beta_1\beta_2\rho_o}/(2\beta_1\beta_2(1-\rho_o)), \tag{2.44}$$

where $\beta_1 = \sqrt{\overline{\gamma}_{b,o}}/\beta$, $\beta_2 = \sqrt{\overline{\gamma}_{e,o}}/\beta$, and ρ_o stands for the correlation coefficient between main (from Alice to Bob) and wiretap (from Alice to Eve) FSO channels.

Similarly, for the *mm*Wave links, by applying the change of variable, we can express the instantaneous SNRs received at Bob and Eve as $\Omega_b = \overline{\gamma}_{b,f}H_b^2$ and $\Omega_e = \overline{\gamma}_{e,f}H_e^2$, respectively. It is worthy to recall that the *mm*Wave links are modeled by the RVs H_b and H_e that have Nakagami-m distribution, as given in (1.6), and it is well-known that the square envelopes of Nakagami-m distributed channels, H_b^2 and H_e^2, follow a Gamma distribution. Therefore, we have two Gamma RVs denoted as $\Omega_b \sim \mathsf{Gam.}(m, \overline{\gamma}_{b,f}/m)$ and $\Omega_e \sim \mathsf{Gam.}(m, \overline{\gamma}_{e,f}/m)$. Then, the joint CDF of $\Omega = \Omega_b - \Omega_e$ can be also expressed as [87, (22a)]

$$f_{\Omega}(\omega) = C_f|\omega|^{a_f-1}\exp[-b_f\omega]K_{a_f-1}(c_f|\omega|), \tag{2.45}$$

where $\omega \neq 0$, and coefficients C_f, a_f, b_f and c_f are expressed as

$$C_f = \frac{((\theta_1+\theta_2)^2 - 4\theta_1\theta_2\rho_f)^{-(2\theta-1)/4}}{\Gamma(\theta)\sqrt{\pi\theta_1\theta_2(1-\rho_f)}}, \tag{2.46}$$

$$a_f = \theta + 1/2, \tag{2.47}$$

$$b_f = (\theta_2 - \theta_1)/(2\theta_1\theta_2(1-\rho_f)), \tag{2.48}$$

$$c_f = \sqrt{(\theta_1+\theta_2)^2 - 4\theta_1\theta_2\rho_f}/(2\theta_1\theta_2(1-\rho_f)), \tag{2.49}$$

where $\theta_1 = \overline{\gamma}_{b,f}/m$, $\theta_2 = \overline{\gamma}_{e,f}/m$, and ρ_f stands for the correlation coefficient between main (from Alice to Bob) and wiretap (from Alice to Eve) RF channels.

2.4.4.1 FSO Eavesdropper

This subsection defines the FSO eavesdropper case, in which wiretapping only happens on the FSO link. In other words, since FSO-Eve is equipped with a single photodetector, there is no contribution of $\gamma_{e,f}$, and therefore, the probability of SPSC given in (2.5) is expressed as

$$P_S^+ = \text{Prob.}\big((\Psi_b - \Psi_e) + \gamma_{b,f} > 0\big), \tag{2.50}$$

where Ψ_b and Ψ_e, as explained in the second paragraph of Subsection 2.4.4, denote the instantaneous electrical SNRs of FSO links at Bob and Eve, respectively. Then, by letting $\Xi = \Psi + \gamma_{b,f}$, where $\Psi = \Psi_b - \Psi_e$, the CDF of Ξ can be calculated as

$$\begin{aligned} F_\Xi^{\text{FSO}}(\xi) &= \int_{-\infty}^{\infty}\int_{-\infty}^{\xi-\psi} f_{\gamma_f}(\gamma_{b,f}) f_\Psi(\psi)\cdot d\gamma_{b,f} d\psi, \\ &= \int_{-\infty}^{\infty} F_{\gamma_f}(\xi-\psi) f_\Psi(\psi)\cdot d\psi, \end{aligned} \tag{2.51}$$

by substituting (1.9) and (2.40), the integral in (2.51) is re-written as

$$F_{\Xi}^{\text{FSO}}(\xi) = C_o \int_{-\infty}^{\infty} \left[1 - \sum_{k=0}^{\infty} \frac{1}{k!} \left(\frac{m}{\overline{\gamma}_{b,f}} \right)^k (\xi - \psi)^k e^{-\frac{m}{\overline{\gamma}_{b,f}}(\xi - \psi)} \right] |\psi|^{a_o - 1} e^{-b_o \psi} K_{a_o - 1}(c_o |\psi|) \cdot d\psi, \tag{2.52}$$

the integral can be broken into two parts due to the absolute operator

$$\begin{aligned} F_{\Xi}^{\text{FSO}}(\xi) = C_o \int_{-\infty}^{0} \left[1 - \sum_{k=0}^{\infty} \frac{1}{k!} \left(\frac{m}{\overline{\gamma}_{b,f}} \right)^k (\xi - \psi)^k e^{-\frac{m}{\overline{\gamma}_{b,f}}(\xi - \psi)} \right] (-\psi)^{a_o - 1} e^{-b_o \psi} K_{a_o - 1}(-c_o \psi) \cdot d\psi \\ + C_o \int_{0}^{\infty} \left[1 - \sum_{k=0}^{\infty} \frac{1}{k!} \left(\frac{m}{\overline{\gamma}_{b,f}} \right)^k (\xi - \psi)^k e^{-\frac{m}{\overline{\gamma}_{b,f}}(\xi - \psi)} \right] \psi^{a_o - 1} e^{-b_o \psi} K_{a_o - 1}(c_o \psi) \cdot d\psi, \end{aligned} \tag{2.53}$$

for $\xi = 0$, by using [82, 6.621-3], the integrals can be solved as

$$\begin{aligned} F_{\Xi}^{\text{FSO}} = C_o \sqrt{\pi} (2c_o)^{a_o - 1} \Bigg[& \frac{\Gamma(2a_o - 1)}{\Gamma(a_o + 1/2)} \\ & \times \left(\frac{1}{(c_o - b_o)^{2a_o - 1}} {}_2F_1\left(2a_o - 1, a_o - \frac{1}{2}; a_o + \frac{1}{2}; \frac{-b_o - c_o}{-b_o + c_o} \right) \right. \\ & \left. + \frac{1}{(c_o + b_o)^{2a_o - 1}} {}_2F_1\left(2a_o - 1, a_o - \frac{1}{2}; a_o + \frac{1}{2}; \frac{b_o - c_o}{b_o + c_o} \right) \right) \\ & - \sum_{k=0}^{\infty} \frac{1}{k!} \left(\frac{m}{\overline{\gamma}_{b,f}} \right)^k \frac{\Gamma(2a_o + k - 1)\Gamma(k + 1)}{\Gamma(a_o + k + 1/2)} \\ & \times \left(\frac{1}{(c_o - b_o + \frac{m}{\overline{\gamma}_{b,f}})^{2a_o + k - 1}} {}_2F_1\left(2a_o + k - 1, a_o - \frac{1}{2}; a_o + k + \frac{1}{2}; \frac{m - \overline{\gamma}_{b,f}(b_o + c_o)}{m - \overline{\gamma}_{b,f}(b_o - c_o)} \right) \right. \\ & \left. \left. - \frac{1}{(c_o + b_o - \frac{m}{\overline{\gamma}_{b,f}})^{2a_o + k - 1}} {}_2F_1\left(2a_o + k - 1, a_o - \frac{1}{2}; a_o + k + \frac{1}{2}; \frac{\overline{\gamma}_{b,f} - m(b_o - c_o)}{\overline{\gamma}_{b,f} - m(b_o + c_o)} \right) \right) \right]. \end{aligned} \tag{2.54}$$

Accordingly, the probability of secure communication for EnB scenario in presence of FSO-Eve is calculated by using (2.54) as follows

$$P_S^+ = 1 - F_{\Xi}^{\text{FSO}}. \tag{2.55}$$

2.4.4.2 RF Eavesdropper

In a like manner, this subsection defines the RF eavesdropper case, in which wiretapping only happens on the RF link. Correspondingly, since RF-Eve is equipped with a receiving antenna, there is no contribution of $\gamma_{e,o}$, and therefore, the probability of SPSC given in (2.5) is expressed as

$$P_S^+ = \text{Prob.}\big(\gamma_{b,o} + (\Omega_b - \Omega_e) > 0\big), \tag{2.56}$$

where Ω_b and Ω_e, as explained in the third paragraph of Subsection 2.4.4, depict the instantaneous electrical SNRs of RF links at Bob and Eve, respectively. Then, by applying the change of variable as $\Xi = \gamma_{b,o} + \Omega$, where $\Omega = \Omega_b - \Omega_e$, the CDF of Ξ can be calculated as

$$\begin{aligned} F_{\Xi}^{\text{RF}}(\xi) &= \int_{-\infty}^{\infty} \int_{-\infty}^{\xi-\omega} f_{\gamma_o}(\gamma_{b,o}) f_{\Omega}(\omega) \cdot d\gamma_{b,o} d\omega, \\ &= \int_{-\infty}^{\infty} F_{\gamma_o}(\xi - \omega) f_{\Omega}(\omega) \cdot d\omega, \end{aligned} \tag{2.57}$$

by substituting (1.19) and (2.45), the integral in (2.57) is re-written as

$$F_{\Xi}^{\text{RF}}(\xi) = \frac{C_f}{\Gamma(\alpha)\Gamma(\beta)} \int_{-\infty}^{\infty} |\omega|^{a_f - 1} e^{-b_f \omega} K_{a_f - 1}(c_f|\omega|) G_{1,3}^{2,1}\left(\frac{\alpha\beta}{\sqrt{\bar{\gamma}_{b,o}}} \sqrt{(\xi - \omega)} \middle| \begin{matrix} 1 \\ \alpha, \beta, 0 \end{matrix} \right) \cdot d\omega, \tag{2.58}$$

by considering $\xi = 0$, the integral can be re-written as

$$F_{\Xi}^{\text{RF}} = \frac{C_f}{\Gamma(\alpha)\Gamma(\beta)} \Bigg[\int_{-\infty}^{0} (-\omega)^{a_f-1} e^{-b_f\omega} K_{a_f-1}(-c_f\omega) G_{1,3}^{2,1}\left(\frac{\alpha\beta}{\overline{\gamma}_{b,o}}(-\omega) \middle| \begin{matrix} 1 \\ \alpha, \beta, 0 \end{matrix} \right) \cdot d\omega + \int_{0}^{\infty} \omega^{a_f-1} e^{-b_f\omega} K_{a_f-1}(c_f\omega) G_{1,3}^{2,1}\left(\frac{\alpha\beta}{\overline{\gamma}_{b,o}}(-\omega) \middle| \begin{matrix} 1 \\ \alpha, \beta, 0 \end{matrix} \right) \cdot d\omega \Bigg], \tag{2.59}$$

and it can be re-written as

$$F_{\Xi}^{\text{RF}} = \frac{C_f}{\Gamma(\alpha)\Gamma(\beta)} \Bigg[\int_{0}^{\infty} \omega^{a_f-1} e^{b_f\omega} K_{a_f-1}(c_f\omega) G_{1,3}^{2,1}\left(\frac{\alpha\beta}{\overline{\gamma}_{b,o}}\omega \middle| \begin{matrix} 1 \\ \alpha, \beta, 0 \end{matrix} \right) \cdot d\omega + \int_{0}^{\infty} \omega^{a_f-1} e^{-b_f\omega} K_{a_f-1}(c_f\omega) G_{1,3}^{2,1}\left(-\frac{\alpha\beta}{\overline{\gamma}_{b,o}}\omega \middle| \begin{matrix} 1 \\ \alpha, \beta, 0 \end{matrix} \right) \cdot d\omega \Bigg], \tag{2.60}$$

where exponential function can be expressed in terms of power series expansion

$$e^{\pm b_f\omega} = \sum_{\ell=0}^{\infty} \frac{1}{\ell!} (\pm b_f)^{\ell} \omega^{\ell}, \tag{2.61}$$

then, the integral can be re-written as

$$F_{\Xi}^{\text{RF}} = \frac{C_f}{\Gamma(\alpha)\Gamma(\beta)} \Bigg[\sum_{\ell=0}^{\infty} \frac{1}{\ell!} b_f^{\ell} \int_{0}^{\infty} \omega^{a_f+\ell-1} K_{a_f-1}(c_f\omega) G_{1,3}^{2,1}\left(\frac{\alpha\beta}{\overline{\gamma}_{b,o}}\omega \middle| \begin{matrix} 1 \\ \alpha, \beta, 0 \end{matrix} \right) \cdot d\omega + \sum_{\ell=0}^{\infty} \frac{1}{\ell!} (-b_f)^{\ell} \int_{0}^{\infty} \omega^{a_f+\ell-1} K_{a_f-1}(c_f\omega) G_{1,3}^{2,1}\left(-\frac{\alpha\beta}{\overline{\gamma}_{b,o}}\omega \middle| \begin{matrix} 1 \\ \alpha, \beta, 0 \end{matrix} \right) \cdot d\omega \Bigg], \tag{2.62}$$

by using [83, (2.24.4-3)], the resultant integral can be solved as

$$F_{\Xi}^{\text{RF}} = \frac{C_f 2^{a_f+\alpha+\beta-4}}{\pi\Gamma(\alpha)\Gamma(\beta)}\Bigg[\sum_{\ell=0}^{\infty}\frac{1}{\ell!}\frac{b_f^{\ell}2^{\ell}}{c_f^{a_f+\ell}}\Bigg(G_{4,6}^{4,4}\Bigg(\frac{\alpha^2\beta^2}{2\overline{\gamma}_{b,o}^2}c_f^2\Bigg|\begin{matrix}(3-2a_f-\ell)/2,(1-\ell)/2,1/2,1\\ \alpha/2,\alpha,\beta,\beta/2,0,1/2\end{matrix}\Bigg) \\ +(-1)^{\ell}G_{4,6}^{4,4}\Bigg(-\frac{\alpha^2\beta^2}{2\overline{\gamma}_{b,o}^2}c_f^2\Bigg|\begin{matrix}(3-2a_f-\ell)/2,(1-\ell)/2,1/2,1\\ \alpha/2,\alpha,\beta,\beta/2,0,1/2\end{matrix}\Bigg)\Bigg)\Bigg]. \tag{2.63}$$

Consequently, the probability of secure communication for EnB scenario in presence of RF-Eve is calculated by using (2.63) as follows

$$P_S^{+} = 1 - F_{\Xi}^{\text{RF}}. \tag{2.64}$$

2.4.4.3 Hybrid Eavesdropper

Since Hybrid-Eve is equipped with a single photodetector and single receiving antenna, the probability of SPSC is expressed as given in (2.5). Afterward, using the notation adopted in subsections 2.4.4.1 and 2.4.4.2, which is $\Xi = \Psi + \Omega$, where $\Psi = \Psi_b - \Psi_e$ and $\Omega = \Omega_b - \Omega_e$, the CDF of Ξ can be calculated as

$$F_{\Xi}^{\text{HYB}}(\xi) = \int_{-\infty}^{\infty}\int_{-\infty}^{\xi-\omega} f_{\Psi}(\psi)f_{\Omega}(\omega)\cdot d\psi d\omega, \tag{2.65}$$

by substituting (2.40) into (2.65), the integral can be written as

$$F_{\Xi}^{\text{HYB}}(\xi) = C_o\int_{-\infty}^{\infty}\Bigg(\underbrace{\int_{0}^{\xi-\omega}\psi^{a_o-1}e^{-b_o\psi}K_{a_o-1}(c_o\psi)\cdot d\psi}_{\mathcal{I}} \\ +\int_{-\infty}^{0}\psi^{a_o-1}e^{-b_o\psi}K_{a_o-1}(c_o\psi)\cdot d\psi\Bigg)f_{\Omega}(\omega)\cdot d\omega, \tag{2.66}$$

for $\xi = 0$, the integral $\mathcal{I}$ can be written as

$$\begin{aligned}\mathcal{I} &= \int_0^{-\omega} \psi^{a_o-1} e^{-b_o\psi} K_{a_o-1}(c_o\psi) \cdot d\psi \\ &= \sum_{\ell=0}^{\infty} \frac{1}{\ell!}(-b_f)^{\ell} \int_0^{-\omega} \psi^{a_o+\ell-1} K_{a_o-1}(c_o\psi) \cdot d\psi \end{aligned} \tag{2.67}$$

by changing the integral boundaries from 0 to 1, where $x = -\psi/\omega$ and $\psi = -x\omega$

$$\begin{aligned}\mathcal{I} =& \sum_{\ell=0}^{\infty} \frac{1}{\ell!}(-b_f)^{\ell} \int_0^{-\omega} \psi^{a_o+\ell-1} K_{a_o-1}(c_o\psi) \cdot d\psi \\ =& \sum_{\ell=0}^{\infty} \frac{1}{\ell!}(-b_f)^{\ell}(-\omega)^{a_o+\ell} \int_0^{1} x^{a_o+\ell-1} K_{a_o-1}(-\omega c_o x) \cdot dx \end{aligned} \tag{2.68}$$

then by using [82, (6.592-2)], the integral is solved as

$$\begin{aligned}\mathcal{I} &= \sum_{\ell=0}^{\infty} \frac{1}{\ell!}(-b_f)^{\ell}(-\omega)^{a_o+\ell} \frac{2^{a_o-3}}{(-\omega c_o)^{a_o-1}} G_{1,3}^{2,1}\left(\frac{\omega^2 c_o^2}{4} \middle| \begin{matrix} (1-\ell)/2 \\ a_o-1, 0, -(\ell+1)/2 \end{matrix} \right) \\ &= \frac{2^{a_o-3}}{(c_o)^{a_o-1}} \sum_{\ell=0}^{\infty} \frac{1}{\ell!}(-b_f)^{\ell}(-\omega)^{\ell+1} G_{1,3}^{2,1}\left(\frac{\omega^2 c_o^2}{4} \middle| \begin{matrix} (1-\ell)/2 \\ a_o-1, 0, -(\ell+1)/2 \end{matrix} \right) \end{aligned} \tag{2.69}$$

by substituting (2.69), (2.66) can be written as

$$\begin{aligned} F_{\Xi}^{\text{HYB}} = C_o \int_{-\infty}^{\infty} \Bigg(& \frac{2^{a_o-3}}{(c_o)^{a_o-1}} \sum_{\ell=0}^{\infty} \frac{1}{\ell!}(-b_f)^{\ell}(-\omega)^{\ell+1} G_{1,3}^{2,1}\left(\frac{\omega^2 c_o^2}{4} \middle| \begin{matrix} (1-\ell)/2 \\ a_o-1, 0, -(\ell+1)/2 \end{matrix} \right) \\ & + (-1)^{a_o-1} \frac{\sqrt{\pi}(-2c_o)^{a_o-1}}{(-b_o-c_o)^{2a_o-1}} \frac{\Gamma(2a_o-1)}{\Gamma(a_o+1/2)} \\ & \times {}_2F_1\left(2a_o-1, a_o-1/2; a_o+1/2; \frac{-b_o+c_o}{-b_o-c_o}\right) \Bigg) f_{\Omega}(\omega) \cdot d\omega, \end{aligned} \tag{2.70}$$

then, by substituting (2.45), (2.70) can be written as

$$
\begin{aligned}
F_{\Xi}^{\mathrm{HYB}} &= C_o C_f \frac{2^{a_o-3}}{(c_o)^{a_o-1}} \sum_{\ell=0}^{\infty} \frac{1}{\ell!}(-b_f)^{\ell} \\
&\quad \times \int_{-\infty}^{\infty} (-\omega)^{\ell+1} G_{1,3}^{2,1}\left(\frac{\omega^2 c_o^2}{4} \middle| \begin{matrix} (1-\ell)/2 \\ a_o - 1, 0, -(\ell+1)/2 \end{matrix} \right) |\omega|^{a_f-1} \exp[-b_f\omega] K_{a_f-1}(c_f|\omega|) \cdot d\omega \\
&\quad + C_o C_f (-1)^{a_o-1} \frac{\sqrt{\pi}(-2c_o)^{a_o-1}}{(-b_o-c_o)^{2a_o-1}} \frac{\Gamma(2a_o-1)}{\Gamma(a_o+1/2)} {}_2F_1\left(2a_o-1, a_o-1/2; a_o+1/2; \frac{-b_o+c_o}{-b_o-c_o} \right) \\
&\quad \times \int_{-\infty}^{\infty} |\omega|^{a_f-1} \exp[-b_f\omega] K_{a_f-1}(c_f|\omega|) \cdot d\omega, \qquad (2.71)
\end{aligned}
$$

the integral can be re-written as

$$
\begin{aligned}
F_{\Xi}^{\mathrm{HYB}} &= C_o C_f \frac{2^{a_o-3}}{(c_o)^{a_o-1}} \sum_{\ell=0}^{\infty} \frac{1}{\ell!}(-b_f)^{\ell} \\
&\quad \times \left[(-1)^{\ell+1} \int_0^{\infty} \omega^{\ell+a_f} G_{1,3}^{2,1}\left(\frac{\omega^2 c_o^2}{4} \middle| \begin{matrix} (1-\ell)/2 \\ a_o - 1, 0, -(\ell+1)/2 \end{matrix} \right) \exp[b_f\omega] K_{a_f-1}(c_f\omega) \cdot d\omega \right. \\
&\quad \left. + (-1)^{\ell+1} \int_0^{\infty} \omega^{\ell+a_f} G_{1,3}^{2,1}\left(\frac{\omega^2 c_o^2}{4} \middle| \begin{matrix} (1-\ell)/2 \\ a_o - 1, 0, -(\ell+1)/2 \end{matrix} \right) \exp[-b_f\omega] K_{a_f-1}(c_f\omega) \cdot d\omega \right] \\
&\quad + C_o C_f (-1)^{a_o-1} \frac{\sqrt{\pi}(-2c_o)^{a_o-1}}{(-b_o-c_o)^{2a_o-1}} \frac{\Gamma(2a_o-1)}{\Gamma(a_o+1/2)} {}_2F_1\left(2a_o-1, a_o-1/2; a_o+1/2; \frac{-b_o+c_o}{-b_o-c_o} \right) \\
&\quad \times \left[\int_0^{\infty} \omega^{a_f-1} \exp[-b_f\omega] K_{a_f-1}(c_f\omega) \cdot d\omega + \int_0^{\infty} \omega^{a_f-1} \exp[b_f\omega] K_{a_f-1}(c_f\omega) \cdot d\omega \right], \qquad (2.72)
\end{aligned}
$$

by using [82, (6.592-2)], last two integrals are solved as in (2.73),

$$F_{\Xi}^{\text{HYB}} = C_o C_f \frac{2^{a_o-3}}{(c_o)^{a_o-1}} \sum_{\ell=0}^{\infty} \frac{1}{\ell!}(-b_f)^{\ell}(-1)^{\ell+1} \Bigg[\int_0^{\infty} \omega^{\ell+a_f} G_{1,3}^{2,1}\left(\frac{\omega^2 c_o^2}{4} \middle| {}^{(1-\ell)/2}_{a_o-1,0,-(\ell+1)/2} \right)$$
$$\times e^{b_f \omega} K_{a_f-1}(c_f\omega)\cdot d\omega + \int_0^{\infty} \omega^{\ell+a_f} G_{1,3}^{2,1}\left(\frac{\omega^2 c_o^2}{4} \middle| {}^{(1-\ell)/2}_{a_o-1,0,-(\ell+1)/2} \right) e^{-b_f \omega} K_{a_f-1}(c_f\omega)\cdot d\omega \Bigg]$$
$$+ C_o C_f (-1)^{a_o-1} \frac{\sqrt{\pi}(-2c_o)^{a_o-1}}{(-b_o-c_o)^{2a_o-1}} \frac{\Gamma(2a_o-1)}{\Gamma(a_o+1/2)} {}_2F_1\left(2a_o-1, a_o-1/2; a_o+1/2; \frac{-b_o+c_o}{-b_o-c_o} \right)$$
$$\times \Bigg[\sqrt{\pi} 2 c_f^{a_f-1} \frac{\Gamma(2a_f-1)}{\Gamma(a_f+1/2)} \Bigg(\frac{1}{(b_f+c_f)^{2a_f-1}} {}_2F_1\left(2a_f-1, a_f-1/2; a_f+1/2; \frac{b_f-c_f}{b_f+c_f} \right)$$
$$+ \frac{1}{(-b_f+c_f)^{2a_f-1}} {}_2F_1\left(2a_f-1, a_f-1/2; a_f+1/2; \frac{-b_f-c_f}{-b_f+c_f} \right) \Bigg) \Bigg], \tag{2.73}$$

where exponential and Bessel functions can be expressed in terms of power series expansion and Meijer-G function, respectively, as in (2.74).

$$F_{\Xi}^{\text{HYB}} = C_o C_f \frac{2^{a_o-4}}{(c_o)^{a_o-1}} \sum_{\ell=0}^{\infty} \frac{1}{\ell!}(-b_f)^{\ell}(-1)^{\ell+1} \Bigg[\sum_{k=0}^{\infty} \frac{1}{k!} b_f^k \int_0^{\infty} \omega^{\ell+a_f+k} G_{0,2}^{2,0}\left(\frac{\omega^2 c_f^2}{4} \middle| {}_{(a_f-1)/2,(a_f-1)/2} \right)$$
$$\times G_{1,3}^{2,1}\left(\frac{\omega^2 c_o^2}{4} \middle| {}^{(1-\ell)/2}_{a_o-1,0,-(\ell+1)/2} \right) \cdot d\omega + \sum_{t=0}^{\infty} \frac{1}{t!}(-b_f)^t \int_0^{\infty} \omega^{\ell+a_f+t} G_{0,2}^{2,0}\left(\frac{\omega^2 c_f^2}{4} \middle| {}_{(a_f-1)/2,(a_f-1)/2} \right)$$
$$\times G_{1,3}^{2,1}\left(\frac{\omega^2 c_o^2}{4} \middle| {}^{(1-\ell)/2}_{a_o-1,0,-(\ell+1)/2} \right) \cdot d\omega \Bigg] + C_o C_f (-1)^{a_o-1} \frac{\sqrt{\pi}(-2c_o)^{a_o-1}}{(-b_o-c_o)^{2a_o-1}} \frac{\Gamma(2a_o-1)}{\Gamma(a_o+1/2)}$$
$$\times {}_2F_1\left(2a_o-1, a_o-1/2; a_o+1/2; \frac{-b_o+c_o}{-b_o-c_o} \right) \Bigg[\sqrt{\pi} 2 c_f^{a_f-1} \frac{\Gamma(2a_f-1)}{\Gamma(a_f+1/2)} \Bigg(\frac{1}{(b_f+c_f)^{2a_f-1}}$$
$$\times {}_2F_1\left(2a_f-1, a_f-1/2; a_f+1/2; \frac{b_f-c_f}{b_f+c_f} \right) + \frac{1}{(-b_f+c_f)^{2a_f-1}}$$
$$\times {}_2F_1\left(2a_f-1, a_f-1/2; a_f+1/2; \frac{-b_f-c_f}{-b_f+c_f} \right) \Bigg) \Bigg], \tag{2.74}$$

Then, by using [83, (2.24.1-3)], integrals are solved as in (2.75)

$$F_{\Xi}^{\mathrm{HYB}} = C_o C_f \frac{2^{a_o-4}}{(c_o)^{a_o-1}} \sum_{\ell=0}^{\infty} \frac{1}{\ell!}(-b_f)^{\ell}(-1)^{\ell+1} \sum_{k=0}^{\infty} \frac{1}{k!} \left(\frac{c_f}{2}\right)^{-2(\ell+k+a_f+1)}$$
$$\times \left[b_f^k G_{3,3}^{2,3}\left(\frac{c_o^2}{c_f^2} \middle| \begin{matrix} \frac{1-\ell}{2}, \frac{1-2\ell-2k-3a_f}{2}, \frac{1-2\ell-2k-3a_f}{2} \\ a_o-1, 0, -\frac{\ell+1}{2} \end{matrix} \right) + (-b_f)^k G_{3,3}^{2,3}\left(\frac{c_o^2}{c_f^2} \middle| \begin{matrix} \frac{1-\ell}{2}, \frac{1-2\ell-2k-3a_f}{2}, \frac{1-2\ell-2k-3a_f}{2} \\ a_o-1, 0, -\frac{\ell+1}{2} \end{matrix} \right) \right]$$
$$+ C_o C_f (-1)^{a_o-1} \frac{\sqrt{\pi}(-2c_o)^{a_o-1}}{(-b_o-c_o)^{2a_o-1}} \frac{\Gamma(2a_o-1)}{\Gamma(a_o+1/2)} {}_2F_1\left(2a_o-1, a_o-1/2; a_o+1/2; \frac{-b_o+c_o}{-b_o-c_o}\right)$$
$$\times \left[\sqrt{\pi} 2 c_f^{a_f-1} \frac{\Gamma(2a_f-1)}{\Gamma(a_f+1/2)} \left(\frac{1}{(b_f+c_f)^{2a_f-1}} {}_2F_1\left(2a_f-1, a_f-1/2; a_f+1/2; \frac{b_f-c_f}{b_f+c_f}\right) \right.\right.$$
$$\left.\left. + \frac{1}{(-b_f+c_f)^{2a_f-1}} {}_2F_1\left(2a_f-1, a_f-1/2; a_f+1/2; \frac{-b_f-c_f}{-b_f+c_f}\right) \right) \right], \tag{2.75}$$

Thereupon, the probability of secure communication for EnB scenario in presence of Hybrid-Eve is calculated by using (2.75) as follows

$$P_S^{+} = 1 - F_{\Xi}^{\mathrm{HYB}}. \tag{2.76}$$

2.5 Results and Discussion

In this section, in order to validate the analytical accuracy of our derivations that are obtained in Section 2.4, Monte-Carlo simulations are presented along with related numerical results. In particular, a detailed characterization of the information-theoretic security of hybrid FSO-*mm*Wave systems is investigated in terms of the probability of SPSC using the PDFs of SNRs at Bob and Eve. Further, we consider three different types of eavesdropper to discuss the main implications that arise in practical scenarios of interest. Additionally, unless otherwise stated, the upper bounds of all the summation terms are set to 150.

2.5.1 Non-Identical Independent Channels

The impact of upper limit of the integer l in (2.17) is investigated in Fig. 2.3 for FSO-type eavesdropper at $15\,\mathrm{dB}$. The shape parameter of *mm*Wave link between Alice and Bob is set as $\delta_b = 3$ whereas it is $\lambda_b = \lambda_e = 1/2$ for FSO links. As it is seen from the figure, the upper limit

of l is an important parameter for the analytical accuracy of the probability of SPSC metric. By selecting a small value like $l = 50$, we show a perfect approximation to the exact value. Hence, the upper limit of l is set to 50 in the remaining results of this study.

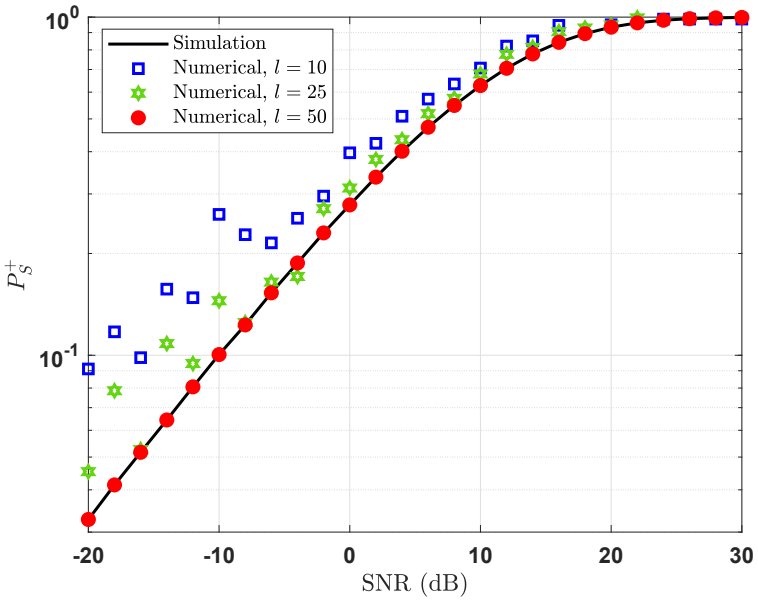


Figure 2.3: Effect of upper limit of l in (2.17) on the probability of SPSC versus average SNR at Bob, for FSO-type eavesdropper at $15\,$dB. ($\delta_b = 3$, $\lambda_b = \lambda_e = 1/2$, $t = 100$, $d_b = d_e = 1\,$km, $R_{b,f} = 0.95$, $R_{b,o} = 0.85$, $R_{e,o} = 0.05$).

Similarly, the impact of upper limit of t in (2.22) on the probability of SPSC versus SNR behavior of the system is presented in Fig. 2.4 for RF-type eavesdropper at $10\,$dB. The shape parameter of *mm*Wave link between Alice and Bob is set as $\delta_b = 2$ whereas it is $\delta_e = 3$ for the link between Alice and Eve. Similarly to l, the upper limit of t is also an important parameter for the analytical accuracy of the security metric P_S^+. It is clear that adjusting a value like $t = 100$, we obtain a perfect match with the exact value. Correspondingly, the upper limit of t is set to 100 in the rest of results.

In Fig. 2.5, the probability of secrecy as a function of the average SNR at Bob is represented in the presence an FSO-type eavesdropper at different fixed SNRs values, $-5\,$dB, $0\,$dB, $5\,$dB, and $10\,$dB. The shape parameter of *mm*Wave link between Alice and Bob is set to $\delta_b = 2$ whereas

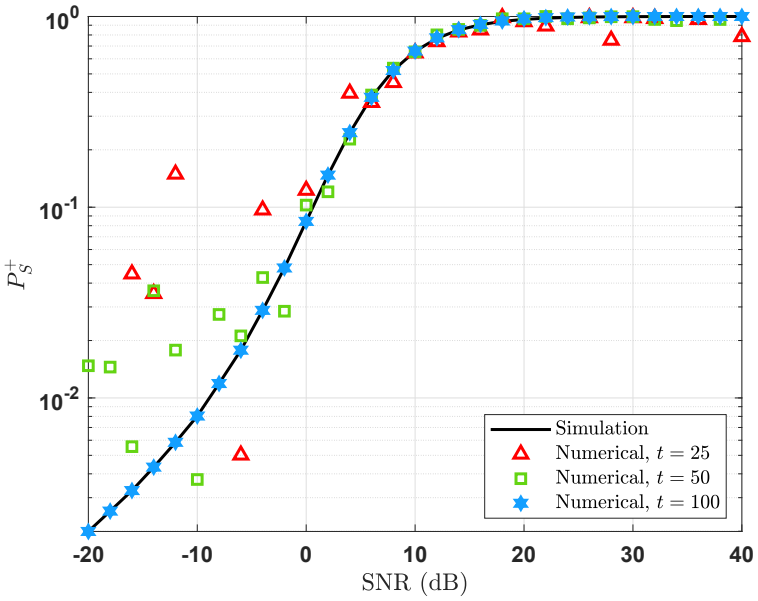


Figure 2.4: Effect of upper limit of t in (2.22) on the probability of SPSC versus average SNR at Bob, for RF-type eavesdropper at 10 dB. ($\delta_b = 2$, $\lambda_b = 1/2$, $\delta_e = 3$, $d_b = d_e = 1.5$ km, $R_{b,f} = 0.8$, $R_{e,f} = 0.1$, $R_{b,o} = 0.9$).

it is $\lambda_b = \lambda_e = 1/2$ for FSO links. The fraction of power collected by Bob over FSO and RF links are assumed as $R_{b,o} = 0.9$ and $R_{b,f} = 0.7$, respectively, whereas the irradiance captured by Eve over FSO link is $R_{e,o} = 0.03$. As observed from the figure, the probability of secure communication decreases with the increment of average SNR of Eve. The analytical result is obtained by using (2.17), and it is clear that numerical findings and simulation results are in perfect agreement.

Likewise, in Fig. 2.6, the probability of SPSC versus average SNR performance of the system is illustrated for RF-type eavesdropper at different fixed SNRs values, -5 dB, 0 dB, 5 dB, and 10 dB. The shape parameter of *mm*Wave link between Alice and Bob is set to $\delta_b = 3$ whereas it is $\delta_e = 5$ for Eve's link. As expected, the security metric decreases with the increment of average SNR of Eve. The analytical results are obtained using (2.22), which exactly match the simulation results for the whole range of the SNR.

Hybrid eavesdroppers, in which Eve is able to eavesdrop both FSO and *mm*Wave links, are investigated in Fig. 2.7. The probability of existence of secure communication between Alice and

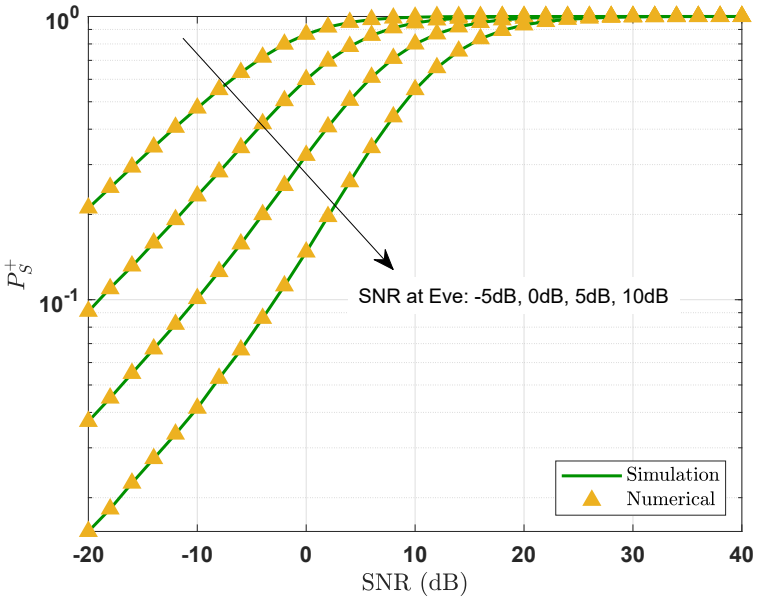


Figure 2.5: The probability of secure communication against average SNR at Bob, for weak turbulence condition, in presence of an FSO-type eavesdropper at different fixed SNRs. ($\delta_b = 2$, $\lambda_b = \lambda_e = 1/2$, $d_b = d_e = 1.25\,\text{km}$, $R_{b,f} = 0.7$, $R_{b,o} = 0.9$, $R_{e,o} = 0.03$).

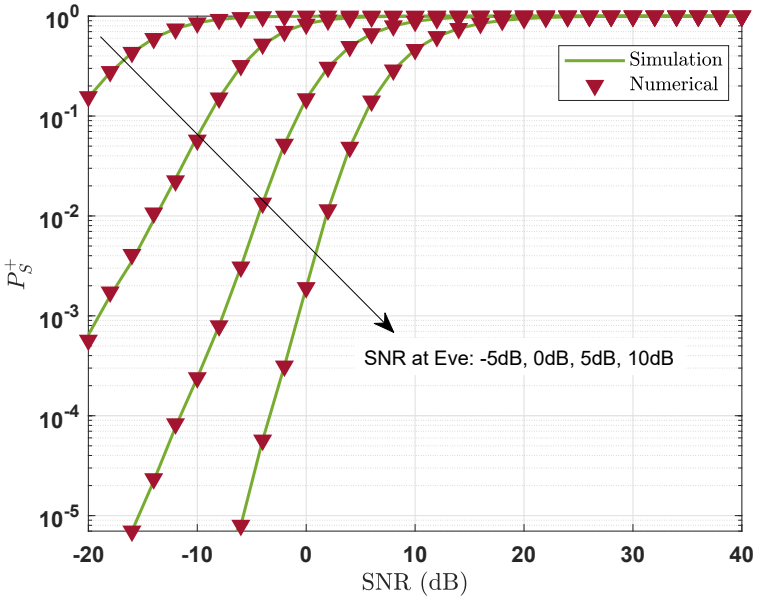


Figure 2.6: The probability of secure communication against average SNR at Bob, for moderate turbulence condition, in presence of an RF-type eavesdropper at different fixed SNRs. ($\delta_b = 3$, $\lambda_b = 1/2$, $\delta_e = 5$, $d_b = d_e = 0.75\,\text{km}$, $R_{b,f} = 0.8$, $R_{b,o} = 0.7$, $R_{e,o} = 0.1$).

Bob versus average SNR performance of the system is depicted in Fig. 2.7 considering a hybrid-type eavesdropper at different fixed SNRs values, $-5\,\text{dB}$, $0\,\text{dB}$, $5\,\text{dB}$, and $10\,\text{dB}$. As seen in the figure, security performance of the system reduces with the increase of Eve's average SNR. The analytical result is obtained by using (2.25), and it is clear that numerical derivation and simulation are in perfect agreement.

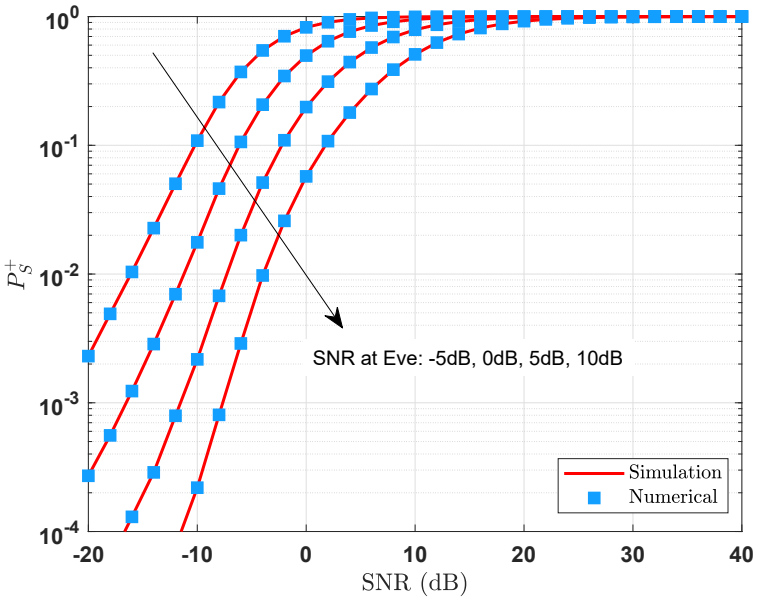


Figure 2.7: The probability of secure communication against average SNR at Bob, for weak turbulence condition, in presence of a hybrid-type eavesdropper at different fixed SNRs. ($\delta_b = 4$, $\delta_e = 5$, $\lambda_b = \lambda_e = 1/2$, $d_b = d_e = 1\,\text{km}$, $R_{b,f} = 0.9$, $R_{e,f} = 0.05$, $R_{b,o} = 0.8$, $R_{e,o} = 0.03$).

A comparison of the probability of SPSC against the average SNR at Bob is presented in Fig. 2.8, in the presence of FSO-, RF- and hybrid-type eavesdroppers at fixed $10\,\text{dB}$ SNR. The shape parameters of the communication links are adjusted as follows: $\delta_b = 3$, $\delta_e = 4$, $\lambda_b = \lambda_e = 1/2$. It can be observed that the hybrid-type eavesdropper significantly decrease the performance of secure communication between Alice and Bob. For instance, at $15\,\text{dB}$ SNR, the probability of SPSC is approximately 95%, 87.5% and 45% for FSO-, RF- and hybrid-Eve, respectively. There is a slight performance difference between FSO- and RF-type Eve due to the parameter selection of

this scenario. However, when we consider hybrid-type eavesdropper, the legitimate pairs experience remarkable loss in secure communication. This is because hybrid Eve is able to exploit both FSO and *mm*Wave link to eavesdrop the communication.

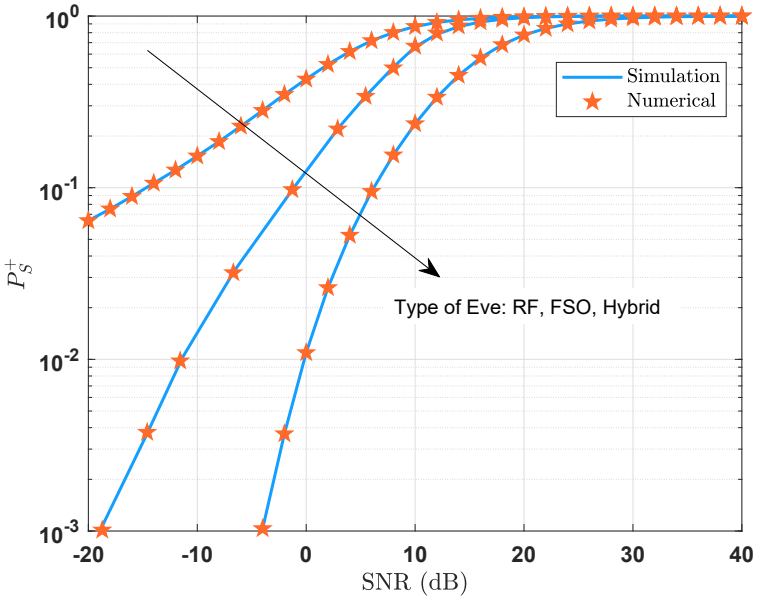


Figure 2.8: A comparison of the probability of secrecy capacity as a function of SNR at Bob, for FSO- RF- and hybrid-type eavesdroppers at fixed 10 dB SNR, over moderate turbulence condition. ($\delta_b = 3$, $\delta_e = 4$, $\lambda_b = \lambda_e = 1/2$, $d_b = d_e = 0.5$ km, $R_{b,f} = 0.8$, $R_{e,f} = 0.1$, $R_{b,o} = 0.85$, $R_{e,o} = 0.1$).

The secure communication metric is investigated in Fig. 2.9 as a function of the ratios $R_{b,o}/R_{e,o} = R_{b,f}/R_{e,f}$, for different turbulence conditions, in the presence of a hybrid-type eavesdropper. The distance between legitimate pairs is set to $d_b = 1$ km whereas Eve is assumed to be in the middle, $d_e = 0.5$ km. Notice that the best possible scenario is considered for Eve, which means that Eve is able collect the diverged part of the laser beam as well as the fraction of the radio power not captured by Bob, i.e. $R_{b,o} = 1 - R_{e,o}$ and $R_{b,f} = 1 - R_{e,f}$. In other words, this corresponds to the worst scenario in terms of secure communication. A scenario in which the power received at Eve is greater than the one at Bob, i.e. $R_{e,o} > R_{b,o}$ and $R_{e,f} > R_{b,f}$, is practically unrealistic. This is due to the fact that Alice and Bob could easily become aware of the presence of an eavesdropper

and stop the communication. In addition, when the rate is 10^0, i.e. $R_{b,o} = R_{e,o}$ and $R_{b,f} = R_{e,f}$, this scenario is also unattainable because this implies that Eve blocks 50% of the total power collected by Bob. From the feasibility point of view, we consider the scenarios in which the power received at Bob is far greater than the one at Eve, i.e., $R_{b,o} \gg R_{e,o}$ and $R_{b,f} \gg R_{e,f}$.

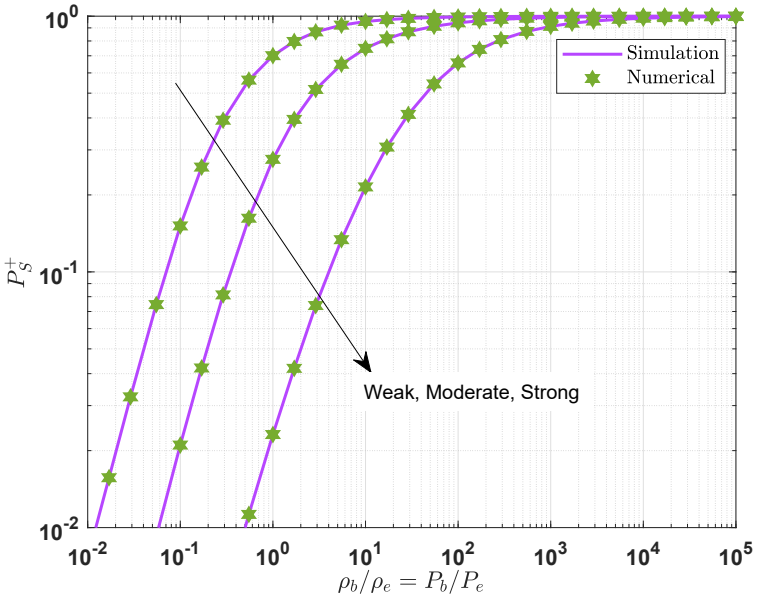


Figure 2.9: The probability of secure communication between Alice and Bob in presence of a hybrid-type eavesdropper as a function of the ratios $R_{b,o}/R_{e,o} = R_{b,f}/R_{e,f}$ for different turbulence conditions. ($\delta_b = 2$, $\delta_e = 3$, $\lambda_b = \lambda_e = 1/2$, $d_b = 1\,\text{km}$, $d_e = 0.5\,\text{km}$).

The probability of SPSC as a function of the distance d_b between legitimate pairs is represented in Fig. 2.10, in the presence of a hybrid-type eavesdropper, for different turbulence conditions. The distance between Alice and Eve is set to $d_e = 0.4\,\text{km}$. A value of the fraction of power received at Eve is assumed as $R_{e,o} = R_{e,f} = 0.01$, where $R_{b,o} = 1 - R_{e,o}$ and $R_{b,f} = 1 - R_{e,f}$. In this scenario, we observe different behaviors that show highly informative inferences. As it is seen from the figure, for the range of distance where $d_b \leq d_e$, the perfect secrecy can be obtained regardless of atmospheric severity. This is due to the fact that power collected by Bob is much greater than Eve. However, for a distance $d_b > d_e$, we observe opposite and distinctive behaviors about the security metric. Secure communication begins diminishing first as the turbulence-dependent

attenuation becomes more severe. This behavior is also in agreement with the fact that strong turbulence conditions imply larger and frequent fluctuations in channel gains. Since the more severe the turbulence conditions, the lower the SNR, this explains why the slope of decay in P_S^+ curves aggravate as the turbulence condition changes from weak to strong. One also should notice that in some cases, even the average SNR at Bob is larger than the one at Eve, there is an unignorable probability of eavesdropper having an instantaneous SNR better than Bob. For example, considering the distance $d_b = 0.45\,\text{km}$, the probability of secure communication is approximately 92%, 75% and 20% for weak, moderate and strong turbulence conditions, respectively.

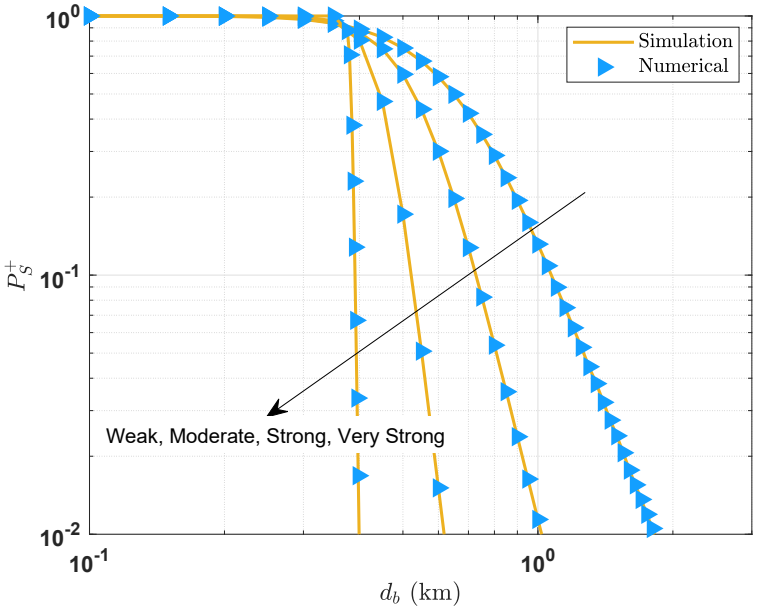


Figure 2.10: The probability of secure communication as a function of the distance d_b between legitimate pairs, for different turbulence conditions, in presence of a hybrid-type eavesdropper. ($\delta_b = 2$, $\delta_e = 3$, $\lambda_b = \lambda_e = 1/2$, $d_e = 0.4\,\text{km}$, $R_{b,o} = R_{b,f} = 0.99$, $R_{e,o} = R_{e,f} = 0.01$).

The value of ratios $R_{b,o}/R_{e,o} = R_{b,f}/P_e$ that leads to a certain value of the probability of strictly positive secrecy capacity is investigated in Fig. 2.11 as a function of the distance d_b between Alice and Bob, over moderate turbulence condition. The values for this metric are considered as 0.2, 0.5 and 0.8, meaning that in the presence of a hybrid-type eavesdropper, secure communication is only

possible with a 20%, 50% and 80% of probability at best, respectively. We observe a remarkable dependence between the probability of secure communication and the distance of legitimate pairs.

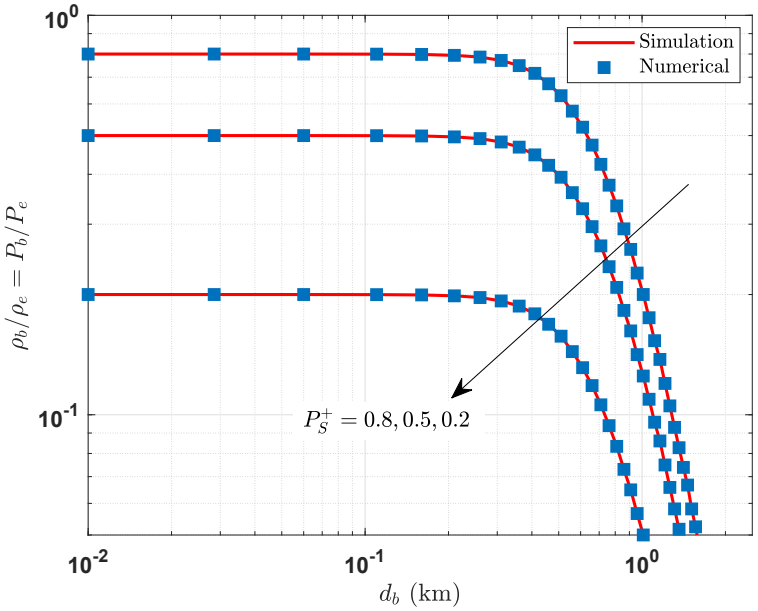
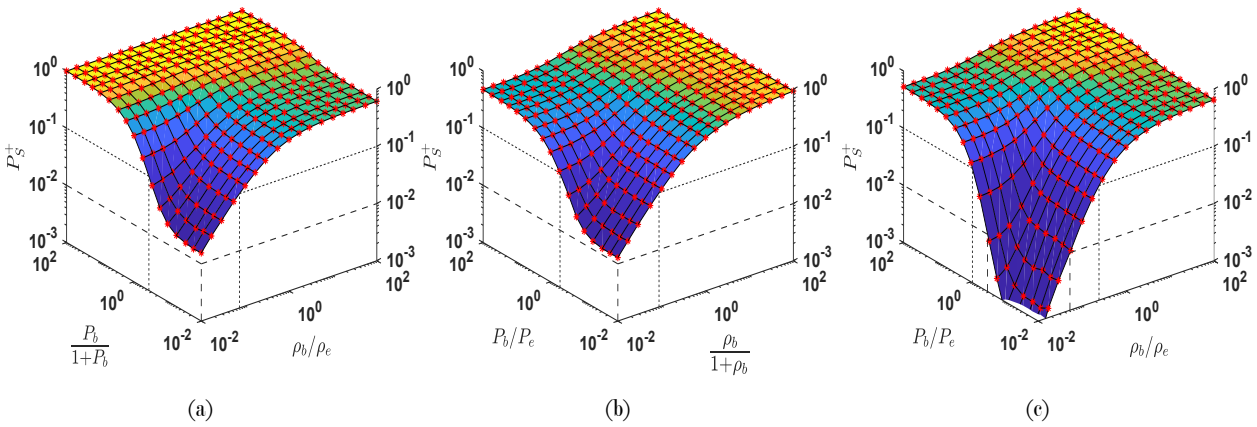


Figure 2.11: The value of ratios $R_{b,o}/R_{e,o} = R_{b,f}/P_e$ that satisfies a certain probability of strictly positive secrecy capacity as a function of the distance d_b between Alice and Bob, in the presence of a hybrid-type eavesdropper. ($\delta_b = 2$, $\delta_e = 3$, $\lambda_b = \lambda_e = 1/2$, $d_e = 0.75\,$km).

The probability of secrecy capacity as a function of the ratios $R_{b,o}/R_{e,o}$ and $R_{b,f}/P_e$ is investigated in Fig. 2.12, over weak turbulence condition, in the presence of different types of eavesdroppers. The shape parameters of *mm*Wave links are set to $\delta_b = 2$ and $\delta_e = 3$, whereas $\lambda_b = \lambda_e = 1/2$ for FSO links. The distances between legitimate pairs and eavesdroppers are assumed to be the same as $d_b = d_e = 1\,$km. In all three scenarios, the best possible eavesdropper cases are considered for Eve. Then, we examine how the wiretapping ability changes for FSO-, RF and hybrid-type eavesdroppers which has a very important impact on the secrecy. It is clear from the figure, a hybrid-type Eve dramatically decreases the probability of secure communication, compared to an FSO- or RF-type. For the worst case considered in this scenario which is



(a) (b) (c)

Figure 2.12: The probability of secure communication between legitimate pairs as a function of the ratios $R_{b,o}/R_{e,o}$ and $R_{b,f}/P_e$, over weak turbulence condition, in the presence of different types of eavesdroppers: (a) FSO-type Eve, (b) RF-type Eve, (c) Hybrid-type Eve. Each intersection of solid-black lines on the surface and red-color markers represent the simulation and numerical results, respectively. ($\delta_b = 3$, $\delta_e = 2$, $\lambda_b = \lambda_e = 1/2$, $d_b = d_e = 1\,\text{km}$).

$R_{b,o}/R_{e,o} = R_{b,f}/P_e = 0.01$, the probabilities of secrecy capacity are approximately 1.5%, 1.3% and 0.03% for FSO-, RF- and hybrid-type Eve, respectively. Alternatively, when we consider the value of the ratios $R_{b,o} = R_{e,o}$ and $R_{b,f} = P_e$, secure communication can be obtained with 70%, 65% and 42% probabilities at best for FSO-, RF- and hybrid-type Eve, respectively. On the other hand, if we fix the probability of having secure communication to $P_S^+ = 0.1$ and consider the worst case scenario for received power by Bob over FSO or *mm*Wave link, a set of the minimum required power that needs to be collected by Bob over other link is, in turn, $\{R_{b,o}{=}0.07, R_{b,f}{=}0.26\}$, $\{R_{b,o}{=}0.09, R_{b,f}{=}0.31\}$ and $\{R_{b,o}{=}0.2, R_{b,f}{=}0.5\}$ for FSO-, RF- and hybrid-type Eve. In conclusion, we show that the hybrid eavesdropper has a powerful ability to wiretap the legitimate communication and the presence of this type of eavesdroppers should also be considered in designing a wireless system.

2.5.2 Non-Identical Dependent Channels

A comparison of the probability of SPSC against the average SNR at Bob is presented in Fig. 2.13 to compare the wiretapping ability of FSO-, RF- and hybrid-type eavesdroppers for Eve-near-Alice scenario. The distance between legitimate pairs d_b is assumed as $1\,\text{km}$, where

the received power fractions are considered as $R_{b,f} = R_{b,o} = 0.8$, and $R_{e,f} = R_{e,o} = 0.1$. This is in practice implies that 10% of the transmitted/emitted power by Alice is lost during the transmission. Despite the high security assumption of FSO link, one can easily observe that an FSO-type eavesdropper has the ability of degrading the secrecy performance dramatically. Therefore, during the design of such a communication system, we also need to take the effects of FSO-Eve into account. On the other hand, it can be observed that a hybrid eavesdropper significantly decrease the performance of secure communication between Alice and Bob in comparison with FSO- and RF-Eve. For instance, considering a $10\,$dB SNR at Bob, the probability of SPSC is approximately 75%, 72% and 53% for RF-, FSO- and Hybrid-Eve, respectively. There is a slight performance difference between FSO- and RF-type Eve due to parameter selection of this scenario. However, when we consider hybrid-type eavesdropper, the legitimate pairs experience remarkable loss in secure communication. This is because hybrid Eve is able to exploit both FSO and *mm*Wave link to eavesdrop the communication.

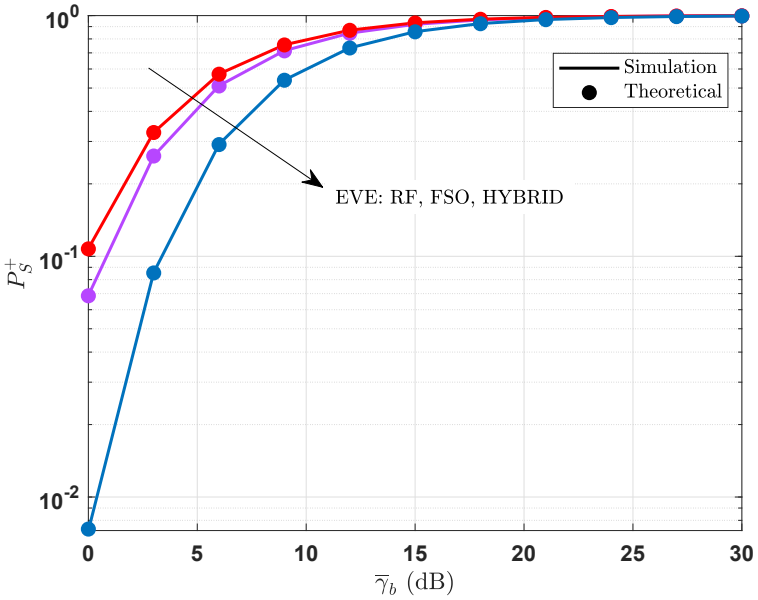


Figure 2.13: A comparison of the probability of secrecy capacity as a function of SNR at Bob, for RF- FSO- and hybrid-type eavesdroppers. (EnA Scenario, Hazy Weather, $d_b = 1\,$km, $R_{b,f} = R_{b,o} = 0.8$, $R_{e,f} = R_{e,o} = 0.1$) Reprinted with permission from [43].

The probability of secrecy capacity as a function of the received power ratios $R_{b,o}/R_{f,o}$ and $R_{b,f}/R_{e,f}$ is investigated in Fig. 2.14, for Eve-near-Alice scenario, over clean weather condition, in the presence of different types of eavesdroppers. The distances between legitimate pairs is assumed to be $d_b = 0.75$ km. In all three scenarios, the best possible eavesdropper cases are considered for Eve, where $R_{b,f} + R_{e,f} = 1$. Then, we examine how the wiretapping ability changes for FSO-, RF and hybrid-type eavesdroppers which has a very important impact on the secrecy. It is clear from the figure, a hybrid-type Eve dramatically decreases the probability of secure communication, compared to an FSO- and/or RF-type. For the worst case considered in this scenario which is $R_{b,o}/R_{e,o} = R_{b,f}/R_{e,f} = 0.01$, the probabilities of secrecy capacity are approximately 2.8%, 2.2% and 0.2% for FSO-, RF- and hybrid-type Eve, respectively. Alternatively, when we consider the value of the ratios $R_{b,o} = R_{e,o}$ and $R_{b,f} = R_{e,f}$, secure communication can be obtain with 75%, 68% and 41% probabilities at best for FSO-, RF- and hybrid-type Eve, respectively. On the other hand, if we fix the probability of having secure communication to $P_S^+ = 0.7$ and consider the worst case scenario for received power by Bob over FSO or *mm*Wave link, a set of the minimum required power that needs to be collected by Bob over other link is, in turn, $\{R_{b,o} = 0.65, R_{b,f} = 0.72\}$, $\{R_{b,o} = 0.65, R_{b,f} = 0.72\}$, $\{R_{b,o} = 0.71, R_{b,f} = 0.69\}$, $\{R_{b,o} = 0.81, R_{b,f} = 0.84\}$ for FSO-, RF- and hybrid-type Eve. In conclusion, we show that the hybrid eavesdropper has a powerful ability to wiretap the legitimate communication and the presence of this type of eavesdroppers should also be considered in designing a wireless system.

For Eve-near-Alice scenario, secrecy performance as a function of the distance d_b between legitimate pairs is represented in Fig. 2.15, considering the impact of different weather conditions on the system, with a fixed $\gamma_b = 5$ dB SNR at Bob. A value of the fraction of power received at Bob is assumed as $R_{b,o} = R_{b,f} = 0.8$, where $R_{b,o} = R_{b,f} = 0.15$. As it is seen from the figure, the secrecy performance is heavily degraded for weather conditions when it goes from clean to moderate rain. As it is seen from the graph, for each weather scenario, the hybrid-type Eve mostly decreases the probability of secure communication compared to FSO- and RF-Eve. To express it in a different way, regardless of a weather condition, hybrid-Eve has the highest probability of

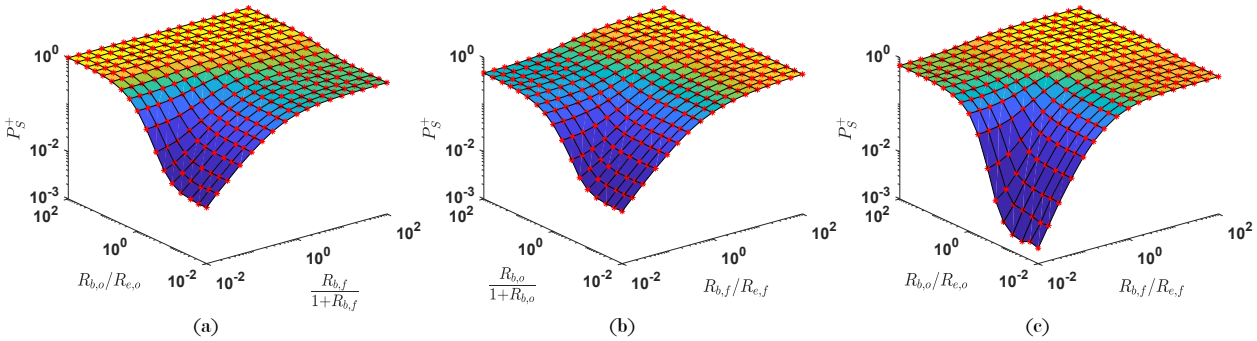


Figure 2.14: The probability of secure communication between legitimate pairs as a function of the ratios $R_{b,o}/R_{e,o}$ and $R_{b,f}/R_{e,f}$ for Eve-near-Alice scenario: (a) FSO-type Eve, (b) RF-type Eve, (c) Hybrid-type Eve. Each intersection of solid-black lines on the surface and red-color markers represent the simulation and numerical results, respectively. (EnA scenario, Hazy weather, $d_b = 0.75$ km) Reprinted with permission from [43].

affecting the secure communication. However, when we investigate the RF- and FSO-type Eve, we observe that different turbulence conditions have distinct effects on them. Thus, this behavior practically answers why the different types of eavesdropper needs to be considered in a secure system design. For instance, if we want to achieve a secure communication with a probability of 85%, the minimum distance can be $d_b = 0.25$, 0.55 and 0.8 km for clean, hazy and moderate rain weather conditions.

In Fig. 2.16, the value of $R_{e,o} = R_{e,f}$ (fractions of the laser beam and radio power leaked to Eve) is investigated, which leads to a predetermined value of probability of strictly secrecy capacity, as a function of the distance d_b between Alice and Bob, for Eve-near-Alice scenario, over different weather conditions. The set of values for this probability is fixed at 0.2, 0.5 and 0.8, which implies that secure communication is only possible, in turn, with a 20%, 50% and 80% of probability at a given distance, in the presence of an eavesdropper. As it is seen from the figure, we can easily observe a significant dependence with the weather condition-related attenuation loss experienced by Bob. Additionally, we can express that Eve-near-Alice scenarios are very vulnerable to eavesdropping even for very low received powers ($R_{e,o}$ and $R_{e,f}$) by Eve due to the very close location of Eve with respect Alice. Therefore, this behavior needs to be considered in the design of secure wireless system with secrecy constraints. Moreover, the impact of different

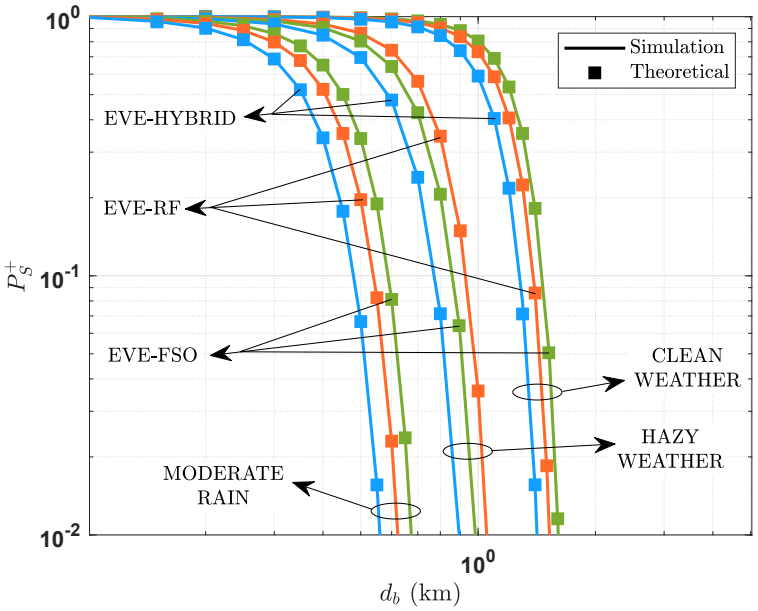


Figure 2.15: The probability of secure communication as a function of the distance d_b between legitimate pairs for different weather conditions in presence of FSO-, RF-, and hybrid-type eavesdropper. (EnA Scenario, $\gamma_b = 5\,\text{dB}$, $R_{b,f} = R_{b,o} = 0.8$, $R_{e,f} = R_{e,o} = 0.15$) Reprinted with permission from [43].

weather conditions on the secrecy performance of the system is also observed in this figure, which verifies the use of a hybrid communication system.

A comparison of the probability of SPSC against the average SNR at Bob is presented in Fig. 2.17, in the presence of FSO-, RF- and hybrid-type eavesdroppers for Eve-near-Bob scenario. We observed that the hybrid-type eavesdropper remarkably decreases the performance of secure communication between Alice and Bob. For instance, at $12\,\text{dB}$ SNR, the probability of SPSC is approximately 92%, 87% and 76% for FSO-, RF- and Hybrid-Eve, respectively. There is a slight performance difference between FSO- and RF-type Eve due to parameter selection of this scenario. However, when we consider hybrid-type eavesdropper, the legitimate pairs experience remarkable loss in secure communication. This is because hybrid Eve is able to exploit both FSO and *mm*Wave link to eavesdrop the communication.

As also discussed in [88–90], the non-monotonic impact of the correlation coefficients ρ_o and ρ_f on the secrecy performance is illustrated in Fig. 2.18, where the SPSC is plotted as a function

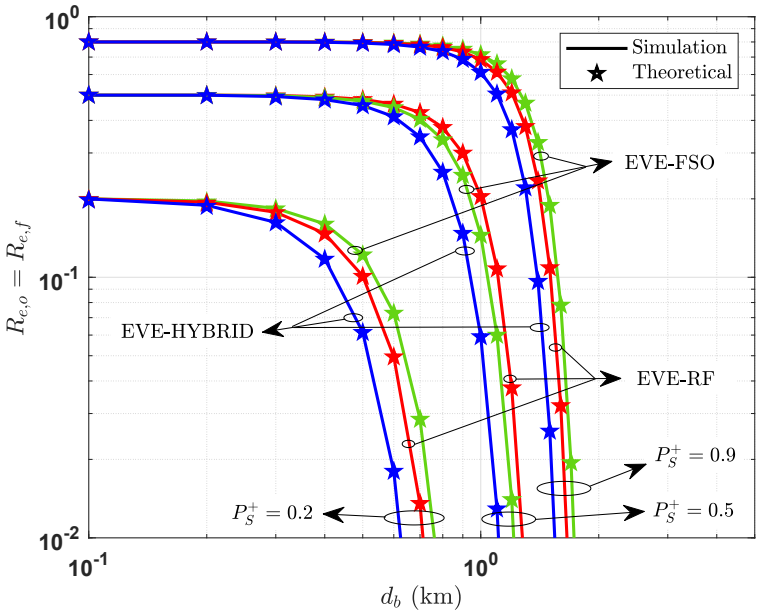


Figure 2.16: The received power value of $R_{b,o} = R_{b,f}$ that satisfies a certain probability of strictly positive secrecy capacity as a function of the distance d_b between Alice and Bob, in presence of FSO-, RF-, and hybrid-type eavesdropper. (EnA Scenario, Clean Weather) Reprinted with permission from [43].

of the distance $d_b = d_e$ for different types of eavesdroppers. Despite the correlation coefficients ρ_o and ρ_f are fixed to 0.7, varying the distance parameters change the channel distribution of the FSO system, based on (1.16) and (1.17). Therefore, the impact of the same correlation coefficient on different channel distributions has an interesting impact. For this figure, clean weather conditions are considered and the received powers are selected as $R_{e,f} = 0.1$, $R_{e,o} = 0.25$ and $\rho_o = \rho_f = 0.65$ with the fixed average SNRs $\gamma_b = 5$ dB and $\gamma_e = 0$ dB. One can easily observe that as the distance parameters $d_b = d_e$ increases, the secrecy performance of the system first decreases, however after a specific value of the distance, the secrecy performance starts to increase. Thus, this behavior implies that the correlation between the main and wiretap channels can be utilized to improve the secrecy performance of the system, and needs to be considered as an important security constraint in a practical system design.

Specifically, considering a hybrid-type eavesdropper, the impact of the correlation on both FSO and RF links is investigated in Fig. 2.19, in terms of the secrecy performance between legitimate

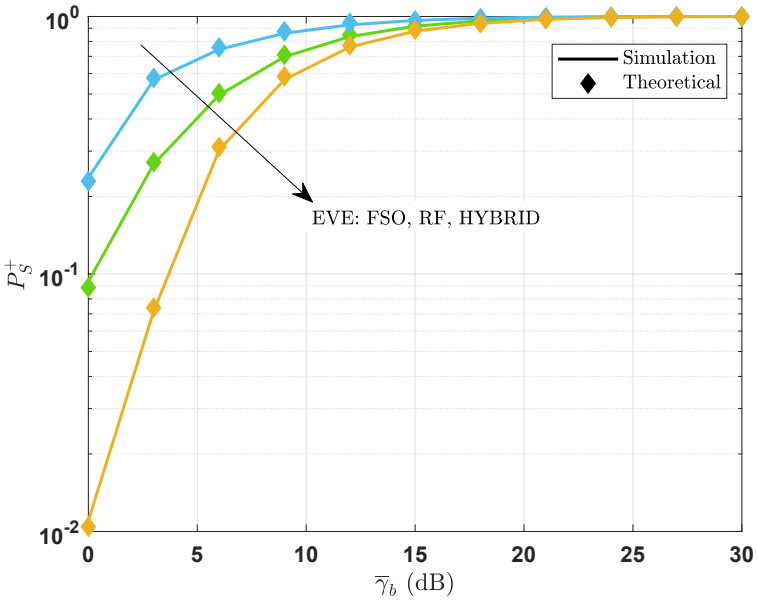


Figure 2.17: A comparison of the probability of secrecy capacity as a function of SNR at Bob, for RF- FSO- and hybrid-type eavesdroppers. (EnB Scenario, Clean Weather, $\gamma_e = 5\,\text{dB}$, $d_b = d_e = 0.75\,\text{km}$, $R_{b,f} = R_{b,o} = 0.75$, $R_{e,f} = R_{e,o} = 0.05$, $\rho_o = \rho_f = 0.7$) Reprinted with permission from [43].

pairs as a function of both ρ_o and ρ_f, where we consider hazy weather conditions, the distance of $d_b = d_e = 0.7\,\text{km}$, the fixed SNRs of $\gamma_b = 10\,\text{dB}$ and $\gamma_e = 5\,\text{dB}$, and the received powers of $R_{b,f} = R_{b,o} = 0.65$ and $R_{e,f} = R_{e,o} = 0.25$. In this figure, to show the monotonic behavior of the correlation on the secrecy performance, we particularly select a distance of $d_b = d_e = 0.7\,\text{km}$. In other words, we exploit the correlation between the main and eavesdropper channels to take advantage of the similarities in each link [91, 92]. As shown in the figure, increasing the correlation coefficient of ρ_o and ρ_f increases the SPSC performance of the system. For instance, the probability of secure communication is obtained as 73.5%, 82.2%, and 97.3%, when we set $\rho_o = \rho_f$ to 0.05, 0.5, and 0.95, respectively. Additionally, when we consider a high correlation in one link and a low correlation in the other, we observe the following results for the SPSC metric: P_S^+ is 0.8211 for $\rho_o = 0.05$ and $\rho_f = 0.95$, while P_S^+ is 0.8085 for $\rho_o = 0.95$ and $\rho_f = 0.05$.

The probability of secrecy capacity as a function of the ratios $R_{b,o}/R_{f,o}$ and $R_{b,f}/R_{e,f}$ is investigated in Fig. 2.20, over moderate rainy weather, in the presence of different types of eaves-

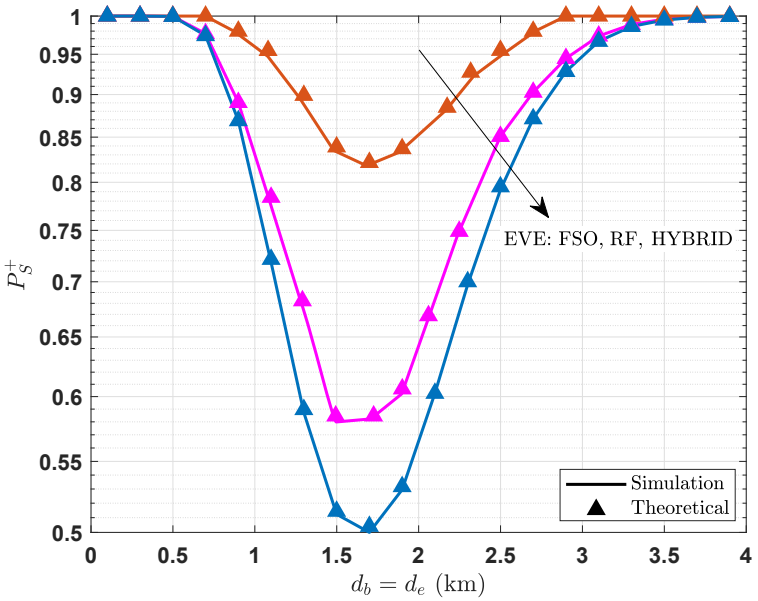


Figure 2.18: A comparison of the probability of secrecy capacity as a function of distance $d_b = d_e$, for RF- FSO- and hybrid-type eavesdroppers. (EnB Scenario, Clean Weather, $\gamma_b = 5\,\text{dB}$, $\gamma_e = 0\,\text{dB}$, $R_{b,f} = R_{b,o} = 0.7$, $R_{e,f} = 0.1$, $R_{e,o} = 0.25$, $\rho_o = \rho_f = 0.65$) Reprinted with permission from [43].

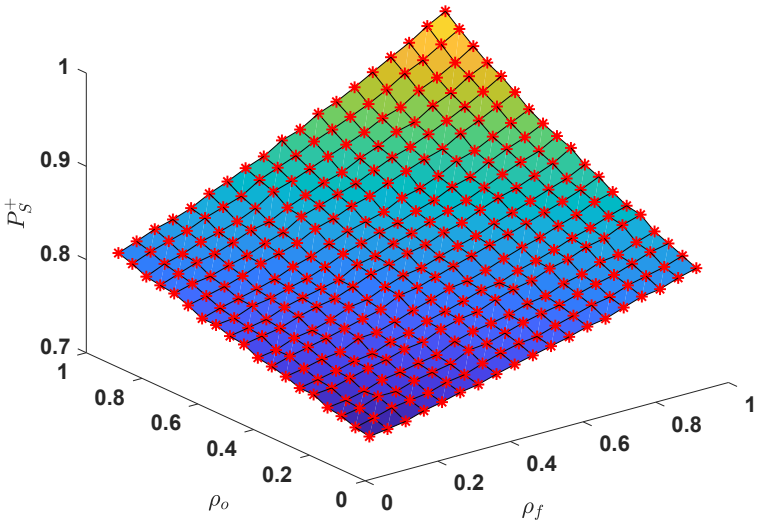


Figure 2.19: The probability of secrecy performance between legitimate pairs as a function of the correlation coefficients ρ_o and ρ_f. (EnB Scenario, Haze Weather, $\gamma_b = 10\,\text{dB}$, $\gamma_e = 5\,\text{dB}$, $R_{b,f} = R_{b,o} = 0.65$, $R_{e,f} = R_{e,o} = 0.25$, $d_b = d_e = 0.7\,\text{km}$) Reprinted with permission from [43].

droppers, for Eve-near-Bob scenario. The distances between legitimate pairs and eavesdroppers are assumed to be the same as $d_b = d_e = 1$ km. In all three scenarios, the best possible eavesdropper cases are considered for Eve, $R_{e,o} = 1 - R_{b,o}$ and $R_{e,f} = 1 - R_{b,f}$. Then, we examine how the wiretapping ability changes for FSO-, RF and hybrid-type eavesdroppers with a correlation coefficient of 0.7 for both RF and FSO links, which has a very important impact on the secrecy. It can be observed from the figure, a hybrid-type Eve remarkably decreases the probability of secure communication, compared to an FSO- or RF-types. For the worst case considered in this scenario which is $R_{b,o}/R_{e,o} = R_{b,f}/R_{e,f} = 0.01$, the probabilities of secrecy capacity are approximately 1.2%, 1.5% and 0.01% for FSO-, RF- and hybrid-type Eve, respectively. Alternatively, when we consider the value of the ratios $R_{b,o} = R_{e,o}$ and $R_{b,f} = R_{e,f}$, secure communication can be obtain with 87%, 83% and 71% probabilities at best for FSO-, RF- and hybrid-type Eve, respectively. On the other hand, if we fix the probability of having secure communication to $P_S^+ = 0.95$ and consider the worst case scenario for received power by Bob over FSO and *mm*Wave link, a set of the minimum required power that needs to be collected by Bob over other link is, in turn, $\{R_{b,o} = 0.78, R_{b,f} = 0.71\}$, $\{R_{b,o} = 0.75, R_{b,f} = 0.76\}$, $\{R_{b,o} = 0.86, R_{b,f} = 0.89\}$ for FSO-, RF- and hybrid-type Eve. In conclusion, we show that the hybrid eavesdropper has a powerful ability to wiretap the legitimate communication and the presence of this type of eavesdroppers should also be considered in designing a wireless system.

2.6 Concluding Remarks

In this chapter, the existence of secure communication between a legitimate transmitter Alice and a legitimate receiver Bob is investigated for hybrid FSO-*mm*Wave systems. In particular, the communication between legitimate pairs is carried over FSO exponential turbulence and *mm*Wave Weibull fading channels simultaneously for non-identical independent case, where FSO Gamma-Gamma turbulence and *mm*Wave Nakagami-m fading channels are considered for non-identical dependent case. The MRC combining technique is employed at both the legitimate receiver Bob and the eavesdropper Eve. As a security performance metric, the probability of SPSC is derived in the presence of different types of eavesdroppers, namely RF-, FSO- and hybrid-Eve, with two spe-

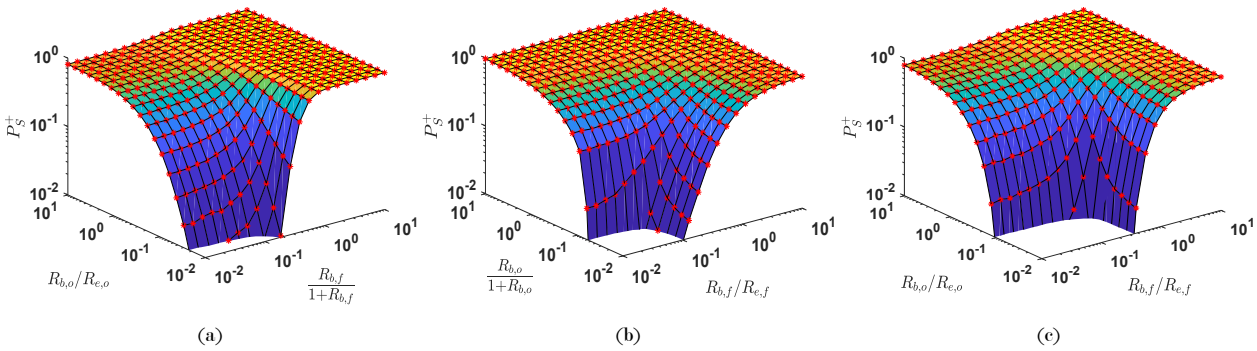


Figure 2.20: The probability of secure communication between legitimate pairs as a function of the ratios $R_{b,o}/R_{e,o}$ and $R_{b,f}/R_{e,f}$ for Eve-near-Bob scenario: (a) FSO-type Eve, (b) RF-type Eve, (c) Hybrid-type Eve. Each intersection of solid-black lines on the surface and red-color markers represent the simulation and numerical results, respectively. (EnB Scenario, Moderate Rainy Weather, $d_b = 1\,\text{km}$, $\rho_o = \rho_f = 0.7$) Reprinted with permission from [43].

cific locations, i.e., Eve-near-Alice and Eve-near-Bob. Analytical results that are presented in this study allow us to understand how secure communication can be achieved in different scenarios of interest in the context of hybrid FSO-*mm*Wave communications, where the effects of different locations of Eve on the secure communication are discussed including several fundamental physical layer parameters. In the light of results, we show that the different types of eavesdroppers need to be taken into accounts in the design of a secure communication system due to their natural behavior under specific weather conditions. Additionally, we present the correlation between main and wiretap channel can be used to exploit and enhance the security performance of the designed system. Moreover, by investigating the impact of different weather conditions on each link, we verify the use of a hybrid system significantly improves the secrecy performance. As such, the analysis made in this study can be very necessary for the system designer to secure transmitted data and improve its confidentiality against eavesdroppers. Specifically, based on the type of eavesdropper and its expected location, a system designer can limit its transmit power to degrade the SNR at the eavesdropper and achieve the secrecy capacity at the legitimate receiver.

3. INDEX MODULATION-BASED LINK SELECTION FOR HYBRID FSO-RF SYSTEMS*

3.1 Introduction

3.1.1 Motivation

One of the main problem in hybrid FSO-*mm*Wave systems is the mechanism followed to activate one of the links. Most of the proposed selection mechanisms suffer from high overhead and required side information at the transmitter. In this chapter, a novel selection mechanism is proposed for hybrid FSO-*mm*Wave systems without the need for any feedback or channel state information at the transmitter side. The activation of each link, either FSO or *mm*Wave, is determined by the use of the IM concept.

3.2 Related Works

The works [95–98] propose switching mechanisms for hybrid FSO-*mm*Wave systems with different configurations, and the priority is always given to the FSO link. Specifically, in the work presented in [95], denoted as a single-threshold switching mechanism, the FSO link is only used until the instantaneous SNR falls below a defined threshold, at which point the *mm*Wave link is activated. Then, the authors consider a dual-threshold to reduce the frequent on-off transitions, where lower and upper thresholds are defined. The FSO link is operational until the SNR falls below the lower threshold, and then the FSO link is only re-activated again if the SNR is above the upper threshold, otherwise the *mm*Wave link is used. The authors in [99–101] propose a cooperative FSO-*mm*Wave system for dual-hop decode-and-forward (DF) relaying transmissions with related mathematical derivations of average bit-error-rate (BER) and outage probability. The impact of different system and channel parameters on the system performance is also investigated. Since unmanned aerial vehicle (UAV)-based wireless communications is a very promising new technol-

*Reprinted with permission from "Performance analysis of index modulation based link-selection mechanism for hybrid FSO-mmWave systems" by Sezer C. Tokgoz, Saud Althunibat, Scott L. Miller, and Khalid A. Qaraqe, 2020. Optics Communications, 479, 126305, Copyright [2020] by Elsevier [93], and from "A Link-Selection Mechanism for Hybrid FSO-mmWave Systems based on Index Modulation" by Sezer C. Tokgoz, Saud Althunibat, and Khalid A. Qaraqe, 2020. International Conference on Communications (ICC), 1–7, Copyright [2020] by IEEE [94].

ogy that provides a wide range of new capabilities to current networks, the performance of hybrid and mixed FSO-*mm*Wave communications for UAVs are investigated in [102–106] including the source-relay-destination link utilization, the trajectory optimization problem of buffer-constrains, and the impact of hovering. In [107–109], a *mm*Wave-assisted FSO system is proposed for 5G vehicle-to-vehicle communications, where the unreliability of the FSO system due to misalignment is compensated by the help of a *mm*Wave link in high mobility conditions.

3.3 System Model

In this chapter, a wireless communication system is considered with a single transmitter T_x and a single receiver R_x. T_x is equipped with a single transmitting antenna and a single laser light source, while R_x is equipped with a single receiving antenna and a single photodiode. Thus, the communication between both ends is performed through two parallel links: an RF link and an FSO link. Specifically, the two RF antennas are used to compose the RF link, while FSO transmission is accomplished using the laser and the photodiode. To provide identical bandwidth over the two links, the RF link is considered to operate over the *mm*Wave frequency range.

The message signal to be transmitted is modulated by using a phase shift keying (PSK) modulation technique for both FSO and *mm*Wave systems due to its implementation practicability. First, the serial information bits are converted into parallel streams which are, then, mapped onto complex symbols depending on the modulation order. The resultant electrical PSK signal is expressed as [110, (3.2-24)]

$$x[n] = \sum_{k} e^{\jmath\phi_k} p_k(n - kT_p), \tag{3.1}$$

where $p_k(\cdot)$ depicts the pulse shaping filter, T_p denotes the effective pulse width, $\phi_k \in [0, 1, \ldots, (m-1)\frac{2\pi}{M}]$ is the instantaneous phase for the k^{th} symbol, $0 < m \leq M$, M stands for the modulation order, which specifies the bit rate $B = \frac{\log_2 M}{T_p}$. Hereafter, FSO and *mm*Wave systems are described to investigate the proposed selection mechanism. Then, modulated signal is transmitted though either FSO or *mm*Wave link based on the selection mechanism.

3.3.1 FSO Subsystem

After minor modifications due to the non-negativity of the light depending on the IM/DD technique, the electrical PSK signal can be transmitted through the FSO link. To avoid any clipping problem, the electrical PSK signal is scaled and then DC biased. The intensity-modulated optical PSK signal is expressed as [111]

$$x_o[n] = 1 + \mu x[n], \tag{3.2}$$

where $\mu \in (0, 1]$ is the shrinking factor in order to ensure that the transmitter avoids over-modulation.

After passing through the FSO link, the incident optical signal is converted into an electrical signal which is expressed as

$$y_o = \eta I_r I x_o + w_o, \tag{3.3}$$

where η is the optical-to-electrical conversion ratio, I depicts the Gamma-Gamma (GG) atmospheric-turbulence fading channel, as defined in subsection 1.2.2, w_o is the additive white Gaussian noise (AWGN) with zero mean and variance σ^2, $w_o \sim \mathcal{N}(0,\, \sigma^2)$, and I_r stands for the received optical power including the path loss: $I_r = I_t L_o$, where I_t denotes the transmitted optical power, and L_o depicts the path loss, as given in (1.25). Based on (3.2) and (3.3), the instantaneous electrical SNR at the FSO receiver is expressed as in (1.23).

3.3.2 mmWave Subsystem

In contrast to FSO transmission, the electrical PSK signal can be directly transmitted over the *mm*Wave link and is expressed as

$$x_f[n] = x[n], \tag{3.4}$$

and after passing through the *mm*Wave link, the received signal at the receive antenna, y_f, is expressed as

$$y_f = \sqrt{P_r} H x_f + w_f, \tag{3.5}$$

where H stands for the Nakagami-m fading channel, as defined in subsection 1.1.2, w_f depicts the complex AWGN with $\mathcal{CN}(0,\, 2\sigma^2)$, of the form $w_f = w_f^I + \jmath w_f^Q$ with both w_f^I and w_f^Q being $\mathcal{N}(0,\, \sigma^2)$, $\jmath = \sqrt{-1}$, and P_r denotes the received average electrical power including the path loss, $P_r = P_t L_f$, where P_t denotes the transmitted electrical power, and L_f depicts the path loss, as given in (1.22). Based on (3.4) and (3.5), the instantaneous electrical SNR at the *mm*Wave receiver is expressed as in (1.20).

3.4 Proposed IM-based Selection Mechanism

The proposed selection mechanism in this study takes advantage of the IM concept. One bit among each bit block is reserved to determine whether the FSO or *mm*Wave link is to be activated at that particular instant. Therefore, the proposed link activation mechanism is an information-driven algorithm, which consequently improves the spectral efficiency. Block diagrams of the proposed IM-based link selection mechanism is illustrated in Figure 3.1 without an eavesdropper and in Figure 3.2 in the presence of an eavesdropper.

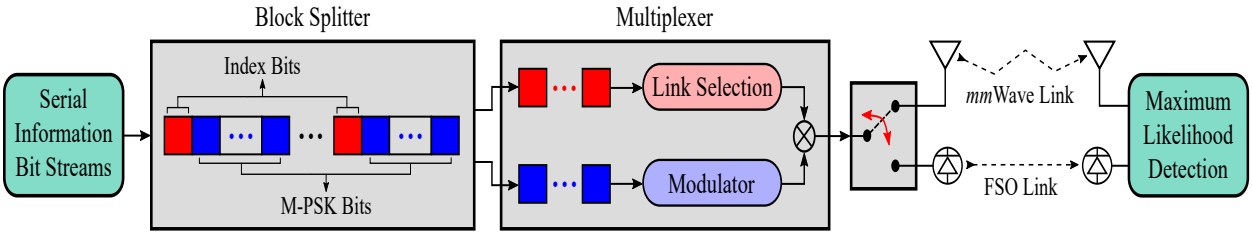


Figure 3.1: Block diagram of the proposed IM-based link selection mechanism. Reprinted with permission from [93].

The proposed IM-based selection mechanism for hybrid FSO-*mm*Wave systems is described hereafter. The serial information bits to be transmitted are divided into modulation blocks, where the length of each block is $\ell = 1 + \log_2(M)$, and M denotes the PSK modulation order (M-PSK).

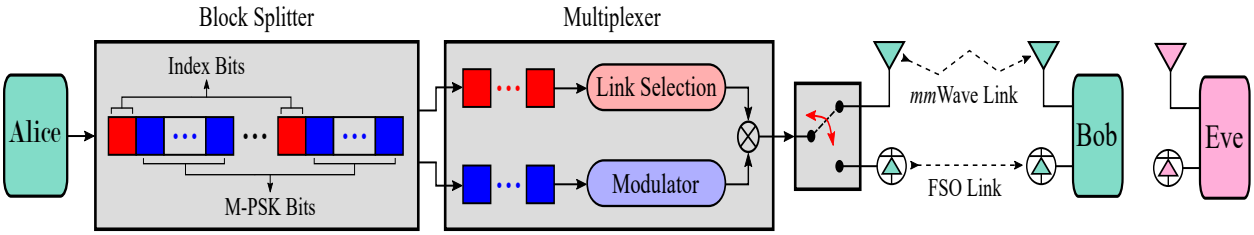


Figure 3.2: Block diagram of the proposed IM-based link selection mechanism in the presence of an eavesdropper.

Then, the transmitted block at each transmission time is

$$B = \Big[\underbrace{b_1}_{1}, \underbrace{b_2, \ldots, b_\ell}_{\log_2(M)} \Big]_{1\times\ell}. \tag{3.6}$$

In the proposed selection mechanism, the first bit of each block, b_1, that determines which link is to be activated, is an also information bit. Notice that T_x has no pre-information about the channel state information at this time instance, therefore, information bit itself determines the value of b_1. Then, a decision function, $\mathcal{D}(\cdot)$, comes up with a binary decision $\mathcal{D}(b_1) \in \{0, 1\}$ representing the activated link. Thereby, the selection process for the activation is

$$\mathcal{D}_i = \begin{cases} \text{FSO}, & \text{if } \ b_1 = 0, \\ mm\text{Wave}, & \text{if } \ b_1 = 1, \end{cases}. \tag{3.7}$$

The remaining bits of each block, $\big[b_2, \ldots, b_\ell\big]$, are modulated to generate a symbol that is transmitted through the activated link. Therefore, the transmitted signals, x_o and x_f, from both links can

be formulated as

$$(x_o, x_f) = \begin{cases} \begin{cases} x_o \text{ as defined in (3.2)}, \\ x_f \ = 0, \end{cases} & \text{if } \ b_1 = 0, \\ \begin{cases} x_o \ = 0, \\ x_f \text{ as defined in (3.4)}, \end{cases} & \text{if } \ b_1 = 1, \end{cases} . \tag{3.8}$$

Consequently, the received signals at Bob, y_o and y_f, from both links can be formulated as

$$(y_o, y_f) = \begin{cases} \begin{cases} y_o \ = \ \eta I_r I x_o + w_o, \\ y_f \ = \ w_f, \end{cases} & \text{if } \ b_1 = 0, \\ \begin{cases} y_o \ = \ w_o, \\ y_f \ = \ \sqrt{P_r} H x_f + w_f, \end{cases} & \text{if } \ b_1 = 1, \end{cases} . \tag{3.9}$$

Likewise, the received signals at Eve, $y_{o,e}$ and $y_{f,e}$, from both links can be formulated as

$$(y_{o,e}, y_{f,e}) = \begin{cases} \begin{cases} y_{o,e} \ = \ \eta I_r I_e x_o + w_o, \\ y_{f,e} \ = \ w_f, \end{cases} & \text{if } \ b_1 = 0, \\ \begin{cases} y_{o,e} \ = \ w_o, \\ y_{f,e} \ = \ \sqrt{P_r} H_e x_f + w_f, \end{cases} & \text{if } \ b_1 = 1, \end{cases} . \tag{3.10}$$

At the R_x end, maximum lilelihood (MLi) detection is performed to decode the transmitted blocks over both the FSO and *mm*Wave links due to its efficiency and numerical stability against the multiple channel transmission systems [112]. Notice that R_x has no predetermined information about the link activation at this time instance, therefore, the receiver needs to perform a joint

estimation of the activated link and the modulated symbol using MLi detection as follows

$$\hat{i} = \min\left\{\hat{i}_f, \hat{i}_o\right\}, \tag{3.11}$$

where $\hat{i}_f$ and $\hat{i}_o$ are, in turn, expressed as

$$\hat{i}_o = \underset{i\in[0,2M-1]}{\arg\min} \left|y_o - \eta I_r I x_o^{(i)}\right|^2 + |y_f|^2, \tag{3.12}$$

$$\hat{i}_f = \underset{i\in[0,2M-1]}{\arg\min} |y_o|^2 + \left|y_f - \sqrt{P_r} H x_f^{(i)}\right|^2, \tag{3.13}$$

where $|\cdot|^2$ is the squared norm operator, and $x_o^{(i)}$ and $x_f^{(i)}$ represent the corresponding transmitted signals (computed by (3.2) and (3.4)), if the transmitted bit block is the binary representation of i. The detected integer $\hat{i} \in [0, 2M-1]$ is converted to binary form to retrieve the transmitted block.

3.4.1 Example

This section provides a simple example to explain the proposed selection mechanism. Assuming that $M = 2$ (BPSK) is adopted at T_x, the transmitted data are grouped into two-bit blocks. A two-bit block has 4 different states, 00, 01, 10 and 11, as shown in Table 3.1. Following the proposed IM-based link selection mechanism, the first bit of the transmitted block determines which link is to be activated. Since the first bit of the transmitted block is an information bit, the proposed IM-based link selection is a data-driven algorithm. Notice that in the proposed mechanism, there is no feedback or channel-state-information required at the transmitter side at this time instance. As such, for the first two blocks in Table 3.1, i.e., 00 and 01, the FSO link is activated while the RF link will not be used. Similarly, for the other two blocks, i.e., 10 and 11, only the RF link will be activated. The rest of the transmitted block, a single bit in this example, is modulated using the BPSK modulator and sent over the activated link.

It is worth noting that, in this example, two bits are being sent at each transmission time over a single link using BPSK modulation. Using a single link should be more power-efficient than activating both links. Moreover, one more bit is conveyed without being modulated, which should

Table 3.1: An example of the proposed selection mechanism for BPSK. Reprinted with permission from [93].

Two-bit Blocks	IM Bits	Modulated Bits	Active Link
00	0	0	FSO
01	0	1	FSO
10	1	0	*mm*Wave
11	1	1	*mm*Wave

be more spectrally efficient.

3.5 CSI-based Precoding

A security level is provided by applying a precoding on the transmitted signal based on CSIs, which further enhances the secrecy robustness against eavesdroppers. Prior to the transmission, signal are multiplexed by the precoding vector of the active link. The precoding vector is determined as follows

$$P_c = \begin{cases} \frac{1}{\widetilde{I}}, & \text{if } b_1 = 0, \\ \frac{\widetilde{H}^*}{|H^2|}, & \text{if } b_1 = 1, \end{cases}, \tag{3.14}$$

where $\widetilde{X}$ stands for the estimated versions of X, and X^* depicts the complex conjugate of X. Similar to the equation (3.9), the received secure signals, $y_{s,o}$ and $y_{s,f}$, from both links can be formulated as

$$(y_{s,o}, y_{s,f}) = \begin{cases} \begin{cases} y_{s,o} &= \eta I_r \frac{I}{\widetilde{I}} x_o + w_o, \\ y_{s,f} &= w_f, \end{cases} & \text{if } b_1 = 0, \\ \begin{cases} y_{s,o} &= w_o, \\ y_{s,f} &= \sqrt{P_r} \frac{\widetilde{H}^* H}{|\widetilde{H}^2|} x_f + w_f, \end{cases} & \text{if } b_1 = 1, \end{cases} . \tag{3.15}$$

3.5.1 FSO Eavesdropper

FSO-type of eavesdropper is described in section 2.4.1.1. This type eavesdropper can only wiretap on the FSO link and has no power to attack on the data transmitted over the *mm*Wave link. Therefore, FSO-Eve needs to obtain two quantities. First is the estimated version of the CSI for the FSO link between legitimate transmitter Alice and Eve, denoted by $\widetilde{I}_e$. Second is the estimated version of the CSI for the FSO link between legitimate transmitter Alice and receiver Bob (i.e., I), denoted by $\widetilde{I}_{ab,e}$.

Since eavesdropper also employs an MLi receiver, each transmitted symbol will be detected over the FSO link and will tried to be decoded as follows

$$\hat{i}_o = \underset{i\in[0,2M-1]}{\arg\min} \left| y_{o,e} - \eta I_{r,e} \frac{\widetilde{I}_e}{\widetilde{I}_{ab,e}} x_o^{(i)} \right|^2, \tag{3.16}$$

where $y_{o,e}$ is expressed as

$$y_{o,e} = \eta I_{r,e} \frac{I_e}{\widetilde{I}} x_o + w_{o,e}, \tag{3.17}$$

where $w_{o,e}$ is the AWGN at Eve with zero mean and variance σ_e^2, i.e., $w_{o,e} \sim \mathcal{N}(0,\, \sigma_e^2)$.

3.5.2 RF Eavesdropper

RF-type of eavesdropper is described in section 2.4.1.2. This type eavesdropper can only wiretap on the *mm*Wave link and has no power to attack on the data transmitted over the RF link. Thus, RF-Eve also needs to obtain two quantities. First is the estimated version of the CSI for the RF link between legitimate transmitter Alice and Eve, denoted by $\widetilde{H}_e$. Second is the estimated version of the CSI for the RF link between legitimate transmitter Alice and receiver Bob (i.e., H), denoted by $\widetilde{H}_{ab,e}$.

Since eavesdropper also employs an MLi receiver, each transmitted symbol will be detected over the RF link and will tried to be decoded as follows

$$\hat{i}_f = \underset{i\in[0,2M-1]}{\arg\min} \left| y_{f,e} - \sqrt{P_{r,e}} \frac{\widetilde{H}_{ab,e}^* \widetilde{H}_e}{\widetilde{H}_{ab,e}} x_f^{(i)} \right|^2, \tag{3.18}$$

where $y_{f,e}$ is expressed as

$$y_{f,e} = \sqrt{P_{r,e}} \frac{\widetilde{H}^* H_e}{|\widetilde{H}^2|} x_f + w_{f,e}, \tag{3.19}$$

$w_{f,e}$ depicts the complex AWGN at Eve with $\mathcal{CN}(0,\, 2\sigma^2)$, of the form $w_{f,e} = w_{f,e}^I + \jmath w_{f,e}^Q$ with both $w_{f,e}^I$ and $w_{f,e}^Q$ being $\mathcal{N}(0,\, \sigma_e^2)$.

3.5.3 Hybrid Eavesdropper

Hybrid-type of eavesdropper is described in section 2.4.1.3. In contrast to FSO- and RF-Eves, this type eavesdropper can wiretap on the data transmitted over both FSO and *mm*Wave link. Hybrid-Eve is more powerful than others, however, it needs to estimate all available CSI, i.e., $\widetilde{I}_e$, $\widetilde{I}_{ab,e}$, $\widetilde{H}_e$ and $\widetilde{H}_{ab,e}$. Therefore, hybrid-eve needs to perform a joint estimation using MLi detection as follows

$$\hat{i} = \min\left\{\hat{i}_f, \hat{i}_o\right\}, \tag{3.20}$$

where $\hat{i}_f$ and $\hat{i}_o$ are, in turn, expressed as

$$\hat{i}_o = \underset{i\in[0,2M-1]}{\arg\min} \left| y_{o,e} - \eta I_{r,e} \frac{\widetilde{I}_e}{\widetilde{I}_{ab,e}} x_o^{(i)} \right|^2 + |y_{f,e}|^2, \tag{3.21}$$

$$\hat{i}_f = \underset{i\in[0,2M-1]}{\arg\min} |y_{o,e}|^2 + \left| y_{f,e} - \sqrt{P_{r,e}} \frac{\widetilde{H}_{ab,e}^* \widetilde{H}_e}{\widetilde{H}_{ab,e}} x_f^{(i)} \right|^2, \tag{3.22}$$

where $y_{o,e}$ and $y_{f,e}$ are defined in (3.17) and (3.19), respectively.

3.6 Performance Analysis

In this section, analytical expressions for the average BER, asymptotic BER, outage probability, and ergodic capacity of the proposed IM-based system are derived in terms of closed-form expressions.

3.6.1 Average Bit-Error-Rate

The average pairwise error probability (PEP) is defined as the probability that the block k is detected given that the block q is transmitted, where $\{k, q\} \in [0, 2M-1]$ represent the decimal

values of the transmitted bit blocks. The average PEP, denoted by PEP_{kq} can be formulated as

$$\text{PEP}_{kq} = \text{Prob.}\Bigg\{ \left(\left| y_o - \eta I_r I x_o^{(q)} \right|^2 + \left| y_f - \sqrt{P_r} H x_f^{(q)} \right|^2 \right) > \left(\left| y_o - \eta I_r I x_o^{(k)} \right|^2 + \left| y_f - \sqrt{P_r} H x_f^{(k)} \right|^2 \right\} \Bigg). \quad (3.23)$$

As $(x_o^{(q)}, x_f^{(q)})$ have been transmitted, the above equation can be simplified to

$$\text{PEP}_{kq} = \text{Prob.}\Bigg\{ \left(|w_o|^2 + |w_f|^2 \right) > \left(|w_o - \eta I_r I \Delta_o|^2 + \left| w_f - \sqrt{P_r} H \Delta_f \right|^2 \right) \Bigg\}, \quad (3.24)$$

where $\Delta_o = x_o^{(q)} - x_o^{(k)}$ and $\Delta_f = x_f^{(q)} - x_f^{(k)}$. By expanding the squared norms at the right hand side of the probability above and canceling the identical terms, it can be re-written as

$$\text{PEP}_{kq} = \text{Prob.}\Bigg\{ \left(2\Re\{ w_o \eta I_r I \Delta_o + w_f \sqrt{P_r} H \Delta_f \} \right) > \left(|\eta I_r I \Delta_o|^2 + \left| \sqrt{P_r} H \Delta_f \right|^2 \right) \Bigg\}. \quad (3.25)$$

This can be expressed by the Q-function for a given H and I as

$$\text{PEP}_{kq/H,I} = Q\left(\sqrt{\frac{|\eta I_r I \Delta_o|^2 + \left| \sqrt{P_r} H \Delta_f \right|^2}{2\sigma^2}} \right), \quad (3.26)$$

which can be further expressed using the alternative formula of the Q-function, aka Craig formula [113], as

$$\text{PEP}_{kq/H,I} = \frac{1}{\pi} \int_0^{\frac{\pi}{2}} \exp\left(-\frac{\varphi_o |I|^2 + \varphi_f |H|^2}{4\sigma^2 \sin^2\theta} \right) \cdot d\theta, \quad (3.27)$$

where $\varphi_o = |\eta I_r \Delta_o|^2$, $\varphi_f = \left| \sqrt{P_r} \Delta_f \right|^2$. The average value of (3.27) can be computed by performing integrations over the PDF of H and I as given in (1.6) and (1.15)

$$\text{PEP}_{kq} = \frac{1}{\pi} \int_0^{\infty} \int_0^{\infty} \int_0^{\frac{\pi}{2}} \exp\left(-\frac{\varphi_o |I|^2 + \varphi_f |H|^2}{4\sigma^2 \sin^2\theta} \right) f_I(I) f_{|H|^2}(|H|^2) \cdot d\theta \, dI \, d|H|^2. \quad (3.28)$$

This integral can be solved in a closed form expression as shown in (3.29), where the derivation is detailed in A along with the definition of χ, A'_T, and c'.

$$\text{PEP}_{kq} = \begin{cases} \chi^m \sum_{t=0}^{m-1} \binom{m-1+t}{t} (1-\chi)^t, & \text{for } \Delta_o = 0 \ \& \ \Delta_f \neq 0, \\ \frac{\xi}{8\pi} \left(\frac{\varphi_o}{4\sigma^2}\right)^{\frac{-\mu}{2}} H_{4,4}^{3,3}\left(c' \middle| \begin{matrix} (\frac{1}{2}-\frac{\mu}{2},\frac{1}{2}),(\frac{1}{2},0),(1-\frac{\mu}{2},\frac{1}{2}),(0,1) \\ (\frac{\beta-\alpha}{2},1),(\frac{\alpha-\beta}{2},1),(\frac{\alpha-\beta}{2},1),(0,1),(\frac{-\mu}{2},\frac{1}{2}) \end{matrix} \right), & \text{for } \Delta_o \neq 0 \ \& \ \Delta_f = 0, \\ \frac{\xi}{8\pi} \sum_{t=0}^{\infty} A'_t H_{4,4}^{3,3}\left(c' \middle| \begin{matrix} (\frac{1}{2}-m-t-\frac{\mu}{2},\frac{1}{2}),(\frac{1}{2},0),(1-\frac{\mu}{2},\frac{1}{2}),(0,1) \\ (\frac{\beta-\alpha}{2},1),(\frac{\alpha-\beta}{2},1),(0,1),(-m-t-\frac{\mu}{2},\frac{1}{2}) \end{matrix} \right), & \text{for } \Delta_o \neq 0 \ \& \ \Delta_f \neq 0. \end{cases} \tag{3.29}$$

The average BER can be approximated using the union bounding technique

$$\text{BER} \approx \frac{1}{2^B} \sum_{p=1}^{2^B} \sum_{q=1}^{2^B} \frac{\tau_{pq}}{B} \text{PEP}_{kq}, \tag{3.30}$$

where τ_{pq} is the Hamming distance between the transmitted blocks p and q, and PEP_{kq} is substituted from (3.29).

3.6.2 Asymptotic Bit-Error-Rate

To compute the asymptotic BER, we first need to calculate the asymptotic PEP_{kq}. We start from the PDF of the FSO channel given in (1.15), where the Bessel function of the second kind can be approximated for small arguments by [114]

$$K_{\alpha-\beta}(2\sqrt{\alpha\beta I}) \approx \frac{|\alpha-\beta|}{2} \left(\frac{1}{\sqrt{\alpha\beta I}}\right)^{|\alpha-\beta|}. \tag{3.31}$$

Therefore, the PDF of the FSO link given in (1.15) can be approximated as

$$f_I(I) \approx \overline{\xi} I^{\beta-1}, \tag{3.32}$$

where $\overline{\xi} = \frac{(\alpha\beta)^{\beta}\Gamma(\alpha-\beta)}{\Gamma(\alpha)\Gamma(\beta)}$, and $\alpha > \beta$ for a practical GG atmospheric-turbulence channel model [115].

On the other hand, the PDF of the *mm*Wave link given in (1.6) can be approximated as [116]

$$f_{|H|^2}(\gamma) \approx \frac{m^m}{\Gamma(m)} \gamma^{m-1}. \tag{3.33}$$

Further, using (3.32) and (3.33) into (3.28), a closed form expression of asymptotic PEP can be obtained as given in (3.35), where the derivation is presented in B.

The asymptotic BER can be computed using the union bounding technique to be

$$\text{BER}^{\text{Asym}} \approx \frac{1}{2^B} \sum_{p=1}^{2^B} \sum_{q=1}^{2^B} \frac{\tau_{pq}}{B} \text{PEP}_{kq}^{\text{Asym}}, \tag{3.34}$$

where $\text{PEP}_{kq}^{\text{Asym}}$ can be substituted from (3.35), given as

$$\text{PEP}_{kq}^{\text{Asym}} = \begin{cases} \dfrac{m^m}{2} \left(\dfrac{P_r \left|\Delta_f\right|^2}{4\sigma^2} \right)^{-m}, & \text{for } \Delta_o = 0 \ \& \ \Delta_f \neq 0, \\ \dfrac{\overline{\xi}}{4} \Gamma\left(\dfrac{\beta}{2}\right) \left(\dfrac{\eta^2 (I_r)^2 \left|\Delta_o\right|^2}{4\sigma^2} \right)^{\frac{-\beta}{2}}, & \text{for } \Delta_o \neq 0 \ \& \ \Delta_f = 0, \\ m^m \dfrac{\overline{\xi}}{4} \Gamma\left(\dfrac{\beta}{2}\right) \left(\dfrac{P_r \left|\Delta_f\right|^2}{4\sigma^2} \right)^{-m} \left(\dfrac{\eta^2 (I_r)^2 \left|\Delta_o\right|^2}{4\sigma^2} \right)^{-\frac{\beta}{2}}, & \text{for } \Delta_o \neq 0, \Delta_f \neq 0. \end{cases} \tag{3.35}$$

3.6.3 Outage Probability

Outage probability is defined as the probability that information rate is less than the required threshold information rate

$$P_{\text{OUT}} = \text{Prob.}\left\{h_o\right\} \times \text{Prob.}\left\{\log_2(1+\gamma_o) < \mathcal{R}_o\right\} + \text{Prob.}\left\{h_f\right\} \times \text{Prob.}\left\{\log_2(1+\gamma_f) < \mathcal{R}_f\right\}, \tag{3.36}$$

where Prob. $\{h_o\}$ = Prob. $\{h_f\} = 0.5$ denote the average link usage probabilities, and $\mathcal{R}_o$ and $\mathcal{R}_f$ depict the required threshold information rate for FSO and *mm*Wave links, respectively. Then, (3.36) can be re-written as

$$P_{\text{OUT}} = \frac{1}{2}\left[\text{Prob.}\left\{\gamma_o < 2^{\mathcal{R}_o} - 1\right\} + \text{Prob.}\left\{\gamma_f < 2^{\mathcal{R}_f} - 1\right\}\right]. \tag{3.37}$$

Therefore, the outage probability can be expressed in terms of CDFs as

$$P_{\text{OUT}} = \frac{1}{2}\left[F_{\gamma_o}\left(\sqrt{\frac{2^{\mathcal{R}_o}-1}{\overline{\gamma}_o}}\right) + F_{\gamma_f}\left(\sqrt{\frac{2^{\mathcal{R}_f}-1}{\overline{\gamma}_f}}\right)\right]. \tag{3.38}$$

Finally, the outage probability can be expressed as

$$P_{\text{OUT}} = \frac{1}{2}\left[\frac{1}{\Gamma(\alpha)\Gamma(\beta)} G_{1,3}^{2,1}\left(\alpha\beta\sigma\frac{\sqrt{2^{\mathcal{R}_o}-1}}{\eta I_t L_o}\middle| \begin{matrix} 1 \\ \alpha, \beta, 0 \end{matrix}\right) + \frac{1}{\Gamma(m)}\Gamma\left(m, m\sigma^2\frac{2^{\mathcal{R}_f}-1}{P_t L_f}\right)\right]. \tag{3.39}$$

Additionally, the asymptotic outage probability can be obtained by approximating the CDFs of the FSO and *mm*Wave links. An approximation for the CDF of the FSO link can be calculated by using (3.32)

$$F_I(i) \approx \overline{\xi}\int_0^i i^{\beta-1}\cdot di. \tag{3.40}$$

Then, the resultant integral can be solved as

$$F_I(i) \approx \frac{\overline{\xi}}{\beta} i^{\beta}. \tag{3.41}$$

The CDF of the *mm*Wave link can be obtained by approximating the lower incomplete Gamma function as [117]

$$F_H(\gamma) \approx \frac{1}{\Gamma(m+1)} \left(m\gamma^2\right)^m. \tag{3.42}$$

Therefore, the asymptotic outage probability can be computed by substituting (3.41) and (3.42) into (3.38) resulting in

$$P_{\text{OUT}}^{\text{Asym}} \approx \frac{1}{2}\left[\frac{\overline{\xi}}{\beta}\sqrt[\beta]{\frac{2^{\mathcal{R}_o}-1}{\overline{\gamma}_o}} + \frac{1}{\Gamma(m+1)}\left(m\frac{2^{\mathcal{R}_f}-1}{\overline{\gamma}_f}\right)^m\right]. \tag{3.43}$$

Finally, the the asymptotic outage probability can be expressed as

$$P_{\text{OUT}}^{\text{Asym}} \approx \frac{1}{2}\left[\frac{\overline{\xi}}{\beta}\left(\sigma\frac{\sqrt{2^{\mathcal{R}_o}-1}}{\eta I_t L_o}\right)^{\beta} + \frac{1}{\Gamma(m+1)}\left(m\sigma^2\frac{2^{\mathcal{R}_f}-1}{P_t L_f}\right)^m\right]. \tag{3.44}$$

3.6.4 Ergodic Capacity

The overall channel capacity of the system can be expressed as weighted average of the capacities of the FSO and *mm*Wave links

$$C = \frac{1}{2}(C_o + C_f), \tag{3.45}$$

where C_o and C_f denote the instantaneous channel capacities of the FSO and *mm*Wave links, respectively. According to Shannon's theory, the ergodic capacity of the fading channel can be

expressed as

$$C = \frac{1}{2}B\bigg[\int_0^\infty \log_2(1+\gamma_o)p(\gamma_o)\cdot d\gamma_o + \int_0^\infty \log_2(1+\gamma_f)p(\gamma_f)\cdot d\gamma_f\bigg]. \tag{3.46}$$

The channel capacity for FSO link can be expressed as

$$C_o = \frac{2(\alpha\beta)^{(\alpha+\beta)/2}}{\Gamma(\alpha)\Gamma(\beta)}\frac{1}{\ln(2)}\int_0^\infty \ln(1+\gamma_o)\gamma_o^{\frac{\alpha+\beta}{2}-1}K_{\alpha-\beta}(2\sqrt{\alpha\beta\gamma_o})\cdot d\gamma_o, \tag{3.47}$$

where the terms $\ln(1+\gamma_o)$ and $K_{\alpha-\beta}(2\sqrt{\alpha\beta\gamma_o})$ can be expressed in terms of the Meijer's G-function [118, (11)-(14)]. Then, (3.47) can be re-written as

$$C_o = \frac{(\alpha\beta)^{(\alpha+\beta)/2}}{\Gamma(\alpha)\Gamma(\beta)}\frac{1}{\ln(2)}\int_0^\infty (i^2)^{\frac{\alpha+\beta}{2}-1}G_{0,2}^{2,0}\left(\alpha\beta i^2\middle|\begin{matrix}\\ \frac{\alpha-\beta}{2},\frac{\alpha-\beta}{2}\end{matrix}\right)G_{2,2}^{1,2}\left(\overline{\gamma}_o i^2\middle|\begin{matrix}1,1\\1,0\end{matrix}\right)\cdot di^2. \tag{3.48}$$

After a simple power transformation of the random variable in order to achieve a linear relation and using [83, (2.24.1-1)], a closed-form expression of C_o can be derived as

$$C_o = \frac{1}{\ln(2)\Gamma(\alpha)\Gamma(\beta)}G_{4,2}^{1,4}\left(\frac{\overline{\gamma}_o}{\alpha\beta}\middle|\begin{matrix}1,1,1-\alpha,1-\alpha\\1,0\end{matrix}\right). \tag{3.49}$$

The channel capacity for the *mm*Wave link can be expressed as

$$C_f = \frac{m^m}{\Gamma(m)}\frac{1}{\ln(2)}\int_0^\infty \ln(1+\gamma_f)\gamma_f^{m-1}\exp\left(-m\gamma_f\right)\cdot d\gamma_f, \tag{3.50}$$

where the logarithm term $\ln(1+\gamma_f)$ can be expressed in terms of the Meijer's G-function [118, (11)]. Then, (3.50) can be re-written as

$$C_f = \frac{m^m}{\Gamma(m)}\frac{1}{\ln(2)}\int_0^\infty (|h|^2)^{m-1}\exp\left(-m|h|^2\right)G_{2,2}^{1,2}\left(\overline{\gamma}_f|h|^2\middle|\begin{matrix}1,1\\1,0\end{matrix}\right)\cdot d|h|^2. \tag{3.51}$$

After a simple power transformation of the random variable in order to achieve a linear relation and using [82, (7.813-1)], a closed-form expression of C_f can be derived as

$$C_f = \frac{1}{\ln(2)\Gamma(m)} G_{3,2}^{1,3}\left(\frac{\overline{\gamma}_f}{m} \middle| \begin{matrix} 1-m, 1, 1 \\ 1, 0 \end{matrix} \right). \tag{3.52}$$

Finally, by combining (3.49) and (3.52) into (3.45), the ergodic capacity of the system can be expressed as

$$C = \frac{1}{2}\left[\frac{1}{\ln(2)\Gamma(\alpha)\Gamma(\beta)} G_{4,2}^{1,4}\left(\frac{\overline{\gamma}_o}{\alpha\beta} \middle| \begin{matrix} 1, 1, 1-\alpha, 1-\alpha \\ 1, 0 \end{matrix} \right) + \frac{1}{\ln(2)\Gamma(m)} G_{3,2}^{1,3}\left(\frac{\overline{\gamma}_f}{m} \middle| \begin{matrix} 1-m, 1, 1 \\ 1, 0 \end{matrix} \right) \right]. \tag{3.53}$$

3.7 Results and Discussion

In this section, Monte Carlo simulations and theoretical verification are presented to evaluate performance of the proposed hybrid FSO-*mm*Wave system. Specifically, the impact of different physical layer parameters on the performance of the proposed IM-based link selection mechanism is discussed. Note that Monte Carlo simulations are made through MATLAB® software in which random bits are generated using a random number generator with a predefined seed. The generated information bits are, firstly, divided into transmit blocks based on the modulation order, as defined in (3.6). The first bit of each modulation block determines which link to be activated, and the remaining bits are modulated to symbols. Then, the modulated symbols are sent over the FSO or *mm*Wave links that are determined by the first bit of the corresponding modulation block. At the receiver side, MLi detection is performed to jointly decode the transmitted blocks over both links, as given (3.11). Once the transmitted blocks are retrieved, the statistics are, finally, obtained for performance evaluation. Additionally, results of the conventional threshold-based selection mechanism [95] are also presented as a benchmark. Comparison results include various scenarios including different spectral efficiencies, link distances, and weather conditions.

Recall that in the threshold-based selection mechanism [95] the FSO link has priority unless its SNR falls below a predefined threshold, denoted by γ_{th}, in which case it switches to the *mm*Wave link. The received SNR of the FSO link is checked every L transmission symbols, called a feedback period. The impact of both γ_{th} and L will be investigated later in this section.

A comparison of the average BER against the average SNR is illustrated in Fig. 3.3 for the proposed IM-based and threshold-based selection mechanisms with different spectral efficiencies, $S = 2$, 3, 4, and 5 bps/Hz, over a distance of $2.5\,\text{km}$ in hazy atmospheric conditions. In the figure, theoretical and asymptotic BER curves are obtained using (3.30) and (3.34), respectively. The turbulence parameters are calculated as $\alpha = 3.2018$, and $\beta = 2.9275$, while the Nakagami-m parameter is set to 1. Here, the values of α and β are obtained using (1.16) and (1.17) based on the parameters in Table 1.1 and 1.2, and link distance. The proposed mechanism shows much better BER performance at all spectral efficiencies considered. For instance, at BER of 10^{-4}, the SNR gain of the proposed mechanism is 5, 6, 7 and 7.5 dB for $S = 2$, 3, 4 and 5 bps/Hz, respectively, compared to the threshold-based mechanism. The reason behind such an improvement is that the use of the IM mechanism exploits link selection to increase spectral efficiency thereby lowering modulation order.

Fig. 3.4 presents the comparison of average BER performance against the link distance for a fixed value of noise power $3 \times 10^{-11}\,\text{A}^2$ with 3 bps/Hz in moderate rain conditions. The turbulence parameters, α and β, change depending on the link distance. As seen from the figure, the proposed system provides lower BER than the conventional system. For example, assuming the forward error correction (FEC) limit to be 10^{-3}, the threshold-based system is able to satisfy this limit at a link distance around $2.1\,\text{km}$, while the proposed system approximately provides $2.6\,\text{km}$ which is about $500\,\text{m}$ longer.

In Fig. 3.5, the proposed mechanism is compared to the conventional threshold-based mechanism at different values of L with $4\,\text{bps/Hz}$ spectral efficiency over a distance of $1.75\,\text{km}$ in clean air atmospheric conditions. The turbulence parameters are calculated as $\alpha = 2.9846$, and $\beta = 2.5254$. The threshold γ_{th} is set to $10\,\text{dB}$, and the feedback period is varied among $L = 1$, 100, 200 and

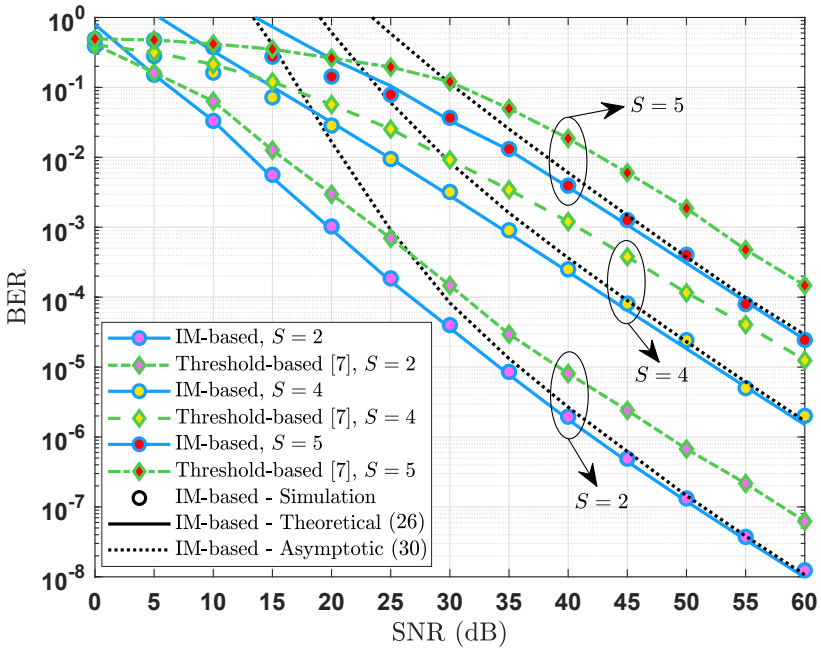


Figure 3.3: The average BER versus average SNR for the proposed IM-based scheme and threshold-based mechanisms at different spectral efficiencies. (Haze, $d = 2.5\,\text{km}$, $\gamma_{\text{th}} = 15\,\text{dB}$, and $L = 150$ symbols). Reprinted with permission from [93].

300 symbols. As is seen from the figure and as expected, an increment in period L decreases the BER performance of the conventional threshold-based mechanism. The main reason is that frequently checking the instantaneous SNR ensures the use of a higher quality link, however, as a tradeoff, this frequent control also increases the power consumption and overall complexity of the system.

Fig. 3.6 presents a comparison between the proposed IM-based and the conventional threshold-based mechanisms at different values of γ_{th} with a feedback period of 100 symbols and 4 bps/Hz spectral efficiency over a link distance of 1.5 km in moderate rain atmospheric conditions. The turbulence parameters are calculated as $\alpha = 23.9161$, and $\beta = 22.1541$. The threshold value for the conventional scheme is varied among $\gamma_{\text{th}} = 0$, 5, 10 and 15 dB. The average BER performance is degraded as the value of γ_{th} increases for the threshold-based scheme. This is due to the fact that increasing γ_{th} increases the probability to switch to the *mm*Wave link which is worse than the FSO link based on the considered scenario parameters. Also, as seen from the figure, the achievable

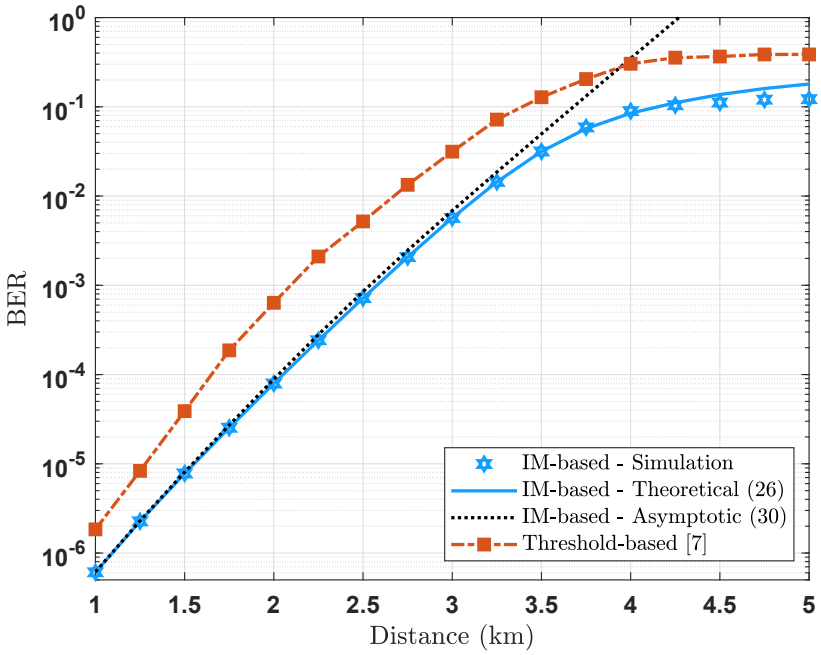


Figure 3.4: The average BER versus link distance for the proposed IM-based and threshold-based mechanisms. (Haze, $S = 3\,\text{bps/Hz}$, $\gamma_{\text{th}} = 10\,\text{dB}$, and $L = 150\,\text{symbols}$). Reprinted with permission from [93].

BER performance of the proposed mechanism is much better than the conventional mechanism.

In Fig. 3.7, the outage probability of the proposed IM-based mechanism is illustrated against the average SNR values for different information threshold rates. The link distance is set to $2.5\,\text{km}$, and a hazy weather condition is considered. The theoretical and asymptotic curves in the figure are obtained by using (3.39) and (3.44), respectively. As is seen from the figure, the outage probability decreases for all information rates considered with the increase of average SNR. An information threshold of $-5\,\text{dB}$, as expected, results in the lowest outage probability among those considered.

The ergodic capacity of the proposed IM-based scheme is presented in Fig. 3.8 against the average SNR for clear, hazy, and moderate rain weather conditions, where the theoretical curves are obtained by using (3.53). The link distance is set to $3\,\text{km}$. As is seen from the figure, the ergodic capacity increases for all weather conditions considered with the increase of average SNR. The clean air conditions, as expected, results in the highest capacity among the cases considered.

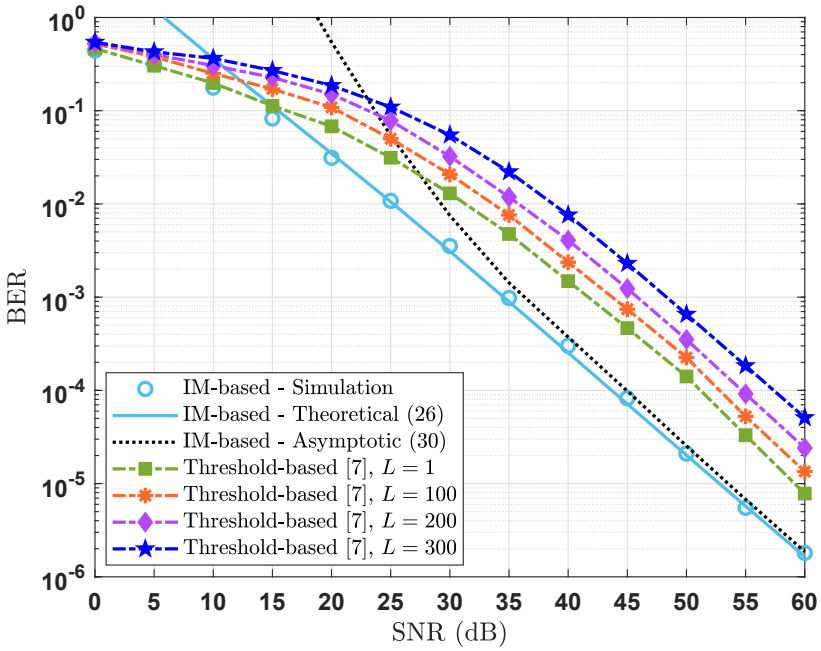


Figure 3.5: The average BER versus average SNR for the proposed IM-based scheme and conventional threshold-based scheme with different values of L. (Clean air, $S = 4\,\text{bps/Hz}$, $d = 1.75\,\text{km}$, and $\gamma_{\text{th}} = 10\,\text{dB}$). Reprinted with permission from [93].

3.8 Concluding Remarks

In this chapter, a novel selection mechanism is proposed and analyzed for hybrid FSO-*mm*Wave systems without a need for any feedback or channel state information at the transmitter side. Thus, the proposed mechanism does not suffer from high overhead and required side information at the transmitter, which automatically decreases the complexity and energy consumption. Notice that the proposed link selection mechanism is a data-driven algorithm, therefore, the link selection is made by information bits. The system takes advantage of the IM concept to activate the communication link, either FSO or *mm*Wave, at each point in time. IM uses information based link selection to maintain spectral efficiency while lowering the modulation order. Consequently, the proposed switching mechanism can be implemented with a very simple switching circuitry whose input directly connected to the first bit of each transmit block which determines the link activation. At the receiver side, maximum likelihood detection is employed to jointly detect the modulated symbol and the active link, which is, consequently, used to retrieve the whole transmitted bit block.

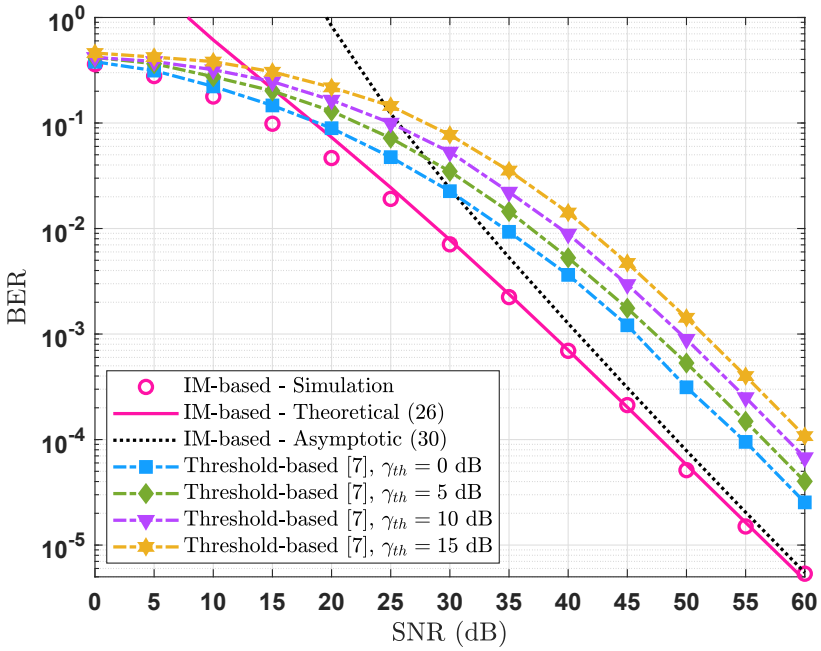


Figure 3.6: The average BER versus average SNR for the proposed IM-based scheme and conventional threshold-based scheme at different thresholds values. (Moderate Rain, $S = 4\,\mathrm{bps/Hz}$, $d = 1.25\,\mathrm{km}$, and $L = 100\,\mathrm{symbol}$). Reprinted with permission from [93].

Compared to other studies in the literature, activating only one link at a time provides lower power consumption at the transmitter side, and does not require the combining or multiplexing methods at the receiver side. The average BER, outage probability and ergodic capacity are derived in closed-form analytical expressions, and related Monte Carlo simulations are made under several scenarios including different modulation orders, link distances and weather conditions. In the light of results, it is shown that the proposed mechanism is able to outperform the threshold-based mechanism in terms of both spectral efficiency and BER under all scenarios considered.

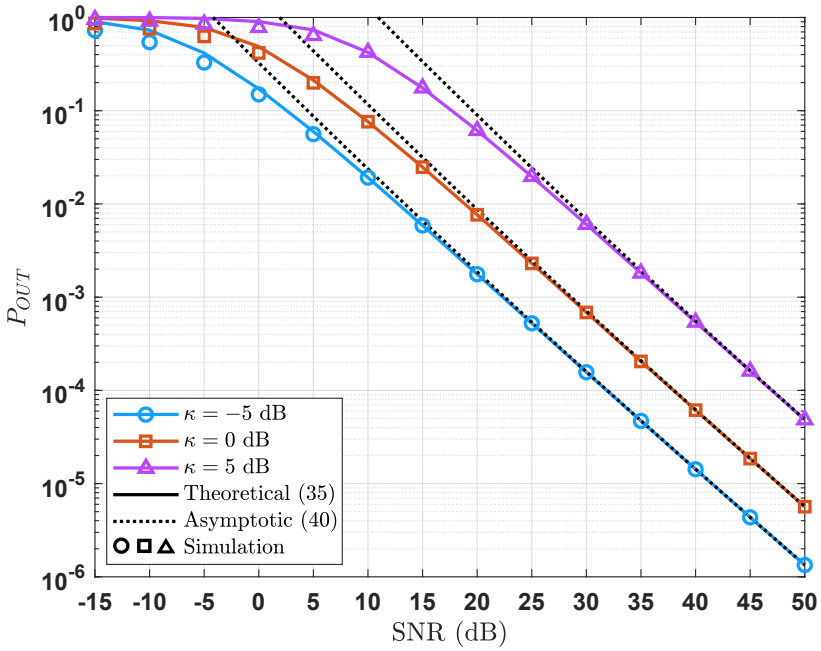


Figure 3.7: Outage probability versus average SNR for the proposed IM-based scheme at different information rates. ($\kappa = \mathcal{R}_o = \mathcal{R}_f$, Haze, and $d = 2.5\,\mathrm{km}$). Reprinted with permission from [93].

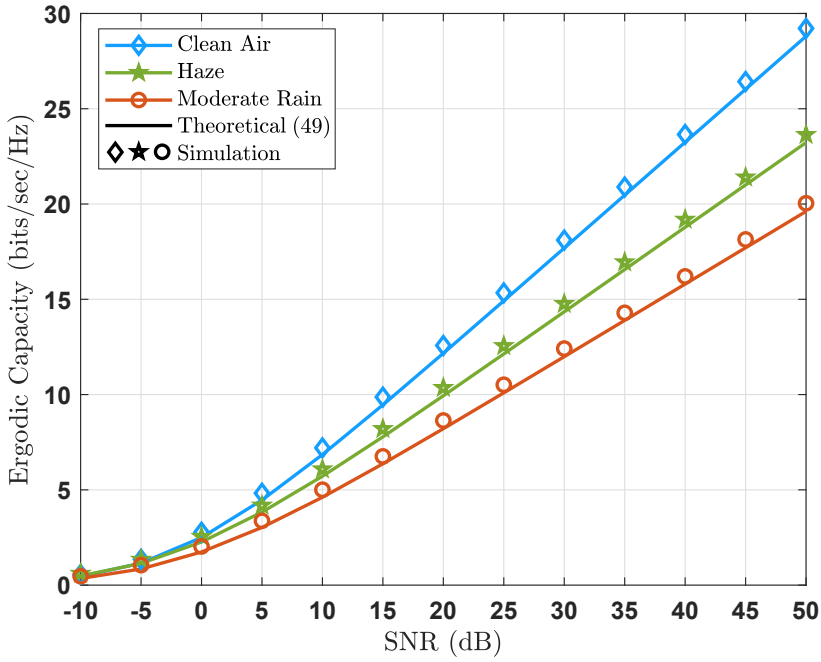


Figure 3.8: Ergodic capacity versus average SNR for the proposed IM-based scheme at different weather conditions. ($d = 3\,\mathrm{km}$). Reprinted with permission from [93].

4. DL-BASED SECRECY ENHANCEMENT OF MIMO HYBRID FSO-RF SYSTEMS

4.1 Introduction

4.1.1 Motivation

The impressive improvements in capacity performance motivates the recent interest in MIMO systems. In addition to the high gains, however, there exist a price in hardware complexity as a tradeoff. A very promising method for reducing this complexity while satisfying a reasonably large capacity of a MIMO transmission is to employ some form of antenna selection. Thus a lower number of transmitters and receivers can be employed for an optimal allocation. In this case only the best set of transmitters or receivers is used, while the remaining ones are not activated, thus reducing the number of required overall power. Therefore, in this chapter, a convolutional neural network (CNN)-based link selection schemes is provided to maximize the secrecy performance by activating the antennas and lasers at the transmitter side based on predefined configurations.

4.1.2 Related Works

The number of studies in the literature has been increased over the past few years for link selection schemes for MIMO systems [119–130], in which comprehensive analyses are presented along with related discussions and conclusions. Moreover, physical layer security area is introduced to MIMO systems taking link selection mechanisms into account [131–140], including detailed secrecy analyses for different configurations and scenarios.

Furthermore, for the first time, considering a link selection process as a multiclass-classification problem, the authors in [141] investigate the data-driven machine learning (ML) algorithms by exploiting SVM and k-nearest neighbors (k-NN). The authors also compare the learning-based antenna selection systems with a conventional system that maximizes the minimum of either the eigenvalue or the norm of channels. Hereupon, the number of studies are boosted [142–151] in which ML and deep learning (DL) techniques are employed to optimize the transmit link selection in MIMO systems.

On top of that, the authors in [152] attempt to conflate ML-based link selection in MIMO with physical layer security to enhance secrecy performance, where they propose NB-based link selection scheme. The authors consider a scenario, where the CSIs of the legitimate receiver is available to the legitimate transmitter, while the CSIs of the eavesdropper can be either known or not known. Then, in compared with the conventional antenna selection scheme, the authors show that the proposed schemes can achieve almost the same secrecy performance with a small feedback overhead. Afterwards, a deep reinforcement learning framework of deep-Q-network (DQN) is proposed in [153] to predict the optimal transmit antenna in a MIMO wiretap channel based on outdated CSI, in which the legitimate receiver captures the pilot signals radiated by each transmit antenna of legitimate transmitter, and obtains related SNRs by employing a MRC receiver, and then, uses the DQN to predict the transmitting antenna at the next moment according to these SNRs values.

Alternatively, other than antenna selection, the authors in [154–156] employ DL techniques for MIMO systems to solve precoding, uplink transmission, and beamforming problems in terms of a physical layer security perspective. For instance, in [154], a supervised DL-based novel precoding technique is introduced for MIMO systems considering Gaussian wiretap channels. It is shown that compared to traditional precoding methods, the proposed DL-based precoding is remarkably faster and reaches almost the same secrecy rate. In the presence of massive MIMO eavesdroppers, the authors in [155] adopt the uplink original symbol phase rotated (UOSPR) scheme to secure the uplink transmission for lightweight single-antenna user equipments, which randomly rotate the original information bearing symbols before they are transmitted to the base station on the uplink. In work [156], the authors propose an artificial-noise beamforming based secure transmission scheme for a full-duplex unmanned aerial vehicle (UAV) relaying scenario to combat active eavesdroppers, in which a UAV-relay equipped with multiple antennas to securely serve multiple ground users in the presence of randomly located active eavesdroppers.

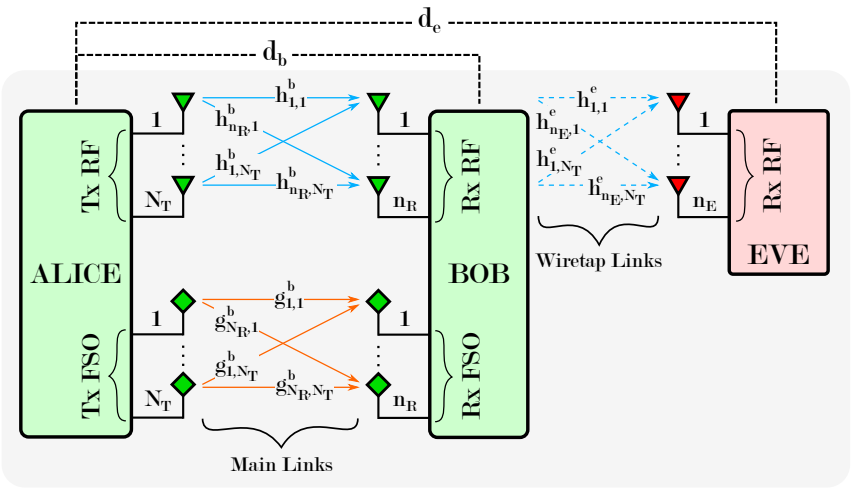
4.2 System Model

In this chapter, we consider a multiple-input multiple-output system with multi-receiver-eavesdropper (MIMOME) scenario, in which the legitimate transmitter, Alice, wants to send confidential information to the legitimate receiver, Bob, while an eavesdropper, Eve, tries to wiretap confidential information by sniffing the received signals by Bob, as illustrated in Fig. 4.1. The communication between legitimate pairs is accomplished through parallel links, namely, FSO links and RF links. It is assumed that Alice has N_T transmit antennas and N_T lasers, while Bob has n_B receive antennas and n_B photodetectors, and Eve has n_E receive antennas and n_E photodetectors. Moreover, due to the resource efficiency or availability, Alice can use only n_A $(N_T \geq n_A \geq 1)$ antennas and n_A $(N_T \geq n_A \geq 1)$ lasers at each transmission time. Consequently, to maximize the secrecy capacity, in other words, to increase the probability of having secure transmission, Alice wants to select/activate best set of n_A antennas out of $\binom{N_T}{n_A}$ and n_A lasers out of $\binom{N_T}{n_A}$ options. We also assume that all the channels are subject to identical and independent distributed (i.i.d) fading and the channel distributions are presented in the following subsection. It is worthy to note that transmitted data are divided into $\log_2(M)$ bit blocks, where M is the modulation order. Each block is modulated and emitted via each active link. To provide identical bandwidth as with the FSO links, the RF links operate over the mmWave frequency range.

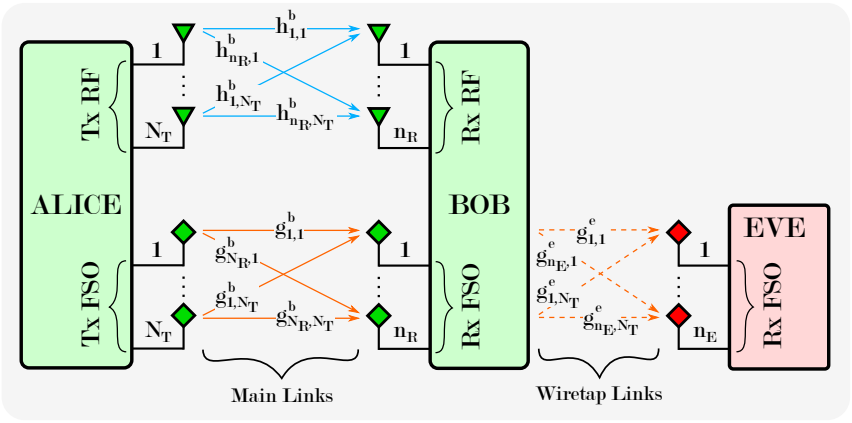
4.2.1 Channel Characteristics

A RV $\boldsymbol{H}$ is considered to denote the instantaneous RF channel power that is modeled as Nakagami-m distribution as defined in 1.1.2. Likewise, an another RV $\boldsymbol{G}$ is considered to represent the instantaneous FSO channel power that is modeled as Gamma-Gamma distribution as defined in 1.2.2. Furthermore, regarding the impact of pointing errors, we consider the most widely used misalignment model [157], called as zero boresight error model[1], in which the effects of beam width, detector size and jitter variance are taken into account, where the radial displacement

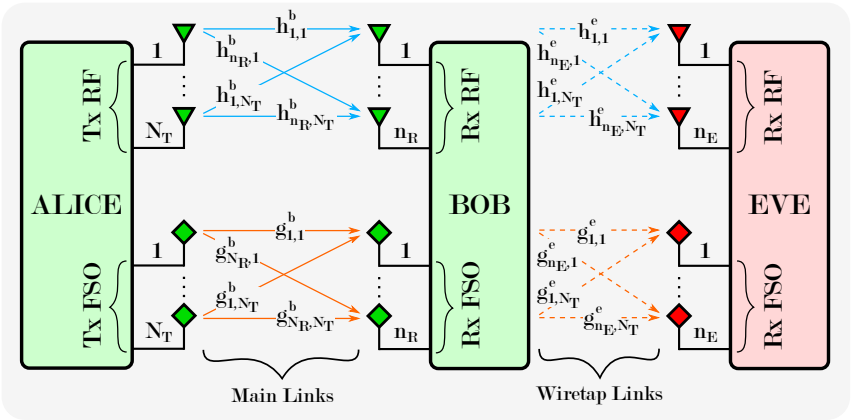
[1]It is worthy to note that the non-zero boresight error (i.e., Beckmann model) can be treated by the same PDF given in (4.1) using the approximation provided in [158].



(a)



(b)



(c)

Figure 4.1: Block diagrams of hybrid FSO-*mm*Wave multiple input multiple-output communication system between the legitimate transmitter Alice and receiver Bob in presence of different types of eavesdroppers: (a) Eve-RF, (b) Eve-FSO, and (c) Eve-Hybrid.

follows a Rayleigh distribution. Thus, the PDF of the pointing error impairment is expressed as

$$f_{P_o}(p_o) = \frac{\xi^2}{A_0^{\xi^2}} p_o^{\xi^2-1}, \tag{4.1}$$

where A_0 denotes the maximum fraction of the collected power, $\xi = \omega_{\xi eq}/2\sigma_\xi$, $\omega_{\xi eq}$ depicts the equivalent beamwidth, and σ_ξ stands for the jitters variance. Therefore, using the PDFs for turbulence fading given in (1.15) and misalignment error given in (4.1), a closed-form expression of the PDF of instantaneous FSO channel power with pointing errors is expressed as

$$f_{G_p}(g_p) = \frac{\xi^2}{g_p \Gamma(\alpha)\Gamma(\beta)} G_{1,3}^{3,0}\left(\alpha\beta \frac{g_p}{A_0} \middle| \begin{matrix} 1+\xi^2 \\ \xi^2, \alpha, \beta \end{matrix}\right), \tag{4.2}$$

where $G[\cdot]$ denotes the Meijer's G function.

4.2.2 Average Signal-to-Noise Ratios

Both Bob and Eve apply the MRC method on the received signals over FSO and RF links, where subscript $x \in \{b, e\}$ denotes the receiving side, i.e., $x = b$ for Bob, and $x = e$ for Eve. The average electrical SNRs of the RF link $\overline{\gamma}_{x,f}$ and FSO link $\overline{\gamma}_{x,o}$ are expressed in (1.21) and (1.24), respectively.

4.2.3 Eavesdropper Models

To present a fair comparison in terms of secrecy performance, we consider that the legitimate receiver Bob and eavesdropper Eve equip identical photodetectors and antennas to provide the equivalent conversion efficiency, and antenna gain.

4.2.3.1 FSO-type Eavesdropper

FSO-type of eavesdropper is described in section 2.4.1.1, where it can be described as a sensing device that collects a fraction of the optical irradiance emitted by a laser at legitimate transmitter Alice. It is worthy noting that the presence of Eve-FSO should not affect the received power at Bob. Actually, blocking the LOS between Alice and Bob or decreasing the amount of received

power at Bob makes Bob aware of the attack and, therefore, can terminate the communication for security reasons. Thus, we consider that Eve-FSO collects a fraction of the available power that is radiated by a laser at Alice.

4.2.3.2 RF-type Eavesdropper

RF-type of eavesdropper is described in section 2.4.1.2, where it can be described as a sensing device that collects a fraction of the power radiated by an antenna at Alice. It is worthy noting that the presence of Eve-RF should not affect the received power at Bob. Actually, jamming the link between Alice and Bob or decreasing the amount of received power at Bob makes Bob aware of the attack and, therefore, can stop the communication for security reasons. Thus, we consider that Eve-RF collects a fraction of the available power that is radiated by an antenna at Alice.

4.2.3.3 Hybrid-type Eavesdropper

Hybrid-type of eavesdropper is described in section 2.4.1.3, where it can be considered as multiple sensing devices that collect fractions of the power radiated by Alice over both links. In another word, Hybrid-Eve can be considered as two cooperative eavesdroppers, i.e one for RF and other one for FSO. Therefore, based on its ability and resources, this kind of eavesdropper can simultaneously wiretap both FSO and RF links. It is worthy noting that the presence of eavesdropper should not affect the received power at Bob. Actually, blocking the LoS or jamming the link between Alice and Bob, or decreasing the amount of received power at Bob makes the legitimate pair aware of the attack and, therefore, can terminate the communication for security reasons.

4.3 Secrecy Capacity

Based on (1.26), the secrecy capacity is defined as

$$C_S = \left[C_B - C_E\right]^+, \tag{4.3}$$

where C_B and C_E are the instantaneous secrecy capacities of the channels between Alice and Bob and between Alice and Eve, respectively, and are expressed as

$$C_B = \log_2\left(\det\left[\mathbf{I}_{n_B} + \frac{\overline{\gamma}_{b,o}}{n_A}\mathbf{G}_b\mathbf{G}_b^{\intercal} + \frac{\overline{\gamma}_{b,f}}{n_A}\mathbf{H}_b\mathbf{H}_b^{\dagger}\right]\right), \tag{4.4}$$

$$C_E = \begin{cases} \log_2\left(\det\left[\mathbf{I}_{n_E} + \frac{\overline{\gamma}_{e,f}}{n_A}\mathbf{H}_e\mathbf{H}_e^{\dagger}\right]\right), & \text{for RF-Eve,} \\ \log_2\left(\det\left[\mathbf{I}_{n_E} + \frac{\overline{\gamma}_{e,o}}{n_A}\mathbf{G}_e\mathbf{G}_e^{\intercal}\right]\right), & \text{for FSO-Eve,} \\ \log_2\left(\det\left[\mathbf{I}_{n_E} + \frac{\overline{\gamma}_{e,o}}{n_A}\mathbf{G}_e\mathbf{G}_e^{\intercal} + \frac{\overline{\gamma}_{e,f}}{n_A}\mathbf{H}_e\mathbf{H}_e^{\dagger}\right]\right), & \text{for Hybrid-Eve,} \end{cases} \tag{4.5}$$

where $\log_2$ is the logarithm of basis two, and $\mathbf{I}_x$ denotes the identity matrix of rank x, $\mathbf{X}^{\intercal}$ stands for the transpose of matrix $\mathbf{X}$, and $\mathbf{X}^{\dagger}$ depicts the Hermitian transpose of matrix $\mathbf{X}$. $\overline{\gamma}_{x,o}$ and $\overline{\gamma}_{x,f}$ represent the average electrical SNR of FSO and RF links, respectively, as given in (1.24) and (1.21). $\mathbf{G}_x$ and $\mathbf{H}_x$ stand for the FSO and RF channel matrices, respectively. Note that, for the sake of simplicity, we assumed a normalized bandwidth. To characterize the secure communication between Alice and Bob, we use the probabilistic metric of the SOP, defined as

$$P_{SO}(\mathcal{R}) = \text{Prob.}\big(C_S < \mathcal{R}\big), \tag{4.6}$$

which is the probability that the achievable secrecy rate is less than a target secrecy rate $\mathcal{R} > 0$. Additionally, we examine another security metric, called as EST, which is known as the average effective rate of transmitted information that can be correctly retrieved by the legitimate receiver Bob while satisfying perfect secrecy, defined as

$$E_{ST}(\mathcal{R}) = \mathcal{R}\big(1 - P_{\text{SO}}(\mathcal{R})\big). \tag{4.7}$$

4.4 Link Selection

4.4.1 Conventional Link Selection

As well-known rules of the conventional link selection scheme, the index of the selected transmitter set is obtained as [120]

$$n^* = \begin{cases} \underset{1\leq n\leq N}{\text{argmax}} \quad C_{S,n}, & \text{for Full CSI,} \\ \underset{1\leq n\leq N}{\text{argmax}} \quad C_{B,n}, & \text{for Partial CSI,} \end{cases} \tag{4.8}$$

where n^* is the index of best set of selected n_A transmit antennas and n_A lasers out of $N = \binom{N_T}{n_A}\binom{N_T}{n_A}$ options.

4.4.2 CNN-based Link Selection

In this section, the proposed CNN architecture is described as a link selection scheme, which consists of four kind of layers such as convolution (Conv), fully-connected (FC), rectified linear units (ReLU), and batch-normalization (BN). It is worthy to note that after each Conv layer, BN and FC layers are applied in turn, and in the last layer of each architecture, a softmax activation layer is used to transforms the outputs of the last FC layer into a probability distribution, and ADAM optimizer is used in all CNN architectures. The number of activations and learnable parameters are weights $\mathbf{W}$, biases $\mathbf{b}$, and scalers $\mathbf{s}$. It should be noted that the proposed architectures are achieved in an empirical way to get best accuracy by employing the Bayesian optimization method, where Conv layers, FC layers, number of filters, and initial learning rate are selected as hyperparameters.

4.4.2.1 CNN for $(N_T, n_A, n_B, n_E) = (2, 1, 1, 1)$

This CNN architecture is the simplest one since the number classes and features are 4 and 8, respectively. The input size is (4×2) for full CSI, and (2×2) for partial CSI case. In total we have 4 Conv layer, and the number of filters in each layer is 16, 32, 32, 8, respectively. Then, 2 FC layer is applied with the sizes of 32 and 4.

4.4.2.2 *CNN for* $(N_T, n_A, n_B, n_E) = (3, 1, 1, 1)$

In this CNN, we have 9 total number classes, while features and input size $\{\cdot, \cdot\}$ are $\{12, (3\times4)\}$ and $\{6, (3 \times 2)\}$ for full and partial CSI cases, respectively. In total we have 5 Conv layer, and the number of filters in each layer is 16, 32, 32, 16, 8, respectively. Then, 2 FC layer is applied with the sizes of 48 and 16.

4.4.2.3 *CNN for* $(N_T, n_A, n_B, n_E) = (4, 1, 1, 1)$

In this CNN, we have 16 total number classes, while features and input size $\{\cdot, \cdot\}$ are $\{16, (4 \times 4)\}$ and $\{8, (4 \times 2)\}$ for full and partial CSI cases, respectively. In total we have 6 Conv layer, and the number of filters in each layer is 16, 32, 32, 16, 16, respectively. Then, 2 FC layer is applied with the sizes of 48 and 16.

4.4.2.4 *CNN for* $(N_T, n_A, n_B, n_E) = (3, 2, 2, 2)$

In this CNN, we have 9 total number classes, while features and input size $\{\cdot, \cdot\}$ are $\{48, (8\times6)\}$ and $\{24, (6 \times 4)\}$ for full and partial CSI cases, respectively. In total we have 8 Conv layer, and the number of filters in each layer is 32, 32, 32, 64, 64, 32, 16, 16 respectively. Then, 3 FC layer is applied with the sizes of 32, 16, and 8.

4.4.2.5 *CNN for* $(N_T, n_A, n_B, n_E) = (4, 2, 2, 2)$

In this CNN, we have 36 total number classes, while features and input size $\{\cdot, \cdot\}$ are $\{96, (12 \times 8)\}$ and $\{48, (8 \times 6)\}$ for full and partial CSI cases, respectively. In total we have 12 Conv layer, and the number of filters in each layer is 16, 16, 32, 32, 32, 64, 64, 32, 32, 32, 16, 16 respectively. Then, 3 FC layer is applied with the sizes of 32, 16, and 16.

4.4.2.6 *Dataset Generation*

To train the proposed CNN-based link selection scheme and make a fair comparison, we create the training dataset based on CSIs, as explained in [141, 152]: (1) generate CSIs based on pre-defined scenarios, (2) specify performance indicator, and (3) label the dataset based on selected metric, i.e., index of the best set of transmitters.

Recall that the channel matrices $\mathbf{G}_x \in \mathbb{R}_{\geq 0}^{n_x \times n_A}$ and $\mathbf{H}_x \in \mathbb{C}^{n_x \times n_A}$ can be expressed as

$$\mathbf{H}_x = \begin{bmatrix} h_{11}^x & \dots & h_{1n_A}^x \\ \vdots & \ddots & \vdots \\ h_{n_x1}^x & \dots & h_{n_xn_A}^x \end{bmatrix}, \ \mathbf{G}_x = \begin{bmatrix} g_{11}^x & \dots & g_{1n_A}^x \\ \vdots & \ddots & \vdots \\ g_{n_x1}^x & \dots & g_{n_xn_A}^x \end{bmatrix}, \tag{4.9}$$

and by letting $T = 10^7$ be the number of iterations, we generate an $1 \times F$ feature vector based on channel gains for each iteration time t, denoted as $\mathbf{f}^{(t)} = [f_1^{(t)}, f_2^{(t)}, \dots, f_F^{(t)}]$, where $F = 2Nn_A(n_B + n_E)$ for full CSI case, and $F = 2Nn_An_B$ for partial CSI case

$$\begin{aligned} \mathbf{f}_{\text{Full}}^{(t)} = \Big[& g_{1,1}^{b,(t)}, \dots, g_{1,n_A}^{b,(t)}, g_{2,1}^{b,(t)}, \dots, g_{n_B,n_A}^{b,(t)}, \dots, g_{1,1}^{e,(t)}, \dots, g_{1,n_A}^{e,(t)}, g_{2,1}^{e,(t)}, \dots, g_{n_E,n_A}^{e,(t)}, \dots, \\ & \left|h_{1,1}^{b,(t)}\right|, \dots, \left|h_{1,n_A}^{b,(t)}\right|, \left|h_{2,1}^{b,(t)}\right|, \dots, \left|h_{n_B,n_A}^{b,(t)}\right|, \dots, \left|h_{1,1}^{e,(t)}\right|, \dots, \left|h_{1,n_A}^{e,(t)}\right|, \left|h_{2,1}^{e,(t)}\right|, \dots, \left|h_{n_E,n_A}^{e,(t)}\right| \Big], \end{aligned} \tag{4.10}$$

and

$$\mathbf{f}_{\text{Partial}}^{(t)} = \Big[g_{1,1}^{b,(t)}, \dots, g_{1,n_A}^{b,(t)}, g_{2,1}^{b,(t)}, \dots, g_{n_B,n_A}^{b,(t)}, \dots, \left|h_{1,1}^{b,(t)}\right|, \dots, \left|h_{1,n_A}^{b,(t)}\right|, \left|h_{2,1}^{b,(t)}\right|, \dots, \left|h_{n_B,n_A}^{b,(t)}\right| \Big], \tag{4.11}$$

where $g_{k,\ell}^{x,(t)}$ and $h_{k,\ell}^{x,(t)}$ denote the $(k,\ell)^{\text{th}}$ element of $\mathbf{G}_x^{(t)}$ and $\mathbf{H}_x^{(t)}$, respectively, where $x = b$ for Bob and $x = e$ for Eve. Then, in order to avoid bias, row based feature normalization is applied to the training dataset as follows

$$\hat{f}_\ell^{(t)} = \Big(f_\ell^{(t)} - \mu_{\mathbf{f}^{(t)}} \Big) \Big/ \Big(\max\left[\mathbf{f}^{(t)}\right] - \min\left[\mathbf{f}^{(t)}\right] \Big), \tag{4.12}$$

where $f_\ell^{(t)}$ is the ℓ^{th} element of $\mathbf{f}^{(t)}$, and $\mu_{\mathbf{x}}$ denotes the mean of vector $\mathbf{x}$. Since our aim is to maximize the capacity between legitimate pair Alice and Bob by selecting/activating the best set of transmitters, capacity metric is chosen as performance indicator. Then, in order to determine the correct label of each training vector $\mathbf{f}^{(t)}$, we calculate the index of best transmitter set that

maximizes the capacity, based on (4.8).

4.5 Results and Discussion

In this section, in order to validate the accuracy of the CNN architectures proposed in the previous section, Monte-Carlo simulations are presented along with related discussions. In particular, a detailed characterization of link selection scheme for hybrid FSO-*mm*Wave MIMO system is investigated in the presence of different types of eavesdroppers in terms of secrecy capacity, SOP and effective secrecy throughput. Additionally, results of the conventional [120], SVM-based [141], and NB-based [152] link selection mechanisms are also presented as a benchmark. The results include various scenarios including different SNRs, link distances, weather conditions, channel estimation error, pointing error, and availability of CSI.

It is worthy to note that the estimated channels, $\widetilde{\mathbf{H}}_x$ and $\widetilde{\mathbf{G}}_x$ can be modeled as

$$\begin{cases} \widetilde{\mathbf{H}}_x = \mathbf{H}_x + \mathbf{E}_{x,f}, \\ \widetilde{\mathbf{G}}_x = \mathbf{G}_x + \mathbf{E}_{x,o}, \end{cases} \tag{4.13}$$

where $\mathbf{E}_{x,f}$ and $\mathbf{E}_{x,o}$ denotes the amounts of the estimation error matrices due to channel estimation algorithm. Without loss of generality, $\mathbf{E}_{x,f}$ and $\mathbf{E}_{x,o}$ are modeled as complex and real Gaussian random variables, respectively, with zero means and $\varepsilon\sigma_x^2$ variances, where $\varepsilon \geq 0$, and $x \in \{b, e\}$.

A comparison is made in Fig. 4.2 for the proposed CNN-based link selection scheme in terms of overall/average misclassification errors. In addition, the results of SVM- and NB-based link selection schemes are presented as a benchmark. In this scenarios, the communication is carried over a distance of 0.75 km in haze atmospheric conditions with 5 dB SNR at Eve. Additionally, the perfect channel estimation error is assumed on both systems, and no pointing error is considered in FSO links. The turbulence parameters are calculated as $\alpha = 26.0860$ and $\beta = 24.0784$, while the Nakagami-m parameter is set to $m = 2$. As it is clear from the figure, we observed that the errors of SVM- and NB-based schemes increase when we use higher transmit and receive diversity orders, where the proposed CNN-based scheme remains almost the same. We consider the conventional

link selection as optimal.

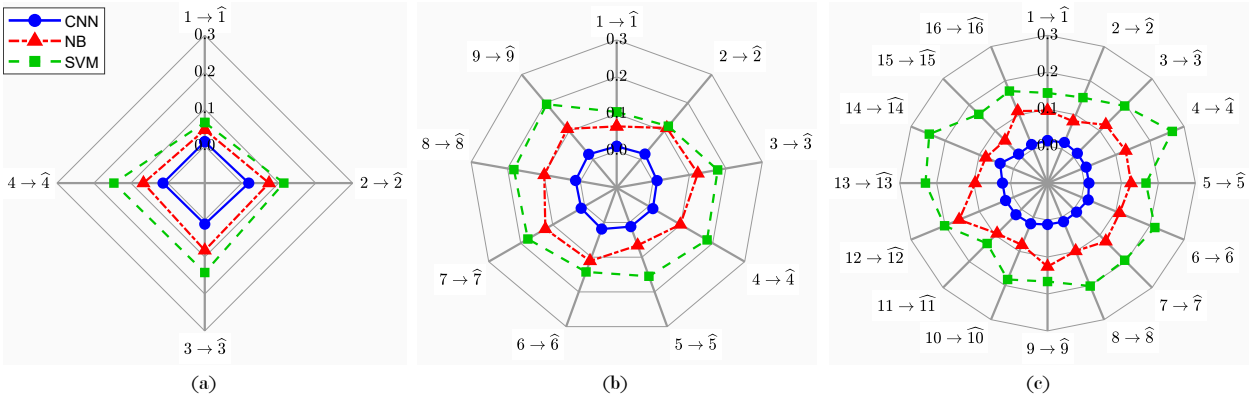


Figure 4.2: Overall misclassfication errors of the proposed CNN-based link selection scheme in comparison with the SVM-based and NB-based schemes for different diversity orders, (N_T, n_A, n_B, n_E): (a) $(2,1,1,1)$, (b) $(3,2,2,2)$, (c) $(4,1,1,1)$. (Haze, Full CSI, $\alpha = 26.0860$, $\beta = 24.0784$, $m = 2$, $d_b = d_e = 0.75\,\text{km}$, $\varepsilon = 0$, $\gamma_b \in [-6, 12]\,\text{dB}$, $\gamma_e = 5\,\text{dB}$)

Another performance comparison of the SOP with $\mathcal{R} = 1\,\text{bit}$ threshold against the average SNR of Bob is illustrated Fig. in 4.3 for the proposed CNN-based, conventional, SVM-based, and NB-based link selection schemes over a distance of $1\,\text{km}$ in clean atmospheric conditions with $0\,\text{dB}$ SNR at Eve. The turbulence parameters are calculated as $\alpha = 5.0096$ and $\beta = 4.7489$, while the Nakagami-m parameter is set to $m = 1$. In this figure, we consider three different transmitter and receiver configurations as $(N_T, n_T, n_B, n_E) = \{(2,1,1,1), (3,2,2,2), (4,2,2,2)\}$,where the number of classes and features $(\cdot, \cdot)$ are $(4, 8)$, $(9, 48)$, and $(36, 96)$, respectively. It is clear that SOP dramatically decreases with the increase of number of transmitters and receivers. Also, one can easily observe that the proposed CNN-based architecture performs the same performance with conventional scheme by outperforming SVM- and NB-based link selection schemes.

Fig. 4.4 illustrates how different types of eavesdropper can degrade the system's security performance in terms of SOP with a threshold of $\mathcal{R} = 1\,\text{bit}$ over a distance of $1.5\,\text{km}$ in hazy weather conditions. Additionally, we consider full CSI, Nakagami-m parameter as 1, no channel estimation and pointing errors, and set the average SNR of Eve to $3\,\text{dB}$. The turbulence parameters α

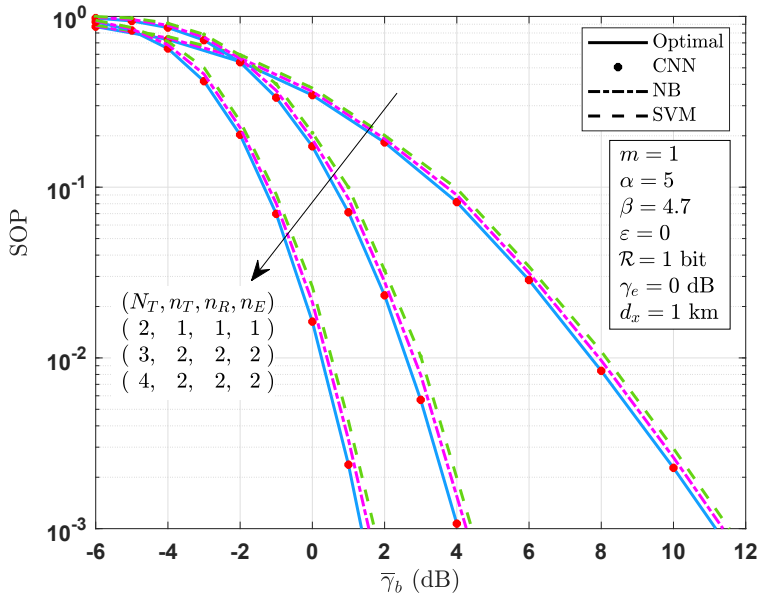


Figure 4.3: SOP versus average SNR performance of the system for the proposed CNN-based, conventional, SVM-based, and NB-based link selection schemes. (Clean, Full CSI, $d_b = d_e = 1$ km, $\kappa = 1$ bit, $\varepsilon = 0$, $\gamma_e = 0$ dB, $(N_T, n_T, n_B, n_E) = \{(2,1,1,1), (3,2,2,2), (4,2,2,2)\}$)

and β are calculated as 14.6608 and 14.0573, respectively. One can easily observe from the figure, hybrid-Eve dramatically degrade the secrecy performance in comparison with RF- and FSO-type Eves. For example, considering a target SOP of 10^{-3}, we can satisfy this requirement at 8, 8.5 and 10 dB for FSO-, RF- and hybrid-Eve, respectively. We also observe a slight difference between FSO and RF type eavesdroppers because of hazy turbulence condition, in which RF links perform better then FSO links. It is also clear that the proposed CNN network gives the same results as the conventional link selection.

The impact of different turbulence conditions on the system's secrecy performance is presented in Fig. 4.5 over a distance of 0.5 km with a SOP threshold of 2 bits in presence of a hybrid-type eavesdropper, where the configuration of transmitters and receivers is selected as $(N_T, n_A, n_B, n_E) = (3, 1, 1, 1)$. Considering an average 2 dB fixed SNR at Eve, if the secure system is required a SOP of 10^{-3}, the average SNR of Bob needs to be approximately 6, 7, 8 and 11 dB for clean, haze, moderated rain and moderate fog weather conditions, respectively. As seen from the figure, the proposed CNN-based link selection performs as good as the optimal link selection

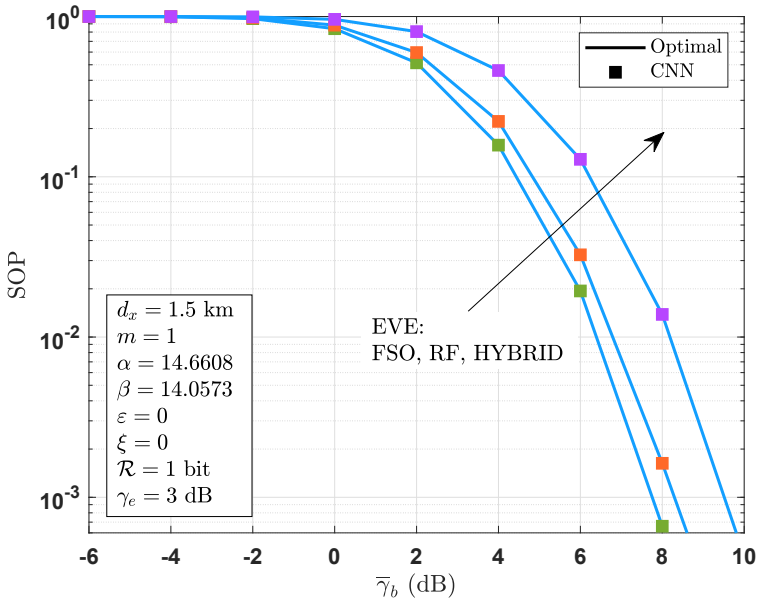


Figure 4.4: SOP versus average SNR performance of the system for different types of eavesdroppers. (Haze, Full CSI, $d_b = d_e = 1.5\,\text{km}$, $\mathcal{R} = 1\,\text{bit}$, $\xi = 0$, $\varepsilon = 0$, $\gamma_e = 3\,\text{dB}$, $(N_T, n_A, n_B, n_E) = (3, 2, 2, 2)$)

mechanism.

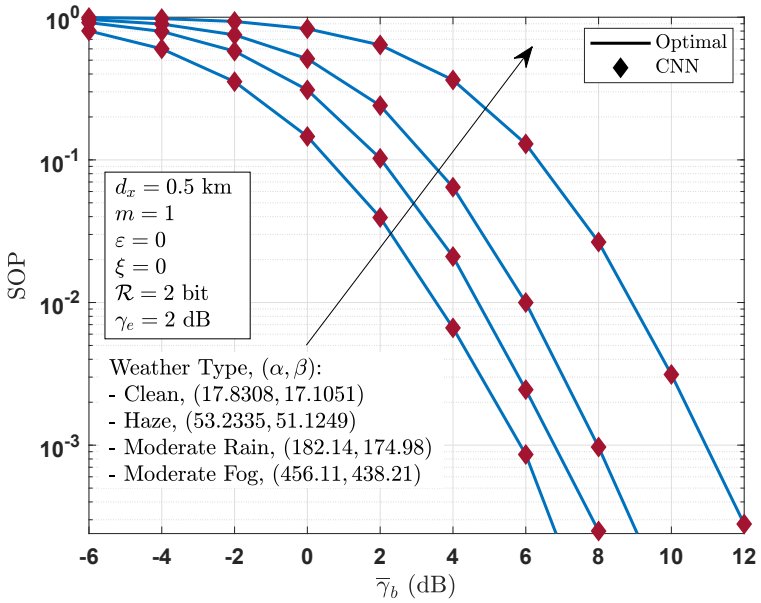


Figure 4.5: SOP versus average SNR performance of the system for different weather conditions in the presence of a hybrid eavesdropper. (Full CSI, $d_b = d_e = 0.5\,\text{km}$, $\mathcal{R} = 1\,\text{bit}$, $\xi = 0$, $\varepsilon = 0$, $\gamma_e = 2\,\text{dB}$, $(N_T, n_A, n_B, n_E) = (3, 1, 1, 1)$)

In Fig. 4.6, the effect of Nakagam-m parameter is investigated in terms of SOP with a threshold of 1 bit over a distance of 0.75 km considering the configuration of transmitters and receivers of $(N_T, n_A, n_B, n_E) = (2, 1, 1, 1)$. The turbulence parameters α and β are calculated as 8.3701 and 8.0023, respectively. Additionally, the pointing and channel estimation errors are considered as zero. Since we consider a fixed 3 dB SNR at Eve, we observe opposite behavior for secrecy performance of the system when Bob's average SNR becomes greater than Eve. In other words, increasing the Nakagami-m parameter implies the fading in RF channel becomes less severe. Therefore, this explains the opposite behavior in the figure, in which eavesdropper takes the advantage in low SNR region of Bob. Additionally, a target 1% secrecy outage can be satisfied after 8, 9.2 and 12.3 dB SNR of Bob for Nakagami-m parameters of 3, 2 and 1, respectively.

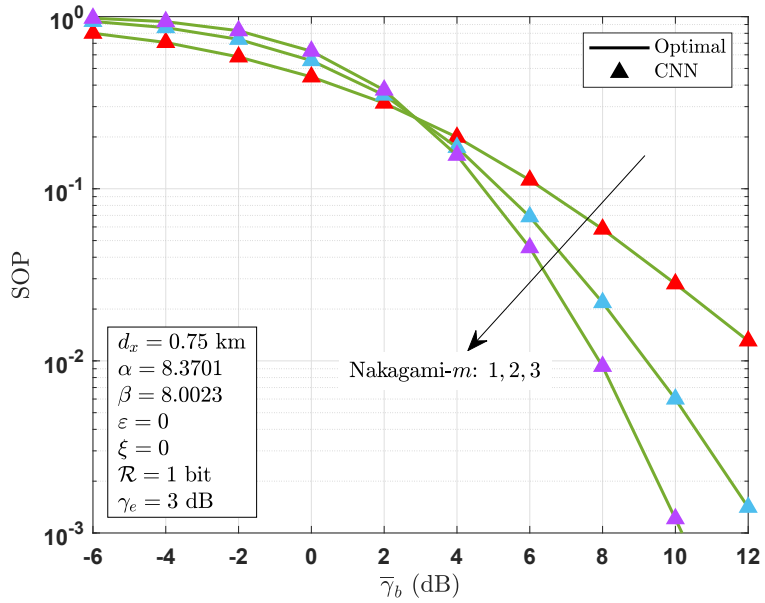


Figure 4.6: SOP versus average SNR performance of the system for different Nakagami-m parameter in the presence of a hybrid eavesdropper. (Full CSI, $d_b = d_e = 0.75$ km, $\mathcal{R} = 1$ bit, $\xi = 0$, $\varepsilon = 0$, $\gamma_e = 3$ dB, $(N_T, n_A, n_B, n_E) = (2, 1, 1, 1)$)

Since one of the main limitation in FSO systems is the pointing errors which exist because of its inherent line-of-sight requirement. In Fig. 4.7, the impact of pointing errors on the secrecy performance is illustrated for several distance values with a SOP threshold of 2 bits. The SNRs

of Bob and Eve are fixed at 15 and 5 dB, respectively, and then, full CSI and perfect channel estimation are assumed in this scenario. Nakagami-m parameter is set to 1, and the configuration of transmitters-receivers are selected as $(N_T, n_A, n_B, n_E) = (4, 2, 2, 2)$. As seen from the figure, the pointing error dramatically decreases overall system's secrecy performance. For instance, considering a target outage of 10^{-2}, the distance between legitimate pairs can be approximately 185, 300, 425, 550 and 680 meters for pointing errors of 0.33, 0.4, 0.5, 0.75 and without pointing errors, respectively.

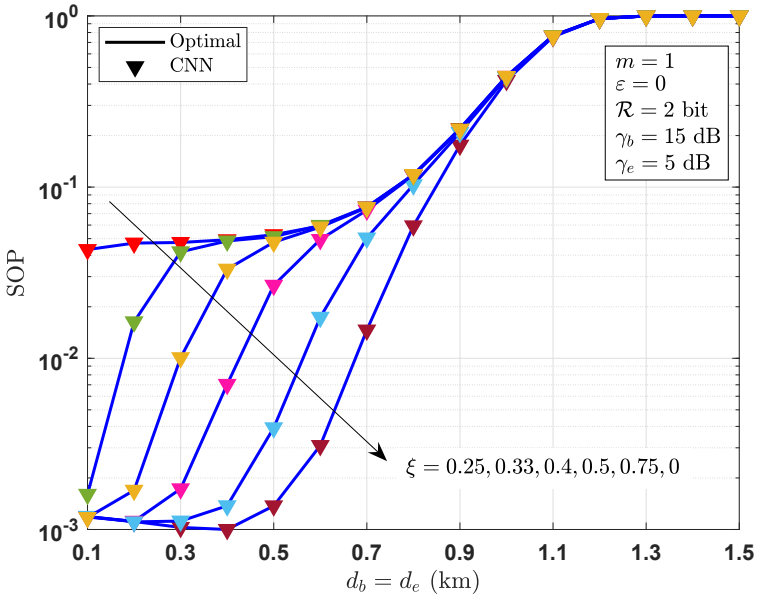


Figure 4.7: SOP versus distance performance of the system for different pointing errors at FSO link in the presence of a hybrid eavesdropper. (Full CSI, $\mathcal{R} = 2$ bit, $\varepsilon = 0$, $\gamma_b = 15$ dB, $\gamma_e = 5$ dB, $(N_T, n_A, n_B, n_E) = (4, 2, 2, 2)$)

The effect of full and partial of CSI on the system's secrecy performance versus distance is illustrated in Fig. 4.8 for different weather conditions over a distance of 1.25 km with 3 dB SNR at Eve. The secrecy rate $\mathcal{R}$ is set to 1 bit and number of transmitter and receivers is considered as $(N_T, n_A, n_B, n_E) = (4, 2, 2, 2)$. Comparison with partial CSI, having full CSI increases secrecy performance of the system for all scenarios considered. For instance, considering hazy atmospheric condition and 10^{-3} of outage probability, we will need approximately 2 dB more SNR at Bob for

partial CSI case. Also, as shown in the figure, the proposed CNN-based scheme achieves almost the same performance as the conventional scheme for both full and partial CSI cases.

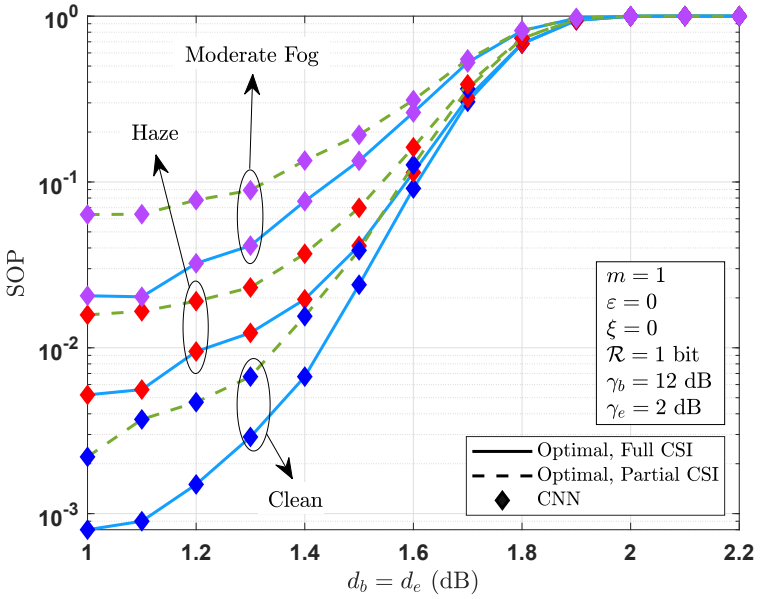


Figure 4.8: Impact of full and partial CSI on the secrecy performance for different weather conditions in presence of a hybrid eavesdropper. ($d_b = d_e = 1.25$ km, $\mathcal{R} = 3$ bits, $\varepsilon = 0$, $\xi = 0$, $\gamma_e = 3$ dB, $(N_T, n_A, n_B, n_E) = (4, 2, 2, 2)$)

It is worth highlighting that since instantaneous SNRs are random variables based on channel distributions and are used to characterize the secrecy capacity, channel estimation is an important process for system analysis. Therefore, the impact of channel estimation error is investigated in Fig. 4.9 for different link distances in moderate foggy condition at fixed 10 dB and 5 dB SNRs of Bob and Eve, respectively. For example, to obtain average 6 bits of secrecy capacity, the maximum supported link distance increase 0.75 km to 1.2 km when the channel estimation error increases from $\varepsilon = 0$ to $\varepsilon = 2$. It is also revealed that the proposed CNN architecture satisfy the same performance as the conventional scheme for all cases considered.

Secrecy throughput performance of the hybrid system is investigated in Fig. 4.10 for different types of eavesdroppers over a distance of 2 km in clean weather conditions, where we consider fixed SNRs of 10 and 5 dB at Bob and Eve, respectively. Nakagami-m parameter is set to 1, and

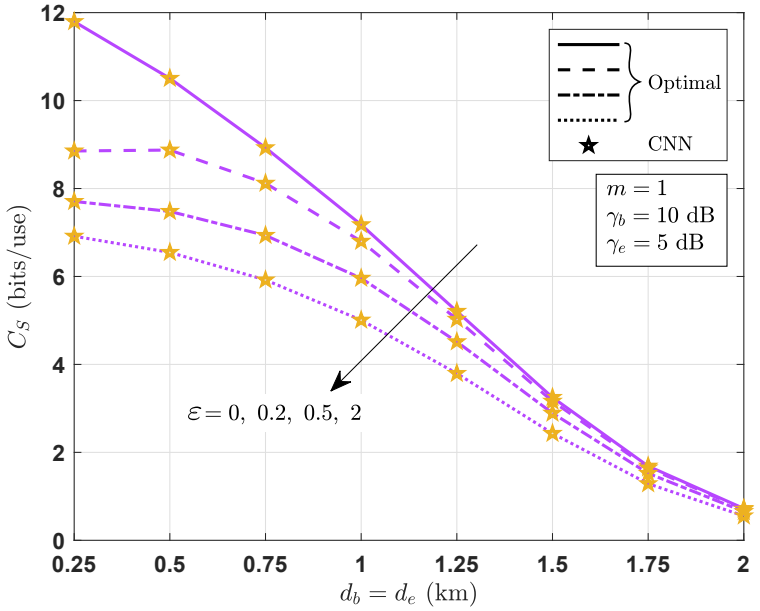


Figure 4.9: Impact of channel estimation on the secrecy capacity for different error values in presence of a hybrid eavesdropper. (Moderate fog, Full CSI, $\varepsilon = 0$, $\xi = 0$, $\gamma_b = 10\,\text{dB}$, $\gamma_e = 5\,\text{dB}$, $(N_T, n_A, n_B, n_E) = (3, 2, 2, 2)$)

the turbulence parameters α and β are calculated as 3.3166 and 2.5891, respectively. Additionally, the channel estimation and pointing errors are, in turn, introduced as 0.1 and 0.8. As it is seen from the figure, hybrid-Eve significantly degrades the secrecy throughput performance of the system in comparison with RF- and FSO-Eve. For all curves, it can be also observed that the EST monotonically increases with the increase of the secrecy threshold $\mathcal{R}$ until a specific point, and then it starts decreasing. This behavior clearly shows the dependency of EST to secrecy threshold, in which after a specific point of $\mathcal{R}$, secure communication between legitimate pairs cannot be satisfied due to the increase in target bit rate requirement.

As illustrated and discussed in Figs. 4.3–4.10, results of the proposed CNN networks for link selection are in exact agreement with results of the conventional link selection mechanism, where the accuracy and correctness are validated by Monte-Carlo simulations.

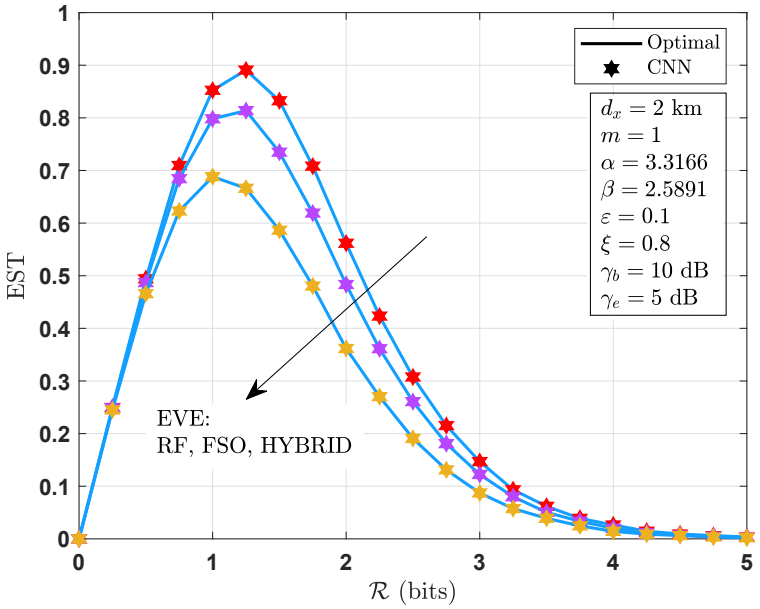


Figure 4.10: EST versus average the threshold of SOP performance of the system in presence of different types of eavesdroppers. (Clean, Full CSI, $\gamma_b = 10\,\text{dB}$, $\gamma_e = 5\,\text{dB}$, $\varepsilon = 0.1$, $\xi = 0.8$, $(N_T, n_A, n_B, n_E) = (4, 2, 2, 2)$)

4.6 Concluding Remarks

In this chapter, the use of DL-based link selection schemes is investigated for a hybrid FSO-*mm*Wave MIMO system in the presence of multiple eavesdroppers, where the communication between legitimate pair is carried over FSO gamma-gamma turbulence and *mm*Wave Nakagami-m fading channels simultaneously, and the MRC receiver is employed at the receiving side. In particular, CNN-based link selection schemes are proposed to maximize the secrecy performance by selecting/activating the antennas and lasers at the transmitter side. Considering the predefined total and active numbers of antennas and lasers at the legitimate transmitter, we examine the impact of fundamental physical layer parameters on the secrecy performance of a hybrid system by taking the availability of channel state information (CSI), channel estimation errors, weather conditions, link distances, signal-to-noise ratios, path loss models into account. In the light of the results, we show that the proposed CNN-based link selection scheme achieves the same performance as the conventional link selection scheme.

5. SECRECY ANALYSIS OF RELAY-BASED DUAL-HOP HYBRID FSO-RF SYSTEMS

5.1 Introduction

5.1.1 Motivation

Relaying schemes is widely used as an energy saving technique to increase the coverage area and transmission reliability as well as the system capacity. Therefore, considering high demands/requirements of 5G and beyond era, relay-based methods have been extensively employed to improve quality of services. In such systems, the message signal is transmitted over either FSO or RF link from source to relay node which is then forwards this message over other link to the destination node.

5.2 Related Works

In addition to the works [45–72] that are discussed in 2.2, there are also other works in which the mixed and/or dual-hop schemes are investigated in [159–166] for RF and FSO systems considering both fixed- and variable-gain AF relaying schemes taking several fundamental physical layer parameters into account under various scenarios and configurations. The authors in [167–170] examine a partial AF relay selection is assumed for mixed system, in which is based on outdated channel state information, where RF link is subject to Rayleigh fading and the FSO link is affected by Gamma-Gamma atmospheric turbulence. Further, generalized performance analyses of mixed FSO-RF systems is in detail examined in [171–173] considering cooperative transmissions, in which the effect of co-channel interference is considered at both relay and destination, threshold-based selective switching schemes, higher order moments, amount of fading, and moment generating function are also taken into account.

5.3 System Model

A scenario is taken into consideration in which dual-hop relaying systems are considered for data transmissions. The source wants to send an information signal to the destination by the use

of a relay, as illustrated in Fig. 5.1-(a). The communication in first hop (from source to relay) and second hop (from relay to destination) are established over two parallel links, called as, FSO and RF links. Therefore, it is presumed that transmitter nodes (source and relay) have a single transmitting antenna and laser, while receiver nodes (relay and destination) have a single receiving antenna and photodetector.

Additionally, another scenario is considered for a relay-based dual-hop hybrid FSO-*mm*Wave system, where the classic Wyner's wiretap channels take place [80]. The legitimate transmitter, Alice, wants to send a confidential information to the legitimate receiver, Bob, by the aid of a relay node, while an eavesdropper, Eve, tries to wiretap on the legitimate communication by sniffing the received signals at the Bob's side, as illustrated in Fig. 5.1(b–d). The communication in first-hop (from Alice to relay) and second-hop (from relay to Bob) are accomplished through two parallel links, namely, an FSO link and an RF link. Accordingly, it is assumed that Alice has a single transmit antenna and a single laser, while Bob has a single receive antenna and a single photodetector. For the relay node, two well-known AF relaying schemes are considered, in which the power amplification operation is based on partial and full channel state information of the first- and second-hops, namely, fixed-gain and variable-gain AF relaying methods.

Information bits to be transmitted are divided into $\log_2(\varpi)$ bit chunks, where ϖ denotes the modulation order, and then, each chunk is emitted and modulated over FSO and RF links, respectively. Additionally, the RF systems are operated on the *mm*Wave bands to provide equal bandwidth to exploit the diversity. Furthermore, we employ two well-known AF relaying schemes during data transmission. In the AF relay methods, the power amplification operation is on the basis of partial and full channel state information of the source-relay and relay-destination channels, called as, fixed- and variable-gain AF relaying methods, respectively.

5.3.1 Channel Characteristics

The channel models that are used in this chapter are presented in subsections 1.1.2 and 1.2.2 for *mm*Wave and FSO links, respectively. In particular, Nakagami-m and Gamma-Gamma distributions are considered for *mm*Wave fading and Gamma-Gamma turbulence channels, respectively.

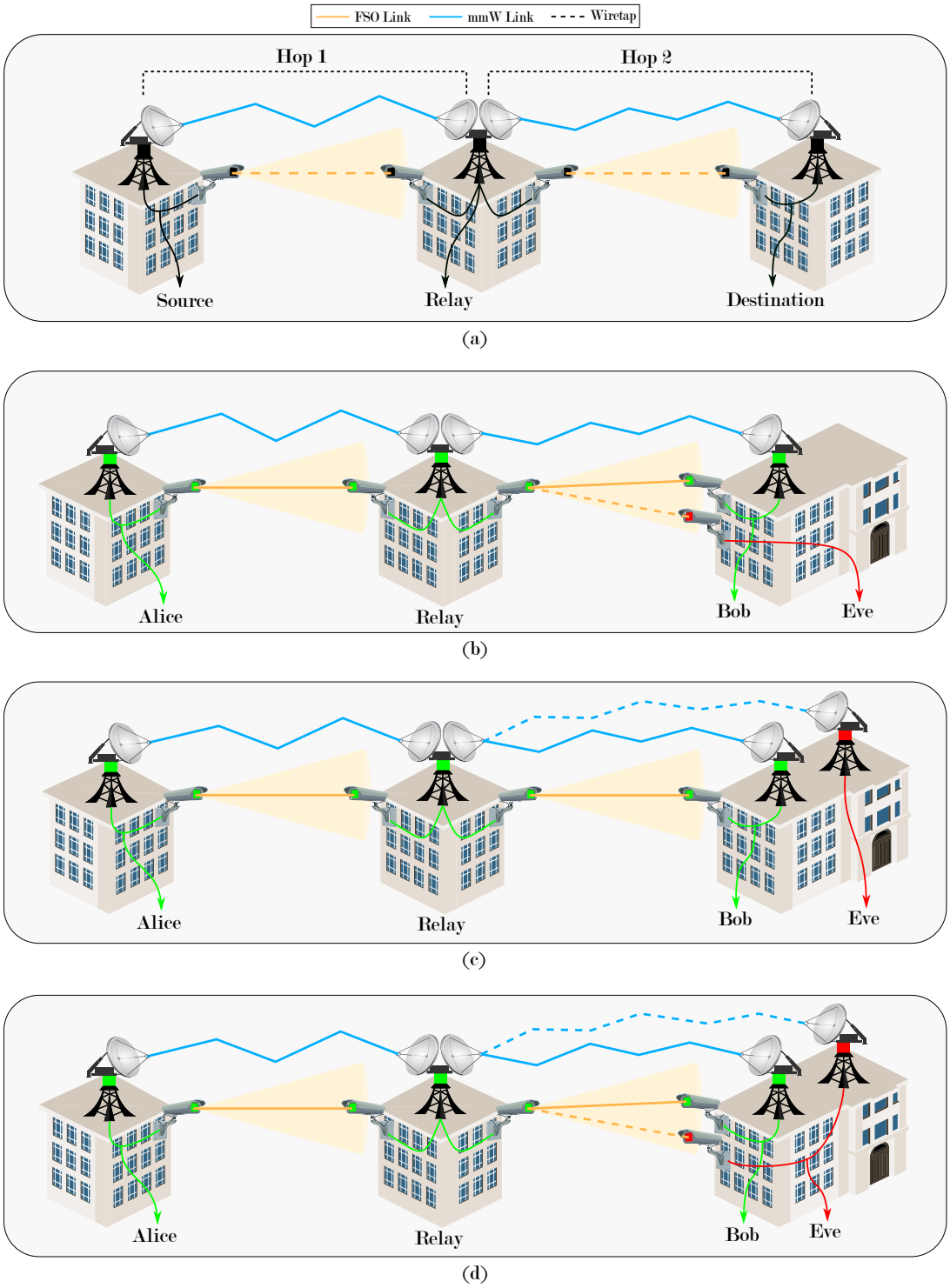


Figure 5.1: System model of relay-based dual hop hybrid FSO-*mm*Wave communications between the legitimate transmitter Alice and receiver Bob in the presence of different type eavesdroppers: (a) Without Eve, (b) FSO-Eve, (c) RF-Eve, and (d) Hybrid-Eve.

5.3.2 Average Signal-to-Noise Ratios

Relay and destination nodes uses the MRC diversity technique on the captured signals through RF and FSO systems, where the subscript $x \in \{1, 2\}$ represents receiver node, i.e., $x = 1$ for the first hop, and $x = 2$ for the second hop. Therefore, in each hop, the total electrical SNR is calculated by summing the instantaneous electrical SNRs for MRC receiver

$$\gamma_x = \gamma_{x,o} + \gamma_{x,f}, \tag{5.1}$$

where $\gamma_{x,o}$ and $\gamma_{x,f}$ are the instantaneous electrical SNR of FSO and RF links, respectively. The expression of $\gamma_{x,o}$ is given as

$$\gamma_{x,o} = \Upsilon_{\tau,x} I_x^2, \tag{5.2}$$

where I_x depicts the normalized irradiation, $\Upsilon_{\tau,x}$ denotes the average electrical SNR received from the FSO link, and the parameter $\tau \in \{1, 2\}$ defines the optical signal detection technique, i.e., $\tau = 1$ indicates the heterodyne detection ($\Upsilon_{1,x} = \Upsilon_{\text{Heterodyne}}$) while $\tau = 2$ indicates the IM/DD detection ($\Upsilon_{2,x} = \Upsilon_{\text{IM/DD}}$), defined as

$$\Upsilon_{1,x} = \overline{\gamma}_{x,o}, \qquad \text{for } \tau = 1, \tag{5.3}$$

$$\Upsilon_{2,x} = \frac{\overline{\gamma}_{x,o} \alpha_x \beta_x (\xi_x^2 + 2)}{(\alpha_x + 1)(\beta_x + 1)(\xi_x^2 + 1)^2}, \qquad \text{for } \tau = 2, \tag{5.4}$$

where $\overline{\gamma}_{x,o}$ is given in (1.24), and ξ denotes the ratio between the equivalent beam radius and the pointing error displacement standard deviation, called as jitter. Notice that the impact of pointing errors is considered as negligible when $\xi \to \infty$. Afterwards, by using a change of variable on the

RV I in (1.15), the PDF of γ_o is obtained as

$$f_{\gamma_o}(\gamma_{x,o}) = \frac{\mathcal{P}_0(x)}{\gamma_{x,o}} G_{1,3}^{3,0}\left(\alpha_x\beta_x\left(\frac{\gamma_{x,o}}{\Upsilon_{\tau,x}}\right)^{\frac{1}{\tau}}\middle|\begin{matrix}\xi_x^2+1\\ \xi_x^2,\alpha_x,\beta_x\end{matrix}\right), \tag{5.5}$$

then, its CDF is expressed as

$$F_{\gamma_o}(\gamma_{x,o}) = \mathcal{P}_1(x) G_{\tau+1,3\tau+1}^{3\tau,1}\left(\frac{(\alpha_x\beta_x)^\tau}{\tau^{2\tau}\Upsilon_{\tau,x}}\gamma_{x,o}\middle|\begin{matrix}1,\mathcal{P}_2(x)\\ \mathcal{P}_3(x),0\end{matrix}\right). \tag{5.6}$$

where the parameters $\mathcal{P}_0(x)$, $\mathcal{P}_1(x)$, $\mathcal{P}_2(x)$ and $\mathcal{P}_3(x)$ are given as

$$\begin{aligned}
\mathcal{P}_0(x) &= \big(\xi_x^2\big)\big/\big(\tau\Gamma(\alpha_x)\Gamma(\beta_x)\big),\\
\mathcal{P}_1(x) &= \big(\tau^{\alpha_x+\beta_x-2}\xi_x^2\big)\big/\big((2\pi)^{\tau-1}\Gamma(\alpha_x)\Gamma(\beta_x)\big),\\
\mathcal{P}_2(x) &= \Delta(\tau,\xi_x^2+1),\\
\mathcal{P}_3(x) &= \Delta(\tau,\xi_x^2),\Delta(\tau,\alpha_x),\Delta(\tau,\beta_x).
\end{aligned}$$

Likewise, the expression of $\gamma_{x,f}$ is given as

$$\gamma_{x,f} = \overline{\gamma}_{x,f} H_x^2, \tag{5.7}$$

where H_x stands for the instantaneous channel power, as given in (1.6) and, $\overline{\gamma}_{x,f}$ represents the average electrical SNR of the RF link, as given in (1.21).

5.3.2.1 Mixed SNR of a Hop

Since the overall SNR for each hop is given in (5.1), we can obtain the CDF of the overall SNR in each hop by using a simple variable transformation as follows. If we let $\Delta = \gamma_{x,o} + \gamma_{x,f}$, the

CDF of Δ is expressed as

$$F_{\Delta}(\delta) = \int_{-\infty}^{\infty} \int_{-\infty}^{\delta-\gamma_{x,f}} f_{\gamma_o}(\gamma_{x,o}) f_{\gamma_f}(\gamma_{x,f}) \cdot d\gamma_{x,o} d\gamma_{x,f}, \\ = \int_{0}^{\infty} F_{\gamma_o}(\delta - \gamma_{x,f}) f_{\gamma_f}(\gamma_{x,f}) \cdot d\gamma_{x,f}, \tag{5.8}$$

the integral in (5.8) is re-expressed by using (1.7) and (5.6)

$$F_{\Delta}(\delta) = \mathcal{P}_1(x) \frac{m_x^{m_x}}{\Gamma(m_x)\overline{\gamma}_{x,f}^{m_x}} \int_0^{\infty} \gamma_{x,f}^{m_x-1} e^{-\frac{m_x}{\overline{\gamma}_{x,f}}\gamma_{x,f}} G_{\tau+1,3\tau+1}^{3\tau,1}\left(\frac{(\alpha_x\beta_x)^{\tau}}{\tau^{2\tau}\Upsilon_{\tau,x}}(\delta-\gamma_{x,f}) \middle| \begin{matrix} 1, \mathcal{P}_2(x) \\ \mathcal{P}_3(x), 0 \end{matrix} \right) \cdot d\gamma_{x,f}, \tag{5.9}$$

then, by letting $u = \delta - \gamma_{x,f}$, the integral is re-expressed as

$$F_{\Delta}(\delta) = -\mathcal{P}_1(x) \frac{m^m}{\Gamma(m)\overline{\gamma}_{x,f}^{m}} e^{-\frac{m}{\overline{\gamma}_{x,f}}\delta} \int_0^{\infty} (\delta-u)^{m-1} e^{\frac{m}{\overline{\gamma}_{x,f}}u} G_{\tau+1,3\tau+1}^{3\tau,1}\left(\frac{(\alpha_x\beta_x)^{\tau}}{\tau^{2\tau}\Upsilon_{\tau,x}}u \middle| \begin{matrix} 1, \mathcal{P}_2(x) \\ \mathcal{P}_3(x), 0 \end{matrix} \right) \cdot du, \tag{5.10}$$

here, the polynomial expression is re-organized by the aid of binomial expansion

$$(\delta-u)^{m-1} = \sum_{\ell=0}^{m-1} \binom{m-1}{\ell} \delta^{m-\ell-1}(-u)^{\ell}, \tag{5.11}$$

since the summation is upper limited by the parameter m_x of Nakagami-m distribution because of the binomial expansion, only the integer values of m_x are used in the results. Then, the integral is

re-expressed as

$$F_{\Delta}(\delta) = -\mathcal{P}_1(x)\frac{m_x^{m_x}}{\Gamma(m_x)\overline{\gamma}_{x,f}^{m_x}}e^{-\frac{m_x}{\overline{\gamma}_{x,f}}\delta}\sum_{\ell=0}^{m_x-1}\binom{m_x-1}{\ell}(-1)^{\ell}\delta^{m_x-\ell-1} \times\int_0^{\infty}u^{\ell}e^{\frac{m_x}{\overline{\gamma}_{x,f}}u}G_{\tau+1,3\tau+1}^{3\tau,1}\left(\frac{(\alpha_x\beta_x)^{\tau}}{\tau^{2\tau}\Upsilon_{\tau,x}}u\middle|\begin{matrix}1,\mathcal{P}_2(x)\\ \mathcal{P}_3(x),0\end{matrix}\right)\cdot du, \tag{5.12}$$

and the integral is solved by using [82, (7.813-1)]

$$F_{\Delta}(\delta) = \mathcal{P}_1(x)\frac{m_x^{m_x}}{\Gamma(m_x)\overline{\gamma}_{x,f}^{m_x}}e^{-\frac{m_x}{\overline{\gamma}_{x,f}}\delta}\sum_{\ell=0}^{m_x-1}\binom{m_x-1}{\ell}\delta^{m_x-\ell-1}\left(\frac{\overline{\gamma}_{x,f}}{m_x}\right)^{\ell+1} \times G_{\tau+2,3\tau+1}^{3\tau,2}\left(-\frac{(\alpha_x\beta_x)^{\tau}\overline{\gamma}_{x,f}}{\tau^{2\tau}m_x\Upsilon_{\tau,x}}\middle|\begin{matrix}-\ell,1,\mathcal{P}_2(x)\\ \mathcal{P}_3(x),0\end{matrix}\right). \tag{5.13}$$

further, by using a change of variable, (5.13) can be re-expressed as

$$F_{\Delta}(\delta) = C_0(x)\sum_{\ell=0}^{m_x-1}C_1(x)\delta^{m_x-\ell-1}e^{-\frac{m_x}{\overline{\gamma}_{x,f}}\delta}, \tag{5.14}$$

where

$$C_0(x) = \mathcal{P}_1(x)\frac{m_x^{m_x}}{\Gamma(m_x)\overline{\gamma}_{x,f}^{m_x}}, \tag{5.15}$$

$$C_1(x) = \binom{m_x-1}{\ell}\left(\frac{\overline{\gamma}_{x,f}}{m_x}\right)^{\ell+1}G_{\tau+2,3\tau+1}^{3\tau,2}\left(-\frac{(\alpha_x\beta_x)^{\tau}\overline{\gamma}_{x,f}}{\tau^{2\tau}m_x\Upsilon_{\tau,x}}\middle|\begin{matrix}-\ell,1,\mathcal{P}_2(x)\\ \mathcal{P}_3(x),0\end{matrix}\right). \tag{5.16}$$

Accordingly, the PDF of the overall SNR in each hop is calculated as

$$\begin{aligned} f_{\Delta}(\delta) &= \frac{d}{d\delta} F_{\Delta}(\delta), \\ &= \frac{d}{d\delta} \left(C_0(x) \sum_{\ell=0}^{m_x-1} C_1(x) \delta^{m_x-\ell-1} e^{-\frac{m_x}{\overline{\gamma}_{x,f}}\delta} \right), \\ &= C_0(x) \sum_{\ell=0}^{m_x-1} C_1(x)(m_x-\ell-1)\delta^{m_x-\ell-2} e^{-\frac{m_x}{\overline{\gamma}_{x,f}}\delta} - \frac{m_x}{\overline{\gamma}_{x,f}} \delta^{m_x-\ell-1} e^{-\frac{m_x}{\overline{\gamma}_{x,f}}\delta}. \end{aligned} \tag{5.17}$$

5.4 Performance Analysis

In this section outage probability and effective throughput are derived for the fixed-gain (FG) and variable-gain (VG) dual-hop relaying schemes.

5.4.1 Outage Probability

The outage probability P_{out} is widely used to statistically characterize outage performance of a system when the overall end-to-end SNR of the system is lower than a predefined threshold value $\mathcal{R}$. It is defined as

$$\begin{aligned} P_{\text{out}}(\mathcal{R}) &= \text{Prob}\big(C < \mathcal{R}\big), \\ &= \text{Prob}\big(B \log_2(1+\gamma_s) < \mathcal{R}\big), \\ &= \text{Prob}\big(\gamma_s < 2^{\mathcal{R}/\mathcal{B}} - 1\big), \end{aligned} \tag{5.18}$$

where the bandwidth is considered as unity, $B = 1$, and therefore, the outage probability can be expressed in terms of the CDF of overall end-to-end system SNR

$$P_{\text{out}}(\mathcal{R}) = F_{\gamma_s}\big(2^{\mathcal{R}} - 1\big). \tag{5.19}$$

5.4.1.1 *Fixed-Gain Relaying*

In the fixed-gain relaying scheme, the received SNR at destination is expressed as

$$\gamma_s^{\text{FG}} = \frac{\gamma_1\gamma_2}{\gamma_2 + A}, \tag{5.20}$$

where A denotes the gain of relaying scheme. Accordingly, the CDF of the SNR at destination is expressed as

$$\begin{aligned} F_{\gamma_s}^{\text{FG}}(\gamma_s) &= \text{Prob.}\left(\frac{\gamma_1\gamma_2}{\gamma_2 + A} \leq \gamma_s\right), \\ &= \int_0^{\infty} F_{\gamma_1}\left(\left(1 + \frac{A}{\gamma_2}\right)\gamma_s\right) f_{\gamma_2}(\gamma_2) \cdot d\gamma_2. \end{aligned} \tag{5.21}$$

the integral (5.21) is re-expressed by using (5.14) and (5.17)

$$\begin{aligned} F_{\gamma_s}^{\text{FG}}(\gamma_s) = \int_0^{\infty} e^{-\frac{m_1}{\overline{\gamma}_{1,f}}\gamma_s} C_0(1) \sum_{\ell_1=0}^{m_1-1} C_1(1) \left(\gamma_s + \frac{A\gamma_s}{\gamma_2}\right)^{m_1-\ell_1-1} e^{-\frac{m_1}{\overline{\gamma}_{1,f}}\frac{A\gamma_s}{\gamma_2}} \\ \times C_0(2) \sum_{\ell_2=0}^{m_2-1} C_1(2)(m_2 - \ell_2 - 2)\gamma_2^{m_2-\ell_2-3} e^{-\frac{m_2}{\overline{\gamma}_{2,f}}\gamma_2} - \frac{m_2}{\overline{\gamma}_{2,f}}\gamma_2^{m_2-\ell_2-2} e^{-\frac{m_2}{\overline{\gamma}_{2,f}}\gamma_2} \cdot d\gamma_2, \end{aligned} \tag{5.22}$$

by using binomial theorem, the polynomial term can be re-expressed as

$$\left(\gamma_s + \frac{A\gamma_s}{\gamma_2}\right)^{m_1-\ell_1-1} = \sum_{k=0}^{m_1-\ell_1-1} \binom{m_1 - \ell_1 - 1}{k} \gamma_s^{m_1-\ell_1-1} A^k \gamma_2^{-k}, \tag{5.23}$$

further, the integral (5.22) is re-expressed as

$$\begin{aligned} F_{\gamma_s}^{\text{FG}}(\gamma_s) = e^{-\frac{m_1}{\overline{\gamma}_{1,f}}\gamma_s} C_0(1) \sum_{\ell_1=0}^{m_1-1} C_1(1) C_0(2) \sum_{\ell_2=0}^{m_2-1} C_1(2) \sum_{k=0}^{m_1-\ell_1-1} \binom{m_1 - \ell_1 - 1}{k} A^k \gamma_s^{m_1-\ell_1-1} \\ \times \left[(m_2 - \ell_2 - 2)\int_0^{\infty} \gamma_2^{m_2-\ell_2-k-3} e^{-\frac{m_1 A\gamma_s}{\overline{\gamma}_{1,f}\gamma_2} - \frac{m_2}{\overline{\gamma}_{2,f}}\gamma_2} \cdot d\gamma_2 - \frac{m_2}{\overline{\gamma}_{2,f}}\int_0^{\infty} \gamma_2^{m_2-\ell_2-k-2} e^{-\frac{m_1 A\gamma_s}{\overline{\gamma}_{1,f}\gamma_2} - \frac{m_2}{\overline{\gamma}_{2,f}}\gamma_2} \cdot d\gamma_2\right], \end{aligned} \tag{5.24}$$

accordingly, the CDF of the SNR at destination is given as

$$F_{\gamma_s}^{\text{FG}}(\gamma_s) = e^{-\frac{m_1}{\overline{\gamma}_{1,f}}\gamma_s} C_0(1) \sum_{\ell_1=0}^{m_1-1} C_1(1) C_0(2) \sum_{\ell_2=0}^{m_2-1} C_1(2) \sum_{k=0}^{m_1-\ell_1-1} \binom{m_1-\ell_1-1}{k} A^k \gamma_s^{m_1-\ell_1-1}$$
$$\times \Bigg[(m_2-\ell_2-2) \int_0^{\infty} \gamma_2^{m_2-\ell_2-k-3} e^{-\frac{m_1 A\gamma_s}{\overline{\gamma}_{1,f}\gamma_2} - \frac{m_2}{\overline{\gamma}_{2,f}}\gamma_2} \cdot d\gamma_2 - \frac{m_2}{\overline{\gamma}_{2,f}} \int_0^{\infty} \gamma_2^{m_2-\ell_2-k-2} e^{-\frac{m_1 A\gamma_s}{\overline{\gamma}_{1,f}\gamma_2} - \frac{m_2}{\overline{\gamma}_{2,f}}\gamma_2} \cdot d\gamma_2 \Bigg], \tag{5.25}$$

thereafter, by using [174, (2.5.37-2)], the resultant integrals can be solved as follows

$$F_{\gamma_s}^{\text{FG}}(\gamma_s) = 2e^{-\frac{m_1}{\overline{\gamma}_{1,f}}\gamma_s} C_0(1) \sum_{\ell_1=0}^{m_1-1} C_1(1) C_0(2) \sum_{\ell_2=0}^{m_2-1} C_1(2) \sum_{k=0}^{m_1-\ell_1-1} \binom{m_1-\ell_1-1}{k} A^k \gamma_s^{m_1-\ell_1-1}$$
$$\times \left(\frac{A m_1 \overline{\gamma}_{2,f}}{m_2 \overline{\gamma}_{1,f}} \gamma_s \right)^{\frac{m_2-\ell_2-k-1}{2}} \Bigg[(m_2-\ell_2-2) \left(\frac{m_2 \overline{\gamma}_{1,f}}{A m_1 \overline{\gamma}_{2,f} \gamma_s} \right)$$
$$\times K_{m_2-\ell_2-k-2} \left(2\sqrt{\frac{A m_1 m_2}{\overline{\gamma}_{1,f}\overline{\gamma}_{2,f}}\gamma_s} \right) - \frac{m_2}{\overline{\gamma}_{2,f}} K_{m_2-\ell_2-k-1} \left(2\sqrt{\frac{A m_1 m_2}{\overline{\gamma}_{1,f}\overline{\gamma}_{2,f}}\gamma_s} \right) \Bigg]. \tag{5.26}$$

$$F_{\gamma_s}^{\text{FG}}(\gamma_s) = C_0(1) \sum_{\ell_1=0}^{m_1-1} C_1(1) C_0(2) \sum_{\ell_2=0}^{m_2-1} C_1(2) \sum_{k=0}^{m_1-\ell_1-1} B_1$$
$$\times \Bigg[B_2 \gamma_s^{\frac{2m_1+m_2-2\ell_1-\ell_2-k-5}{2}} e^{-\frac{m_1}{\overline{\gamma}_{1,f}}\gamma_s} G_{0,2}^{2,0} \left(\frac{\mathcal{G} m_1 m_2}{\overline{\gamma}_{1,f}\overline{\gamma}_{2,f}} \gamma_s \middle| \begin{matrix} -,- \\ \frac{m_2-\ell_2-k-2}{2}, \frac{m_2-\ell_2-k-2}{2} \end{matrix} \right)$$
$$- B_3 \gamma_s^{\frac{2m_1+m_2-2\ell_1-\ell_2-k-3}{2}} e^{-\frac{m_1}{\overline{\gamma}_{1,f}}\gamma_s} G_{0,2}^{2,0} \left(\frac{\mathcal{G} m_1 m_2}{\overline{\gamma}_{1,f}\overline{\gamma}_{2,f}} \gamma_s \middle| \begin{matrix} -,- \\ \frac{m_2-\ell_2-k-1}{2}, \frac{m_2-\ell_2-k-1}{2} \end{matrix} \right) \Bigg]. \tag{5.27}$$

$$F_{\gamma_s}^{\text{FG}}(\gamma_s) = C_0(1) \sum_{\ell_1=0}^{m_1-1} C_1(1) C_0(2) \sum_{\ell_2=0}^{m_2-1} C_1(2) \sum_{k=0}^{m_1-\ell_1-1} B_1$$
$$\times \Bigg[\widehat{B}_2 G_{0,1}^{1,0} \left(\frac{m_1}{\overline{\gamma}_{1,f}} \gamma_s \middle| \begin{matrix} - \\ \frac{2m_1+m_2-2\ell_1-\ell_2-k-5}{2} \end{matrix} \right) G_{0,2}^{2,0} \left(\frac{\mathcal{G} m_1 m_2}{\overline{\gamma}_{1,f}\overline{\gamma}_{2,f}} \gamma_s \middle| \begin{matrix} -,- \\ \frac{m_2-\ell_2-k-2}{2}, \frac{m_2-\ell_2-k-2}{2} \end{matrix} \right)$$
$$- \widehat{B}_3 G_{0,1}^{1,0} \left(\frac{m_1}{\overline{\gamma}_{1,f}} \gamma_s \middle| \begin{matrix} - \\ \frac{2m_1+m_2-2\ell_1-\ell_2-k-3}{2} \end{matrix} \right) G_{0,2}^{2,0} \left(\frac{\mathcal{G} m_1 m_2}{\overline{\gamma}_{1,f}\overline{\gamma}_{2,f}} \gamma_s \middle| \begin{matrix} -,- \\ \frac{m_2-\ell_2-k-1}{2}, \frac{m_2-\ell_2-k-1}{2} \end{matrix} \right) \Bigg]. \tag{5.28}$$

5.4.1.2 Variable-Gain Relaying

In the variable-gain relaying scheme, the relay part exploits the channel state information and the received SNR at destination is expressed as

$$\gamma_s^{\text{VG}} = \frac{\gamma_1\gamma_2}{\gamma_1+\gamma_2+1} \approx \min\big(\gamma_1,\gamma_2\big), \tag{5.29}$$

and, the CDF of the SNR at destination is given as

$$\begin{aligned} F_{\gamma_s}^{\text{VG}}(\gamma_s) &= \text{Prob.}\big(\min\big(\gamma_1,\gamma_2 \le \gamma_1\big)\big) \\ &= F_{\gamma_1}(\gamma_s) + F_{\gamma_2}(\gamma_s) - F_{\gamma_1}(\gamma_s)F_{\gamma_2}(\gamma_s), \end{aligned} \tag{5.30}$$

then, by substituting (5.13) into (5.30), the CDF of the SNR at destination for variable-gain relaying is expressed as

$$
\begin{aligned}
F_{\gamma_s}^{\mathrm{VG}}(\gamma_s) = &- \frac{m_1^{m_1} e^{-\frac{m_1}{\overline{\gamma}_{1,f}}\gamma_s}}{\Gamma(\alpha_1)\Gamma(\beta_1)\Gamma(m_1)\overline{\gamma}_{1,f}^{m_1}} \sum_{\ell=0}^{m_1-1} \binom{m_1-1}{\ell} (-1)^{\ell} \gamma_s^{m_1-\ell-1} \frac{2^{\alpha_1+\beta_1-1}}{2\pi} \left(-\frac{m_1}{\overline{\gamma}_{1,f}}\right)^{-(\ell+1)} \\
&\times G_{3,6}^{4,3}\left(-\frac{\overline{\gamma}_{2,f}}{\overline{\gamma}_{2,o}} \frac{\alpha_1^2\beta_1^2}{16 m_1} \middle| \begin{matrix} -\ell, \frac{1}{2}, 1 \\ \frac{\alpha_1}{2}, \frac{\alpha_1+1}{2}, \frac{\beta_1}{2}, \frac{\beta_1+1}{2}, 0, \frac{1}{2} \end{matrix} \right) - \frac{1}{\Gamma(\alpha_2)\Gamma(\beta_2)} \frac{m_2^{m_2}}{\Gamma(m_2)\overline{\gamma}_{2,f}^{m_2}} e^{-\frac{m_2}{\overline{\gamma}_{2,f}}\gamma_s} \\
&\times \sum_{\ell=0}^{m_2-1} \binom{m_2-1}{\ell} (-1)^{\ell} \gamma_s^{m_2-\ell-1} \frac{2^{\alpha_2+\beta_2-1}}{2\pi} \left(-\frac{m_2}{\overline{\gamma}_{2,f}}\right)^{-(\ell+1)} \\
&\times G_{3,6}^{4,3}\left(-\frac{\overline{\gamma}_{2,f}}{\overline{\gamma}_{2,o}} \frac{\alpha_2^2\beta_2^2}{16 m_2} \middle| \begin{matrix} -\ell, \frac{1}{2}, 1 \\ \frac{\alpha_2}{2}, \frac{\alpha_2+1}{2}, \frac{\beta_2}{2}, \frac{\beta_2+1}{2}, 0, \frac{1}{2} \end{matrix} \right) \\
&- \frac{m_1^{m_1}}{\Gamma(\alpha_1)\Gamma(\beta_1)\Gamma(m_1)\overline{\gamma}_{1,f}^{m_1}} \frac{m_2^{m_2}}{\Gamma(\alpha_2)\Gamma(\beta_2)\Gamma(m_2)\overline{\gamma}_{2,f}^{m_2}} e^{\left(-\frac{m_1}{\overline{\gamma}_{1,f}} - \frac{m_2}{\overline{\gamma}_{2,f}}\right)\gamma_s} \\
&\times \sum_{\ell=0}^{m_1-1} \binom{m_1-1}{\ell} (-1)^{\ell} \gamma_s^{m_1-\ell-1} \frac{2^{\alpha_1+\beta_1-1}}{2\pi} \left(-\frac{m_1}{\overline{\gamma}_{1,f}}\right)^{-(\ell+1)} \\
&\times G_{3,6}^{4,3}\left(-\frac{\overline{\gamma}_{2,f}}{\overline{\gamma}_{2,o}} \frac{\alpha_1^2\beta_1^2}{16 m_1} \middle| \begin{matrix} -\ell, \frac{1}{2}, 1 \\ \frac{\alpha_1}{2}, \frac{\alpha_1+1}{2}, \frac{\beta_1}{2}, \frac{\beta_1+1}{2}, 0, \frac{1}{2} \end{matrix} \right) \\
&\times \sum_{\ell=0}^{m_2-1} \binom{m_2-1}{\ell} (-1)^{\ell} \gamma_s^{m_2-\ell-1} \frac{2^{\alpha_2+\beta_2-1}}{2\pi} \left(-\frac{m_2}{\overline{\gamma}_{2,f}}\right)^{-(\ell+1)} \\
&\times G_{3,6}^{4,3}\left(-\frac{\overline{\gamma}_{2,f}}{\overline{\gamma}_{2,o}} \frac{\alpha_2^2\beta_2^2}{16 m_2} \middle| \begin{matrix} -\ell, \frac{1}{2}, 1 \\ \frac{\alpha_2}{2}, \frac{\alpha_2+1}{2}, \frac{\beta_2}{2}, \frac{\beta_2+1}{2}, 0, \frac{1}{2} \end{matrix} \right).
\end{aligned} \tag{5.31}
$$

5.4.2 Effective Throughput

While conveying the information from source to destination over a relay, the system needs to satisfy a specific reliability level. To characterize this behavior of the system, we consider a metric called effective throughput T_{Eff}, which defined in terms of the outage probability, and it can be

expressed as

$$T_{\text{Eff}}(\mathcal{R}) = \mathcal{R} \times \big(1 - P_{\text{out}}(\mathcal{R})\big). \tag{5.32}$$

5.4.2.1 Fixed-Gain Relaying

For the fixed-gain relaying scheme, the effective throughput is calculated by using overall end-to-end SNR

$$T_{\text{Eff}}^{\text{FG}}(\mathcal{R}) = \mathcal{R} \times \big(1 - F_{\gamma_s}^{\text{FG}}(2^{\mathcal{R}} - 1)\big). \tag{5.33}$$

where $F_{\gamma_s}^{\text{FG}}(\gamma_s)$ is given in (5.26).

5.4.2.2 Variable-Gain Relaying

For the variable-gain relaying scheme, the effective throughput is calculated by using overall end-to-end SNR

$$T_{\text{Eff}}^{\text{VG}}(\mathcal{R}) = \mathcal{R} \times \big(1 - F_{\gamma_s}^{\text{VG}}(2^{\mathcal{R}} - 1)\big). \tag{5.34}$$

where $F_{\gamma_s}^{\text{VG}}(\gamma_s)$ is given in (5.31).

5.5 Secrecy Performance Analysis

In this section, the physical layer security analysis are presented for the variable-gain (VG) and fixed-gain (FG) dual-hop relaying schemes using average secrecy capacity, secrecy outage probability, and effective secrecy throughput metrics.

5.5.1 Average Secrecy Capacity

Since the wireless communication channels have time-varying nature, secrecy capacity is obtained by averaging the end-to-end instantaneous secrecy capacity that is expressed as [45, (15)]

$$C_S = \int_0^\infty \frac{1}{1+\gamma_b} F_{\gamma_e}(\gamma_b)\big[1 - F_{\gamma_b}(\gamma_b)\big] \cdot d\gamma_b, \tag{5.35}$$

where the term $1/(1+\gamma_b)$ can be expressed in terms of Meijer-G function [83, (8.4.2-5)], and (5.35) can be re-written as

$$C_S = \int_0^\infty G_{1,1}^{1,1}\big(\,\gamma_b \big|\, {0 \atop 0}\big) F_{\gamma_e}(\gamma_b)\big[1 - F_{\gamma_b}(\gamma_b)\big] \cdot d\gamma_b. \tag{5.36}$$

5.5.1.1 FSO Eavesdropper for Variable-Gain

For the FSO-type eavesdropper, the CDF of SNR $F_{\gamma_e}(\gamma_e)$ is given in (5.6). Therefore, by substituting (5.6) and (5.31) into (5.36), the ASC is obtained as (5.53), in terms of $\mathcal{I}_{1,o}^{\text{VG}}$, $\mathcal{I}_{2,o}^{\text{VG}}$, $\mathcal{I}_{3,o}^{\text{VG}}$ and $\mathcal{I}_{4,o}^{\text{VG}}$, which are derived in the following.

The derivation of integral $\mathcal{I}_{1,o}^{\text{VG}}$ is made as follows

$$\mathcal{I}_{1,o}^{\text{VG}} = \int_0^\infty \frac{1}{1+\gamma_b} G_{1,3}^{2,1}\left(\frac{\alpha_e\beta_e}{\sqrt{\overline{\gamma}_{e,o}}}\sqrt{\gamma_b}\,\middle|\, {1 \atop \alpha_e, \beta_e, 0}\right) \cdot d\gamma_b, \tag{5.37}$$

then, the resultant integral is solved by using [83, 2.24.2-4]

$$\mathcal{I}_{1,o}^{\text{VG}} = \frac{2^{\alpha_e+\beta_e-2}}{\pi} G_{3,7}^{5,3}\left(\frac{\alpha_e^2\beta_e^2}{8\overline{\gamma}_{e,o}}\,\middle|\, {0, \frac{1}{2}, 1 \atop 0, \frac{\alpha_e}{2}, \frac{\alpha_e+1}{2}, \frac{\beta_e}{2}, \frac{\beta_e+1}{2}, 0, \frac{1}{2}}\right). \tag{5.38}$$

Since the integrals $\mathcal{I}_{2,o}^{\text{VG}}$, $\mathcal{I}_{3,o}^{\text{VG}}$ and $\mathcal{I}_{4,o}^{\text{VG}}$ are in the same form with different parameters, their

derivations can be made as

$$\mathcal{I}_{\upsilon,o}^{\text{VG}} = \int_0^\infty \gamma_b^{a_1} e^{-a_2\gamma_b} G_{1,1}^{1,1}\left(\gamma_b \middle| \begin{matrix} 0 \\ 0 \end{matrix}\right) G_{1,3}^{2,1}\left(\frac{\alpha_e\beta_e}{\sqrt{\overline{\gamma}_{e,o}}}\sqrt{\gamma_b} \middle| \begin{matrix} 1 \\ \alpha_e, \beta_e, 0 \end{matrix}\right) \cdot d\gamma_b, \tag{5.39}$$

where the power and exponential terms can be expressed in terms of Meijer-G function by using [83, 8.2.2-15] and [118, (11)]

$$e^{-a_2\gamma_b} = G_{0,1}^{1,0}\left(a_2\gamma_b \middle| \begin{matrix} - \\ 0 \end{matrix}\right), \tag{5.40}$$

$$\gamma_b^{a_1} G_{1,1}^{1,1}\left(\gamma_b \middle| \begin{matrix} 0 \\ 0 \end{matrix}\right) = G_{1,1}^{1,1}\left(\gamma_b \middle| \begin{matrix} a_1 \\ a_1 \end{matrix}\right), \tag{5.41}$$

therefore, the integral in (5.39) is written as

$$\mathcal{I}_{\upsilon,o}^{\text{VG}} = \int_0^\infty G_{1,1}^{1,1}\left(\gamma_b \middle| \begin{matrix} a_1 \\ a_1 \end{matrix}\right) G_{0,1}^{1,0}\left(a_2\gamma_b \middle| \begin{matrix} - \\ 0 \end{matrix}\right) G_{1,3}^{2,1}\left(\frac{\alpha_e\beta_e}{\sqrt{\overline{\gamma}_{e,o}}}\sqrt{\gamma_b} \middle| \begin{matrix} 1 \\ \alpha_e, \beta_e, 0 \end{matrix}\right) \cdot d\gamma_b, \tag{5.42}$$

and the resultant integral can be solved in terms of extended generalized binary Meijer's G (EGBMG) function by using [175, (20)]

$$\mathcal{I}_{\upsilon,o}^{\text{VG}} = G_{1,1:0,1:1,3}^{1,1:1,0:2,1}\left(\begin{matrix} a_1+1 \\ a_1+1 \end{matrix} \middle| \begin{matrix} - \\ 0 \end{matrix} \middle| \begin{matrix} 1 \\ \alpha_e, \beta_e, 0 \end{matrix} \middle| a_2, \frac{\alpha_e\beta_e}{\sqrt{\overline{\gamma}_{e,o}}}\right), \tag{5.43}$$

where $\upsilon \in \{2, 3, 4\}$, and the parameters a_1 and a_2 are given in Appendix C with (C.1).

5.5.1.2 RF Eavesdropper for Variable-Gain

For the RF-type eavesdropper, the CDF of SNR $F_{\gamma_e}(\gamma_e)$ is given in (1.9). Therefore, by substituting (1.9) and (5.31) into (5.36), the ASC is obtained as (5.54), in terms of $\mathcal{I}_{1,f}^{\text{VG}}$, $\mathcal{I}_{2,f}^{\text{VG}}$, $\mathcal{I}_{3,f}^{\text{VG}}$ and

$\mathcal{I}_{4,f}^{\text{VG}}$, which are derived in the following.

The derivation of integral $\mathcal{I}_{1,f}^{\text{VG}}$ is made as follows

$$\mathcal{I}_{1,f}^{\text{VG}} = \int_0^{\infty} G_{1,1}^{1,1}\left(\gamma_b \middle| \begin{matrix} 0 \\ 0 \end{matrix}\right) G_{1,2}^{1,1}\left(\frac{\gamma_b}{\overline{\gamma}_{e,f}} \middle| \begin{matrix} 1 \\ m_e, 0 \end{matrix}\right) \cdot d\gamma_b, \tag{5.44}$$

then, the resultant integral is solved by using [82, 7.811-1]

$$\mathcal{I}_{1,f}^{\text{VG}} = G_{2,3}^{2,2}\left(\frac{1}{\overline{\gamma}_{e,f}} \middle| \begin{matrix} 0, 1 \\ 0, m_e, 0 \end{matrix}\right). \tag{5.45}$$

Since the integrals $\mathcal{I}_{2,f}^{\text{VG}}$, $\mathcal{I}_{3,f}^{\text{VG}}$ and $\mathcal{I}_{4,f}^{\text{VG}}$ are in the same form with different parameters, their derivations can be made as

$$\mathcal{I}_{\upsilon,f}^{\text{VG}} = \int_0^{\infty} \gamma_b^{a_1} e^{-a_2\gamma_b} G_{1,1}^{1,1}\left(\gamma_b \middle| \begin{matrix} 0 \\ 0 \end{matrix}\right) G_{1,2}^{1,1}\left(\frac{\gamma_{b,f}}{\overline{\gamma}_{e,f}} \middle| \begin{matrix} 1 \\ m_e, 0 \end{matrix}\right) \cdot d\gamma_b, \tag{5.46}$$

where the power and exponential terms can be expressed in terms of Meijer-G function by using [83, 8.2.2-15]

$$\gamma_b^{a_1} G_{1,1}^{1,1}\left(\gamma_b \middle| \begin{matrix} 0 \\ 0 \end{matrix}\right) = G_{1,1}^{1,1}\left(\gamma_b \middle| \begin{matrix} a_1 \\ a_1 \end{matrix}\right), \tag{5.47}$$

$$e^{-a_2\gamma_b} = G_{0,1}^{1,0}\left(a_2\gamma_b \middle| \begin{matrix} - \\ 0 \end{matrix}\right), \tag{5.48}$$

therefore, the integral in (5.46) is written as

$$\mathcal{I}_{\upsilon,f}^{\text{VG}} = \int_0^{\infty} G_{0,1}^{1,0}\left(a_2\gamma_b \middle| \begin{matrix} - \\ 0 \end{matrix}\right) G_{1,1}^{1,1}\left(\gamma_b \middle| \begin{matrix} a_1 \\ a_1 \end{matrix}\right) G_{1,2}^{1,1}\left(\frac{\gamma_b}{\overline{\gamma}_{e,f}} \middle| \begin{matrix} 1 \\ m_e, 0 \end{matrix}\right) \cdot d\gamma_b, \tag{5.49}$$

and the resultant integral can be solved in terms of EGBMG function by using [175, (20)]

$$\mathcal{I}_{\upsilon,f}^{\text{VG}} = G_{1,1:0,1:1,2}^{1,1:1,0:1,1}\left(\begin{matrix} a_1+1 \\ a_1+1 \end{matrix}\middle| - \middle| \begin{matrix} 1 \\ 0 \end{matrix}\middle| \begin{matrix} \\ m_e, 0 \end{matrix}\middle| a_2, \frac{1}{\overline{\gamma}_{e,f}}\right), \tag{5.50}$$

where $\upsilon \in \{2,3,4\}$, and the parameters a_1 and a_2 are given in Appendix C with (C.1).

5.5.1.3 Hybrid Eavesdropper for Variable-Gain

For the hybrid-type eavesdropper, the CDF of SNR $F_{\gamma_e}(\gamma_e)$ is given in (5.14). Therefore, by substituting (5.14) and (5.31) into (5.36), the ASC is obtained as (5.55), in terms of $\mathcal{I}_{1,h}^{\text{VG}}$, $\mathcal{I}_{2,h}^{\text{VG}}$, $\mathcal{I}_{3,h}^{\text{VG}}$ and $\mathcal{I}_{4,h}^{\text{VG}}$, which are derived in the following.

Since the integrals $\mathcal{I}_{1,h}^{\text{VG}}$, $\mathcal{I}_{2,h}^{\text{VG}}$, $\mathcal{I}_{3,h}^{\text{VG}}$ and $\mathcal{I}_{4,h}^{\text{VG}}$ are in the same form with different parameters, their derivations can be made as

$$\mathcal{I}_{\upsilon,h}^{\text{VG}} = \int_0^\infty \gamma_b^{a_1} e^{-a_2} G_{1,1}^{1,1}\left(\gamma_b \middle| \begin{matrix} 0 \\ 0 \end{matrix}\right) \cdot d\gamma_b, \tag{5.51}$$

then, the resultant integral is solved by using [82, 7.813-1]

$$\mathcal{I}_{\upsilon,h}^{\text{VG}} = a_2^{-a_1-1} G_{2,1}^{1,2}\left(\frac{1}{a_2}\middle| \begin{matrix} -a_1, 0 \\ 0 \end{matrix}\right), \tag{5.52}$$

where $\upsilon \in \{1,2,3,4\}$, and the parameters a_1 and a_2 are given in Appendix C with (C.2).

$$C_S^{\text{FSO,VG}} = \frac{1}{\Gamma(\alpha_e)\Gamma(\beta_e)}\Bigg[\mathcal{I}_{1,o}^{\text{VG}} - C_0(1)\sum_{\ell=0}^{m_1-1} C_1(1)\mathcal{I}_{2,o}^{\text{VG}} - C_0(2)\sum_{\ell=0}^{m_2-1} C_1(2)\mathcal{I}_{3,o}^{\text{VG}} + C_0(1)C_0(2)\sum_{\ell=0}^{m_1-1} C_1(1)\sum_{\ell=0}^{m_2-1} C_1(2)\mathcal{I}_{4,o}^{\text{VG}}\Bigg], \quad (5.53)$$

$$C_S^{\text{RF,VG}} = \frac{1}{\Gamma(m_e)}\Bigg[\mathcal{I}_{1,f}^{\text{VG}} - C_0(1)\sum_{\ell=0}^{m_1-1} C_1(1)\mathcal{I}_{2,f}^{\text{VG}} - C_0(2)\sum_{\ell=0}^{m_2-1} C_1(2)\mathcal{I}_{3,f}^{\text{VG}} + C_0(1)C_0(2)\sum_{\ell=0}^{m_1-1} C_1(1)\sum_{\ell=0}^{m_2-1} C_1(2)\mathcal{I}_{4,f}^{\text{VG}}\Bigg], \quad (5.54)$$

$$C_S^{\text{HYB,VG}} = C_0(e)\sum_{\ell_e=0}^{m_e-1} C_1(e)\Bigg[\mathcal{I}_{1,h}^{\text{VG}} - C_0(1)\sum_{\ell=0}^{m_1-1} C_1(1)\mathcal{I}_{2,h}^{\text{VG}} - C_0(2)\sum_{\ell=0}^{m_2-1} C_1(2)\mathcal{I}_{3,h}^{\text{VG}} + C_0(1)C_0(2)\sum_{\ell=0}^{m_1-1} C_1(1)\sum_{\ell=0}^{m_2-1} C_1(2)\mathcal{I}_{4,h}^{\text{VG}}\Bigg]. \quad (5.55)$$

5.5.1.4 FSO Eavesdropper for Fixed-Gain

For the FSO-type eavesdropper considering fixed-gain relay scheme, the CDF of SNR $F_{\gamma_e}(\gamma_e)$ is given in (5.6). Therefore, by substituting (5.6) and (5.27) into (5.36), the ASC is obtained as (5.65), in terms of $\mathcal{I}_{1,o}^{\text{FG}}$, $\mathcal{I}_{2,o}^{\text{FG}}$ and $\mathcal{I}_{3,o}^{\text{FG}}$, which are derived in the following.

The derivation of integral $\mathcal{I}_{1,o}^{\text{FG}}$ is the same as $\mathcal{I}_{1,o}^{\text{VG}}$ and is derived in (5.38).

Since the integrals $\mathcal{I}_{2,o}^{\text{FG}}$ and $\mathcal{I}_{3,o}^{\text{FG}}$ are in the same form with different parameters, their derivations can be made as follows

$$\mathcal{I}_{v,o}^{\text{FG}} = \int_0^\infty \gamma_s^{a_1} e^{-b_1\gamma_s} G_{1,1}^{1,1}\left(\gamma_s \middle| \begin{matrix}0\\0\end{matrix}\right) G_{0,2}^{2,0}\left(b_2\gamma_s \middle| \begin{matrix}-,-\\a_2,a_2\end{matrix}\right) G_{1,3}^{2,1}\left(\alpha_e\beta_e\sqrt{\gamma_s} \middle| \begin{matrix}1\\\alpha_e,\beta_e,0\end{matrix}\right)\cdot d\gamma_s, \quad (5.56)$$

then, by using the series expansion of exponential function and the equality in [83, 8.2.2-15], the

integral is re-expressed as

$$\mathcal{I}_{\upsilon,o}^{\text{FG}}=\sum_{n=0}^{\infty}\frac{(-b_1)^n}{n!}\int_0^{\infty}G_{0,2}^{2,0}\left(b_2\gamma_s\middle|\begin{matrix}-,-\\a_2,a_2\end{matrix}\right)G_{1,1}^{1,1}\left(\gamma_s\middle|\begin{matrix}n+a_1\\n+a_1\end{matrix}\right)G_{1,3}^{2,1}\left(\alpha_x\beta_x\sqrt{\gamma_s}\middle|\begin{matrix}1\\\alpha_x,\beta_x,0\end{matrix}\right)\cdot d\gamma_s, \tag{5.57}$$

and the resultant integral can be solved in terms of EGBMG function by using [175, (20)]

$$\mathcal{I}_{\upsilon,o}^{\text{FG}}=\sum_{n=0}^{\infty}\frac{(-b_1)^n}{n!}G_{1,1:0,2:1,3}^{1,1:2,0:2,1}\left(\begin{matrix}n+a_1+1\\n+a_1+1\end{matrix}\middle|\begin{matrix}-,-\\a_2,a_2\end{matrix}\middle|\begin{matrix}1\\\alpha_e,\beta_e,0\end{matrix}\middle|b_2,\frac{\alpha_e\beta_e}{\sqrt{\overline{\gamma}_{e,o}}}\right), \tag{5.58}$$

where $\upsilon\in\{2,3\}$, and the parameters a_1,a_2,b_1,b_2 are given in Appendix C with (C.3).

5.5.1.5 RF Eavesdropper for Fixed-Gain

For the RF-type eavesdropper considering fixed-gain relay scheme, the CDF of SNR $F_{\gamma_e}(\gamma_e)$ is given in (1.9). Therefore, by substituting (1.9) and (5.27) into (5.36), the ASC is obtained as (5.66), in terms of $\mathcal{I}_{1,f}^{\text{FG}}$, $\mathcal{I}_{2,f}^{\text{FG}}$ and $\mathcal{I}_{3,f}^{\text{FG}}$, which are derived in the following.

The derivation of integral $\mathcal{I}_{1,f}^{\text{FG}}$ is the same as $\mathcal{I}_{1,f}^{\text{VG}}$ and is derived in (5.45).

Since the integrals $\mathcal{I}_{2,f}^{\text{FG}}$ and $\mathcal{I}_{3,f}^{\text{FG}}$ are in the same form with different parameters, their derivations can be made as follows

$$\mathcal{I}_{\upsilon,f}^{\text{FG}}=\int_0^{\infty}\gamma_s^{a_1}e^{-b_1\gamma_s}G_{1,1}^{1,1}\left(\gamma_s\middle|\begin{matrix}0\\0\end{matrix}\right)G_{0,2}^{2,0}\left(b_2\gamma_s\middle|\begin{matrix}-,-\\a_2,a_2\end{matrix}\right)G_{1,2}^{1,1}\left(\frac{\gamma_s}{\overline{\gamma}_{e,f}}\middle|\begin{matrix}1\\m_x,0\end{matrix}\right)\cdot d\gamma_s \tag{5.59}$$

then, by using the series expansion of exponential function and the equality in [83, 8.2.2-15], the integral is re-expressed as

$$\mathcal{I}_{\upsilon,f}^{\text{FG}}=\sum_{n=0}^{\infty}\frac{(-b_1)^n}{n!}\int_0^{\infty}G_{0,2}^{2,0}\left(b_2\gamma_s\middle|\begin{matrix}-,-\\a_2,a_2\end{matrix}\right)G_{1,1}^{1,1}\left(\gamma_s\middle|\begin{matrix}n+a_1\\n+a_1\end{matrix}\right)G_{1,2}^{1,1}\left(\frac{\gamma_s}{\overline{\gamma}_{e,f}}\middle|\begin{matrix}1\\m_e,0\end{matrix}\right)\cdot d\gamma_s \tag{5.60}$$

and the resultant integral can be solved in terms of EGBMG function by using [175, (20)]

$$\mathcal{I}_{\upsilon,f}^{\text{FG}} = \sum_{n=0}^{\infty} \frac{(-b_1)^n}{n!} G_{1,1:0,2:1,3}^{1,1:2,0:2,1} \left(\begin{matrix} n+a_1+1 \\ n+a_1+1 \end{matrix} \middle| \begin{matrix} -,- \\ a_2, a_2 \end{matrix} \middle| \begin{matrix} 1 \\ \alpha_e, \beta_e, 0 \end{matrix} \middle| b_2, \frac{1}{\overline{\gamma}_{e,f}} \right), \tag{5.61}$$

where $\upsilon \in \{2, 3\}$, and the parameters a_1, a_2, b_1, b_2 are given in Appendix C with (C.3).

5.5.1.6 Hybrid Eavesdropper for Fixed-Gain

For the hybrid-type eavesdropper, the CDF of SNR $F_{\gamma_e}(\gamma_e)$ is given in (5.14). Therefore, by substituting (5.14) and (5.27) into (5.36), the ASC is obtained as (5.67), in terms of $\mathcal{I}_{1,h}^{\text{FG}}$, $\mathcal{I}_{2,h}^{\text{FG}}$ and $\mathcal{I}_{3,h}^{\text{FG}}$, which are derived in the following.

The derivation of integral $\mathcal{I}_{1,h}^{\text{FG}}$ is the same as $\mathcal{I}_{1,h}^{\text{VG}}$ and is derived in (5.52).

Since the integrals $\mathcal{I}_{2,h}^{\text{FG}}$ and $\mathcal{I}_{3,h}^{\text{FG}}$ are in the same form with different parameters, their derivations can be made as

$$\mathcal{I}_{\upsilon,o}^{\text{FG}} = \int_0^{\infty} \gamma_b^{a_1} e^{-b_1\gamma_b} G_{1,1}^{1,1} \left(\gamma_b \middle| \begin{matrix} 0 \\ 0 \end{matrix} \right) G_{0,2}^{2,0} \left(b_2\gamma_b \middle| \begin{matrix} -,- \\ a_2, a_2 \end{matrix} \right) \cdot d\gamma_b, \tag{5.62}$$

by using [118, (11)] and [83, (8.2.2-15)], the integral can be re-expressed as

$$\mathcal{I}_{\upsilon,o}^{\text{FG}} = b_1^{-a_1} \int_0^{\infty} G_{0,1}^{1,0} \left(b_1\gamma_b \middle| \begin{matrix} - \\ a_1 \end{matrix} \right) G_{1,1}^{1,1} \left(\gamma_b \middle| \begin{matrix} 0 \\ 0 \end{matrix} \right) G_{0,2}^{2,0} \left(b_2\gamma_b \middle| \begin{matrix} -,- \\ a_2, a_2 \end{matrix} \right) \cdot d\gamma_b, \tag{5.63}$$

and the resultant integral can be solved in terms of EGBMG function by using [175, (20)]

$$\mathcal{I}_{\upsilon,f}^{\text{FG}} = b_1^{-a_1} G_{1,1:0,1:0,2}^{1,1:1,0:2,0} \left(\begin{matrix} 1 \\ 1 \end{matrix} \middle| \begin{matrix} - \\ a_1 \end{matrix} \middle| \begin{matrix} -,- \\ a_2, a_2 \end{matrix} \middle| b_1, b_2 \right), \tag{5.64}$$

where $\upsilon \in \{2, 3\}$, and the parameters a_1, a_2, b_1, b_2 are given in Appendix C with (C.4).

$$C_S^{\text{FSO,FG}} = \frac{1}{\Gamma(\alpha_e)\Gamma(\beta_e)}\Bigg(\mathcal{I}_{1,o}^{\text{FG}} - C_0(1)\sum_{\ell_1=0}^{m_1-1} C_1(1)C_0(2)\sum_{\ell_2=0}^{m_2-1} C_1(2) \times \sum_{k=0}^{m_1-\ell_1-1} B_1\Big[B_2\mathcal{I}_{2,o}^{\text{FG}} - B_3\mathcal{I}_{3,o}^{\text{FG}}\Big]\Bigg), \quad (5.65)$$

$$C_S^{\text{RF,FG}} = \frac{1}{\Gamma(m_e)}\Bigg(\mathcal{I}_{1,f}^{\text{FG}} - C_0(1)\sum_{\ell_1=0}^{m_1-1} C_1(1)C_0(2)\sum_{\ell_2=0}^{m_2-1} C_1(2) \times \sum_{k=0}^{m_1-\ell_1-1} B_1\Big[B_2\mathcal{I}_{2,f}^{\text{FG}} - B_3\mathcal{I}_{3,f}^{\text{FG}}\Big]\Bigg), \quad (5.66)$$

$$C_S^{\text{HYB,FG}} = C_0(e)\sum_{\ell_e=0}^{m_e-1} C_1(e)\Bigg(\mathcal{I}_{1,h}^{\text{FG}} - C_0(1)\sum_{\ell_1=0}^{m_1-1} C_1(1)C_0(2)\sum_{\ell_2=0}^{m_2-1} C_1(2) \times \sum_{k=0}^{m_1-\ell_1-1} B_1\Big[B_2\mathcal{I}_{2,h}^{\text{FG}} - B_3\mathcal{I}_{3,h}^{\text{FG}}\Big]\Bigg). \quad (5.67)$$

5.5.2 Secrecy Outage Probability

The metric SOP is widely used to characterize the secure communication between legitimate pairs, which is described the probability that the instantaneous secrecy capacity falls below a target secrecy rate $\mathcal{R}$, defined as [25, (10)]

$$\begin{aligned} P_{SO} &= \text{Prob.}\big(C_S(\gamma_b,\gamma_e) \le \mathcal{R}\big), \\ &= \text{Prob.}\big(\gamma_b \le 2^{\mathcal{R}}(\gamma_e+1)-1\big), \\ &= \int_0^{\infty} F_{\gamma_b}\big(2^{\mathcal{R}}(\gamma_e+1)-1\big) f_{\gamma_e}\big(\gamma_e\big)\cdot d\gamma_e, \end{aligned} \quad (5.68)$$

where $\mathcal{R} > 0$. It is worthy to note that in some cases, an exact closed-form expression of SOP is not available due to the shifting operation in some special functions. However, instead, a lower

bound of SOP can be derived as follows [25, (11)]

$$\begin{aligned} P_{SO} &= \text{Prob.}\big(\gamma_b \leq 2^{\mathcal{R}}(\gamma_e+1)-1\big), \\ \geq P_{SO_L} &= \text{Prob.}\big(\gamma_b \leq 2^{\mathcal{R}}\gamma_e\big), \\ &= \int_0^{\infty} F_{\gamma_b}\big(2^{\mathcal{R}}\gamma_e\big) f_{\gamma_e}\big(\gamma_e\big)\cdot d\gamma_e. \end{aligned} \tag{5.69}$$

5.5.2.1 FSO Eavesdropper for Variable-Gain

For the FSO-type eavesdropper, the PDF of SNR $f_{\gamma_e}(\gamma_e)$ is given in (1.18). Therefore, by substituting (1.18) and (5.31) into (5.68), the SOP is obtained as (5.76), in terms of $\mathcal{T}_{1,o}^{\text{VG}}$, $\mathcal{T}_{2,o}^{\text{VG}}$ and $\mathcal{T}_{3,o}^{\text{VG}}$.

Since the integrals $\mathcal{T}_{1,o}^{\text{VG}}$, $\mathcal{T}_{2,o}^{\text{VG}}$ and $\mathcal{T}_{3,o}^{\text{VG}}$ are in the same form with different parameters, their derivations can be made as

$$\mathcal{T}_{\upsilon,o}^{\text{VG}} = \int_0^{\infty} \gamma_e^{a_1-1} e^{-a_2\gamma_e} G_{0,2}^{2,0}\left(\frac{\alpha_e\beta_e}{\sqrt{\overline{\gamma}_{e,o}}}\sqrt{\gamma_e}\,\middle|\, \begin{matrix} -,- \\ \frac{\alpha_e-\beta_e}{2}, \frac{\alpha_e-\beta_e}{2} \end{matrix}\right)\cdot d\gamma_e, \tag{5.70}$$

then, the resultant integral is solved by using [83, 2.24.1-1]

$$\mathcal{T}_{\upsilon,o}^{\text{VG}} = \frac{2^{\alpha_e-\beta_e} a_2^{-a_1}}{2\pi} G_{1,4}^{4,1}\left(\frac{\alpha_e^2\beta_e^2}{8a_2\overline{\gamma}_{e,o}}\,\middle|\, \begin{matrix} 1-a_1 \\ \frac{\alpha_e-\beta_e}{4}, \frac{\alpha_e-\beta_e+1}{4}, \frac{\alpha_e-\beta_e}{4}, \frac{\alpha_e-\beta_e+1}{4} \end{matrix}\right), \tag{5.71}$$

where $\upsilon \in \{1,2,3\}$, and the parameters a_1 and a_2 are given in Appendix C with (C.5).

5.5.2.2 RF Eavesdropper for Variable-Gain

For the RF-type eavesdropper, the PDF of SNR $f_{\gamma_e}(\gamma_e)$ is given in (1.7). Therefore, by substituting (1.7) and (5.31) into (5.68), the SOP is obtained as (5.77), in terms of $\mathcal{T}_{1,f}^{\text{VG}}$, $\mathcal{T}_{2,f}^{\text{VG}}$ and $\mathcal{T}_{3,f}^{\text{VG}}$.

Since the integrals $\mathcal{T}_{1,o}^{\text{VG}}$, $\mathcal{T}_{2,o}^{\text{VG}}$ and $\mathcal{T}_{3,o}^{\text{VG}}$ are in the same form with different parameters, their

derivations can be made as

$$\mathcal{T}_{\upsilon,f}^{\text{VG}} = \int_0^{\infty} \gamma_e^{a_1} e^{-a_2\gamma_e} \cdot d\gamma_e, \tag{5.72}$$

then, the resultant integral is solved by using [82, 3.351-3]

$$\mathcal{T}_{\upsilon,f}^{\text{VG}} = a_1! a_2^{-a_1-1}, \tag{5.73}$$

where $\upsilon \in \{1, 2, 3\}$, and the parameters a_1 and a_2 are given in Appendix C with (C.6).

5.5.2.3 Hybrid Eavesdropper for Variable-Gain

For the hybrid-type eavesdropper, the PDF of SNR $f_{\gamma_e}(\gamma_e)$ is given in (5.17). Therefore, by substituting (5.17) and (5.31) into (5.68), the SOP is obtained as (5.78), in terms of $\mathcal{T}_{1,o}^{\text{VG}}$, $\mathcal{T}_{2,o}^{\text{VG}}$, $\mathcal{T}_{3,o}^{\text{VG}}$, $\mathcal{T}_{4,o}^{\text{VG}}$, $\mathcal{T}_{5,o}^{\text{VG}}$ and $\mathcal{T}_{6,o}^{\text{VG}}$.

Similar to the RF eavesdropper case for variable-gain case, $\mathcal{T}_{1,o}^{\text{VG}}$, $\mathcal{T}_{2,o}^{\text{VG}}$, $\mathcal{T}_{3,o}^{\text{VG}}$, $\mathcal{T}_{4,o}^{\text{VG}}$, $\mathcal{T}_{5,o}^{\text{VG}}$ and $\mathcal{T}_{6,o}^{\text{VG}}$ are in the same form with different parameters, their derivations can be made as

$$\mathcal{T}_{\upsilon,f}^{\text{VG}} = \int_0^{\infty} \gamma_e^{a_1} e^{-a_2\gamma_e} \cdot d\gamma_e, \tag{5.74}$$

then, the resultant integral is solved by using [82, 3.351-3]

$$\mathcal{T}_{\upsilon,f}^{\text{VG}} = a_1! a_2^{-a_1-1}, \tag{5.75}$$

where $\upsilon \in \{1, 2, 3, 4, 5, 6\}$, and the parameters a_1 and a_2 are given in Appendix C with (C.7).

$$P_{SO}^{\text{FSO,VG}} = \frac{(\alpha_e\beta_e)^{\frac{(\alpha_e+\beta_e)}{2}}}{\Gamma(\alpha_e)\Gamma(\beta_e)\overline{\gamma}_{e,o}^{\frac{\alpha_e+\beta_e}{4}}}\Bigg[C_0(1)\sum_{\ell=0}^{m_1-1}C_1(1)\sum_{k=0}^{m_1-\ell-1}A_1\mathcal{T}_{1,o}^{\text{VG}} + C_0(2)\sum_{\ell=0}^{m_2-1}C_1(2) \times \sum_{k=0}^{m_2-\ell-1}A_2\mathcal{T}_{2,o}^{\text{VG}} - C_0(1)C_0(2)\sum_{\ell=0}^{m_1-1}C_1(1)\sum_{\ell=0}^{m_2-1}C_1(2) \times \sum_{k=0}^{m_1+m_2-2\ell-2}A_3\mathcal{T}_{3,o}^{\text{VG}}\Bigg]. \tag{5.76}$$

$$P_{SO}^{\text{RF,VG}} = \frac{m_e^{m_e}}{\Gamma(m_e)\overline{\gamma}_{e,f}^{m_e}}\Bigg[C_0(1)\sum_{\ell=0}^{m_1-1}C_1(1)\sum_{k=0}^{m_1-\ell-1}A_1\mathcal{T}_{1,f}^{\text{VG}} + C_0(2)\sum_{\ell=0}^{m_2-1}C_1(2)\sum_{k=0}^{m_2-\ell-1}A_2\mathcal{T}_{2,f}^{\text{VG}} - C_0(1)C_0(2)\sum_{\ell=0}^{m_1-1}C_1(1)\sum_{\ell=0}^{m_2-1}C_1(2)\sum_{k=0}^{m_1+m_2-2\ell-2}A_3\mathcal{T}_{3,f}^{\text{VG}}\Bigg], \tag{5.77}$$

$$P_{SO}^{\text{HYB,VG}} = C_0(e)\sum_{\ell=0}^{m_e-1}C_1(e)\Bigg[C_0(1)\sum_{\ell=0}^{m_1-1}C_1(1)\sum_{k=0}^{m_1-\ell-1}A_1\Big((m_e-\ell-2)\mathcal{T}_{1,h}^{\text{VG}} - \frac{m_e}{\overline{\gamma}_{e,f}}\mathcal{T}_{2,h}^{\text{VG}}\Big) + C_0(2)\sum_{\ell=0}^{m_2-1}C_1(2)\sum_{k=0}^{m_2-\ell-1}A_2\Big((m_e-\ell-2)\mathcal{T}_{3,h}^{\text{VG}} - \frac{m_e}{\overline{\gamma}_{e,f}}\mathcal{T}_{4,h}^{\text{VG}}\Big) - C_0(1)C_0(2)\sum_{\ell=0}^{m_1-1}C_1(1)\sum_{\ell=0}^{m_2-1}C_1(2)\sum_{k=0}^{m_1+m_2-2\ell-2} \times A_3\Big((m_e-\ell-2)\mathcal{T}_{5,h}^{\text{VG}} - \frac{m_e}{\overline{\gamma}_{e,f}}\mathcal{T}_{6,h}^{\text{VG}}\Big)\Bigg]. \tag{5.78}$$

5.5.2.4 FSO Eavesdropper for Fixed-Gain

For the FSO-type eavesdropper considering fixed-gain relay scheme, the PDF of SNR $f_{\gamma_e}(\gamma_e)$ is given in (1.18). Accordingly, by substituting (1.18) and (5.28) into (5.69), the lower bound of SOP is obtained as (5.85), in terms of $\mathcal{T}_{1,o}^{\text{FG}}$, and $\mathcal{T}_{2,o}^{\text{FG}}$.

Since the integrals $\mathcal{T}_{1,o}^{\text{FG}}$ and $\mathcal{T}_{2,o}^{\text{FG}}$ are in the same form with different parameters, their deriva-

tions can be made as

$$\mathcal{T}_{\upsilon,o}^{\text{FG}} = \int_0^\infty G_{0,1}^{1,0}\left(\frac{m_1 2^{\mathcal{R}}}{\overline{\gamma}_{1,f}}\gamma_e \middle| \begin{matrix} - \\ a_1 \end{matrix}\right) G_{0,2}^{2,0}\left(\frac{\mathcal{G}m_1 m_2 2^{\mathcal{R}}}{\overline{\gamma}_{1,f}\overline{\gamma}_{2,f}}\gamma_e \middle| \begin{matrix} -,- \\ a_2, a_2 \end{matrix}\right) G_{0,2}^{2,0}\left(\frac{\alpha_e\beta_e}{\sqrt{\overline{\gamma}_{e,o}}}\sqrt{\gamma_e} \middle| \begin{matrix} -,- \\ \frac{\alpha_e-\beta_e}{2}, \frac{\alpha_e-\beta_e}{2} \end{matrix}\right)\cdot d\gamma_e, \tag{5.79}$$

and the resultant integral can be solved in terms of EGBMG function by using [175, (20)]

$$\mathcal{T}_{\upsilon,o}^{\text{FG}} = \frac{\overline{\gamma}_{1,f}}{m_1 2^{\mathcal{R}}} G_{0,1:0,2:0,2}^{1,0:2,0:2,0}\left(\begin{matrix} a_1+1 \\ - \end{matrix} \middle| \begin{matrix} -,- \\ a_2, a_2 \end{matrix} \middle| \begin{matrix} -,- \\ \frac{\alpha_e-\beta_e}{2}, \frac{\alpha_e-\beta_e}{2} \end{matrix} \middle| \frac{\mathcal{G}m_2}{\overline{\gamma}_{2,f}}, \frac{\alpha_e\beta_e\overline{\gamma}_{1,f}}{m_1 2^{\mathcal{R}}\sqrt{\overline{\gamma}_{e,o}}}\right), \tag{5.80}$$

where $\upsilon \in \{1, 2\}$, and the parameters a_1 and a_2 are given in Appendix C with (C.8).

5.5.2.5 RF Eavesdropper for Fixed-Gain

For the RF-type eavesdropper considering fixed-gain relay scheme, the PDF of SNR $f_{\gamma_e}(\gamma_e)$ is given in (1.7). Therefore, by substituting (1.7) and (5.28) into (5.69), the lower bound of SOP is obtained as (5.86), in terms of $\mathcal{T}_{1,f}^{\text{FG}}$, and $\mathcal{T}_{2,f}^{\text{FG}}$.

Since the integrals $\mathcal{T}_{1,f}^{\text{FG}}$ and $\mathcal{T}_{2,f}^{\text{FG}}$ are in the same form with different parameters, their derivations can be made as

$$\mathcal{T}_{\upsilon,f}^{\text{FG}} = \int_0^\infty G_{0,1}^{1,0}\left(\frac{m_1 2^{\mathcal{R}}}{\overline{\gamma}_{1,f}}\gamma_e \middle| \begin{matrix} - \\ a_1 \end{matrix}\right) G_{0,2}^{2,0}\left(\frac{\mathcal{G}m_1 m_2 2^{\mathcal{R}}}{\overline{\gamma}_{1,f}\overline{\gamma}_{2,f}}\gamma_e \middle| \begin{matrix} -,- \\ a_2, a_2 \end{matrix}\right) G_{0,1}^{1,0}\left(\frac{m_e}{\overline{\gamma}_{e,f}}\gamma_e \middle| \begin{matrix} - \\ m_e - 1 \end{matrix}\right)\cdot d\gamma_e, \tag{5.81}$$

and the resultant integral can be solved in terms of EGBMG function by using [175, (20)]

$$\mathcal{T}_{\upsilon,f}^{\text{FG}} = \frac{\overline{\gamma}_{1,f}}{m_1 2^{\mathcal{R}}} G_{0,1:0,2:0,1}^{1,0:2,0:1,0}\left(\begin{matrix} a_1+1 \\ - \end{matrix} \middle| \begin{matrix} -,- \\ a_2, a_2 \end{matrix} \middle| \begin{matrix} -,- \\ m_e - 1 \end{matrix} \middle| \frac{\mathcal{G}m_2}{\overline{\gamma}_{2,f}}, \frac{\alpha_e\beta_e\overline{\gamma}_{1,f}}{m_1 2^{\mathcal{R}}\sqrt{\overline{\gamma}_{e,o}}}\right), \tag{5.82}$$

where $\upsilon \in \{1, 2\}$, and the parameters a_1 and a_2 are given in Appendix C with (C.8).

5.5.2.6 *Hybrid Eavesdropper for Fixed-Gain*

For the hybrid-type eavesdropper considering fixed-gain relay scheme, the PDF of SNR $f_{\gamma_e}(\gamma_e)$ is given in (5.17). Therefore, by substituting (5.17) and (5.28) into (5.69), the lower bound of SOP is obtained as (5.87), in terms of $\mathcal{T}_{1,h}^{\text{VG}}$, $\mathcal{T}_{2,h}^{\text{VG}}$, $\mathcal{T}_{3,h}^{\text{VG}}$ and $\mathcal{T}_{4,h}^{\text{VG}}$.

Since $\mathcal{T}_{1,h}^{\text{VG}}$, $\mathcal{T}_{2,h}^{\text{VG}}$, $\mathcal{T}_{3,h}^{\text{VG}}$ and $\mathcal{T}_{4,h}^{\text{VG}}$ are in the same form with different parameters, their derivations can be made as

$$\mathcal{T}_{\upsilon,h}^{\text{HYB}} = \int_0^\infty G_{0,1}^{1,0}\left(\frac{m_e}{\overline{\gamma}_{e,f}}\gamma_e \middle| \begin{matrix} - \\ a_3 \end{matrix}\right) G_{0,1}^{1,0}\left(\frac{m_1 2^{\mathcal{R}}}{\overline{\gamma}_{1,f}}\gamma_e \middle| \begin{matrix} - \\ a_1 \end{matrix}\right) G_{0,2}^{2,0}\left(\frac{\mathcal{G} m_1 m_2 2^{\mathcal{R}}}{\overline{\gamma}_{1,f}\overline{\gamma}_{2,f}}\gamma_e \middle| \begin{matrix} -,- \\ a_2, a_2 \end{matrix}\right) \cdot d\gamma_e, \tag{5.83}$$

and the resultant integral can be solved in terms of EGBMG function by using [175, (20)]

$$\mathcal{T}_{\upsilon,h}^{\text{FG}} = \frac{\overline{\gamma}_{1,f}}{m_1 2^{\mathcal{R}}} G_{0,1:0,1:0,2}^{1,0:1,0:2,0}\left(\begin{matrix} a_1+1 \\ - \end{matrix} \middle| \begin{matrix} - \\ a_3 \end{matrix} \middle| \begin{matrix} -,- \\ a_2, a_2 \end{matrix} \middle| \frac{m_e \overline{\gamma}_{1,f}}{m_1 2^{\mathcal{R}} \sqrt{\overline{\gamma}_{e,f}}}, \frac{\mathcal{G} m_2}{\overline{\gamma}_{2,f}}\right), \tag{5.84}$$

where $\upsilon \in \{1,2,3,4\}$, and the parameters a_1, a_2 and a_3 are given in Appendix C with (C.9).

$$P_{SO_L}^{\text{FSO,FG}} = \frac{(\alpha_e \beta_e)^{\frac{(\alpha_e+\beta_e)}{2}}}{\Gamma(\alpha_e)\Gamma(\beta_e)\overline{\gamma}_{e,o}^{\frac{\alpha_e+\beta_e}{4}}} C_0(1) \sum_{\ell_1=0}^{m_1-1} C_1(1) C_0(2) \sum_{\ell_2=0}^{m_2-1} C_1(2) \sum_{k=0}^{m_1-\ell_1-1} B_1 \left[\widehat{B}_2 \mathcal{T}_{1,o}^{\text{FG}} - \widehat{B}_3 \mathcal{T}_{2,o}^{\text{FG}}\right], \tag{5.85}$$

$$P_{SO_L}^{\text{RF,FG}} = \frac{m_e^{m_e}}{\Gamma(m_e)\overline{\gamma}_{e,f}^{m_e}} \left(\frac{m_e}{\overline{\gamma}_{e,f}}\right)^{-(m_e-1)} C_0(1) \sum_{\ell_1=0}^{m_1-1} C_1(1) C_0(2) \sum_{\ell_2=0}^{m_2-1} C_1(2) \times \sum_{k=0}^{m_1-\ell_1-1} B_1 \left[\widehat{B}_2 \mathcal{T}_{1,f}^{\text{FG}} - \widehat{B}_3 \mathcal{T}_{2,f}^{\text{FG}}\right], \tag{5.86}$$

$$P_{SO_L}^{\text{HYB,FG}} = C_0(e) \sum_{\ell=0}^{m_e-1} C_1(e) C_0(1) \sum_{\ell_1=0}^{m_1-1} C_1(1) C_0(2) \sum_{\ell_2=0}^{m_2-1} C_1(2) \sum_{k=0}^{m_1-\ell_1-1} B_1 \left(\frac{m_e}{\overline{\gamma}_{e,f}}\right)^{-(m_e-\ell-1)} \times \left[(m_e-\ell-2)\left(\frac{m_e}{\overline{\gamma}_{e,f}}\right)^{-(m_e-\ell-2)} \left(\widehat{B}_2 \mathcal{T}_{1,h}^{\text{FG}} - \widehat{B}_3 \mathcal{T}_{3,h}^{\text{FG}}\right) - \widehat{B}_2 \mathcal{T}_{2,h}^{\text{FG}} + \widehat{B}_3 \mathcal{T}_{4,h}^{\text{FG}}\right]. \tag{5.87}$$

5.5.3 Effective Secrecy Throughput

While conveying the information from source to destination over a relay, the system needs to satisfy a specific reliability level. To characterize this behavior of the system, we consider a metric called effective throughput T_{Eff}, which is defined in terms of the outage probability and is expressed as [72, 5]

$$T_{ES} = \mathcal{R} \times \big(1 - P_{SO}(\mathcal{R})\big). \tag{5.88}$$

5.5.3.1 Variable-Gain Relaying

For the variable-gain relaying scheme, the effective throughput is calculated by using SOP metric for FSO, RF and hybrid eavesdroppers, respectively, given as

$$T_{ES}^{\text{FSO,VG}}(\mathcal{R}) = \mathcal{R} \times \big(1 - P_{SO}^{\text{FSO,VG}}(2^{\mathcal{R}} - 1)\big), \tag{5.89}$$

$$T_{ES}^{\text{RF,VG}}(\mathcal{R}) = \mathcal{R} \times \big(1 - P_{SO}^{\text{RF,VG}}(2^{\mathcal{R}} - 1)\big), \tag{5.90}$$

$$T_{ES}^{\text{HYB,VG}}(\mathcal{R}) = \mathcal{R} \times \big(1 - P_{SO}^{\text{HYB,VG}}(2^{\mathcal{R}} - 1)\big), \tag{5.91}$$

where $P_{SO}^{\text{FSO,VG}}$, $P_{SO}^{\text{RF,VG}}$ and $P_{SO}^{\text{HYB,VG}}$ denote the SOP, as given in (5.76), (5.77) and (5.78), respectively.

5.5.3.2 Fixed-Gain Relaying

For the fixed-gain relaying scheme, the effective throughput is calculated by using the lower bound of SOP metric for FSO, RF and hybrid eavesdroppers, respectively, given as

$$T_{ES_L}^{\text{FSO,FG}}(\mathcal{R}) = \mathcal{R} \times \big(1 - P_{SO_L}^{\text{FSO,FG}}(2^{\mathcal{R}} - 1)\big), \tag{5.92}$$

$$T_{ES_L}^{\text{RF,FG}}(\mathcal{R}) = \mathcal{R} \times \big(1 - P_{SO_L}^{\text{RF,FG}}(2^{\mathcal{R}} - 1)\big), \tag{5.93}$$

$$T_{ES_L}^{\text{HYB,FG}}(\mathcal{R}) = \mathcal{R} \times \big(1 - P_{SO_L}^{\text{HYB,FG}}(2^{\mathcal{R}} - 1)\big), \tag{5.94}$$

where $P_{SO_L}^{\text{FSO,FG}}$, $P_{SO_L}^{\text{RF,FG}}$ and $P_{SO_L}^{\text{HYB,FG}}$ denote the lower bound of SOP, as given in (5.85), (5.86) and (5.87), respectively.

5.6 Results and Discussion

To present the analytical correctness of the proposed mathematical expressions in Sections 5.4 and 5.5, Monte-Carlo based simulations are given including related theoretical findings. Specifically, detailed investigations of the outage and secrecy performance of dual-hop relaying hybrid FSO-*mm*Wave transmissions are presented in terms of the ergodic capacity, outage probability and effective throughput with the aid of PDFs and CDFs of overall end-to-end instantaneous SNRs. The results provided in this section include several cases which consists of different fundamental system variables like atmospheric conditions, relaying methods, link distances, and average SNRs.

5.6.1 Outage Performance Analysis

A comparison of the outage performance of a relay-based dual-hop hybrid FSO-RF system as a function of the average SNR at first- and second-hop is illustrated in Figs. 5.2 and 5.3 for heterodyne and IM/DD detection techniques, respectively. The performance results of single-hop hybrid and dual-hop mixed FSO-RF system are also included as a benchmark. The performance of two well-known AF relaying scheme are illustrated in clean weather conditions, where the distance in first hop d_1 and second hop d_2 is assumed to be the same as $1.25\,\text{km}$. Additionally, the gain A is set to 0.5 for fixed-gain relaying scheme. Since we consider the same distance and weather condition in each hop, the turbulence parameters are calculated as $\alpha_1 = \alpha_2 = 3.58$, $\beta_1 = \beta_2 = 3.33$, where the Nakagami-m parameter is set to $m_1 = m_2 = 1$. Also, the threshold of outage probability is considered as $\mathcal{R} = 1\,\text{bit}$. As expected, the fixed-gain scheme performs better than the variable-gain, since fixed-gain scheme exploits the full channel state information. Additionally, it can easily seen from the figure that the proposed dual-hop system outperforms the single-hop parallel and dual-hop mixed hybrid systems for both fixed-gain and variable-gain relay methods including heterodyne and IM/DD detection techniques. For instance, considering the heterodyne detection in FSO link, at a fixed end-to-end SNR of $15\,\text{dB}$, the proposed system

experience outage with probabilities of 2×10^{-5} and 5×10^{-5} for fixed-gain and variable-gain, respectively, where these probabilities are 3×10^{-3} and 3×10^{-3} for dual-hop mixed system. Additionally, single-hop parallel system provides an outage probability of 5×10^{-4}. It is clear from the figures that the proposed relay-based dual-hop hybrid system outperforms both benchmark systems for heterodyne and IM/DD detection techniques.

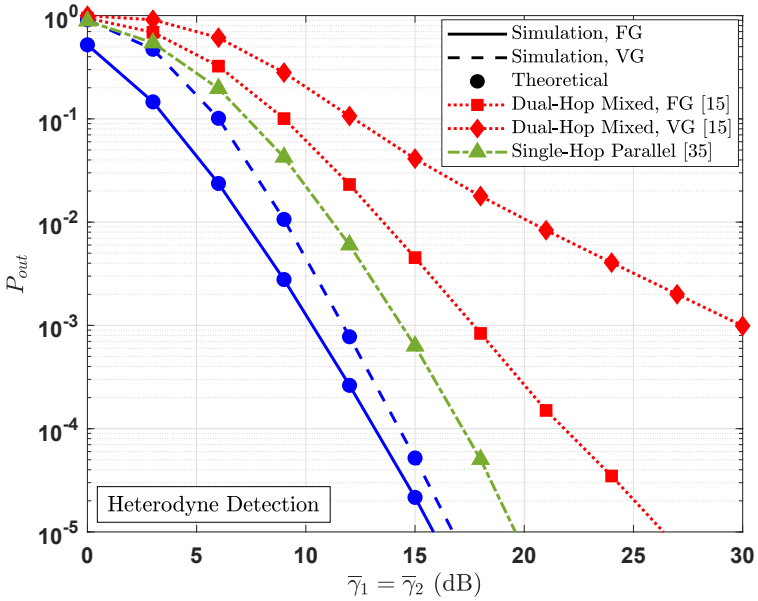


Figure 5.2: A comparison of outage probability as a function of overall system SNR for proposed and reference studies. (Clean weather, $\xi = 1.1$, $\mathcal{R} = 1$ bit, $d_1 = d_2 = 1.25$ km, $m_1 = m_2 = 1$, $\alpha_1 = \alpha_2 = 3.58$, $\beta_1 = \beta_2 = 3.33$, $A = 0.5$)

In Figs. 5.4 and 5.5, the outage probability of the proposed dual-hop hybrid system is investigated for the fixed average SNR of each link, i.e., the average SNR of the first-hop is fixed at 12 dB in Fig. 5.4, and the average SNR of the second-hop is fixed at 12 dB in Fig. 5.5. In the figures, the impact of different weather conditions on the outage performance is examined for both fixed- and variable-gain relaying schemes over a distance of 1.5 km in each hop, considering a pointing error of $\xi = 6.7$ in FSO links, and the outage threshold is set to $\mathcal{R} = 2$ bits. It obvious that the weather conditions have significant effects on the system's outage performance for both

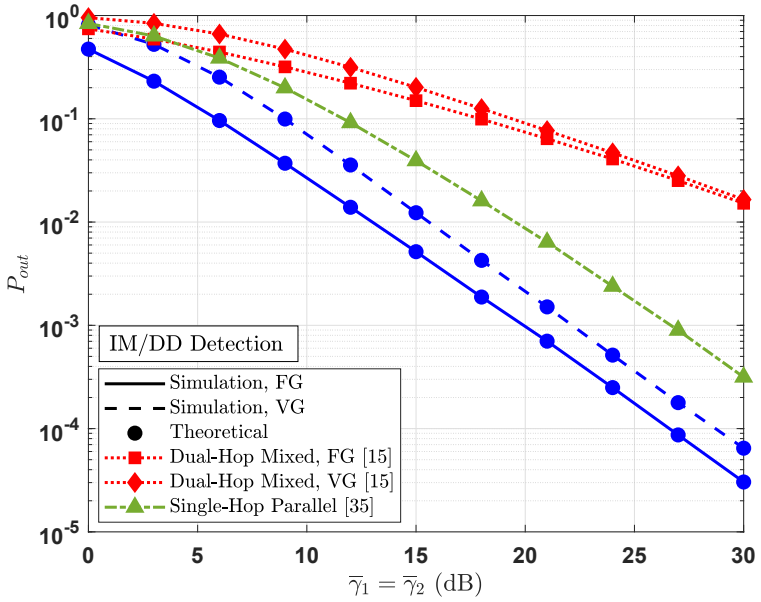


Figure 5.3: A comparison of outage probability as a function of overall system SNR for proposed and reference studies. (Clean weather, $\xi = 1.1$, $\mathcal{R} = 1$ bit, $d_1 = d_2 = 1.25$ km, $m_1 = m_2 = 1$, $\alpha_1 = \alpha_2 = 3.58$, $\beta_1 = \beta_2 = 3.33$, $A = 0.5$)

detection techniques. When the weather conditions become more severe, i.e., from clean to moderate rain, the transmission reliability decreases significantly. For example, in Fig. 5.4, considering a fixed average SNR of $\overline{\gamma}_2 = 20$ dB, the expected outage probabilities are 2×10^{-5}, 8×10^{-5} and 5×10^{-4} for clean, hazy and moderate rain weather conditions, respectively, with heterodyne detection. These number are, in turn, approximately 5×10^{-3}, 8×10^{-3} and 2×10^{-2} for IM/DD detection technique. Furthermore, in comparison between Figs. 5.4 and 5.5, one can easily observe the importance of the average SNR in the first-hop for fixed-gain AF relaying scheme. Since the amplification process directly depends on the received SNR at the relay node, the SNR of first-hop plays an important role on the outage performance for fixed-gain scheme. For instance, limiting the SNR in the first-hop creates a kind of noise floor, which results in a saturation in the reliability, and therefore, the outage performance cannot be improved beyond 10^{-5} for heterodyne detection in a clean weather condition, as seen in Fig. 5.4. However, increasing the SNR in the first-hop and limiting the SNR in the second-hop does not result in the same outage behavior for fixed-gain but for variable-gain AF relaying scheme. This is because of the variable-scheme technique always

utilizes the lowest SNR of both hops.

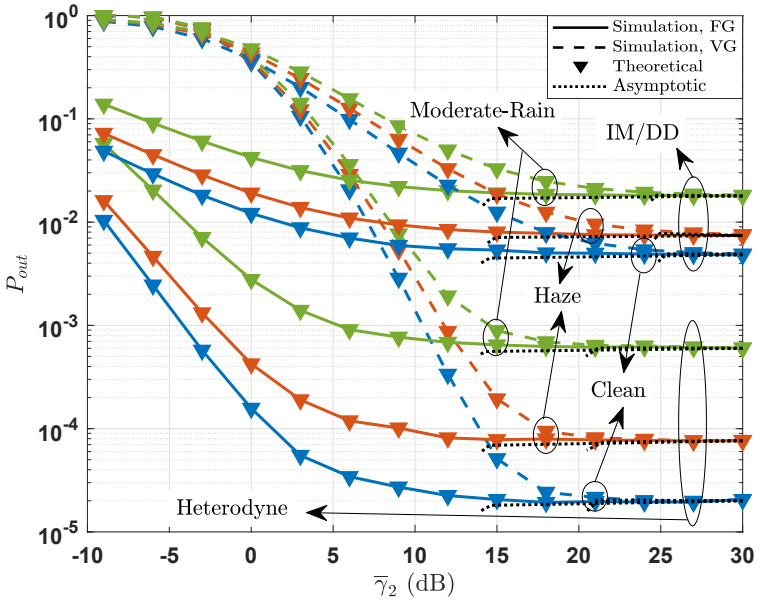


Figure 5.4: The probability of outage as a function of overall system SNR for different weather conditions. ($\xi = 6.7$, $d_1 = d_2 = 1.5$ km, $m_1 = m_2 = 1$, $A = 0.5$, $\mathcal{R} = 2$ bits, $\overline{\gamma}_1 = 12$ dB)

The outage probability of the proposed dual-hop hybrid system is illustrated for the fixed distance in each link considering different pointing errors, i.e., the distance in the first-hop is fixed at 1 km in Fig. 5.6, and the distance in the second-hop is fixed at 1 km in Fig. 5.7. The effect of pointing errors in FSO links on the outage performance is investigated for both fixed- and variable-gain schemes at fixed average SNR of $\overline{\gamma}_1 = \overline{\gamma}_2 = 10$ dB in hazy weather conditions, and the outage threshold is set to $\mathcal{R} = 2$ bits. From the figures, it can be observed that the pointing errors have remarkable influence on the outage probability for heterodyne technique. Recalling that $\xi \to \infty$ implies no pointing errors in the system, a decrease in the value of ξ, which means an increase in the pointing error, dramatically reduce the overall reliability of the transmission. For instance, in Fig. 5.6, considering a distance of $d_2 = 1$ km, the probabilities of transmission outage with fixed-gain relay scheme are 2×10^{-4}, 1×10^{-3} and 4×10^{-3} for the pointing errors of 6.7, 1.1 and 0.33, respectively. On the other hand, in Fig. 5.7, considering a distance of $d_1 = 1$ km, these probabili-

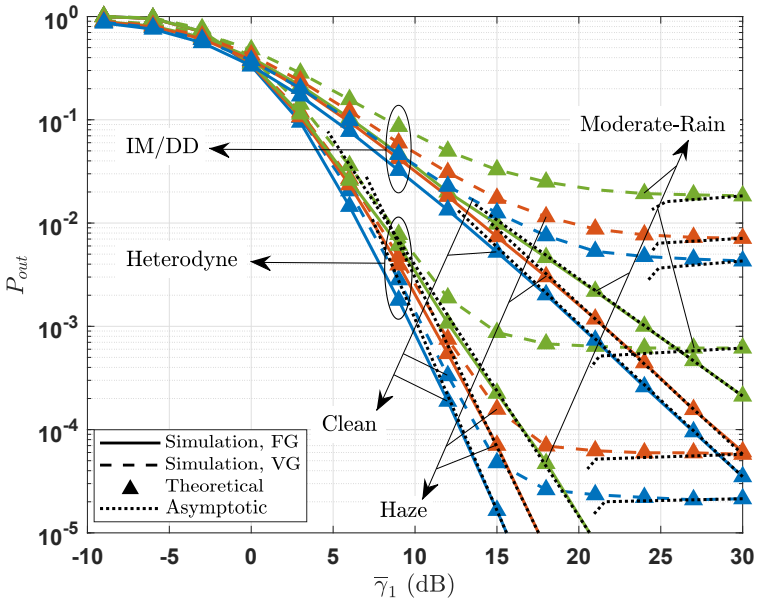


Figure 5.5: The probability of outage as a function of overall system SNR for different weather conditions. ($\xi = 6.7$, $d_1 = d_2 = 1.5$ km, $m_1 = m_2 = 1$, $A = 0.5$, $\mathcal{R} = 2$ bits, $\overline{\gamma}_2 = 12$ dB)

ties can be obtained as 5×10^{-5}, 1×10^{-3} and 4×10^{-3} for the pointing errors of 6.7, 1.1 and 0.33, respectively. Notice that the both scenarios provides approximately identical outage probabilities, however, when we look at the fixed distance lower than 1 km, we observe that the outage performance is not saturated and can be lower in comparison with higher distances. As in the previous two figures, this behavior, also, directly related with average SNR in the first-hop, since lowering the distance results in a higher SNR value.

The outage performance as a function of the overall end-to-end SNR at destination is represented in Fig. 5.8, considering the impact of several atmospheric circumstances on the system, with distance of $d_1 = 1$ km in the first hop and of $d_2 = 1.25$ km in the second hop. Nakagami-m parameters are set to $m_1 = m_2 = 1$. The turbulence parameters in the first hop are calculated as $\{\alpha_1 = 5.0096, \beta_1 = 4.7489\}$, $\{\alpha_1 = 14.6608, \beta_1 = 14.0573\}$ and $\{\alpha_1 = 50.7685, \beta_1 = 48.7564\}$ for clean, hazy and moderate rain weather conditions, where they are, in turn, calculated as $\{\alpha_2 = 3.5848, \beta_2 = 3.3349\}$, $\{\alpha_2 = 9.6652, \beta_2 = 9.2504\}$ and $\{\alpha_2 = 33.5727, \beta_2 = 32.2337\}$ for the second hop. As it is seen from the figure, the reliability performance is heavily degraded for

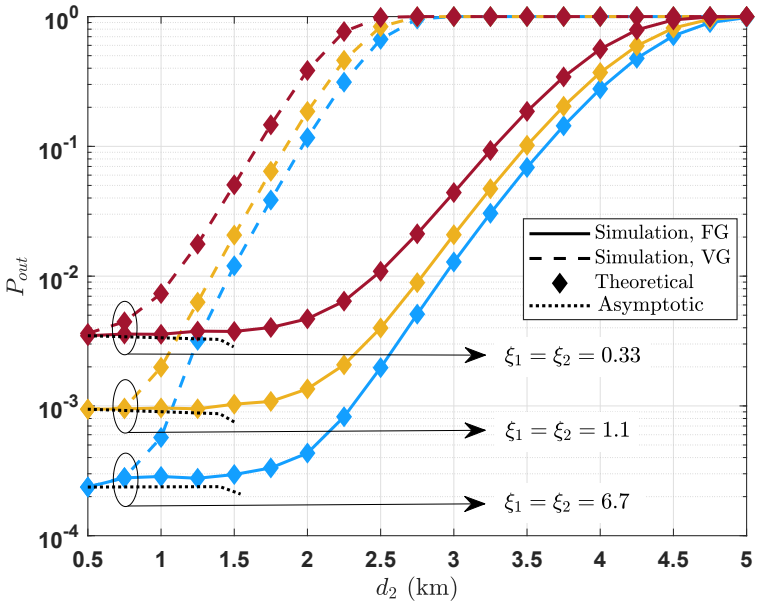


Figure 5.6: The impact of pointing error on the outage performance as a function of distance in second-hop. (Hazy weather, $m_1 = m_2 = 1$, $A = 0.5$, $\mathcal{R} = 2$ bits, $\overline{\gamma}_1 = \overline{\gamma}_2 = 10$ dB, $d_1 = 1$ km)

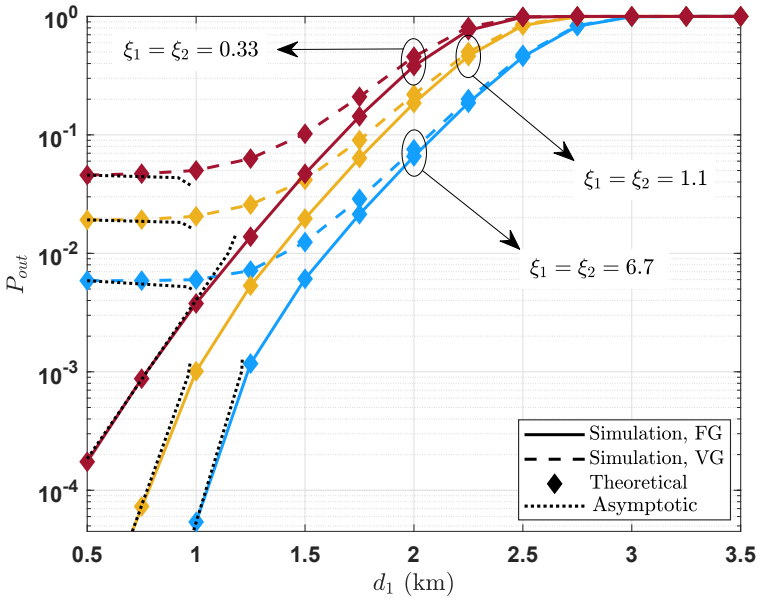


Figure 5.7: The impact of pointing error on the outage performance as a function of distance in first-hop. (Hazy weather, $m_1 = m_2 = 1$, $A = 0.5$, $\mathcal{R} = 2$ bits, $\overline{\gamma}_1 = \overline{\gamma}_2 = 15$ dB, $d_2 = 1.5$ km)

weather conditions when it goes from clean to moderate rain for both schemes. For each weather scenario, the variable-gain relaying scheme mostly performs lower outage probability compared

to fixed-gain scheme. To express it in a different way, regardless of a weather condition, variable-gain relaying provides better quality of service since it exploits the full channel state information. For instance, if we want to achieve a reliable communication with a probability of 10^{-2}, the minimum overall end-to-end SNR pair for variable- and fixed-gain schemes needs to approximately be $\{9, 16\}$, $\{9, 16\}$ and $\{9, 16\}$ dB for clean, hazy and moderate rain weather conditions, respectively.

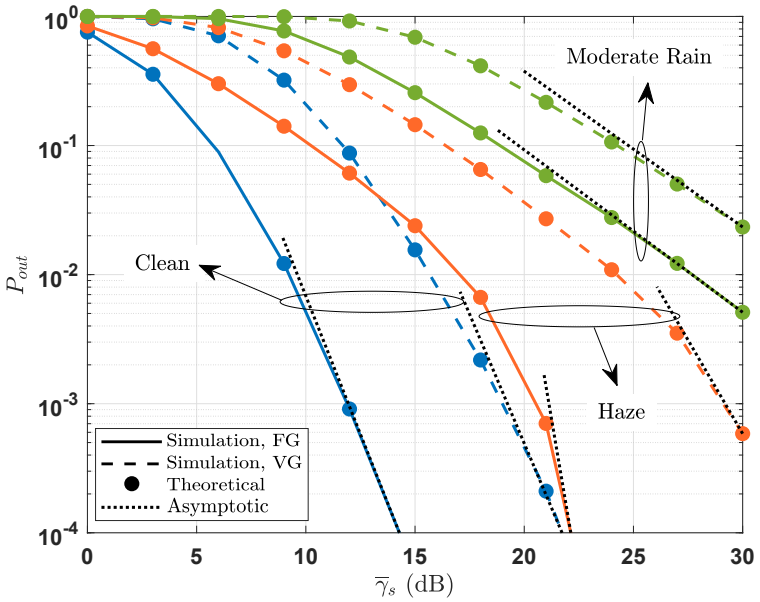


Figure 5.8: The probability of outage as a function of overall system SNR for different weather conditions. ($\xi = 6.7$, $d_1 = 1$ km, $d_2 = 1.25$ km, $m_1 = m_2 = 1$, $A = 0.5$, $\mathcal{R} = 2$ bits)

Alternatively, in Fig. 5.9, the probability of outage as a function of the distance is illustrated for different fixed overall end-to-end SNR in hazy weather conditions. The distance in first hop d_1 and in second hop d_2 is assumed to be the same as variable, and the threshold of outage probability is considered as $\mathcal{R} = 1$ bit. Since the distances d_1 and d_2 change for each case, the turbulence parameters α_1, β_1, α_2 and β_2 needs to be calculated separately based on (1.16) and (1.17), where Nakagami-m parameters are set to $m_1 = m_2 = 1$. The impact of end-to-end SNR can be easily observed from the figure, in which the higher overall SNR results in more reliable communication

system for each fixed- and variable-gain relaying schemes. For example, if we are required to satisfy at most 10^{-2} outage performance, the distance pair for fixed- and variable-gain schemes in each hop approximately needs to be $\{600, 700\}$ m, $\{800, 950\}$ m, and $\{900, 1050\}$ m for the fixed end-to-end SNRs of 3, 6 and 10 dB, respectively.

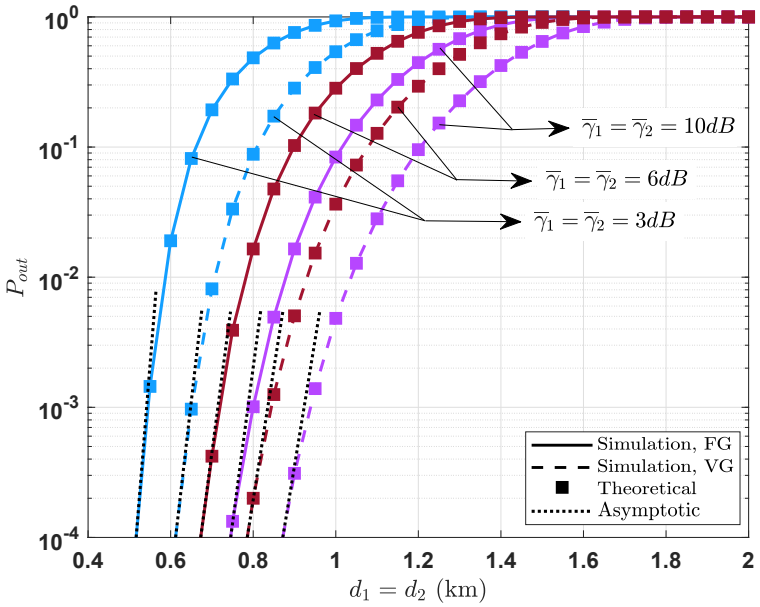


Figure 5.9: The probability of outage as a function of distances in the first- and second-hops for different fixed average SNRs with heterodyne. (Hazy weather, $\xi = 6.7$, $m_1 = m_2 = 1$, $A = 0.5$, $\mathcal{R} = 1$ bit)

Probability of outage as a function of its threshold value is represented in Fig. 5.10, considering the impact of different weather conditions on the system's reliability, with distances of $d_1 = 1.25$ km in the first hop and of $d_2 = 1.5$ km in the second hop. Nakagami-m parameters are set to $m_1 = 2$ and $m_2 = 1$. The turbulence parameters in the first hop are calculated as $\{\alpha_1 = 3.5848, \beta_1 = 3.3349\}$, $\{\alpha_1 = 9.6652, \beta_1 = 9.2504\}$ and $\{\alpha_1 = 33.5727, \beta_1 = 32.2337\}$ for clean, hazy and moderate rain weather conditions, where they are, in turn, calculated as $\{\alpha_2 = 3.0298, \beta_2 = 2.7187\}$, $\{\alpha_2 = 6.9095, \beta_2 = 6.5924\}$ and $\{\alpha_2 = 23.9161, \beta_2 = 22.9541\}$ for the second hop. For both relaying schemes, we can observe that the reliability performance is

dramatically degraded from clean to moderate rain weather conditions as well as with the increase of outage threshold value. For instance, if we consider a outage rate of $\mathcal{R} = 2$ bits, the probability pair of achieving a reliable communication for variable- and fixed-gain schemes are observed as $\{0.68\%, 17.08\%\}$, $\{10.49\%, 40.97\%\}$ and $\{56.73\%, 98.42\%\}$ for clean, hazy and moderate rain weather conditions, respectively.

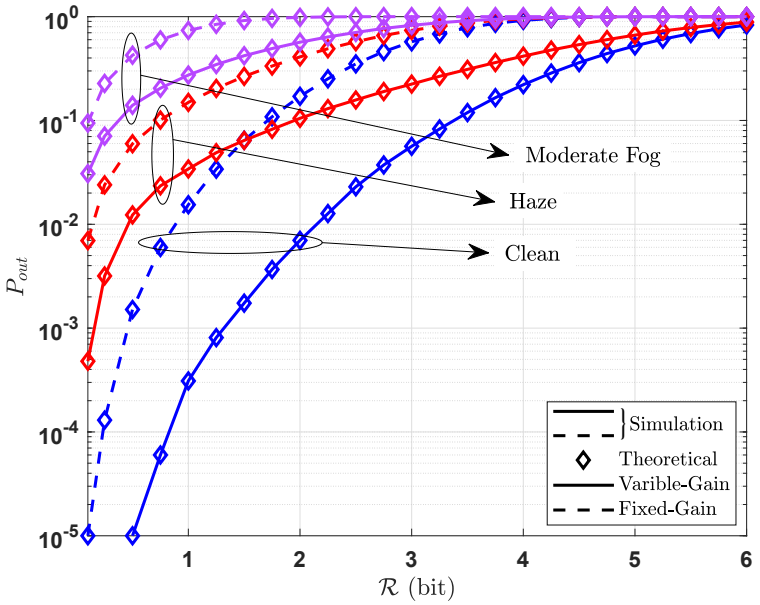


Figure 5.10: The probability of outage as a function of outage threshold for different weather conditions. ($d_1 = 1.25$ km, $d_2 = 1.5$ km, $\gamma_1 = 12$ dB, $\gamma_2 = 15$ dB, $m_1 = 2$, $m_2 = 1$, $A = 0.5$)

A comparison of the effective throughput metric as a function of the outage probability threshold is illustrated in Figs. 5.11 and 5.12 for two different relaying schemes to illustrate the outage performance of the proposed and the benchmark systems in hazy weather conditions. The distance in first hop d_1 and second hop d_2 is assumed to be 1 km and 1.25 km, respectively, while the Nakagami-m parameters are set to $m_1 = m_2 = 1$. Additionally, the turbulence parameters are calculated as $\alpha_1 = 14.6608$, $\beta_1 = 14.0573$, $\alpha_2 = 10.4284$, and $\beta_2 = 9.9853$. From the figure, we can easily observe that the proposed relaying system outperforms the benchmark system for both fixed-gain and variable-gain relaying schemes. For instance, if we consider an outage threshold

of $\mathcal{R} = 2$ bits, for fixed- and variable-gain schemes, the proposed and benchmark systems are able to satisfy the pair of effective throughput $\{1.6072, 1.7345\}$ bits and $\{0.2823, 0.8118\}$ bits, respectively, and additionally, if we consider an outage threshold of $\mathcal{R} = 3$ bits, these numbers are $\{1.7037, 2.1528\}$ bits and $\{0.0519, 0.4218\}$ bits, respectively. Moreover, we can observe that the effective throughput illustrates a non-monotonic behavior with the increase of outage threshold $\mathcal{R}$. In other words, when we increase the outage threshold, the effective throughput starts increasing, and then, it begins decreasing. We can explain this behavior as follows: the increment in outage threshold is higher than the increase in probability of outage, and therefore, effective throughput increases with the increase in threshold. However, after a specific value of threshold, the outage probability becomes dominant, and it dramatically increase the effective throughput.

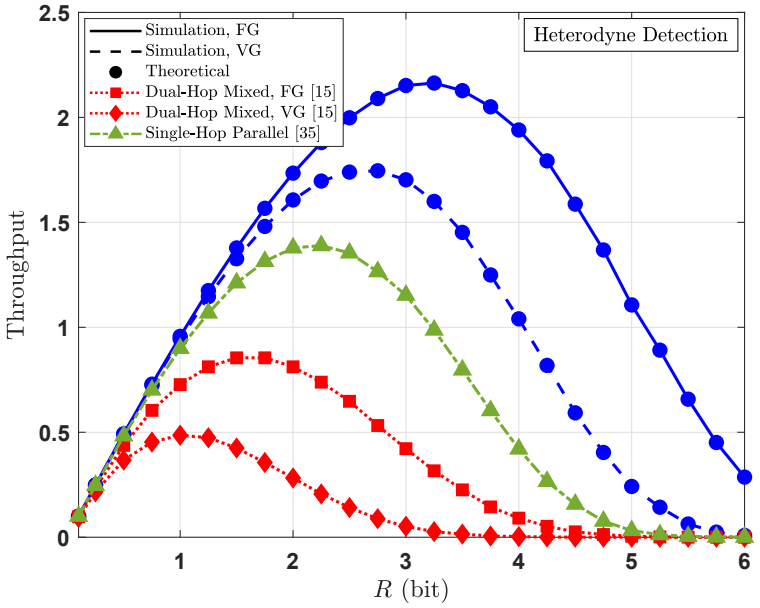


Figure 5.11: A comparison of effective throughput as a function of outage probability threshold with heterodyne detection for the proposed and the reference studies. (Haze weather, $\xi = 1.1$, $d_1 = 1$ km, $d_2 = 1.25$ km, $\gamma_1 = 10$ dB, $\gamma_2 = 15$ dB, $\alpha_1 = 14.6608$, $\beta_1 = 14.0573$, $\alpha_2 = 10.4284$, $\beta_2 = 9.9853$, $m_1 = m_2 = 1$, $A = 0.5$)

Effective throughput as a function of link distances is represented in Fig. 5.13 for different fixed overall end-to-end SNR in clean weather conditions. The distance in first hop d_1 and in second

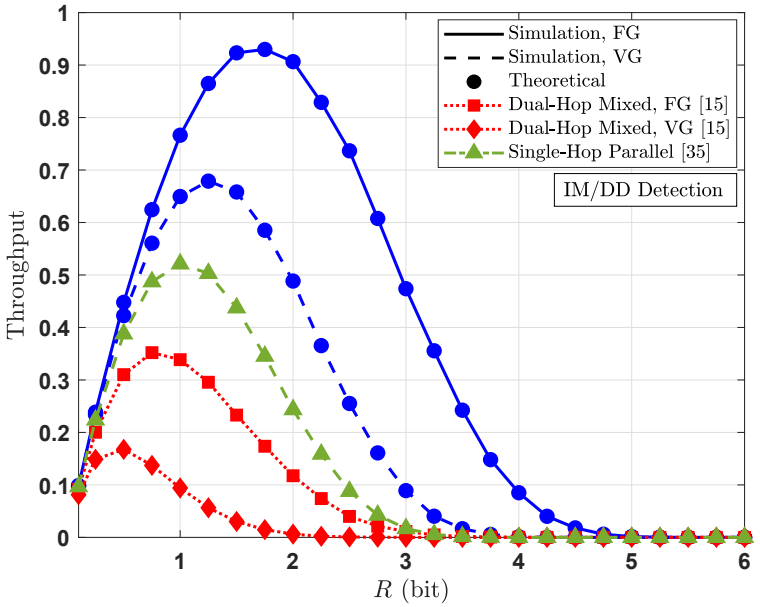


Figure 5.12: A comparison of effective throughput as a function of outage probability threshold with IM/DD detection for the proposed and the reference studies. (Haze weather, $\xi = 1.1$, $d_1 = 1\,\text{km}$, $d_2 = 1.25\,\text{km}$, $\gamma_1 = 10\,\text{dB}$, $\gamma_2 = 15\,\text{dB}$, $\alpha_1 = 14.6608$, $\beta_1 = 14.0573$, $\alpha_2 = 10.4284$, $\beta_2 = 9.9853$, $m_1 = m_2 = 1$, $A = 0.5$)

hop d_2 is assumed to be the same as variable, and the threshold of outage probability is considered as $\mathcal{R} = 3\,\text{bits}$, where Nakagami-$m$ parameters are set to $m_1 = m_2 = 2$. The impact of end-to-end SNR on the effective throughput can be easily observed from the figure. For instance, if we need to satisfy an effective throughput of $2\,\text{bits}$, the distance pair for fixed- and variable-gain schemes in each hop approximately needs to be $\{650, 800\}$ m and $\{1200, 1450\}$ m for the fixed end-to-end SNRs of 5 and $15\,\text{dB}$, respectively.

5.6.2 Secrecy Performance Analysis

A comparison of the secrecy capacity of a relay-based dual-hop hybrid FSO-RF system as a function of the average SNR at first- and second-hop is illustrated in Fig. 5.14 for different types of eavesdroppers. The secrecy performance of two well-known AF relaying schemes is illustrated in clean weather conditions, where the distance in first hop d_1 and second hop d_2 is assumed as $1\,\text{km}$ and $1.25\,\text{km}$, respectively. Additionally, the gain $\mathcal{G}$ is set to 0.5 for FG relaying scheme, and the average SNR at Eve is adjusted as $\overline{\gamma}_e = 5\,\text{dB}$. Since we consider the different distance values

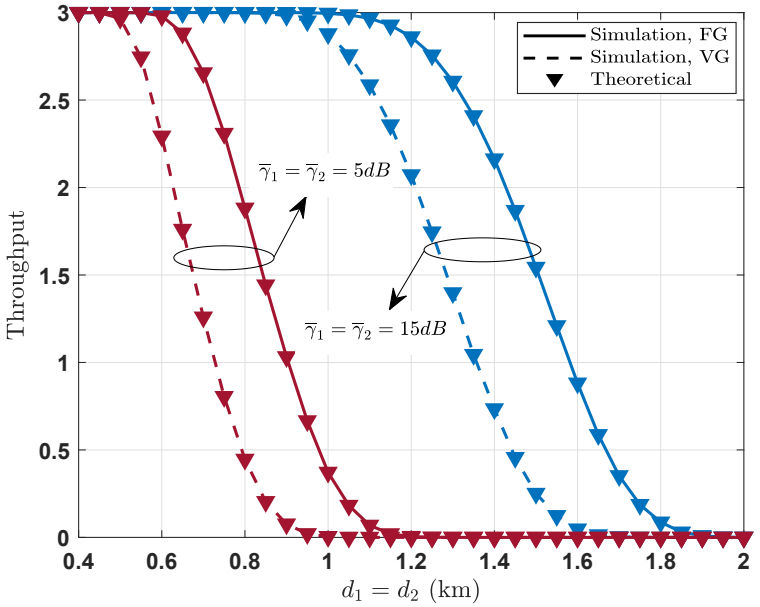


Figure 5.13: The effective throughput as a function of distances in the first- and second-hops for different fixed average SNRs with heterodyne. (Clean weather, $\xi = 1.1$, $m_1 = m_2 = 2$, $A = 0.5$, $\mathcal{R} = 3$ bits)

in each hop, the pairs of turbulence parameters are calculated as $(\alpha_1 = 5.0096, \beta_1 = 4.7489)$ and $(\alpha_2 = 4.2937, \beta_2 = 4.0462)$, where the Nakagami-$m$ parameter is set to $m_1 = m_2 = 1$. As expected, the FG scheme performs better than the VG, since FG scheme exploits the full channel state information. Additionally, it can easily seen from the figure that the hybrid-type eavesdropper dramatically decrease secrecy performance for both FG and VG relaying methods, in comparison with FSO- and RF-Eves. For instance, considering a fixed SNRs of 8 dB, the achievable average secrecy capacities are approximately $2.5, 1.8, 1$ bits for VG scheme in the presence of FSO-, RF- and hybrid eavesdroppers, respectively, where these values are $4.4, 4, 3.7$ bits for FG relaying scheme.

Since a hybrid eavesdropper has the most severe impact on the secrecy performance among other types, the secrecy capacity of the dual-hop hybrid system is investigated as a function of the link distances in the presence of a hybrid Eve, i.e., the link distance of the second-hop is fixed at 1 km in Fig. 5.15, and the link distance of the first-hop is fixed at 1 km in Fig. 5.16. In the figures, the impact of different weather conditions on the secure communication is examined for both

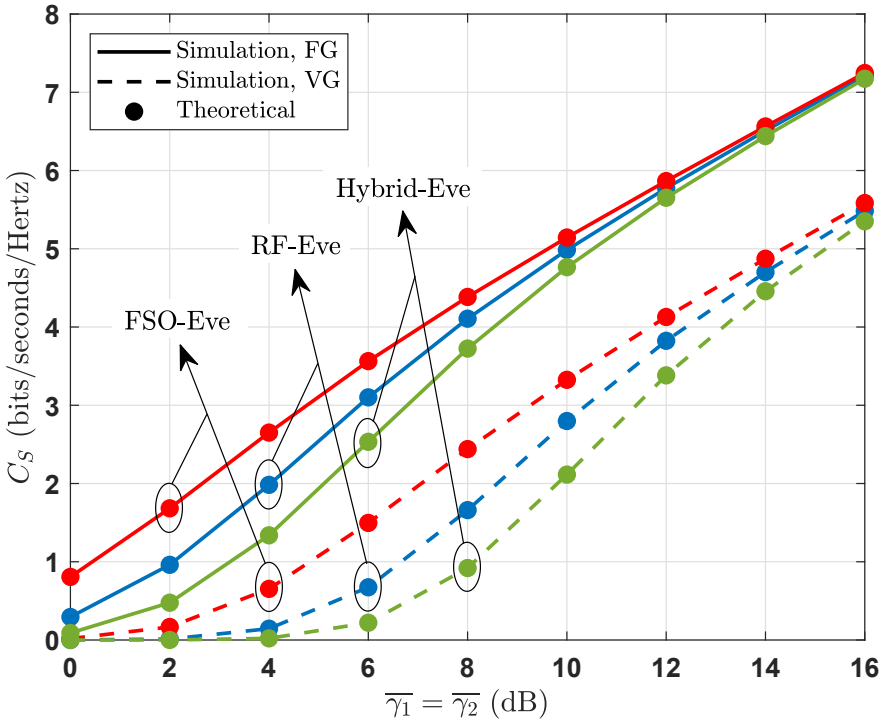


Figure 5.14: Average secrecy capacity as a function of the average SNR for different types of eavesdroppers. (Clean weather, $\mathcal{G} = 0.5$, $d_1 = 1\,\text{km}$, $d_2 = d_e = 1.25\,\text{km}$ $m_1 = m_2 = 1$, $\alpha_1 = 5.01$, $\beta_1 = 4.74$, $\alpha_2 = \alpha_e = 4.29$, $\beta_2 = \beta_e = 4.04$, $R_{1,o} = R_{1,f} = 0.8$, $R_{2,o} = R_{2,f} = 0.7$, $R_{e,o} = R_{e,f} = 0.2$, $\overline{\gamma}_e = 5\,\text{dB}$)

fixed- and variable-gain relaying schemes at the fixed SNRs of $\overline{\gamma}_1 = \overline{\gamma}_2 = 15\,\text{dB}$, and $\overline{\gamma}_e = 3\,\text{dB}$. It obvious that the weather conditions have significant effects on the system's secrecy performance for both relaying techniques. When the weather conditions become more severe, i.e., from clean to moderate rain, the transmission reliability decreases significantly. For instance, in Fig. 5.15, considering a link distance of $d_1 = 1\,\text{km}$, the expected secrecy capacity values are approximately 2.5, 4.2 and $5.9\,\text{bits}$ for moderate rain, hazy and clean weather conditions, respectively. These number are, in turn, approximately 4, 5.9 and $7.4\,\text{bits}$ for FG relaying scheme. Furthermore, one can easily observe the saturated behavior of the capacity curves in Fig. 5.15, which is because of the limited average SNR in the second-hop. On the other hand, limiting the average SNR in the first-hop results in a non-monotonic capacity performance.

In Figs. 5.17 and 5.18, the secrecy outage performance of the dual-hop hybrid system is in-

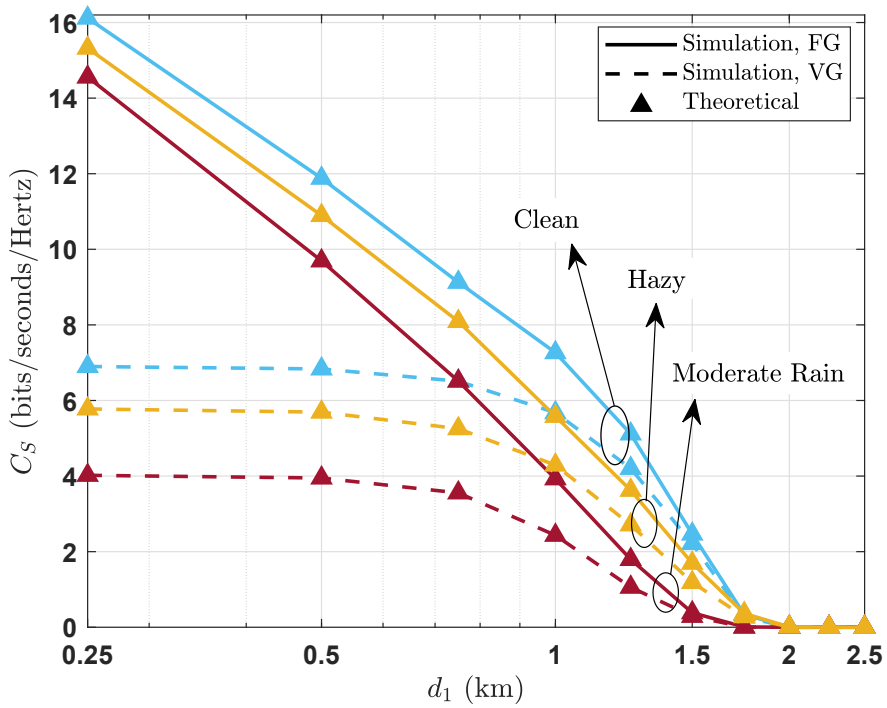


Figure 5.15: Average secrecy capacity as a function of the distance of first-hop in the presence of a hybrid-type Eve for different weather conditions. ($\mathcal{G} = 0.5$, $d_2 = d_e = 1\,\text{km}$, $m_1 = m_2 = 1$, $\alpha_2 = \alpha_e = 6.91$, $\beta_2 = \beta_e = 6.59$, $R_{1,o} = R_{1,f} = R_{2,o} = R_{2,f} = 0.75$, $R_{e,o} = R_{e,f} = 0.2$, $\overline{\gamma}_1 = \overline{\gamma}_1 = 15\,\text{dB}$, $\overline{\gamma}_e = 3\,\text{dB}$)

vestigated for the fixed average SNRs of each link, i.e., the average SNR of the first-hop is fixed at 11 dB in Fig. 5.17, and the average SNR of the second-hop is fixed at 11 dB in Fig. 5.18. In the figures, the impact of different types of eavesdroppers on the secrecy outage is presented for both fixed- and variable-gain relaying schemes over a distance of 1.5 km in each hop, considering a fixed SNR of $\overline{\gamma}_e = 3\,\text{dB}$ at Eve, and the outage threshold is set to $\mathcal{R} = 2\,\text{bits}$. It obvious that the different Eves have different effects on the system's secrecy performance for both relaying techniques. For instance, in Fig. 5.17, considering a fixed average SNR of $\overline{\gamma}_2 = 11\,\text{dB}$, the expected outage probabilities are 5×10^{-5}, 4×10^{-4} and 2×10^{-3} for FSO-, RF- and hybrid type eavesdroppers, respectively, with FG scheme. These number are, in turn, approximately 9×10^{-2}, 3×10^{-1} and 7×10^{-1} for VG relaying technique. Furthermore, in comparison between Figs. 5.17 and 5.18, one can easily observe the importance of the average SNR in the first-hop for FG AF relaying scheme. Since the amplification process directly depends on the received SNR at the re-

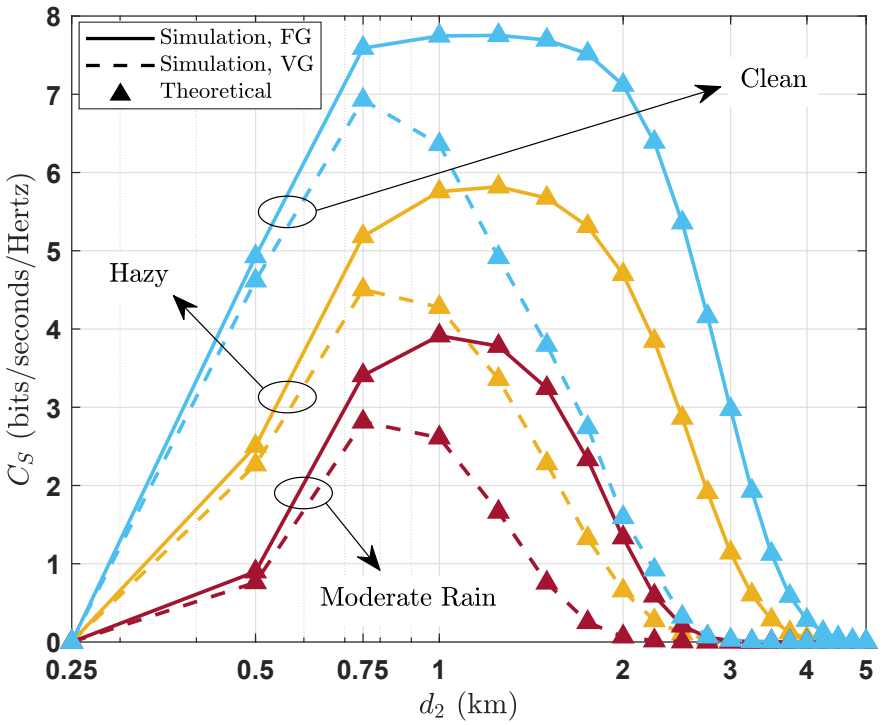


Figure 5.16: Average secrecy capacity as a function of the distance of second-hop in the presence of a hybrid-type Eve for different weather conditions. ($\mathcal{G} = 0.5$, $d_1 = 1\,\text{km}$, $m_1 = m_2 = 1$, $\alpha_1 = 6.91$, $\beta_1 = 6.59$, $R_{1,o} = R_{1,f} = R_{2,o} = R_{2,f} = 0.75$, $R_{e,o} = R_{e,f} = 0.2$, $\overline{\gamma}_1 = \overline{\gamma}_1 = 15\,\text{dB}$, $\overline{\gamma}_e = 3\,\text{dB}$)

lay node, the SNR of first-hop plays an important role on the secrecy outage performance for FG scheme. For instance, limiting the SNR in the first-hop creates a kind of noise floor, which results in a saturation in the reliability, and therefore, the outage performance cannot be improved beyond a specific point, as seen in Fig. 5.17. However, increasing the SNR in the first-hop and limiting the SNR in the second-hop does not result in the same outage behavior for FG but for VG AF relaying scheme. This is because of the variable-scheme technique always utilizes the lowest SNR of both hops.

The secrecy outage performance of the dual-hop hybrid system as a function of the outage threshold is illustrated in the presence of different types of eavesdroppers for FG and VF AF relaying schemes. The weather conditions are considered as clean, and the distances in each link assumed as $d_1 = d_2 = d_e = 2\,\text{km}$, while the average fixed SNRs is set to $\overline{\gamma}_1 = \overline{\gamma}_2 = 10\,\text{dB}$, and

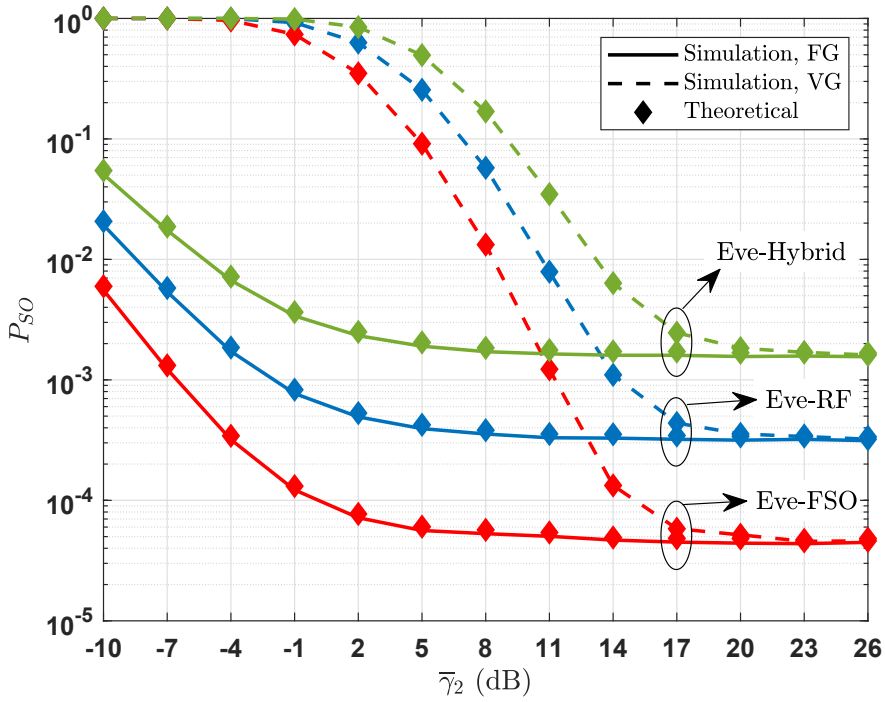


Figure 5.17: Secrecy outage probability as a function of average SNR at second-hop for different types of eavesdroppers. (Clean Weather, $\mathcal{G} = 0.5$, $\mathcal{R} = 1$ bits, $d_1 = d_2 = d_e = 1.5$ km, $m_1 = m_2 = 1$, $\alpha_1 = \alpha_2 = \alpha_e = 3.02$, $\beta_1 = \beta_2 = \beta_e = 2.71$, $R_{1,o} = R_{1,f} = R_{2,o} = R_{2,f} = 0.65$, $R_{e,o} = R_{e,f} = 0.15$, $\overline{\gamma}_1 = 10$ dB, $\overline{\gamma}_e = 3$ dB)

$\overline{\gamma}_e = 3$ dB. Accordingly, the optical channel parameters are calculated as $\alpha_1 = \alpha_2 = \alpha_e = 3.31$, and $\beta_1 = \beta_2 = \beta_e = 2.58$, where the Nakagami-$m$ parameters are set to $m_1 = m_2 = 1$. As expected, increasing the outage threshold decreases the secrecy performance, however, the average throughput also increases as a tradeoff.

A comparison of the effective throughput metric as a function of the outage probability threshold is illustrated in Figs. 5.20 for two different relaying schemes to illustrate the secrecy performance of the hybrid system in the presence of different types of eavesdroppers. The distance in first-hop d_1 and second-hop d_2 is assumed the same as 1.75 km, while the Nakagami-m parameters are set to $m_1 = m_2 = 1$. Additionally, the turbulence parameters are calculated as $\alpha_1 = \alpha_2 = \alpha_e = 2.9846$, and $\beta_1 = \beta_2 = \beta_e = 2.5254$. From the figure, we can observe that the effective throughput illustrates a non-monotonic behavior with the increase of outage threshold $\mathcal{R}$. In other words, when we increase the outage threshold, the effective throughput starts increas-

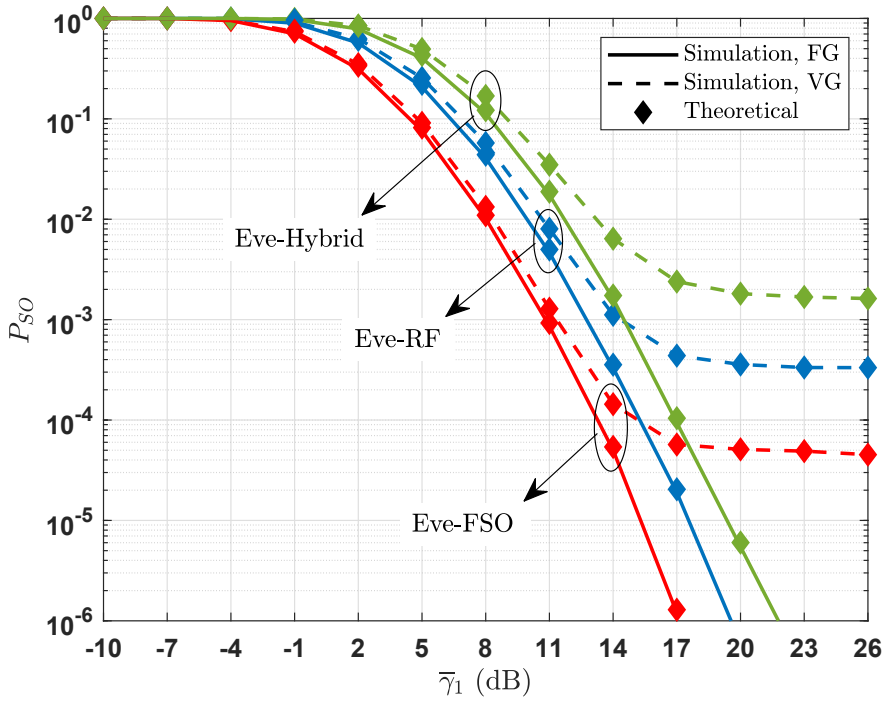


Figure 5.18: Secrecy outage probability as a function of average SNR at first-hop for different types of eavesdroppers. (Clean Weather, $\mathcal{G} = 0.5$, $\mathcal{R} = 1$ bits, $d_1 = d_2 = d_e = 1.5$ km, $m_1 = m_2 = 1$, $\alpha_1 = \alpha_2 = \alpha_e = 3.02$, $\beta_1 = \beta_2 = \beta_e = 2.71$, $R_{1,o} = R_{1,f} = R_{2,o} = R_{2,f} = 0.65$, $R_{e,o} = R_{e,f} = 0.15$, $\overline{\gamma}_1 = 10$ dB, $\overline{\gamma}_e = 3$ dB)

ing, and then, it begins decreasing. We can explain this behavior as follows: the increment in outage threshold is higher than the increase in probability of secrecy outage, and therefore, effective secrecy throughput increases with the increase in threshold. However, after a specific value of threshold, the secrecy probability becomes dominant, and it dramatically increase the effective secrecy throughput.

5.7 Concluding Remarks

In this study, the outage performance and secrecy outage performance of relay-based dual-hop hybrid FSO-*mm*Wave systems are investigated for fixed- and variable-gain relaying transmissions. Specifically, the transmissions in each hop is established through optical gamma-gamma atmospheric turbulence and *mm*Wave Nakagami-m fading channels at the same time, and the MRC diversity combining method is used at the relay and the legitimate receiver Bob, and the eavesdropper

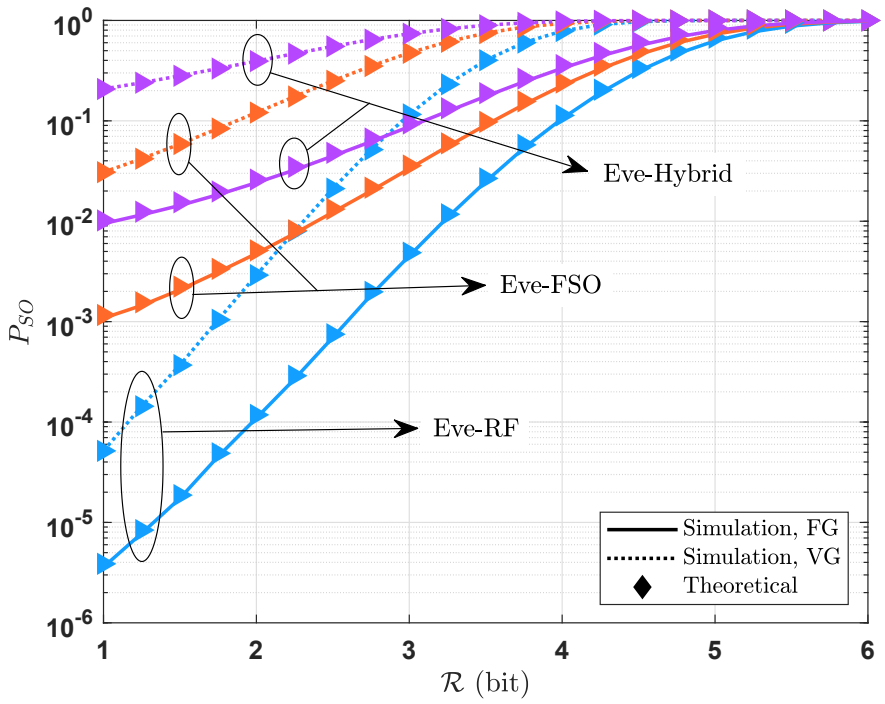


Figure 5.19: Secrecy outage probability as a function of threshold value for different types of eavesdroppers. (Hazy Weather, $\mathcal{G} = 0.5$, $d_1 = d_2 = d_e = 2\,\text{km}$, $m_1 = m_2 = 1$, $\alpha_1 = \alpha_2 = \alpha_e = 3.31$, $\beta_1 = \beta_2 = \beta_e = 2.58$, $R_{1,o} = R_{1,f} = R_{2,o} = R_{2,f} = 0.65$, $R_{e,o} = R_{e,f} = 0.25$, $\overline{\gamma}_1 = \overline{\gamma}_2 = 10\,\text{dB}$, $\overline{\gamma}_e = 3\,\text{dB}$)

Eve. As performance metrics, the outage probability, effective throughput, secrecy capacity, secrecy outage probability, and effective secrecy throughput are derived for fixed- and variable-gain relaying schemes. Additionally, the impact of different fundamental physical layer parameters on the transmission reliability are examined for two relay methods and three types of eavesdroppers. As explained previously, the nature of relay-based dual-hop mixed FSO-RF systems demonstrate that the overall system performance can be significantly degraded by either FSO and/or RF links due to the adverse weather conditions. However, the utilization of hybrid FSO-RF links in each data transmission hop can overcome this problem due to the complementary properties of RF and FSO systems. Analytical findings which are discussed allow us to explain how reliable transmission and reception can be made in several cases of interest in the context of hybrid FSO-*mm*Wave systems. In view of the findings, relay-based dual-hop hybrid FSO-*mm*Wave transmissions can be considered for the design of more reliable communication systems due to their distinctive be-

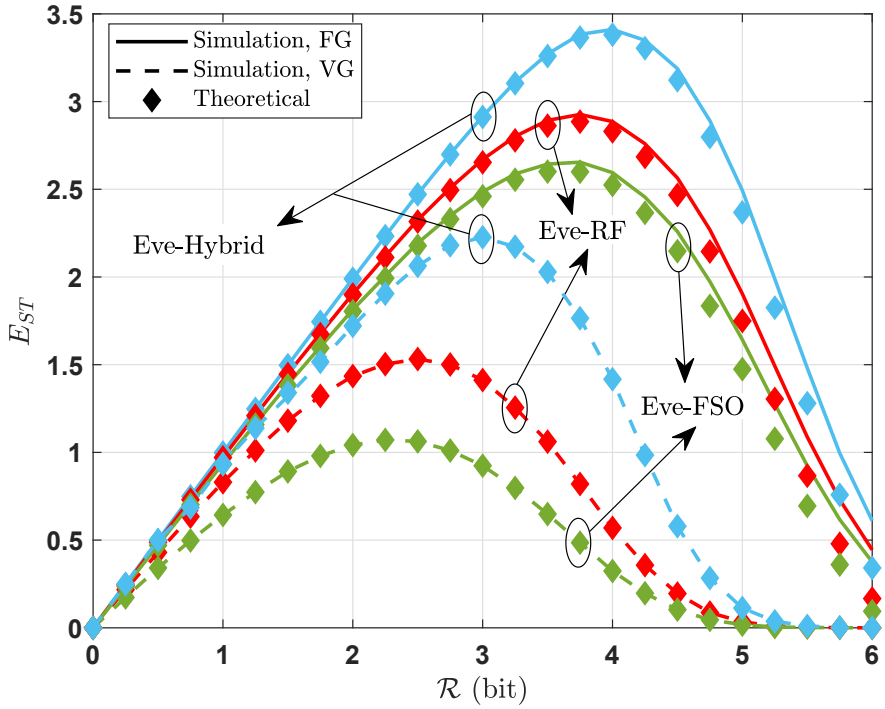


Figure 5.20: Effective secrecy throughput as a function of threshold value for different types of eavesdroppers. (Hazy Weather, $\mathcal{G} = 0.5$, $m_1 = m_2 = 1$, $\alpha_1 = \alpha_2 = \alpha_e = 2.98$, $\beta_1 = \beta_2 = \beta_e = 2.52$, $R_{1,o} = R_{1,f} = R_{2,o} = R_{2,f} = 0.75$, $R_{e,o} = R_{e,f} = 0.25$, $d_1 = d_2 = 1.75$ km, $\overline{\gamma}_1 = \overline{\gamma}_2 = 12$ dB, $d_e = 1.75$ km, $\overline{\gamma}_e = 5$ dB)

havior under different atmospheric conditions. Furthermore, by illustrating the effects of various atmospheric turbulence conditions on each hop and link, the utilization of a hybrid transmission remarkably decrease the outage performance of dual-hop relays. As a conclusion, the examination provided in this work can be useful in the process of system design to build more reliable data transmission under several scenarios.

6. A UNIFIED MGF-BASED FRAMEWORK FOR SECRECY ANALYSIS

6.1 Introduction

6.1.1 Motivation

A unified MGF-based framework is proposed for the physical layer security analysis of wireless communication systems over generalized fading channels. To characterize the secure communication between legitimate pairs, the secrecy capacity, SOP, probability of SPSC, EST, SOR, and SOD metrics are derived for SIMO systems over generalized fading channels in the presence of different types of eavesdroppers. The MGF-based approach proposed in this chapter is explicitly generic enough to unify on the direction of generalized fading channels (i.e., there is no need to separately analyze the security metrics of MRC diversity technique) in addition to the direction of different type eavesdroppers.

6.2 Statistical Background

Let consider the sum of L variates that is given as

$$Y_{\Sigma} = \sum_{\ell=1}^{L} Y_{\ell}, \tag{6.1}$$

where $l = 1, 2, \ldots, L$ is the number of Weibull RVs, and Y_{ℓ} follows Weibull distribution whose PDF is given as

$$f_{Y_{\ell}}(y) = \eta_{\ell} \Lambda_{\ell}^{-\eta_{\ell}} y^{\eta_{\ell}-1} \exp\left(-\Lambda_{\ell}^{-\eta_{\ell}} y^{\eta_{\ell}}\right), \tag{6.2}$$

where $\Lambda_{\ell} = \Omega_{\ell}/\Gamma\left(1 + 1/\eta_{\ell}\right)$ denotes the normalized power, and η_{ℓ} depicts the shape parameter that represents the in-homogeneity in fading conditions, and Ω_{ℓ} stands for the average power.

Additionally, we have

$$\mathbb{E}\left[Y_\ell\right] = \Omega_\ell, \tag{6.3}$$

$$\mathrm{Var}\left[Y_\ell\right] = \Omega_\ell^2 \left(\frac{\Gamma\left(1 + 2/\eta_\ell\right)}{\Gamma^2\left(1 + 1/\eta_\ell\right)} - 1 \right), \tag{6.4}$$

where $\mathbb{E}[\cdot]$ and $\mathrm{Var}[\cdot]$ represent the expectation and variance operators, and the CDF of Y_ℓ, $F_{Y_\ell}(y) = \Pr\left(Y_\ell < y\right)$ is given as

$$F_{Y_\ell}(y) = 1 - \exp\left(-\Lambda_\ell^{-\eta_\ell} y^{\eta_\ell}\right). \tag{6.5}$$

In the following, we obtain the MGF of Weibull distribution in closed-form. Note that the MGF of Y_ℓ is written as $\mathcal{M}_{Y_\ell}(s) = \mathbb{E}\left[\exp\left(-sY_\ell\right)\right]$ and we can rewrite it in terms of averaging using the PDF, that is

Theorem 1 (The MGF of Weibull Distribution)**.** *The MGF of* $Y_\ell \sim \mathsf{Wbl}(\eta_\ell, \Omega_\ell)$ *is given by*

$$\mathcal{M}_{Y_\ell}(s) = \eta_\ell (s\Lambda_\ell)^{-\eta_\ell} \Gamma\left(\eta_\ell, 0, (s\Lambda_\ell)^{-\eta_\ell}, -\eta_\ell\right), \tag{6.6}$$

where $\Gamma(\cdot,\cdot,\cdot,\cdot)$ *denotes the extended incomplete gamma function and defined as*

$$\Gamma(\alpha, y, b, \beta) = \int_y^\infty t^{\alpha-1} \exp\left(-t - bt^{-\beta}\right) dt, \tag{6.7}$$

with $y, \alpha, \beta \in \mathbb{R}$ *and* $b \in \mathbb{C}$.

Proof. The MGF of RV Y_ℓ can be obtained by using Laplace transform as follows

$$\begin{aligned} \mathcal{M}_{Y_\ell}(s) &= \mathbb{E}\left[\exp\left(-sY_\ell\right)\right], \\ &= \int_0^\infty \exp(-sy) f_{Y_\ell}(y) dy, \end{aligned} \tag{6.8}$$

by substituting (6.2) into (6.8), the integral is written as

$$\mathcal{M}_{Y_\ell}(s) = \eta_\ell \Lambda_\ell^{-\eta_\ell} \int_0^\infty y^{\eta_\ell - 1} \exp\left(-sy - \Lambda_\ell^{-\eta_\ell} y^{\eta_\ell}\right) dy, \tag{6.9}$$

and the resultant integral corresponds to the extended incomplete gamma function as given in (6.7).

□

Theorem 2 (MGF of the sum of Weibull RVs)**.** *Let $Y_\ell \sim \mathsf{Wbl}(\eta_\ell, \Omega_\ell)$ where $\ell = 1, 2, \ldots, L$, then the MGF of $Y_\Sigma = \sum_{\ell=1}^{L} Y_\ell$ is given by*

$$\mathcal{M}_{Y_\Sigma}(s) = \frac{\Phi_\Sigma}{s^{\sum_{\ell=1}^{L} \eta_\ell}} \prod_{\ell=1}^{L} \Gamma\Big(\eta_\ell, 0, (s\Lambda_\ell)^{-\eta_\ell}, -\eta_\ell\Big), \tag{6.10}$$

where Φ_Σ is given by

$$\Phi_\Sigma = \prod_{\ell=1}^{L} \eta_\ell \Lambda_\ell^{-\eta_\ell}. \tag{6.11}$$

Proof. Accordingly, assuming that Weibull distributions are mutually independent, we can obtain the MGF of the sum of Weibull distributions, i.e., the MGF of $Y_\Sigma = \sum_{\ell=1}^{L} Y_\ell$ as the product of the individual MGF of Weibull distributions, that is $\mathcal{M}_{Y_\Sigma}(s) = \prod_{\ell=1}^{L} \mathcal{M}_{Y_\ell}(s)$ and obtained as

$$\mathcal{M}_{Y_\Sigma}(s) = \prod_{\ell=1}^{L} \eta_\ell (s\Lambda_\ell)^{-\eta_\ell} \Gamma\left(\eta_\ell, 0, (s\Lambda_\ell)^{-\eta_\ell}, -\eta_\ell\right). \tag{6.12}$$

□

Theorem 3 (PDF of the sum of Weibull RVs)**.** *Let $Y_\ell \sim \mathsf{Wbl}(\eta_\ell, \Omega_\ell)$ where $\ell = 1, 2, \ldots, L$, then the PDF of $Y_\Sigma = \sum_{\ell=1}^{L} Y_\ell$ is given by*

$$f_{Y_\Sigma}(y) \approx \frac{e^{\sigma y}}{2^Q y} \sum_{q=0}^{Q} \binom{Q}{q} \sum_{n=0}^{N+q} (-1)^n B_n \mathcal{M}_{Y_\Sigma, \Re}(y; \sigma, n), \tag{6.13}$$

where σ is a positive arbitrary number which can be bounded by $e^{-2\sigma y}$ for a specific error ε_σ, the coefficient B_n is defined as $B_0 = 1/2$ and $B_n = 1$ for all $n \in \mathbb{Z}^+$, $\mathcal{M}_{Y_\Sigma, \Re}(y; A, n)$ denotes the real

part of the MGF, that is

$$\mathcal{M}_{Y_\Sigma,\Re}(y;\sigma,n)=\Re\left\{\mathcal{M}_{Y_\Sigma}\left(\frac{\sigma y+\pi jn}{y}\right)\right\}, \tag{6.14}$$

and for a predetermined error value $\varepsilon_{N,Q}$, the numbers N and Q, the upper limits of the summations, can be estimated by

$$\varepsilon_{N,Q}=\frac{e^{\sigma y}}{y}\sum_{q=0}^{Q}2^{-Q}(-1)^{N+q+1}\binom{Q}{q}\mathcal{M}_{Y_\Sigma,\Re}(y;\sigma,N+q+1). \tag{6.15}$$

Proof. Using the inverse Laplace transform, we can obtain the PDF of Y_Σ as follows

$$f_{Y_\Sigma}(y)=\frac{1}{2\pi j}\int_{\sigma-j\infty}^{\sigma+j\infty}\mathcal{M}_{Y_\Sigma}(s)e^{sy}ds, \tag{6.16}$$

where σ is an positive arbitrary number. By using the steps of a useful and simple numerical technique presented in [176, 177], $f_{Y_\Sigma}(y)$ can be obtained in a closed-form expression as follows. First, applying to the change of variate $s=\sigma+ju$ and the fact that $f_{Y_\Sigma}(y)$ is real, the inverse Laplace transform given in (6.16) can be expressed in terms of its real and imaginary parts

$$f_{Y_\Sigma}(y)=\frac{e^{\sigma y}}{2\pi}\int_{-\infty}^{\infty}\Big(\Re\big\{\mathcal{M}_{Y_\Sigma}(\sigma+ju)\big\}\cos(yu)-\Im\big\{\mathcal{M}_{Y_\Sigma}(\sigma+ju)\big\}\sin(yu)\Big)du, \tag{6.17}$$

where $\Re\{\cdot\}$ and $\Im\{\cdot\}$ denote the real and imaginary parts of a signal, respectively. Then, recalling that Y_Σ is the sum of L positive RVs, $f_{Y_\Sigma}(y)=0$ for all $y\leq 0$, and $\Re\{\mathcal{M}_{Y_\Sigma}(\sigma+ju)\}$ is even with respect to u, the integral in (6.16) is simplified as

$$f_{Y_\Sigma}(y)=\frac{2e^{\sigma y}}{\pi}\int_{0}^{\infty}\Re\big\{\mathcal{M}_{Y_\Sigma}\big(-(\sigma+ju)\big)\big\}\cos(yu)du, \tag{6.18}$$

where $\Re\{\cdot\}$ denotes the real part. Next, considering $\sigma=A/2y$ and using the trapezoidal rule with

a step size of $\pi/2y$, the integral in (6.18) becomes

$$f_{Y_\Sigma}(y) = \frac{e^{\sigma y}}{y} \sum_{n=0}^{\infty} (-1)^n B_n \mathcal{M}_{Y_\Sigma,\Re}(y; A, n) + \varepsilon_\sigma, \tag{6.19}$$

where ε_σ denotes the discretization error which is bounded with the use of Poisson summation formula by $(e^{-2\sigma y}/1 - e^{-2\sigma y}) \approx e^{-2\sigma y}$, and the coefficient B_n is defined as $B_0 = 1/2$ and $B_n = 1$ for all $n \in \mathbb{Z}^+$. Then, truncating the infinite summation in (6.19) by N, we obtain an alternating series. Further, we apply the Euler summation technique which accelerates the alternating series convergence, can be considered as the binomial average of Q partial series of length $N, N+1, \ldots, N+Q$, respectively. Finally, this concludes the proof as given in (6.13), where $\varepsilon_{\sigma,N,Q}$ depicts the overall error which term, that can be bounded by

$$\varepsilon_{\sigma,N,Q} \approx \frac{e^{-2\sigma y}}{1 - e^{-2\sigma y}} + \left| \frac{e^{\sigma y}}{2^Q y} \sum_{q=0}^{Q} (-1)^{N+q+1} \binom{Q}{q} \mathcal{M}_{Y_\Sigma,\Re}(y; \sigma, N+q+1) \right|. \tag{6.20}$$

□

Theorem 4 (CDF of the sum of Weibull RVs)**.** *Let $Y_\ell \sim \mathsf{Wbl}(\eta_\ell, \Omega_\ell)$ where $\ell = 1, 2, \ldots, L$, then the CDF of $Y_\Sigma = \sum_{\ell=1}^{L} Y_\ell$ is given by*

$$F_{Y_\Sigma}(y) \approx \frac{e^{\sigma y}}{2^Q y} \sum_{q=0}^{Q} \binom{Q}{q} \sum_{n=0}^{N+q} (-1)^n B_n \widehat{\mathcal{M}}_{Y_\Sigma,\Re}(y; \sigma, n), \tag{6.21}$$

where $\widehat{\mathcal{M}}_{Y_\Sigma,\Re}(y; \sigma, n)$ denotes the real part of the MGF, that is

$$\widehat{\mathcal{M}}_{Y_\Sigma,\Re}(y; \sigma, n) = \Re \left\{ \mathcal{M}_{Y_\Sigma} \left(\frac{\sigma y + \pi j n}{y} \right) \Big/ \frac{\sigma y + \pi j n}{y} \right\}. \tag{6.22}$$

Proof. Recall that $f_{Y_\Sigma}(y)$ and $F_{Y_\Sigma}(y)$ stands for the PDF and CDF of Y_Σ, respectively. Since CDF is obtained by a simple integration of PDF, $f_{Y_\Sigma}(y) = dF_{Y_\Sigma}(y)/dy$, and noting that $F_{Y_\Sigma}(0) = 0$, the

CDF of Y_Σ can be expressed as

$$\mathcal{L}\left\{F_{Y_\Sigma}(y)\right\} = F_{Y_\Sigma}(s) = \frac{\mathcal{L}\left\{f_{Y_\Sigma}(y)\right\}}{s}, \tag{6.23}$$

where $\mathcal{L}\{\cdot\}$ denotes the Laplace transform operator. Then, using the relation $\mathcal{L}\left\{f_{Y_\Sigma}(y)\right\} = \mathcal{M}_{Y_\Sigma}(s)$, and following the steps described in the previous section, the proof is completed as given in (6.21).

□

6.3 System Model

A SIMO is considered, where the classic Wyner's wiretap channels take place [80], in which the standard placeholder names are used to denote different entities as follows. The legitimate transmitter, Alice, wants to send confidential information to the legitimate receiver, Bob, while an eavesdropper, Eve, tries to wiretap confidential information by sniffing the received signals, as illustrated in Fig. 6.1. It is assumed that Alice has one transmit antenna and laser while Bob and Eve have n_L receive antennas and photodiodes.

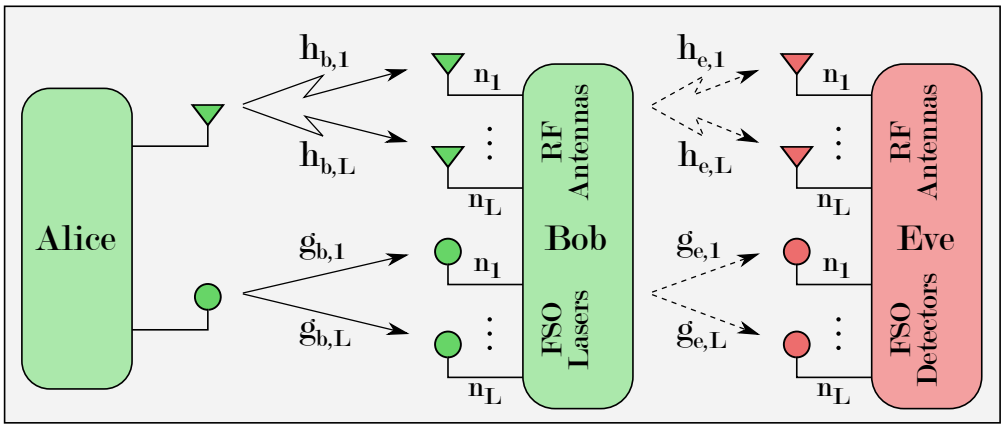


Figure 6.1: System model of SIMO hybrid FSO-*mm*Wave communications between the legitimate transmitter Alice and receiver Bob in the presence of a hybrid type eavesdroppers.

6.3.1 Signal-to-Noise Ratios

Both Bob ($x = b$) and Eve ($x = e$) apply the MRC diversity method on the received signals. Hence, the overall electrical SNR is in fact the sum of the instantaneous electrical SNRs of each antenna and/or photodiode for MRC receiver, expressed as

$$\gamma_{\Sigma,x} = \sum_{\ell_o=1}^{L_o} \gamma_{x,o}^{(\ell_o)} + \sum_{\ell_f=1}^{L_f} \gamma_{x,f}^{(\ell_f)}, \tag{6.24}$$

where $\gamma_{x,o}^{(\ell_o)}$ and $\gamma_{x,f}^{(\ell_f)}$ denote the instantaneous electrical SNRs of ℓ_o^{th} FSO and ℓ_f^{th} RF links, respectively. Note that the average electrical SNRs of the RF link $\overline{\gamma}_{x,f}^{(\ell_f)}$ and FSO link $\overline{\gamma}_{x,o}^{(\ell_o)}$ are expressed in (1.21) and (1.24), respectively.

6.4 Secrecy Analysis

6.4.1 Secrecy Outage Probability

As defined in section 1.4.2, to characterize the secure communication between the legitimate transmitter Alice and the legitimate receiver Bob, we used the probabilistic metric of the SOP, defined as

$$P_{SO}(\mathcal{R}_s) = \text{Prob.}\big(C_S < \mathcal{R}_s\big), \tag{6.25}$$

which is the probability that the achievable secrecy rate is less than a target secrecy rate $\mathcal{R}_s > 0$. Then, by substituting (6.24) into (6.25),

$$P_{SO}(\mathcal{R}_s) = \text{Prob.}\big(\log_2(1+\gamma_{\Sigma,b}) - \log_2(1+\gamma_{\Sigma,e}) < \mathcal{R}_s\big), \tag{6.26}$$

since the logarithm is a monotonic function, we can arrange (6.26) as follows

$$P_{SO}(\mathcal{R}_s) = \text{Prob.}\big(2^{\mathcal{R}_s}(1+\gamma_{\Sigma,e}) - (1+\gamma_{\Sigma,b})\big), \tag{6.27}$$

then, by letting a RV $\Xi = 2^{\mathcal{R}_s}(1+\gamma_{\Sigma,e}) - (1+\gamma_{\Sigma,b})$, the MGF of Ξ is expressed as

$$\mathcal{M}_{\Xi}(s) = \exp\big(-s\big[2^{\mathcal{R}_s}(1+\gamma_{\Sigma,e}) - (1+\gamma_{\Sigma,b})\big]\big), \tag{6.28}$$

$$= \exp\big(-s[2^{\mathcal{R}_s}-1]\big)\mathcal{M}_{\Sigma,e}(-s2^{\mathcal{R}_s})\mathcal{M}_{\Sigma,b}(s), \tag{6.29}$$

where $\mathcal{M}_{\Sigma,x}(s)$ denotes the MGF of $\gamma_{\Sigma,x}$, expressed as

$$\mathcal{M}_{\Sigma,x}(s) = \prod_{\ell_o=1}^{L_o} \mathcal{M}_{\gamma_{x,o}^{(\ell_o)}}(s) \times \prod_{\ell_f=1}^{L_f} \mathcal{M}_{\gamma_{x,f}^{(\ell_f)}}(s), \tag{6.30}$$

therefore, the SOP is simply calculated by using (6.21) as

$$P_{SO}(\mathcal{R}_s) \approx \frac{e^{\sigma x}}{2^Q \mathcal{R}_s} \sum_{q=0}^{Q} \binom{Q}{q} \sum_{n=0}^{N+q} (-1)^n B_n \Re\left\{ \mathcal{M}_{\Xi}\left(\frac{\sigma\mathcal{R}_s + \pi j n}{\mathcal{R}_s}\right) \Big/ \frac{\sigma\mathcal{R}_s + \pi j n}{\mathcal{R}_s} \right\}. \tag{6.31}$$

6.4.2 Probability of Strictly Positive Secrecy Capacity

As defined in section 1.4.3, we also considered a special version of SOP, called the probability of SPSC, which is also known as the probability of existence of secure communications, defined as

$$P_S^+ = 1 - P_{SO}(0^+). \tag{6.32}$$

6.4.3 Effective Secrecy Throughput

Based on the definition of SOP, as defined in section 1.4.4, the EST can be obtained by the product of secrecy rate and the probability of successful transmission. According to this definition, the EST can be formulated as

$$E_{ST}(\mathcal{R}_s) = \mathcal{R}_s\big(1 - P_{SO}(\mathcal{R}_s)\big), \tag{6.33}$$

6.4.4 Secrecy Outage Rate

As defined in section 1.4.5, the average SOR, or the average secrecy LCR, is defined by the instantaneous secrecy capacity at a level of $\mathcal{R}_s$. The average SOR provides the expected number of outage, downward crossings the secrecy capacity in terms of seconds. In other words, it provides the statistic at a specific threshold $\mathcal{R}_s$ in time. The average SOR is expressed based on the generic expression given in [34, (2.90)]

$$R_{SO}(\mathcal{R}_s) = \int_0^\infty \int_0^\infty \dot{\gamma} f_\gamma(\gamma_{\text{th}}) f_{\dot{\gamma}}(\dot{\gamma}) f_{\gamma_e}(y) d\dot{\gamma} dy, \tag{6.34}$$

where $\gamma_{\text{th}} = \sqrt{2^{\mathcal{R}_s}(1+\gamma_e) - 1}$, and $\dot{\gamma}$ is the time derivative of the signal amplitude process. It is worthy to note that the time derivative of the signal amplitude process $\dot{\gamma}$ is always independent of the signal amplitude γ and is normally distributed with zero mean but different variance depending on the type of fading. Therefore, the PDF expression of $\dot{\gamma}$ is given by

$$f_{\dot{\gamma}}(\dot{\gamma}) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{\dot{\gamma}^2}{2\sigma^2}\right), \tag{6.35}$$

where $\sigma^2 = \widetilde{\Omega}\pi^2 f_m^2$, where f_m is the maximum Doppler frequency, and $\widetilde{\Omega}$ is given by

$$\widetilde{\Omega} = \begin{cases} \Omega, & \text{for Rayleigh fading,} \\ \frac{\Omega}{m}, & \text{for Nakagami fading,} \\ \frac{\Omega}{K+1}, & \text{for Rician fading.} \end{cases} \tag{6.36}$$

By substituting (6.35) into (6.34), the integral is re-expressed as

$$R_{SO}(\mathcal{R}_s) = \frac{1}{\sqrt{2\pi}\sigma} \int_0^\infty f_\gamma(\gamma_{\text{th}}) f_{\gamma_e}(y) \int_0^\infty \dot{\gamma} \exp\left(-\frac{\dot{\gamma}^2}{2\sigma^2}\right) d\dot{\gamma} dy, \tag{6.37}$$

by solving the inner integral with respect to $\dot{\gamma}$, (6.37) is re-written as

$$R_{SO}(\mathcal{R}_s) = \frac{\sigma}{\sqrt{2\pi}} \int_0^{\infty} f_{\gamma}(\gamma_{\text{th}}) f_{\gamma_e}(y) dy, \tag{6.38}$$

now, by using the expression of $f_{\gamma_e}(y)$ in (6.13), (6.38) is re-written as

$$R_{SO}(\mathcal{R}_s) = \frac{\sigma}{\sqrt{2\pi}} f_{\gamma}(\gamma_{\text{th}}) \sum_{q=0}^{Q} \binom{Q}{q} \sum_{n=0}^{N+q} (-1)^n B_n \int_0^{\infty} \frac{e^{\sigma y}}{2^Q y} \mathcal{M}_{\mathrm{Y}_{\Sigma},\Re}(y; \sigma, n) dy. \tag{6.39}$$

6.4.5 Secrecy Outage Duration

As defined in section 1.4.6, the average SOD is another secrecy metric, which defines the expected average duration of the secrecy outage status for a wireless communication system. The average SOD is expressed based on the definition of the average outage duration, as given in [34, (2.106)]

$$D_{SO}(\mathcal{R}_s) = \frac{P_{SO}(\mathcal{R}_s)}{R_{SO}(\mathcal{R}_s)}. \tag{6.40}$$

6.5 Results and Discussions

Fig. 6.2 illustrates the analytical accuracy of (6.10), the MGF of sum of L Weibull RVs, in which the analytical and simulations results are in exact agreement. As seen in the figure, increasing the number of Weibull RVs, $L \gg 1$, increases the gradient of the MGF, which means in communications perspective that the performance of the transmission in wireless channels increases. For instance, when $L \to \infty$, the MGF approximates to $\mathcal{M}_{X_{\Sigma}}(s) = 1$ for $s = 0$ and to $\mathcal{M}_{X_{\Sigma}}(s) = 0$ for $s \neq 0$, which implies occurrence of a negligible error at the receiver.

The PDF and CDF of sum of L Weibull RVs given in (6.13) and (6.21) are shown in Fig. 6.3 and 6.4, respectively. One can easily observe from Fig. 6.3 that increasing the number of links and shape parameters forms the resultant PDF around the sum of average powers, $\sum_{\ell=1}^{L} \Omega_{\ell}$, which means the effects of fading are alleviated from the communications points of view. Additionally, as seen in the figures, the analytical and simulations results show perfect agreement.

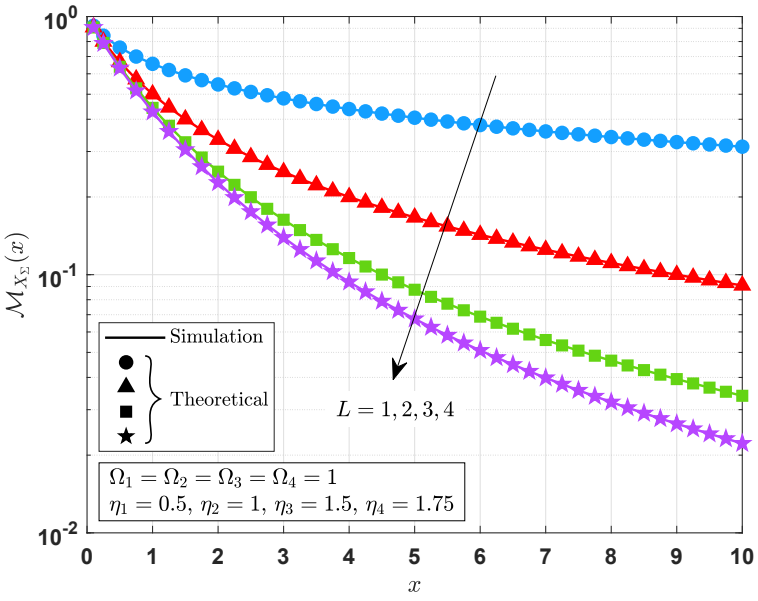


Figure 6.2: MGF of the sum of L Weibull random variates.

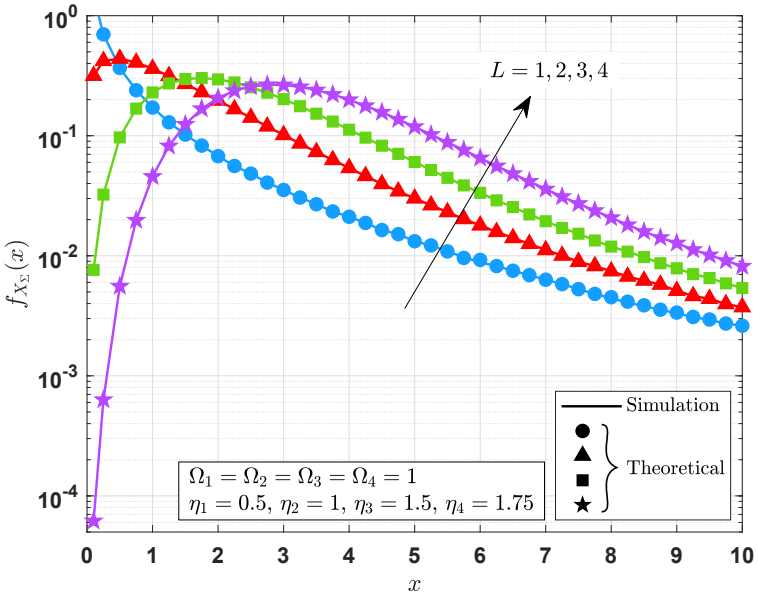


Figure 6.3: PDF of the sum of L Weibull random variates.

Secrecy outage against Bob's average SNR performance of the system is illustrated in Fig. 6.5 for different number of receivers with a fixed $\gamma_e = 0\,\text{dB}$ of average SNR at Eve. Considering a secrecy rate of $\kappa = 1\,\text{bit}$ and target outage probability of $P_{SO} = 10^{-3}$, one can observe that the

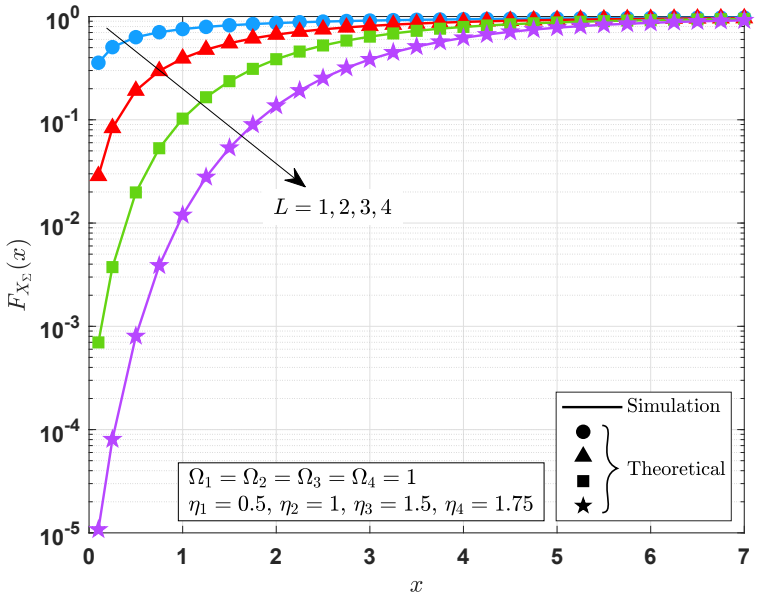


Figure 6.4: CDF of the sum of L Weibull random variates.

system is able to satisfy these requirements at $\gamma_b = 18, 20, 24, 32$ dB for $L = 1, 2, 3, 4$, respectively. As expected, increasing the number of receiving antennas significantly increases the probability of having secure communications.

Likewise, Fig. 6.6 shows the SOP performance of the system for different secrecy rates with $L = 4$ receiving antennas. We consider a fixed average SNR of Eve as $\gamma_e = 5$ dB and set the link distances to $d_b = d_e = 1$ km. Similar to the results obtained from Fig. 6.5, it is clear from this figure that the performance improves as the number of the diversity paths increase, which is as expected.

The secrecy outage performance of a hybrid SIMO system as a function of average SNR at Bob illustrated in Fig. 6.7 for different number of receiver in the presence of a hybrid eavesdropper. The average SNR at Eve is considered as $\gamma_e = 10$ dB, and the communication link distance is set to $d_b = d_e = 1$ km for both Bob and Eve. Note that the parameters $n_{L,o,x}$ and $n_{L,f,x}$ denotes the number of FSO photodiodes and *mm*Wave receiving antennas, where the subscript x denotes the receiving side, i.e., $x = b$ for Bob and $x = e$ for Eve. It is obvious from the figure that increasing the number of photodiodes and receiving antennas improves the secrecy performance

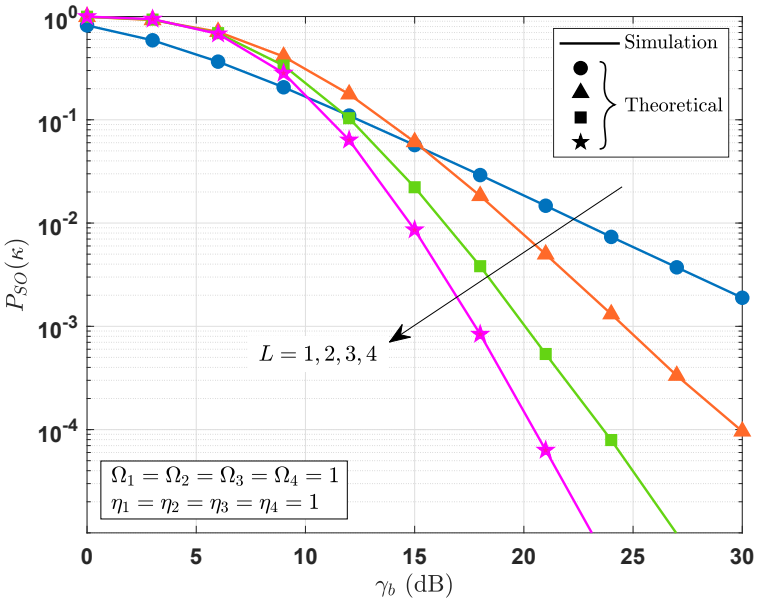


Figure 6.5: Secrecy performance versus average signal-to-noise ratio of the system for different number of receivers. ($\kappa = 1$ bit, $\gamma_e = 0$ dB, $d_b = d_e = 0.5$ km)

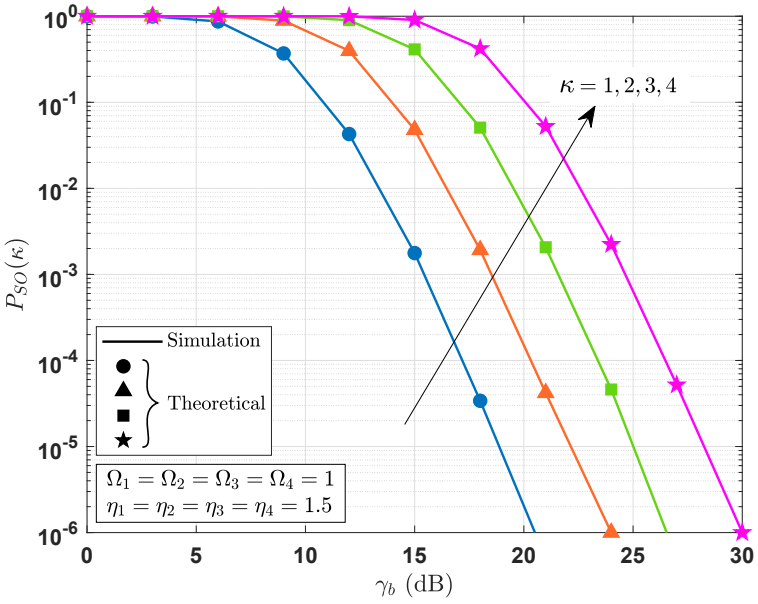


Figure 6.6: Secrecy performance versus average signal-to-noise ratio of the system for different secrecy rates. ($L = 4$, $\gamma_e = 5$ dB, $d_b = d_e = 1$ km)

of Bob. Additionally, the accuracy of the proposed SOP solution has perfect agreement with the Monte Carlo simulations.

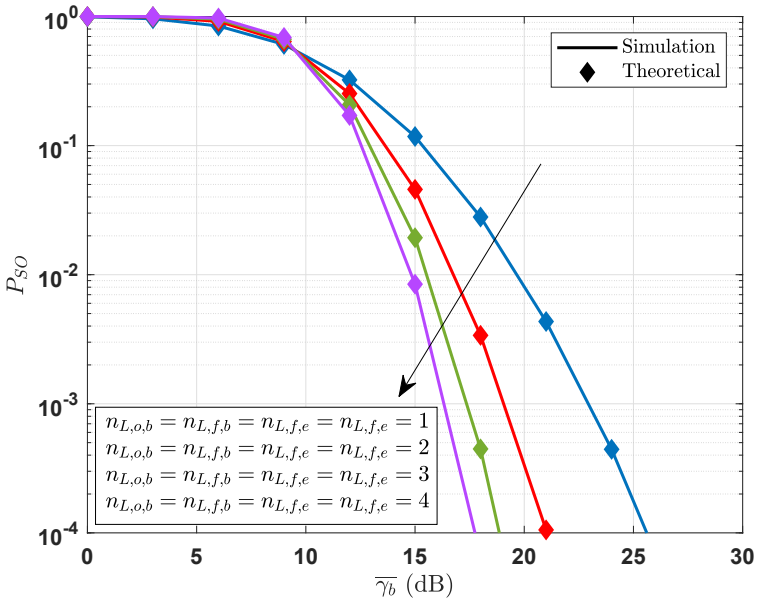


Figure 6.7: Secrecy outage performance of a SIMO system as a function of average SNR in the presence of a hybrid eavesdropper considering different number of receivers. (Clean Weather, $d_b = d_e = 1\,\text{km}$, $\gamma_e = 10\,\text{dB}$)

The secrecy outage performance of a hybrid SIMO system as a function of average SNR at Bob illustrated in Fig. 6.8 for different number of receiver in the presence of different types of eavesdroppers. The average SNR at Eve is considered as $\gamma_e = 5\,\text{dB}$, and the communication link distance is set to $d_b = d_e = 1.25\,\text{km}$ for both Bob and Eve. As it is seen from the figure, SOP performance of different systems can be simply investigated by using the same equation in the presence of different types of eavesdroppers.

6.6 Concluding Remarks

In this chapter, a unified MGF-based framework is proposed for physical layer security analysis of hybrid FSO-RF systems over generalized fading channels. The communication between the legitimate transmitter and the legitimate receiver Bob is established over at least two parallel links, however, the legitimate receiver Bob may have more than one antenna and one photodetector. Three different eavesdroppers, namely, RF-, FSO- and hybrid-Eve, are considered, and an MRC receiver is employed at both Bob's and Eve's side. The proposed metrics, such as SOP,

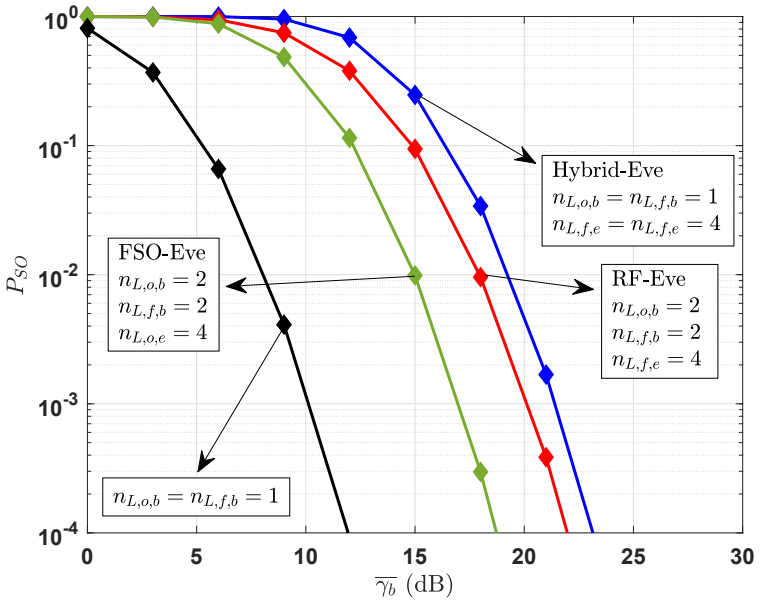


Figure 6.8: Secrecy outage performance of a SIMO system as a function of average SNR in the presence of different types of eavesdroppers considering different number of receivers. (Haze Weather, $d_b = d_e = 1.5$ km, $\gamma_e = 5$ dB)

probability of SPSC, EST, SOR, and SOD, are in the generic forms, which can be used for any fading channels and any types of eavesdroppers. Therefore, the proposed metrics allow us to simulate various scenarios of interest in the context of hybrid FSO-*mm*Wave communications including several fundamental physical layer parameters. In the light of results, the accuracy of the proposed derivations are shown, in which the theory and Monte Carlo simulations are in a good agreement. Moreover, the proposed framework can be also used to investigate the performance analysis of a hybrid FSO-RF system without an eavesdropper.

7. CONCLUSION AND FUTURE WORK

7.1 Conclusion

In this dissertation, hybrid FSO-*mm*Wave systems are investigated from a physical-layer security point of view in the presence of different types of eavesdroppers, where the communication between two legitimate peers takes place over both FSO and mmWave links, simultaneously. Practical scenarios are examined to eavesdrop on the legitimate communication, and the effects of random radio power of mmWave links and optical irradiance of FSO links are discussed on the probability of achieving a secure transmission. The impact of fundamental physical layer parameters on the secrecy performance of the hybrid system is analyzed by obtaining analytical derivations of several performance metrics.

The results presented in this dissertation may open a new perspective of thinking when designing a hybrid FSO-*mm*Wave communication system, and considering a new constraint in case a specific level of security is required. Furthermore, the practical scenarios considered for different types of eavesdroppers is also an interesting and attractive point for future research areas.

In this framework, specific contributions and possible extensions along with future directions of this dissertation are presented below.

7.2 List of Specific Contributions

Similar to the section 1.5, specific contributions of this dissertation can be summarized as follows:

- Performance Analysis of Hybrid FSO-*mm*Wave Systems
  - Secrecy analysis is made for single-hop systems, and dual-hop relay-based systems.
  - Not necessarily identical independent and dependent wiretap channels are investigated.
  - Hybrid-type eavesdropper is proposed in comparison with RF and FSO ones.
  - Fundamental physical layer parameters are examined along with practical scenarios.

- Link Selection in Hybrid FSO-*mm*Wave Systems
  - A novel IM-based link selection mechanism is proposed along with related discussions.
  - An enhanced security algorithm is proposed on the basis of CSI-based precoding.
  - CNN networks are designed to enhance secrecy performance of MIMO transmissions.
- Generic Framework for Hybrid FSO-*mm*Wave Systems
  - A novel unified MGF-based framework is proposed over generalized fading channels.
  - Generic derivations of SOP, SPSC, EST, SOR, and SOD metrics are made for SIMO systems.
  - The proposed framework is generic enough to accommodate any fading model and eavesdropper type.

7.3 Future Directions

In the light of the studies presented in this dissertation, the following items can be considered as possible research topics.

- Mobility. FSO systems are currently considered for fixed point-to-point communications because of the LOS requirement of FSO links. However, beam tracking systems have been introduced to support the mobile wireless communications in FSO systems. Additionally, unmanned aerial vehicles (UAVs) are rapidly adopted to assist current communication systems. Therefore, considering the recent developments, the concept of UAV-based mobile nodes is a promising future research topic in hybrid FSO-RF systems, where an UAV-based mobile node could be considered as a legitimate relay or an eavesdropper.
- Active Eavesdropping. Recently, beam-splitting attacks are being proposed as a practical active eavesdropping scenario in FSO systems. However, it should be noted that the eavesdropper cannot simply put a beam splitter in front of the legitimate receiver or anywhere else in the middle of the FSO link (atmosphere) in practice. Because the beam splitter is an

optics component that must be used within a combination of other optical components in an FSO receiver (telescope, mirrors, lenses, etc). Thus, it cannot be imagined a single beam splitter placed in the legitimate link to split a portion of the beam towards the eavesdropper's location in practice. This kind of beam splitting attack only happens in fiber communication links, although several studies considered this attack for FSO merely for the sake of theoretical calculations. Therefore, the most practical eavesdropping scenario would be a passive attack where Eve tries to put her receiver within the beam footprint of the FSO link to passively eavesdrop a fraction of power. As a conclusion, the investigation of an active eavesdropping scenario is a very important future research topic in hybrid FSO-RF systems.

REFERENCES

[1] T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez, "Millimeter wave mobile communications for 5G cellular: It will work!," *IEEE Access*, vol. 1, pp. 335–349, 2013.

[2] A. I. Sulyman, A. T. Nassar, M. K. Samimi, G. R. Maccartney, T. S. Rappaport, and A. Alsanie, "Radio propagation path loss models for 5G cellular networks in the 28 GHZ and 38 GHZ millimeter-wave bands," *IEEE Communications Magazine*, vol. 52, no. 9, pp. 78–86, 2014.

[3] 3GPP Radio Access Network Working Group, "Study on channel model for frequencies from 0.5 to 100 GHz (Release 15)," Tech. Rep. ETSI TR 138 901 V14.3.0, 3GPP TR 38.901, 2018.

[4] L. Azpilicueta, P. Lopez-Iturri, J. Zuniga-Mejia, M. Celaya-Echarri, F. A. Rodriguez-Corbo, C. Vargas-Rosales, E. Aguirre, D. G. Michelson, and F. Falcone, "Fifth-generation (5G) mmWave spatial channel characterization for urban environments' system analysis," *Sensors*, vol. 20, no. 18, 2020.

[5] T. Nishio, H. Okamoto, K. Nakashima, Y. Koda, K. Yamamoto, M. Morikura, Y. Asai, and R. Miyatake, "Proactive received power prediction using machine learning and depth images for mmWave networks," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 11, pp. 2413–2427, 2019.

[6] O. S. Badarneh and F. S. Almehmadi, "The effects of different noise types and mobility on error rate of digital modulation schemes over millimeter-wave Weibull fading channels," *Wireless Networks*, vol. 25, no. 5, pp. 2259–2268, 2019.

[7] A. Soulimani, M. Benjillali, H. Chergui, and D. B. da Costa, "Performance analysis of M-QAM multihop relaying over mmWave Weibull fading channels," *CoRR*, 2016.

[8] J. Reig, M.-T. Martínez-Inglés, L. Rubio, V.-M. Rodrigo-Peñarrocha, and J.-M. Molina-García-Pardo, "Fading evaluation in the 60 GHz band in line-of-sight conditions," *International Journal of Antennas and Propagation*, vol. 2014, no. 12, 2014.

[9] A. Soulimani and M. Benjillali, "Closed-form performance analysis of generalized M-QAM over multihop Weibull fading channels," in *2015 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, pp. 1–5, 2015.

[10] S. Hur, S. Baek, B. Kim, Y. Chang, A. F. Molisch, T. S. Rappaport, K. Haneda, and J. Park, "Proposal on millimeter-wave channel modeling for 5G cellular system," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 3, pp. 454–469, 2016.

[11] S. K. Yoo, S. L. Cotton, Y. J. Chun, W. G. Scanlon, and G. A. Conway, "Channel characteristics of dynamic off-body communications at 60 GHz under line-of-sight (LOS) and non-LOS conditions," *IEEE Antennas and Wireless Propagation Letters*, vol. 16, pp. 1553–1556, 2017.

[12] J. G. Andrews, T. Bai, M. N. Kulkarni, A. Alkhateeb, A. K. Gupta, and R. W. Heath, "Modeling and analyzing millimeter wave cellular systems," *IEEE Transactions on Communications*, vol. 65, pp. 403–430, January 2017.

[13] S. K. Yoo, S. L. Cotton, R. W. Heath, and Y. J. Chun, "Measurements of the 60 GHz UE to eNB channel for small cell deployments," *IEEE Wireless Communications Letters*, vol. 6, no. 2, pp. 178–181, 2017.

[14] M. K. Simon and M.-S. Alouini, *Digital communication over fading channels*, vol. 95. New Jersey, United States: John Wiley & Sons, second ed., 2005.

[15] M. A. Amirabadi and V. Tabataba Vakili, "A novel hybrid FSO/RF communication system with receive diversity," *Optik*, vol. 184, pp. 293–298, 2019.

[16] M. A. Amirabadi and V. T. Vakili, "Performance comparison of two novel relay-assisted hybrid FSO/RF communication systems," *IET Communications*, vol. 13, pp. 1551–1556, July 2019.

[17] M. Abaza, R. Mesleh, A. Mansour, and el Hadi Aggoune, "Performance analysis of space-shift keying over negative-exponential and log-normal FSO channels," *Chin. Optical Letter*, vol. 13, pp. 051001–051001, May 2015.

[18] V. Srivastava, A. Mandloi, D. Patel, and P. Shah, "Performance analysis of negative exponential turbulent FSO links with wavelength diversity," in *2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*, pp. 1–5, 2020.

[19] S. Tannaz, C. Ghobadi, J. Nourinia, and E. Mostafapour, "The effects of negative exponential and K-distribution modeled FSO links on the performance of diffusion adaptive networks," in *2018 9th International Symposium on Telecommunications (IST)*, pp. 19–22, 2018.

[20] B. Barua and M. M. Hossain, "Free-space optical communication with m-ary pulse position modulation under gamma-gamma and negative exponential atmospheric turbulence model," in *2012 15th International Conference on Computer and Information Technology (ICCIT)*, pp. 295–298, 2012.

[21] M. A. Khalighi and M. Uysal, "Survey on free space optical communication: A communication theory perspective," *IEEE Communications Surveys Tutorials*, vol. 16, pp. 2231–2258, June 2014.

[22] K. Anbarasi, C. Hemanth, and R. Sangeetha, "A review on channel models in free space optical communication systems," *Optics & Laser Technology*, vol. 97, pp. 161–171, 2017.

[23] I. S. Ansari, F. Yilmaz, and M.-S. Alouini, "Performance analysis of FSO links over unified Gamma-Gamma turbulence channels," in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, pp. 1–5, IEEE, 2015.

[24] E. Zedini, I. S. Ansari, and M.-S. Alouini, "Performance analysis of mixed Nakagami-m and gamma–gamma dual-hop FSO transmission systems," *IEEE Photonics Journal*, vol. 7, no. 1, pp. 1–20, 2015.

[25] H. Lei, Z. Dai, I. S. Ansari, K.-H. Park, G. Pan, and M.-S. Alouini, "On secrecy performance of mixed RF-FSO systems," *IEEE Photonics Journal*, vol. 9, no. 4, pp. 1–14, 2017.

[26] L. C. Andrews, R. L. Phillips, and C. Y. Hopen, *Laser beam scintillation with applications*, vol. 99. Bellingham, United States: SPIE press, second ed., 2001.

[27] A. K. Majumdar, "Free-space laser communication performance in the atmospheric channel," *Journal of Optical and Fiber Communications Reports*, vol. 2, pp. 345–396, October 2005.

[28] A. A. Farid and S. Hranilovic, "Outage capacity optimization for free-space optical links with pointing errors," *Journal of Lightwave Technology*, vol. 25, no. 7, pp. 1702–1710, 2007.

[29] H. G. Sandalidis, T. A. Tsiftsis, G. K. Karagiannidis, and M. Uysal, "Ber performance of fso links over strong atmospheric turbulence channels with pointing errors," *IEEE Communications Letters*, vol. 12, no. 1, pp. 44–46, 2008.

[30] F. Yang, J. Cheng, and T. A. Tsiftsis, "Free-space optical communication with nonzero boresight pointing errors," *IEEE Transactions on Communications*, vol. 62, no. 2, pp. 713–725, 2014.

[31] I. I. Kim, B. McArthur, and E. J. Korevaar, "Comparison of laser beam propagation at 785nm and 1550nm in fog and haze for optical wireless communications," vol. 4214, pp. 26–37, 2001.

[32] A. A. Farid and S. Hranilovic, "Outage capacity optimization for free-space optical links with pointing errors," *Journal of Lightwave Technology*, vol. 25, pp. 1702–1710, July 2007.

[33] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[34] G. L. Stüber, *Principles of mobile communication*. Norwell, MA: Kluwer: Springer, second ed., 2000.

[35] R. Boluda-Ruiz, S. C. Tokgoz, A. Garcia-Zambrana, and K. Qaraqe, "Enhancing secrecy capacity in FSO links via MISO systems through turbulence-induced fading channels with misalignment errors," *IEEE Photonics Journal*, vol. 12, no. 4, pp. 1–13, 2020.

[36] R. Boluda-Ruiz, S. C. Tokgoz, A. Garcia-Zambrana, and K. Qaraqe, "Asymptotic average secrecy rate for MISO free-space optical wiretap channels," in *2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 1–5, 2019.

[37] S. C. Tokgoz, R. Boluda-Ruiz, S. Yarkan, and K. A. Qaraqe, "ACO-OFDM transmission over underwater pipeline for VLC-based systems," in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 1–7, 2019.

[38] O. Alaca, S. C. Tokgoz, A. Retnanto, S. L. Miller, and K. A. Qaraqe, "Experimental demonstration of visible light communication based downhole telemetry system," in *2021 International Mediterranean Conference on Communications and Networking (MeditCom)*, pp. 1–6, 2021.

[39] S. C. Tokgoz, S. L. Miller, and K. A. Qaraqe, "On the investigation of achievable links for VLC based wireless downhole telemetry systems," in *2020 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pp. 1–6, 2020.

[40] S. C. Tokgoz, N. Anous, S. Yarkan, A. Boyacı, and K. A. Qaraqe, "Performance evaluation of white LED-based OFDM-VLC systems with blue filters: Experimental study," in *2019 16th International Multi-Conference on Systems, Signals Devices (SSD)*, pp. 686–690, 2019.

[41] S. C. Tokgoz, N. Anous, S. Yarkan, D. Khalil, and K. A. Qaraqe, "Performance improvement of white LED-based VLC systems using blue and flattening filters," in *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*, pp. 1–6, 2019.

[42] K. Dalle, J. Medina, S. C. Tokgoz, S. L. Miller, and K. A. Qaraqe, "Visible light communications for downhole gas pipeline monitoring systems," in *2020 28th Signal Processing and Communications Applications Conference (SIU)*, pp. 1–4, 2020.

[43] S. C. Tokgoz, S. Althunibat, S. L. Miller, and K. A. Qaraqe, "On the secrecy capacity of hybrid FSO-mmWave links with correlated wiretap channels," *Optics Communications*, vol. 499, p. 127252, 2021.

[44] S. C. Tokgoz, S. Althunibat, S. Yarkan, and K. A. Qaraqe, "Physical layer security of hybrid FSO-mmWave communications in presence of correlated wiretap channels," in *ICC 2021 - IEEE International Conference on Communications*, pp. 1–7, 2021.

[45] S. H. Islam, A. S. M. Badrudduza, S. M. Riazul Islam, F. I. Shahid, I. S. Ansari, M. K. Kundu, S. K. Ghosh, M. B. Hossain, A. S. M. S. Hosen, and G. H. Cho, "On secrecy performance of mixed generalized gamma and Malaga RF-FSO variable gain relaying channel," *IEEE Access*, vol. 8, pp. 104127–104138, 2020.

[46] M. J. Saber, J. Mazloum, A. M. Sazdar, A. Keshavarz, and M. J. Piran, "On secure mixed rf-fso decode-and-forward relaying systems with energy harvesting," *IEEE Systems Journal*, vol. 14, no. 3, pp. 4402–4405, 2020.

[47] K. O. Odeyemi and P. A. Owolawi, "Security outage performance of partial relay selection in AF mixed RF/FSO system with outdated channel state information," *Transactions on Emerging Telecommunications Technologies*, vol. 30, July 2019.

[48] Z. Hu, C. Chen, Z. Zhang, and H. Zhang, "Secure cooperative transmission for mixed rf/fso spectrum sharing networks," *IEEE Transactions on Communications*, vol. 68, no. 5, pp. 3010–3023, 2020.

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

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

[51] N. A. Sarker, A. S. M. Badrudduza, S. M. R. Islam, S. H. Islam, I. S. Ansari, M. K. Kundu, M. F. Samad, M. B. Hossain, and H. Yu, "Secrecy performance analysis of mixed hyper-gamma and gamma-gamma cooperative relaying system," *IEEE Access*, vol. 8, pp. 131273–131285, 2020.

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

[53] V. K. Tonk, V. K. Dwivedi, A. Upadhya, S. P. Singh, and P. K. Yadav, "New results in secrecy analysis of mixed rf/fso cooperative relaying networks," *Optics Communications*, vol. 503, p. 127376, 2021.

[54] N. H. Juel, A. S. M. Badrudduza, S. M. R. Islam, S. H. Islam, M. K. Kundu, I. S. Ansari, M. M. Mowla, and K.-S. Kwak, "Secrecy performance analysis of mixed α-μ and exponentiated weibull RF-FSO cooperative relaying system," *IEEE Access*, vol. 9, pp. 72342–72356, 2021.

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

[56] L. Yang, T. Liu, J. Chen, and M. Alouini, "Physical-layer security for mixed η–μ and $\mathcal{M}$-distribution dual-hop RF/FSO systems," *IEEE Transactions on Vehicular Technology*, vol. 67, pp. 12427–12431, December 2018.

[57] A. Kumar and P. Garg, "Physical layer security for dual-hop FSO/RF system using generalized $\Gamma\Gamma/\eta-\mu$ fading channels," *International Journal of Communication Systems*, vol. 31,

no. 3, pp. 1–12, 2018.

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

[59] S. H. Islam, A. S. M. Badrudduza, S. M. R. Islam, F. I. Shahid, I. S. Ansari, M. K. Kundu, and H. Yu, "Impact of correlation and pointing error on secure outage performance over arbitrary correlated nakagami-m and $\mathcal{M}$-turbulent fading mixed RF-FSO channel," *IEEE Photonics Journal*, vol. 13, no. 2, pp. 1–17, 2021.

[60] M. J. Saber and A. Keshavarz, "Secrecy outage probability analysis of dual-hop RF-FSO fixed-gain relaying system," in *2018 9th International Symposium on Telecommunications (IST)*, pp. 11–14, 2018.

[61] D. R. Pattanayak, V. K. Dwivedi, V. Karwal, I. S. Ansari, H. Lei, and M.-S. Alouini, "On the physical layer security of a decode and forward based mixed FSO/RF co-operative system," *IEEE Wireless Communications Letters*, vol. 9, no. 7, pp. 1031–1035, 2020.

[62] D. R. Pattanayak, V. K. Dwivedi, and V. Karwal, "Physical layer security of a two way relay based mixed FSO/RF network in the presence of multiple eavesdroppers," *Optics Communications*, vol. 463, p. 125429, 2020.

[63] M. J. Saber and S. Rajabi, "On secrecy performance of millimeter-wave RF-assisted FSO communication systems," *IEEE Systems Journal*, vol. 15, no. 3, pp. 3781–3788, 2021.

[64] H. Lei, Z. Dai, K.-H. Park, W. Lei, G. Pan, and M.-S. Alouini, "Secrecy outage analysis of mixed RF-FSO downlink swipt systems," *IEEE Transactions on Communications*, vol. 66, no. 12, pp. 6384–6395, 2018.

[65] R. Singh, M. Rawat, and A. Jaiswal, "On the performance of mixed FSO/RF SWIPT systems with secrecy analysis," *IEEE Systems Journal*, pp. 1–30, 2021.

[66] M. J. Saber, A. Keshavarz, J. Mazloum, A. M. Sazdar, and M. J. Piran, "Physical-layer security analysis of mixed SIMO SWIPT RF and FSO fixed-gain relaying systems," *IEEE Systems Journal*, vol. 13, pp. 2851–2858, September 2019.

[67] Y. Ai, A. Mathur, M. Cheffena, M. R. Bhatnagar, and H. Lei, "Physical layer security of hybrid satellite-FSO cooperative systems," *IEEE Photonics Journal*, vol. 11, no. 1, pp. 1–14, 2019.

[68] I. B. Djordjevic, "OAM-based hybrid free-space optical-terahertz multidimensional coded modulation and physical-layer security," *IEEE Photonics Journal*, vol. 9, no. 4, pp. 1–12, 2017.

[69] N. Varshney, A. K. Jagannatham, and P. K. Varshney, "Cognitive mimo-rf/fso cooperative relay communication with mobile nodes and imperfect channel state information," *IEEE Transactions on Cognitive Communications and Networking*, vol. 4, no. 3, pp. 544–555, 2018.

[70] H. Lei, H. Luo, K. Park, Z. Ren, G. Pan, and M. Alouini, "Secrecy outage analysis of mixed RF-FSO systems with channel imperfection," *IEEE Photonics Journal*, vol. 10, pp. 1–13, June 2018.

[71] K. O. Odeyemi and P. A. Owolawi, "Physical layer security in mixed RF/FSO system under multiple eavesdroppers collusion and non-collusion," *Optical and Quantum Electronics*, vol. 50, July 2018.

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

[73] H. Liang, Y. Li, M. Miao, C. Gao, and X. Li, "Analysis of selection combining hybrid FSO/RF systems considering physical layer security and interference," *Optics Communications*, p. 127146, 2021.

[74] Y. Ai, A. Mathur, H. Lei, M. Cheffena, and I. S. Ansari, "Secrecy enhancement of RF backhaul system with parallel FSO communication link," *Optics Communications*, vol. 475, p. 126193, 2020.

[75] W. M. R. Shakir, "Physical layer security performance analysis of hybrid FSO/RF communication system," *IEEE Access*, vol. 9, pp. 18948–18961, 2021.

[76] K. O. Odeyemi, P. A. Owolawi, and O. O. Olakanmi, "Secrecy performance of cognitive underlay hybrid RF/FSO system under pointing errors and link blockage impairments," *Optical and Quantum Electronics*, vol. 52, no. 3, pp. 1–16, 2020.

[77] M. Kafafy, Y. Fahmy, M. Khairy, and M. Abdallah, "Secure backhauling over adaptive parallel mmWave/FSO link," in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, 2020.

[78] S. Althunibat, R. Mesleh, and K. Qaraqe, "Secure index-modulation based hybrid free space optical and millimeter wave links," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6325–6332, 2020.

[79] D. R. Pattanayak, V. K. Dwivedi, and V. Karwal, "On the physical layer security of hybrid RF-FSO system in presence of multiple eavesdroppers and receiver diversity," *Optics Communications*, vol. 477, p. 126334, 2020.

[80] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, October 1975.

[81] M. You, H. Sun, J. Jiang, and J. Zhang, "Effective rate analysis in weibull fading channels," *IEEE Wireless Communications Letters*, vol. 5, no. 4, pp. 340–343, 2016.

[82] I. Gradshteyn and I. Ryzhik, *Table of integrals, series, and products*. San Diego, United States: Academic Press, seven ed., 2014.

[83] A. Prudnikov, Y. A. Brychkov, and O. Marichev, *Integrals and Series, vol 3: more special functions*. New York, United States: New York Gordon and Breach Science Publishers, first ed.

[84] F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," *IEEE Photonics Journal*, vol. 7, pp. 1–14, April 2015.

[85] J. M. Garrido-Balsells, A. Jurado-Navas, J. F. Paris, M. Castillo-Vázquez, and A. Puerta-Notario, "Spatially correlated gamma-gamma scintillation in atmospheric optical channels," *OSA Opt. Express*, vol. 22, pp. 21820–21833, September 2014.

[86] A. Al-Habash, L. C. Andrews, and R. L. Phillips, "Mathematical model for the irradiance probability density function of a laser beam propagating through turbulent media," *SPIE Optical Engineering*, vol. 40, pp. 1554–1562, August 2001.

[87] H. Holm and M. S. Alouini, "Sum and difference of two squared correlated nakagami variates in connection with the McKay distribution," *IEEE Transactions on Communications*, vol. 52, pp. 1367–1376, August 2004.

[88] Y. Ai, A. Mathur, L. Kong, and M. Cheffena, "Secure outage analysis of FSO communications over arbitrarily correlated malaga turbulence channels," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 4, pp. 3961–3965, 2021.

[89] N. S. Ferdinand, D. B. da Costa, A. L. F. de Almeida, and M. Latva-aho, "Physical layer secrecy performance of TAS wiretap channels with correlated main and eavesdropper channels," *IEEE Wireless Communications Letters*, vol. 3, no. 1, pp. 86–89, 2014.

[90] X. Liu, "Outage probability of secrecy capacity over correlated log-normal fading channels," *IEEE Communications Letters*, vol. 17, no. 2, pp. 289–292, 2013.

[91] A. Mathur, Y. Ai, M. Cheffena, and G. Kaddoum, "Secrecy performance of correlated α - μ fading channels," *IEEE Communications Letters*, vol. 23, no. 8, pp. 1323–1327, 2019.

[92] G. Cui, Q. Zhu, L. Xu, and W. Wang, "Secure beamforming and jamming for multibeam satellite systems with correlated wiretap channels," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12348–12353, 2020.

[93] S. C. Tokgoz, S. Althunibat, S. L. Miller, and K. A. Qaraqe, "Performance analysis of index modulation based link-selection mechanism for hybrid FSO-mmWave systems," *Optics Communications*, vol. 479, p. 126305.

[94] S. C. Tokgoz, S. Althunibat, and K. Qaraqe, "A link-selection mechanism for hybrid FSO-mmWave systems based on index modulation," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–7, 2020.

[95] M. Usman, H. Yang, and M. Alouini, "Practical switching-based hybrid FSO/RF transmission and its performance analysis," *IEEE Photonics Journal*, vol. 6, pp. 1–13, October 2014.

[96] T. Rakia, H. Yang, M. Alouini, and F. Gebali, "Outage analysis of practical FSO/RF hybrid system with adaptive combining," *IEEE Communications Letters*, vol. 19, pp. 1366–1369, August 2015.

[97] W. M. R. Shakir, "Performance evaluation of a selection combining scheme for the hybrid FSO/RF system," *IEEE Photonics Journal*, vol. 10, pp. 1–10, February 2018.

[98] P. Krishnan, "Performance analysis of hybrid RF/FSO system using BPSK-SIM and DPSK-SIM over gamma-gamma turbulence channel with pointing errors for smart city applications," *IEEE Access*, vol. 6, pp. 75025–75032, 2018.

[99] S. Althunibat, O. S. Badarneh, R. Mesleh, and K. Qaraqe, "A hybrid free space optical-millimeter wave cooperative system," *Optics Communications*, vol. 453, p. 124400, 2019.

[100] E. Balti and M. Guizani, "Mixed RF/FSO cooperative relaying systems with co-channel interference," *IEEE Transactions on Communications*, vol. 66, no. 9, pp. 4014–4027, 2018.

[101] M. A. Amirabadi and V. Tabataba Vakili, "Performance evaluation of a novel relay-assisted hybrid FSO/RF communication system with receive diversity," *IET Optoelectronics*, vol. 13, no. 5, pp. 203–214, 2019.

[102] B. Makki, T. Svensson, and M. Alouini, "On the performance of millimeter wave-based RF-FSO links with HARQ feedback," in *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–6, September 2016.

[103] H. Kong, M. Lin, W. Zhu, H. Amindavar, and M. Alouini, "Multiuser scheduling for asymmetric FSO/RF links in satellite-UAV-terrestrial networks," *IEEE Wireless Communications Letters*, pp. 1–1, 2020.

[104] H. Ajam, M. Najafi, V. Jamali, and R. Schober, "Ergodic sum rate analysis of UAV-based relay networks with mixed RF-FSO channels," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 164–178, 2020.

[105] M. Khan, S. Bhunia, M. Yuksel, and L. C. Kane, "Line-of-sight discovery in 3D using highly directional transceivers," *IEEE Transactions on Mobile Computing*, vol. 18, no. 12, pp. 2885–2898, 2019.

[106] J. Lee, K. Park, M. Alouini, and Y. Ko, "On the throughput of mixed FSO/RF UAV-enabled mobile relaying systems with a buffer constraint," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pp. 1–6, 2019.

[107] N. D. Chatzidiamantis, G. K. Karagiannidis, E. E. Kriezis, and M. Matthaiou, "Diversity combining in hybrid RF/FSO systems with PSK modulation," in *2011 IEEE International Conference on Communications (ICC)*, pp. 1–6, June 2011.

[108] M. Brambilla, A. Matera, D. Tagliaferri, M. Nicoli, and U. Spagnolini, "RF-assisted free-space optics for 5G vehicle-to-vehicle communications," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, May 2019.

[109] C. Stefanovic, M. Pratesi, and F. Santucci, "Second order statistics of mixed RF-FSO relay systems and its application to vehicular networks," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pp. 1–6, 2019.

[110] J. Proakis and M. Salehi, *Digital Communications*. New York, United States: McGraw-Hill Higher Education, fifth ed., 2007.

[111] M. Uysal, J. Li, and M. Yu, "Error rate performance analysis of coded free-space optical links over gamma-gamma atmospheric turbulence channels," *IEEE Transactions on Wireless Communications*, vol. 5, pp. 1229–1233, June 2006.

[112] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Transactions on Information Theory*, vol. 45, pp. 1456–1467, July 1999.

[113] J. W. Craig, "A new, simple and exact result for calculating the probability of error for two-dimensional signal constellations," in *MILCOM 91 - Conference record*, pp. 571–575, November 1991.

[114] M. . Alouini and A. J. Goldsmith, "A unified approach for calculating error rates of linearly modulated signals over generalized fading channels," *IEEE Transactions on Communications*, vol. 47, pp. 1324–1334, September 1999.

[115] N. Wang and J. Cheng, "Moment-based estimation for the shape parameters of the gamma-gamma atmospheric turbulence model.," *Optical Express*, vol. 18, pp. 12824–12831, June 2010.

[116] Z. Wang and G. B. Giannakis, "A simple and general parameterization quantifying performance in fading channels," *IEEE Transactions on Communications*, vol. 51, pp. 1389–1398, August 2003.

[117] U. Blahak, "Efficient approximation of the incomplete gamma function for use in cloud model applications," *Geoscientific Model Development*, vol. 3, no. 2, p. 329, 2010.

[118] V. S. Adamchik and O. I. Marichev, "The algorithm for calculating integrals of hypergeometric type functions and its realization in reduce system," in *Proceedings of the international symposium on Symbolic and algebraic computation*, pp. 212–224, ACM Press, 1990.

[119] S. Sanayei and A. Nosratinia, "Antenna selection in MIMO systems," *IEEE Communications Magazine*, vol. 42, no. 10, pp. 68–73, 2004.

[120] A. F. Molisch and M. Z. Win, "MIMO systems with antenna selection," *IEEE Microwave Magazine*, vol. 5, no. 1, pp. 46–56, 2004.

[121] A. F. Molisch, M. Z. Win, Yang-Seok Choi, and J. H. Winters, "Capacity of MIMO systems with antenna selection," *IEEE Transactions on Wireless Communications*, vol. 4, no. 4, pp. 1759–1772, 2005.

[122] M. Zhou, L. Song, Y. Li, and X. Li, "Simultaneous bidirectional link selection in full duplex MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 14, no. 7, pp. 4052–4062, 2015.

[123] X. Gao, O. Edfors, F. Tufvesson, and E. G. Larsson, "Massive MIMO in real propagation environments: Do all antennas contribute equally?," *IEEE Trans. on Communications*, vol. 63, no. 11, pp. 3917–3928, 2015.

[124] J. M. Moualeu, D. B. da Costa, F. J. Lopez-Martinez, W. Hamouda, T. M. N. Nkouatchah, and U. S. Dias, "Transmit antenna selection in secure MIMO systems over $\alpha - \mu$ fading channels," *IEEE Transactions on Communications*, vol. 67, no. 9, pp. 6483–6498, 2019.

[125] X. Zhang, A. Molisch, and S.-Y. Kung, "Variable-phase-shift-based RF-baseband codesign for MIMO antenna selection," *IEEE Transactions on Signal Processing*, vol. 53, no. 11, pp. 4091–4103, 2005.

[126] D. Gore and A. Paulraj, "MIMO antenna subset selection with space-time coding," *IEEE Transactions on Signal Processing*, vol. 50, no. 10, pp. 2580–2588, 2002.

[127] R. Heath, S. Sandhu, and A. Paulraj, "Antenna selection for spatial multiplexing systems with linear receivers," *IEEE Communications Letters*, vol. 5, no. 4, pp. 142–144, 2001.

[128] D. Gore, R. Heath, and A. Paulraj, "Transmit selection in spatial multiplexing systems," *IEEE Communications Letters*, vol. 6, no. 11, pp. 491–493, 2002.

[129] R. Blum and J. Winters, "On optimum mimo with antenna selection," in *IEEE International Conference on Communications (ICC)*, vol. 1, pp. 386–390 vol.1, 2002.

[130] Z. Chen, J. Yuan, and B. Vucetic, "Analysis of transmit antenna selection/maximal-ratio combining in rayleigh fading channels," *IEEE Transactions on Vehicular Technology*, vol. 54, no. 4, pp. 1312–1321, 2005.

[131] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Transactions on Communications*, vol. 61, no. 1, pp. 144–154, 2013.

[132] T. Zhang, Y. Cai, Y. Huang, T. Q. Duong, and W. Yang, "Secure transmission in cognitive MIMO relaying networks with outdated channel state information," *IEEE Access*, vol. 4, pp. 8212–8224, 2016.

[133] R. Zhao, H. Lin, Y.-C. He, D.-H. Chen, Y. Huang, and L. Yang, "Secrecy performance of transmit antenna selection for MIMO relay systems with outdated CSI," *IEEE Transactions on Communications*, vol. 66, no. 2, pp. 546–559, 2018.

[134] H. Lei, J. Zhang, K.-H. Park, P. Xu, Z. Zhang, G. Pan, and M.-S. Alouini, "Secrecy outage of max–min TAS scheme in MIMO-NOMA systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 6981–6990, 2018.

[135] J. Xiong, Y. Tang, D. Ma, P. Xiao, and K.-K. Wong, "Secrecy performance analysis for TAS-MRC system with imperfect feedback," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1617–1629, 2015.

[136] H. Zhao, Y. Tan, G. Pan, Y. Chen, and N. Yang, "Secrecy outage on transmit antenna selection/maximal ratio combining in MIMO cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 10236–10242, 2016.

[137] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels," *IEEE Transactions on Wireless Communications*, vol. 13, no. 3, pp. 1656–1667, 2014.

[138] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 254–259, 2013.

[139] D.-D. Tran, H.-V. Tran, D.-B. Ha, and G. Kaddoum, "Secure transmit antenna selection protocol for MIMO NOMA networks over Nakagami-m channels," *IEEE Systems Journal*, vol. 14, no. 1, pp. 253–264, 2020.

[140] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Processing Letters*, vol. 19, no. 6, pp. 372–375, 2012.

[141] J. Joung, "Machine learning-based antenna selection in wireless communications," *IEEE Comm. Letters*, vol. 20, no. 11, pp. 2241–2244, 2016.

[142] P. Yang, Y. Xiao, M. Xiao, Y. L. Guan, S. Li, and W. Xiang, "Adaptive spatial modulation MIMO based on machine learning," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 9, pp. 2117–2131, 2019.

[143] A. Barthelme and W. Utschick, "A machine learning approach to DoA estimation and model order selection for antenna arrays with subarray sampling," *IEEE Transactions on Signal Processing*, vol. 69, pp. 3075–3087, 2021.

[144] J. Li, Y. Qiao, B. He, W. Li, and T. Xin, "Model-driven deep learning scheme for adaptive transmission in MIMO-SCFDE system," *IEEE Access*, vol. 8, pp. 197654–197664, 2020.

[145] A. M. Elbir and K. V. Mishra, "Joint antenna selection and hybrid beamformer design using unquantized and quantized deep learning networks," *IEEE Transactions on Wireless Communications*, vol. 19, no. 3, pp. 1677–1688, 2020.

[146] J. Chen, S. Chen, Y. Qi, and S. Fu, "Intelligent massive MIMO antenna selection using Monte carlo tree search," *IEEE Transactions on Signal Processing*, vol. 67, no. 20, pp. 5380–5390, 2019.

[147] S. Gecgel, C. Goztepe, and G. Karabulut Kurt, "Transmit antenna selection for large-scale MIMO GSM with machine learning," *IEEE Wireless Communications Letters*, vol. 9, no. 1, pp. 113–116, 2020.

[148] T. X. Vu, S. Chatzinotas, V.-D. Nguyen, D. T. Hoang, D. N. Nguyen, M. D. Renzo, and B. Ottersten, "Machine learning-enabled joint antenna selection and precoding design: From offline complexity to online performance," *IEEE Transactions on Wireless Communications*, vol. 20, no. 6, pp. 3710–3722, 2021.

[149] R. Yao, Y. Zhang, S. Wang, N. Qi, N. I. Miridakis, and T. A. Tsiftsis, "Deep neural network assisted approach for antenna selection in untrusted relay networks," *IEEE Wireless Communications Letters*, vol. 8, no. 6, pp. 1644–1647, 2019.

[150] M. Guo and M. C. Gursoy, "Statistical learning based joint antenna selection and user scheduling for single-cell massive MIMO systems," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 1, pp. 471–483, 2021.

[151] Y. Zhang, J. Wang, X. Wang, Y. Xue, and J. Song, "Efficient selection on spatial modulation antennas: Learning or boosting," *IEEE Wireless Communications Letters*, vol. 9, no. 8, pp. 1249–1252, 2020.

[152] D. He, C. Liu, T. Q. S. Quek, and H. Wang, "Transmit antenna selection in MIMO wiretap channels: A machine learning approach," *IEEE Wireless Communications Letters*, vol. 7, no. 4, pp. 634–637, 2018.

[153] Y. Hu, L. Li, J. Yin, H. Zhang, W. Liang, A. Gao, and Z. Han, "Optimal transmit antenna selection strategy for MIMO wiretap channel based on deep reinforcement learning," in *2018 IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 803–807, 2018.

[154] X. Zhang and M. Vaezi, "Deep learning based precoding for the MIMO gaussian wiretap channel," in *2019 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–6, 2019.

[155] B. Chen, C. Zhu, L. Shu, M. Su, J. Wei, V. C. M. Leung, and J. J. P. C. Rodrigues, "Securing uplink transmission for lightweight single-antenna UEs in the presence of a massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 5374–5384, 2016.

[156] M. T. Mamaghani and Y. Hong, "Intelligent trajectory design for secure full-duplex MIMO-UAV relaying against active eavesdroppers: A model-free reinforcement learning approach," *IEEE Access*, 2020.

[157] A. A. Farid and S. Hranilovic, "Outage capacity optimization for free-space optical links with pointing errors," *Journal of Lightwave Technology*, vol. 25, no. 7, pp. 1702–1710, 2007.

[158] R. Boluda-Ruiz, A. García-Zambrana, B. Castillo-Vázquez, and C. Castillo-Vázquez, "Impact of nonzero boresight pointing error on ergodic capacity of MIMO fso communication systems," *Opt. Express*, vol. 24, pp. 3513–3534, Feb 2016.

[159] H. Samimi and M. Uysal, "End-to-end performance of mixed rf/fso transmission systems," *IEEE/OSA Journal of Optical Communications and Networking*, vol. 5, no. 11, pp. 1139–1144, 2013.

[160] Q. Sun, Z. Zhang, Y. Zhang, M. López-Benítez, and J. Zhang, "Performance analysis of dual-hop wireless systems over mixed FSO/RF fading channel," *IEEE Access*, vol. 9, pp. 85529–85542, 2021.

[161] E. Lee, J. Park, D. Han, and G. Yoon, "Performance analysis of the asymmetric dual-hop relay transmission with mixed RF/FSO links," *IEEE Photonics Technology Letters*, vol. 23, no. 21, pp. 1642–1644, 2011.

[162] I. S. Ansari, F. Yilmaz, and M.-S. Alouini, "Impact of pointing errors on the performance of mixed RF/FSO dual-hop transmission systems," *IEEE Wireless Communications Letters*, vol. 2, no. 3, pp. 351–354, 2013.

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

[164] S. Anees and M. R. Bhatnagar, "Performance of an amplify-and-forward dual-hop asymmetric RF-FSO communication system," *IEEE/OSA Journal of Optical Communications and Networking*, vol. 7, no. 2, pp. 124–135, 2015.

[165] L. Yang, M. O. Hasna, and X. Gao, "Performance of mixed RF/FSO with variable gain over generalized atmospheric turbulence channels," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 9, pp. 1913–1924, 2015.

[166] L. Kong, W. Xu, L. Hanzo, H. Zhang, and C. Zhao, "Performance of a free-space-optical relay-assisted hybrid RF/FSO system in generalized M-distributed channels," *IEEE Photonics Journal*, vol. 7, no. 5, pp. 1–19, 2015.

[167] G. N. Kamga, S. Aissa, T. R. Rasethuntsa, and M.-S. Alouini, "Mixed RF/FSO communications with outdated-CSI-based relay selection under double generalized gamma turbulence, generalized pointing errors, and Nakagami-m fading," *IEEE Transactions on Wireless Communications*, vol. 20, no. 5, pp. 2761–2775, 2021.

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

[169] G. T. Djordjevic, M. I. Petkovic, A. M. Cvetkovic, and G. K. Karagiannidis, "Mixed RF/FSO relaying with outdated channel state information," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 9, pp. 1935–1948, 2015.

[170] M. I. Petkovic, A. M. Cvetkovic, G. T. Djordjevic, and G. K. Karagiannidis, "Partial relay selection with outdated channel state estimation in mixed RF/FSO systems," *Journal of Lightwave Technology*, vol. 33, no. 13, pp. 2860–2867, 2015.

[171] N. Varshney and A. K. Jagannatham, "Cognitive decode-and-forward MIMO-RF/FSO cooperative relay networks," *IEEE Communications Letters*, vol. 21, no. 4, pp. 893–896, 2017.

[172] S. Sharma, A. S. Madhukumar, and R. Swaminathan, "Switching-based cooperative decode-and-forward relaying for hybrid FSO/RF networks," *IEEE/OSA Journal of Optical Communications and Networking*, vol. 11, no. 6, pp. 267–281, 2019.

[173] S. Althunibat, O. S. Badarneh, R. Mesleh, and K. Qaraqe, "A hybrid free space optical-millimeter wave cooperative system," *Optics Communications*, vol. 453, p. 124400, 2019.

[174] A. Prudnikov, Y. A. Brychkov, and O. Marichev, *Integrals and Series, vol 1: elementary functions*. New York, United States: New York Gordon and Breach Science Publishers, fourth ed.

[175] H. Lei, C. Gao, I. S. Ansari, Y. Guo, G. Pan, and K. A. Qaraqe, "On physical-layer security over SIMO generalized-K fading channels," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 7780–7785, 2016.

[176] J. Abate and W. Whitt, "Numerical inversion of laplace transforms of probability distributions," *ORSA JC*, vol. 7, no. 1, pp. 36–43, 1995.

[177] Young-Chai Ko, M. S. Alouini, and M. K. Simon, "Outage probability of diversity systems over generalized fading channels," *IEEE Transactions on Communications*, vol. 48, no. 11, pp. 1783–1787, 2000.

[178] A. Kilbas and M. Saigo, *H-transforms. Theory and Applications*. Florida, United States: CRC Press, first ed., 2004.

APPENDIX A

DERIVATION OF PEP IN (3.29)

As both $\boldsymbol{h}_o$ and $\boldsymbol{h}_f$ are independent random variables, (3.28) can be expressed as

$$\text{PEP}_{kq} = \frac{1}{\pi}\int_0^{\frac{\pi}{2}} \boldsymbol{I}_o \boldsymbol{I}_f \cdot d\theta, \tag{A.1}$$

where $\boldsymbol{I}_o$ and $\boldsymbol{I}_f$ are respectively defined as

$$\boldsymbol{I}_o = \int_0^{\infty} \exp\left(-\frac{\varphi_o \left|\boldsymbol{h}_o\right|^2}{4\sigma^2 \sin^2\theta}\right) f_{\boldsymbol{h}_o}(\boldsymbol{h}_o) \cdot d\boldsymbol{h}_o, \tag{A.2}$$

and,

$$\boldsymbol{I}_f = \int_0^{\infty} \exp\left(-\frac{\varphi_f \left|\boldsymbol{h}_f\right|^2}{4\sigma^2 \sin^2\theta}\right) f_{|\boldsymbol{h}_f|^2}(|\boldsymbol{h}_f|^2) \cdot d|\boldsymbol{h}_f|^2. \tag{A.3}$$

Depending on the symbol vectors $\boldsymbol{x}_o$ and $\boldsymbol{x}_f$, there are three different cases for $\boldsymbol{\Delta}_o$ and $\boldsymbol{\Delta}_f$.

Case I: When $\boldsymbol{\Delta}_o = 0$ and $\boldsymbol{\Delta}_f \neq 0$, then, $\boldsymbol{I}_o = 1$, therefore, (A.1) yields

$$^{(1)}\text{PEP}_{kq} = \frac{1}{\pi}\int_0^{\frac{\pi}{2}} \boldsymbol{I}_f \cdot d\theta. \tag{A.4}$$

The integral $\boldsymbol{I}_f$ given in (A.3) can be re-written as

$$\boldsymbol{I}_f = \frac{m^m}{\Gamma(m)}\int_0^{\infty} \gamma^{m-1} e^{-(\omega_f + m)\gamma} \cdot d\gamma, \tag{A.5}$$

where $\omega_f = \frac{\varphi_f}{4\sigma^2 \sin^2\theta}$. It can be solved using [82, (3.381.4)] as

$$\boldsymbol{I}_f = \left(\frac{m}{\omega_f + m}\right)^m. \tag{A.6}$$

Further, using the value of $\omega_f = \frac{\varphi_f}{4\sigma^2 \sin^2\theta}$, $\boldsymbol{I}_f$ can be expressed as

$$\boldsymbol{I}_f = \left(\frac{\sin^2(\theta)}{\frac{\omega_f}{4m\sigma^2} + \sin^2(\theta)} \right)^m. \tag{A.7}$$

By substituting (A.7) into (A.4), the average PEP can be re-written as

$${}^{(1)}\text{PEP}_{kq} = \frac{1}{\pi} \int_0^{\frac{\pi}{2}} \left(\frac{\sin^2(\theta)}{\varrho + \sin^2(\theta)} \right)^m \cdot d\theta, \tag{A.8}$$

where $\varrho = \frac{\omega_f}{4m\sigma^2}$. Then ${}^{(1)}\text{PEP}_{kq}$ can be solved using [114, (64)] in a closed form expression as

$${}^{(1)}\text{PEP}_{kq} = \chi^m \sum_{t=0}^{m-1} \binom{m-1+t}{t} (1-\chi)^t, \tag{A.9}$$

where $\chi = \frac{1}{2}\left(1 - \sqrt{\frac{\varrho}{1+\varrho}}\right)$.

Case II: When $\boldsymbol{\Delta}_f = 0$ and $\boldsymbol{\Delta}_o \neq 0$, then, $\boldsymbol{I}_f = 1$. Therefore, (A.1) yields

$${}^{(2)}\text{PEP}_{kq} = \frac{1}{\pi} \int_0^{\frac{\pi}{2}} \boldsymbol{I}_o \cdot d\theta. \tag{A.10}$$

To solve the integral, we use the Fox-H representation of the PDF $f_{\boldsymbol{h}_o}(\boldsymbol{h}_o)$ [178, (2.9.19)]

$$f_{\boldsymbol{h}_o}(\boldsymbol{h}_o) = \frac{\eta}{2} {\boldsymbol{h}_o}^{\mu-1} H_{0,2}^{2,0}\left(c\,\boldsymbol{h}_o \middle| \begin{matrix} - \\ (\frac{\beta-\alpha}{2}, 1), (\frac{\alpha-\beta}{2}, 1) \end{matrix} \right), \tag{A.11}$$

where $c = \alpha\beta$, $\mu = \frac{\alpha+\beta}{2}$ and $\eta = \frac{2c^\mu}{\Gamma(\alpha)\Gamma(\beta)}$. As such, (A.2) can be re-written as

$$\boldsymbol{I}_o = \frac{\eta}{2} \int_0^\infty \exp\left(-\omega_o |\boldsymbol{h}_o|^2\right) {\boldsymbol{h}_o}^{\mu-1} H_{0,2}^{2,0}\left(c\,\boldsymbol{h}_o \middle| \begin{matrix} - \\ (\frac{\beta-\alpha}{2}, 1), (\frac{\alpha-\beta}{2}, 1) \end{matrix} \right) \cdot d\boldsymbol{h}_o, \tag{A.12}$$

where $\omega_o = \frac{\varphi_o}{4\sigma^2 \sin^2\theta}$. The term $\exp\left(-\omega_o |\boldsymbol{h}_o|^2\right) {\boldsymbol{h}_o}^{\mu-1}$ can also be expressed in terms of the Fox-H

function [178, (2.9.4)], and hence, (A.12) can be re-written as

$$\boldsymbol{I}_o = \frac{\eta}{4}\int_0^{\infty} \omega_o^{\frac{1-\mu}{2}} H_{0,1}^{1,0}\left(\boldsymbol{h}_o\sqrt{\omega_o}\middle|\begin{matrix}-\\(\frac{\mu-1}{2},\frac{1}{2})\end{matrix}\right) H_{0,2}^{2,0}\left(c\,\boldsymbol{h}_o\middle|\begin{matrix}-\\(\frac{\beta-\alpha}{2},1),(\frac{\alpha-\beta}{2},1)\end{matrix}\right)\cdot d\boldsymbol{h}_o, \tag{A.13}$$

which can be further modified using [83, (8.3.2.6)] to be

$$\boldsymbol{I}_o = \frac{\eta}{4}\int_0^{\infty} \omega_o^{\frac{1-\mu}{2}} H_{1,2}^{1,1}\left(\boldsymbol{h}_o\sqrt{\omega_o}\middle|\begin{matrix}(0,1)\\(\frac{\mu-1}{2},\frac{1}{2}),(0,1)\end{matrix}\right) H_{1,3}^{2,1}\left(c\,\boldsymbol{h}_o\middle|\begin{matrix}(0,1)\\(\frac{\beta-\alpha}{2},1),(\frac{\alpha-\beta}{2},1),(0,1)\end{matrix}\right)\cdot d\boldsymbol{h}_o. \tag{A.14}$$

This integral can be simplified using [83, (2.25.1.1)] as

$$\boldsymbol{I}_o = \frac{\eta}{4}\omega_o^{\frac{-\mu}{2}} H_{3,4}^{3,2}\left(\frac{c}{\sqrt{\omega_o}}\middle|\begin{matrix}(0,1),(1-\frac{\mu}{2},\frac{1}{2}),(0,1)\\(\frac{\beta-\alpha}{2},1),(\frac{\alpha-\beta}{2},1),(0,1),(0,1)\end{matrix}\right), \tag{A.15}$$

which can be further reduced to a simpler order using [83, (8.3.2.6)] to be

$$\boldsymbol{I}_o = \frac{\eta}{4}\omega_o^{\frac{-\mu}{2}} H_{2,3}^{3,1}\left(\frac{c}{\sqrt{\omega_o}}\middle|\begin{matrix}(1-\frac{\mu}{2},\frac{1}{2}),(0,1)\\(\frac{\beta-\alpha}{2},1),(\frac{\alpha-\beta}{2},1),(0,1)\end{matrix}\right). \tag{A.16}$$

Now, by substituting (A.16) into (A.10), the average PEP can be re-written as

$${}^{(2)}\text{PEP}_{kq} = \frac{\eta}{4\pi}\left(\frac{\varphi_o}{4\sigma^2}\right)^{\frac{-\mu}{2}}\int_0^{\frac{\pi}{2}} \sin^2(\theta)^{\frac{\mu}{2}} H_{2,3}^{3,1}\left(\frac{c}{\sqrt{\omega_o}}\middle|\begin{matrix}(1-\frac{\mu}{2},\frac{1}{2}),(0,1)\\(\frac{\beta-\alpha}{2},1),(\frac{\alpha-\beta}{2},1),(0,1)\end{matrix}\right)\cdot d\theta, \tag{A.17}$$

which can be solved in a closed form expression using [83, (2.25.2.2)]

$${}^{(2)}\text{PEP}_{kq} = \frac{\eta}{8\pi}\left(\frac{\varphi_o}{4\sigma^2}\right)^{\frac{-\mu}{2}} H_{4,4}^{3,3}\left(c'\middle|\begin{matrix}(\frac{1}{2}-\frac{\mu}{2},\frac{1}{2}),(\frac{1}{2},0),(1-\frac{\mu}{2},\frac{1}{2}),(0,1)\\(\frac{\beta-\alpha}{2},1),(\frac{\alpha-\beta}{2},1),(\frac{\alpha-\beta}{2},1),(0,1),(\frac{-\mu}{2},\frac{1}{2})\end{matrix}\right), \tag{A.18}$$

where $c' = c\left(\frac{4\sigma^2}{\varphi_o}\right)^{\frac{1}{2}}$.

Case III: In this case, both $\boldsymbol{\Delta}_f$ and $\boldsymbol{\Delta}_o$ are non-zero. The integral $\boldsymbol{I}_o$ is already solved in (A.16) as

$$\boldsymbol{I}_o = \frac{\eta}{4}\omega_o^{\frac{-\mu}{2}} H_{2,3}^{3,1}\left(\frac{c}{\sqrt{\omega_o}}\middle|\begin{matrix}(1-\frac{\mu}{2},\frac{1}{2}),(0,1)\\(\frac{\beta-\alpha}{2},1),(\frac{\alpha-\beta}{2},1),(0,1)\end{matrix}\right). \tag{A.19}$$

The integral $\boldsymbol{I}_f$ given in (A.3) can be re-written as

$$\boldsymbol{I}_f = \frac{m^m}{\Gamma(m)}\int_0^\infty e^{-\omega_f\gamma}\gamma^{m-1}e^{-m\gamma}\cdot d\gamma, \tag{A.20}$$

where $\omega_f = \frac{\varphi_f}{4\sigma^2\sin^2\theta}$. By expanding the term $e^{-m\gamma}$ using [82, (1.211.1)], (A.20) can be re-written as

$$\boldsymbol{I}_f = \frac{m^m}{\Gamma(m)}\sum_{t=0}^{\infty}\frac{(-m)^t}{t!}\int_0^\infty e^{-\omega_f\gamma}\gamma^{t+m-1}\cdot d\gamma, \tag{A.21}$$

where the integral can be solved using [82, (3.381.4)] to yield

$$\boldsymbol{I}_f = \sum_{t=0}^{\infty} A_t\left(\sin^2\theta\right)^{m+t}, \tag{A.22}$$

where $A_t = \frac{(-1)^t\Gamma(t+m)}{t!\,\Gamma(m)}\left(\frac{4\sigma^2 m}{\varphi_f}\right)^{t+m}$. Now, substituting (A.16) and (A.22) in (A.1), the average PEP in (A.1) can be re-written as

$${}^{(3)}\text{PEP}_{kq} = \frac{\eta}{4\pi}\sum_{t=0}^{\infty}A_t'\int_0^{\frac{\pi}{2}}\left(\sin^2\theta\right)^{m+t+\frac{\mu}{2}} H_{2,3}^{3,1}\left(c'\sin\theta\middle|\begin{matrix}(1-\frac{\mu}{2},\frac{1}{2}),(0,1)\\(\frac{\beta-\alpha}{2},1),(\frac{\alpha-\beta}{2},1),(0,1)\end{matrix}\right)\cdot d\theta, \tag{A.23}$$

where $A_t' = A_t\left(\frac{4\sigma^2}{\varphi_o}\right)^{\frac{\mu}{2}}$, and $c' = c\left(\frac{4\sigma^2}{\varphi_o}\right)^{\frac{1}{2}}$. Using [83, (2.25.2.2)], the integral in (A.23) can be

solved to yield

$$ {}^{(3)}\text{PEP}_{kq} = \frac{\eta}{8\pi} \sum_{t=0}^{\infty} A'_t H^{3,3}_{4,4} \left(\begin{array}{c} c' \\ \end{array} \middle| \begin{array}{c} (\frac{1}{2} - m - t - \frac{\mu}{2}, \frac{1}{2}), (\frac{1}{2}, 0), (1 - \frac{\mu}{2}, \frac{1}{2}), (0, 1) \\ (\frac{\beta-\alpha}{2}, 1), (\frac{\alpha-\beta}{2}, 1), (0, 1), (-m - t - \frac{\mu}{2}, \frac{1}{2}) \end{array} \right). \tag{A.24} $$

APPENDIX B

DERIVATION OF ASYMPTOTIC PEP IN (3.35)

To solve the integral in (A.1) to obtain asymptotic PEP, we need to re-formulate $\boldsymbol{I}_o$ in (A.2) and $\boldsymbol{I}_f$ in (A.3). First, by substituting (3.32) into (A.2), $\boldsymbol{I}_o$ can be re-written as follows

$$\widetilde{\boldsymbol{I}}_o \approx \overline{\eta} \int_0^{\infty} \exp\left(-\frac{\varphi_o \left|\boldsymbol{h}_o\right|^2}{4\sigma^2 \sin^2\theta}\right) \boldsymbol{h}_o^{\beta-1} \cdot d\boldsymbol{h}_o, \tag{B.1}$$

which can be solved by using [82, (3.381-4)] as

$$\widetilde{\boldsymbol{I}}_o \approx \frac{\overline{\eta}}{2}\Gamma\left(\frac{\beta}{2}\right)\left(\frac{\varphi_o}{4\sigma^2}\right)^{\frac{-\beta}{2}} \sin^{\beta}(\theta). \tag{B.2}$$

Substituting (3.33) into (A.3), $\boldsymbol{I}_f$ can be re-written as

$$\widetilde{\boldsymbol{I}}_f = \frac{m^m}{\Gamma(m)} \int_0^{\infty} \exp\left(-\frac{\varphi_f \gamma}{4\sigma^2 \sin^2\theta}\right) \gamma^{m-1} \cdot d\gamma. \tag{B.3}$$

The resultant integral can be written by using [82, (3.381-4)] as

$$\widetilde{\boldsymbol{I}}_f \approx m^m \left(\frac{\varphi_f}{4\sigma^2}\right)^{-m} \sin^{2m}(\theta). \tag{B.4}$$

Depending on the symbol vectors $\boldsymbol{x}_o$ and $\boldsymbol{x}_f$, there are three different cases for $\boldsymbol{\Delta}_o$ and $\boldsymbol{\Delta}_f$.

Case I: When $\boldsymbol{\Delta}_o = 0$ and $\boldsymbol{\Delta}_f \neq 0$, then, $\widetilde{\boldsymbol{I}}_o = 1$, therefore, (A.1) yields

$$^{(1)}\text{PEP}_{kq}^{\text{Asym}} = \frac{1}{\pi} \int_0^{\frac{\pi}{2}} \widetilde{\boldsymbol{I}}_f \cdot d\theta. \tag{B.5}$$

By substituting (B.4) into (B.5), asymptotic PEP can be re-written as

$$^{(1)}\text{PEP}_{kq}^{\text{Asym}} \approx \frac{1}{\pi}\int_0^{\frac{\pi}{2}} m^m \left(\frac{\varphi_f}{4\sigma^2}\right)^{-m} \sin^{2m}(\theta)\cdot d\theta, \tag{B.6}$$

which can be approximated by setting $\theta = \frac{\pi}{2}$ and solving the integral as

$$^{(1)}\text{PEP}_{kq}^{\text{Asym}} \approx \frac{m^m}{2}\left(\frac{\rho_f^r \left|\boldsymbol{\Delta}_f\right|^2}{4\sigma^2}\right)^{-m}. \tag{B.7}$$

Case II: When $\boldsymbol{\Delta}_f = 0$ and $\boldsymbol{\Delta}_o \neq 0$, then, $\widetilde{\boldsymbol{I}}_f = 1$. Therefore, (A.1) yields

$$^{(2)}\text{PEP}_{kq}^{\text{Asym}} = \frac{1}{\pi}\int_0^{\frac{\pi}{2}} \widetilde{\boldsymbol{I}}_o \cdot d\theta. \tag{B.8}$$

By substituting (B.2) into (B.8), asymptotic PEP can be re-written as

$$^{(2)}\text{PEP}_{kq}^{\text{Asym}} \approx \frac{1}{\pi}\int_0^{\frac{\pi}{2}} \frac{\overline{\eta}}{2}\Gamma\left(\frac{\beta}{2}\right)\left(\frac{\varphi_o}{4\sigma^2}\right)^{\frac{-\beta}{2}} \sin^{\beta}(\theta)\cdot d\theta, \tag{B.9}$$

which can be approximated by setting $\theta = \frac{\pi}{2}$ and solving the integral as

$$^{(2)}\text{PEP}_{kq}^{\text{Asym}} \approx \frac{\overline{\eta}}{4}\Gamma\left(\frac{\beta}{2}\right)\left(\frac{\xi^2(\rho_o^r)^2\left|\boldsymbol{\Delta}_o\right|^2}{4\sigma^2}\right)^{\frac{-\beta}{2}}. \tag{B.10}$$

Case III: Substituting (B.2) and (B.4) into (A.1), the asymptotic PEP can be written as

$$^{(3)}\text{PEP}_{kq}^{\text{Asym}} \approx \frac{1}{\pi}\int_0^{\frac{\pi}{2}} \frac{\overline{\eta}}{2}\Gamma\left(\frac{\beta}{2}\right)\left(\frac{\varphi_o}{4\sigma^2}\right)^{\frac{-\beta}{2}} m^m \left(\frac{\varphi_f}{4\sigma^2}\right)^{-m} \sin^{\frac{\beta}{2}+2m}(\theta)\cdot d\theta. \tag{B.11}$$

By setting $\theta = \frac{\pi}{2}$, the asymptotic PEP can be approximated as

$$^{(3)}\text{PEP}_{kq}^{\text{Asym}} \approx m^m \frac{\overline{\eta}}{4}\Gamma\left(\frac{\beta}{2}\right)\left(\frac{\rho_f^r\left|\boldsymbol{\Delta}_f\right|^2}{4\sigma^2}\right)^{-m}\left(\frac{\xi^2(\rho_o^r)^2\left|\boldsymbol{\Delta}_o\right|^2}{4\sigma^2}\right)^{-\frac{\beta}{2}}. \tag{B.12}$$

APPENDIX C

DEFINITION OF THE PARAMETERS IN SECTION 5.5

The parameters a_1 and a_2 that are used in (5.43) and (5.50)

$$\begin{cases} a_1 = m_1 - \ell - 1, \\ a_2 = m_1/\overline{\gamma}_{1,f}, \end{cases} \quad \text{for } \mathcal{I}^{\text{VG}}_{2,o}, \text{ and } \mathcal{I}^{\text{VG}}_{2,f},$$

$$\begin{cases} a_1 = m_2 - \ell - 1, \\ a_2 = m_2/\overline{\gamma}_{2,f}, \end{cases} \quad \text{for } \mathcal{I}^{\text{VG}}_{3,o}, \text{ and } \mathcal{I}^{\text{VG}}_{3,f},$$

$$\begin{cases} a_1 = m_1 + m_2 - 2\ell - 2, \\ a_2 = m_1/\overline{\gamma}_{1,f} + m_2/\overline{\gamma}_{2,f}, \end{cases} \quad \text{for } \mathcal{I}^{\text{VG}}_{4,o}, \text{ and } \mathcal{I}^{\text{VG}}_{4,f}. \tag{C.1}$$

The parameters a_1 and a_2 that are used in (5.52)

$$\begin{cases} a_1 = m_e - \ell_e - 1, \\ a_2 = m_e/\overline{\gamma}_{e,f}, \end{cases} \quad \text{for} \quad \mathcal{I}^{\text{VG}}_{1,h},$$

$$\begin{cases} a_1 = m_1 + m_e - \ell - \ell_e - 2, \\ a_2 = m_1/\overline{\gamma}_{1,f} + m_e/\overline{\gamma}_{e,f}, \end{cases} \quad \text{for} \quad \mathcal{I}^{\text{VG}}_{2,h},$$

$$\begin{cases} a_1 = m_2 + m_e - \ell - \ell_e - 2, \\ a_2 = m_2/\overline{\gamma}_{2,f} + m_e/\overline{\gamma}_{e,f}, \end{cases} \quad \text{for} \quad \mathcal{I}^{\text{VG}}_{3,h},$$

$$\begin{cases} a_1 = m_1 + m_2 + m_e - 2\ell - \ell_e - 3, \\ a_2 = m_1/\overline{\gamma}_{1,f} + m_2/\overline{\gamma}_{2,f} + m_e/\overline{\gamma}_{e,f}, \end{cases} \quad \text{for} \quad \mathcal{I}^{\text{VG}}_{4,h}. \tag{C.2}$$

The parameters a_1, a_2, b_1 and b_2 that are used in (5.58) and (5.61)

$$\begin{cases} a_1 = (2m_1 + m_2 - 2\ell_1 - \ell_2 - k - 5)/2, \\ a_2 = (m_2 - \ell_2 - k - 2)/2, \\ b_1 = m_1/\overline{\gamma}_{1,f}, \\ b_2 = \mathcal{G}m_1m_2/\overline{\gamma}_{1,f}\overline{\gamma}_{2,f} \end{cases} \quad \text{for } \mathcal{I}^{\text{FG}}_{2,o} \text{ and } \mathcal{I}^{\text{FG}}_{2,f},$$

$$\begin{cases} a_1 = (2m_1 + m_2 - 2\ell_1 - \ell_2 - k - 3)/2, \\ a_2 = (m_2 - \ell_2 - k - 1)/2, \\ b_1 = m_1/\overline{\gamma}_{1,f}, \\ b_2 = \mathcal{G}m_1m_2/\overline{\gamma}_{1,f}\overline{\gamma}_{2,f} \end{cases} \quad \text{for } \mathcal{I}^{\text{FG}}_{3,o} \text{ and } \mathcal{I}^{\text{FG}}_{3,f}. \tag{C.3}$$

The parameters a_1, a_2, b_1 and b_2 that are used in (5.64)

$$\begin{cases} a_1 = (2m_1 + m_2 + 2m_e - 2\ell_1 - \ell_2 - \ell - k - 7)/2, \\ a_2 = (m_2 - \ell_2 - k - 2)/2, \\ b_1 = (m_1/\overline{\gamma}_{1,f}) + (m_e/\overline{\gamma}_{e,f}), \\ b_2 = \mathcal{G}m_1m_2/\overline{\gamma}_{1,f}\overline{\gamma}_{2,f} \end{cases} \quad \text{for} \quad \mathcal{I}^{\text{FG}}_{2,h},$$

$$\begin{cases} a_1 = (2m_1 + m_2 + 2m_e - 2\ell_1 - \ell_2 - \ell - k - 5)/2, \\ a_2 = (m_2 - \ell_2 - k - 1)/2, \\ b_1 = (m_1/\overline{\gamma}_{1,f}) + (m_e/\overline{\gamma}_{e,f}), \\ b_2 = \mathcal{G}m_1m_2/\overline{\gamma}_{1,f}\overline{\gamma}_{2,f} \end{cases} \quad \text{for} \quad \mathcal{I}^{\text{FG}}_{3,h}. \tag{C.4}$$

The parameters a_1 and a_2 that are used in (5.71)

$$\begin{cases} a_1 = m_1 - \ell + \frac{\alpha_e+\beta_e}{4} - 1, \\ a_2 = m_1(2^{\mathcal{R}} - 1)/\overline{\gamma}_{1,f}, \end{cases} \quad \text{for} \quad \mathcal{T}_{1,o}^{\text{VG}},$$

$$\begin{cases} a_1 = m_2 - \ell + \frac{\alpha_e+\beta_e}{4} - 1, \\ a_2 = m_2(2^{\mathcal{R}} - 1)/\overline{\gamma}_{2,f}, \end{cases} \quad \text{for} \quad \mathcal{T}_{2,o}^{\text{VG}},$$

$$\begin{cases} a_1 = m_1 + m_2 - 2\ell + \frac{\alpha_e+\beta_e}{4} - 2, \\ a_2 = m_1/\overline{\gamma}_{1,f} + m_2/\overline{\gamma}_{2,f}, \end{cases} \quad \text{for} \quad \mathcal{T}_{3,o}^{\text{VG}}. \tag{C.5}$$

The parameters a_1 and a_2 that are used in (5.73)

$$\begin{cases} a_1 = m_1 + m_e - \ell - 2, \\ a_2 = m_1(2^{\mathcal{R}} - 1)/\overline{\gamma}_{1,f} + m_e/\overline{\gamma}_{e,f}, \end{cases} \quad \text{for} \quad \mathcal{T}_{1,f}^{\text{VG}},$$

$$\begin{cases} a_1 = m_2 + m_e - \ell - 2, \\ a_2 = m_2(2^{\mathcal{R}} - 1)/\overline{\gamma}_{2,f} + m_e/\overline{\gamma}_{e,f}, \end{cases} \quad \text{for} \quad \mathcal{T}_{2,f}^{\text{VG}},$$

$$\begin{cases} a_1 = m_1 + m_2 + m_e - 2\ell - 3, \\ a_2 = (m_1/\overline{\gamma}_{1,f} + m_2/\overline{\gamma}_{2,f})2^{\mathcal{R}} + m_e/\overline{\gamma}_{e,f}, \end{cases} \quad \text{for} \quad \mathcal{T}_{3,f}^{\text{VG}}. \tag{C.6}$$

The parameters a_1 and a_2 that are used in (5.75)

$$\begin{cases} a_1 = m_1 + m_e - 2\ell - 4, \\ a_2 = m_1(2^{\mathcal{R}} - 1)/\overline{\gamma}_{1,f} + m_e/\overline{\gamma}_{e,f}, \end{cases} \quad \text{for} \quad \mathcal{T}_{1,h}^{\text{VG}},$$

$$\begin{cases} a_1 = m_1 + m_e - 2\ell - 3, \\ a_2 = m_1(2^{\mathcal{R}} - 1)/\overline{\gamma}_{1,f} + m_e/\overline{\gamma}_{e,f}, \end{cases} \quad \text{for} \quad \mathcal{T}_{4,h}^{\text{VG}},$$

$$\begin{cases} a_1 = m_2 + m_e - 2\ell - 4, \\ a_2 = m_2(2^{\mathcal{R}} - 1)/\overline{\gamma}_{2,f} + m_e/\overline{\gamma}_{e,f}, \end{cases} \quad \text{for} \quad \mathcal{T}_{2,h}^{\text{VG}},$$

$$\begin{cases} a_1 = m_2 + m_e - 2\ell - 3, \\ a_2 = m_2(2^{\mathcal{R}} - 1)/\overline{\gamma}_{2,f} + m_e/\overline{\gamma}_{e,f}, \end{cases} \quad \text{for} \quad \mathcal{T}_{5,h}^{\text{VG}},$$

$$\begin{cases} a_1 = m_1 + m_2 + m_e - 2\ell - 5, \\ a_2 = (m_1/\overline{\gamma}_{1,f} + m_2/\overline{\gamma}_{2,f})2^{\mathcal{R}} + m_e/\overline{\gamma}_{e,f}, \end{cases} \quad \text{for} \quad \mathcal{T}_{3,h}^{\text{VG}},$$

$$\begin{cases} a_1 = m_1 + m_2 + m_e - 2\ell - 4, \\ a_2 = (m_1/\overline{\gamma}_{1,f} + m_2/\overline{\gamma}_{2,f})2^{\mathcal{R}} + m_e/\overline{\gamma}_{e,f}, \end{cases} \quad \text{for} \quad \mathcal{T}_{6,h}^{\text{VG}}. \tag{C.7}$$

The parameters a_1 and a_2 that are used in (5.80) and (5.82)

$$\begin{cases} a_1 = (2m_1 + m_2 - 2\ell_1 - \ell_2 - k - 5)/2, \\ a_2 = (m_2 - \ell_2 - k - 2)/2, \end{cases} \quad \text{for} \quad \mathcal{T}_{1,o}^{\text{FG}},$$

$$\begin{cases} a_1 = (2m_1 + m_2 - 2\ell_1 - \ell_2 - k - 3)/2, \\ a_2 = (m_2 - \ell_2 - k - 1)/2, \end{cases} \quad \text{for} \quad \mathcal{T}_{2,o}^{\text{FG}}. \tag{C.8}$$

The parameters a_1 and a_2 that are used in (5.84)

$$\begin{cases} a_1 = (2m_1 + m_2 - 2\ell_1 - \ell_2 - k - 5)/2, \\ a_2 = (m_2 - \ell_2 - k - 2)/2, \\ a_3 = m_e - \ell - 3, \end{cases} \quad \text{for} \quad \mathcal{T}_{1,h}^{\text{FG}},$$

$$\begin{cases} a_1 = (2m_1 + m_2 - 2\ell_1 - \ell_2 - k - 3)/2, \\ a_2 = (m_2 - \ell_2 - k - 1)/2, \\ a_3 = m_e - \ell - 3, \end{cases} \quad \text{for} \quad \mathcal{T}_{2,h}^{\text{FG}},$$

$$\begin{cases} a_1 = (2m_1 + m_2 - 2\ell_1 - \ell_2 - k - 5)/2, \\ a_2 = (m_2 - \ell_2 - k - 2)/2, \\ a_3 = m_e - \ell - 2, \end{cases} \quad \text{for} \quad \mathcal{T}_{3,h}^{\text{FG}},$$

$$\begin{cases} a_1 = (2m_1 + m_2 - 2\ell_1 - \ell_2 - k - 3)/2, \\ a_2 = (m_2 - \ell_2 - k - 1)/2, \\ a_3 = m_e - \ell - 2, \end{cases} \quad \text{for} \quad \mathcal{T}_{4,h}^{\text{FG}}. \tag{C.9}$$

The parameters B_1, B_2, and B_3 that are used in (5.27), (5.28), (5.65), (5.66), (5.67), (5.85), (5.86), and (5.87)

$$\begin{aligned} B_1 &= \binom{m_1 - \ell_1 - 1}{k} \mathcal{G}^k \left(\frac{\mathcal{G} m_1 \overline{\gamma}_{2,f}}{m_2 \overline{\gamma}_{1,f}} \right)^{\frac{m_2 - \ell_2 - k - 1}{2}}, \\ B_2 &= (m_2 - \ell_2 - 2) m_2 \overline{\gamma}_{1,f} / \mathcal{G} m_1 \overline{\gamma}_{2,f}, \\ B_3 &= m_2 / \overline{\gamma}_{2,f}. \end{aligned} \tag{C.10}$$

The parameters $\widehat{B}_2$ and $\widehat{B}_3$ that are used in (5.28) (5.85), (5.86), and (5.87)

$$\begin{aligned}
\widehat{B}_2 &= \frac{(m_2-\ell_2-2)m_2\overline{\gamma}_{1,f}}{\mathcal{G}m_1\overline{\gamma}_{2,f}}\left(\frac{\overline{\gamma}_{1,f}\overline{\gamma}_{2,f}}{\mathcal{G}m_1m_2}\right)^{\frac{2m_1+m_2-2\ell_1-\ell_2-k-5}{2}}, \\
\widehat{B}_3 &= \frac{m_2}{\overline{\gamma}_{2,f}}\left(\frac{\mathcal{G}m_1m_2}{\overline{\gamma}_{1,f}\overline{\gamma}_{2,f}}\right)^{-\frac{2m_1+m_2-2\ell_1-\ell_2-k-5}{2}}.
\end{aligned} \tag{C.11}$$

The parameters A_1, A_2, and A_3 that are used in (5.76), (5.77), and (5.78)

$$\begin{aligned}
A_1 &= \binom{m_1-\ell-1}{k}(2^{\mathcal{R}}-1)^k 2^{\mathcal{R}(m_1-\ell-1)}e^{-\frac{m_1(2^{\mathcal{R}}-1)}{\overline{\gamma}_{1,f}}}, \\
A_2 &= \binom{m_2-\ell-1}{k}(2^{\mathcal{R}}-1)^k 2^{\mathcal{R}(m_2-\ell-1)}e^{-\frac{m_2(2^{\mathcal{R}}-1)}{\overline{\gamma}_{2,f}}}, \\
A_3 &= \binom{m_1+m_2-2\ell-2}{k}(2^{\mathcal{R}}-1)^k 2^{\mathcal{R}(m_1+m_2-2\ell-2)}e^{-\left(\frac{m_1}{\overline{\gamma}_{1,f}}+\frac{m_2}{\overline{\gamma}_{2,f}}\right)(2^{\mathcal{R}}-1)}.
\end{aligned} \tag{C.12}$$