REPUBLIC OF IRAQ

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

AL-FURAT AL-AWSAT TECHNICA UNIVERSITY

ENGINEERING TECHNICAL COLLEGE- NAJAF

SECRECY PERFORMANCE ANALYSIS OF THE FSO LINK FOR THE COMMUNICATION SYSTEMS

RUWAIDA ABDUL AMEER ABDUL KAREEM

(B. Sc. In Communications Techniques Eng.)

2022

SECRECY PERFORMANCE ANALYSIS OF THE FSO LINK FOR THE COMMUNICATION SYSTEMS

A THESIS
SUBMITTED TO THE COMMUNICATION DEPARTMENT
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MSc

By

RUWAIDA ABDUL AMEER ABDUL KAREEM

Supervised by

Asst. Prof. Dr. Wafaa Mohammed Ridha Shakir

2022

Dedication

To whom I beg to God Almighty, the Prophet Mohammad and the good and pure family (blessings and peace of God be upon them all).

To the most precious human being in existence: To the one who played the roles of mother and father, and the roles of sister and friend, to the one who gave everything and never took anything for the soul of my dear, beloved grandmother.

To my husband and all my family members who stood by me and provided me with support and backing throughout my studies.

To all my colleagues and colleagues who did not skimp on any information or support throughout the study period despite their preoccupation and obligations.

Declaration

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

/ / 2022 Ruwaida Abdul Ameer Abdul Kareem

Supervisor Certification

I certify that this thesis entitled "**Secrecy Performance Analysis of the FSO Link for the Communication Systems**" which is submitted by **Ruwaida Abdul Ameer Abdul Kareem** was prepared under my supervision at the Communication Techniques Engineering Department, Engineering Technical College-Najaf, AL-Furat Al-Awsat Technical University, as partial fulfillment of the requirements for the degree of Master of Technical in Communication Engineering.

Signature:
Name: Asst. Prof. Dr. Wafaa Mohammed Ridha Shakir
Date: / / 2022

Given the available recommendation, I forward this thesis for debate by the examining committee.

Signature:

Name: Prof. Dr. Ahmad Taha Abdul Sadda

(Head of comm. Tech. Eng. Dept.)

Date: / / 2022

Committee Report

We certify that we have read this thesis entitled "**Secrecy Performance Analysis of the FSO Link for the Communication Systems** "which is being submitted by **Ruwaida Abdul Ameer Abdul Kareem** and as examining Committee, examined the student in its contents. In our opinion, the thesis is adequate to be awarded the degree of MSc.

Signature:
Name: Asst. Prof. Dr. Wafaa Mohammed Ridha Shakir
(Supervisor) Date: / / 2022

Signature:Dr. Nasr Alkhafaji
Name:
(Member)
Date: / / 2022

Signature: Prof. Dr. AhmedT. Abdulsadda
Name:
(Member)
Date: / / 2022

Signature: Prof. Dr. Sammir Jasim Mohammed
Name:
(Chairman)
Date: / / 2022

Approval of the Engineering Technical College-Najaf

Signature:
Name: Asst. Prof. Dr. Hassanain Ghani Hameed
Dean of Engineering Technical College-Najaf
Date: / / 2022

Linguistic Certification

This is to certify that this thesis entitled "**Secrecy Performance Analysis of the FSO Link for the Communication Systems** "was reviewed linguistically. Its language was amended to meet the style of the English language.

Signature:

Name:

Date: / / 2022

Abstract

The tremendous development in the fields of application of the fifth-generation (5G) and beyond communication services that require high data transfer rates has led to the use of an optical wireless communication technique known as the free-space optical FSO communication technique, which uses the free space as a transmission medium for information.

In this thesis, the secrecy performance of the free space optial (FSO) communication is analyzed in the presence of an eavesdropper located close to the legal receiver by presenting the closed-form expression for an accurate and comprehensive analysis of the secrecy performance metrics of the FSO communication system that uses intensity modulation /direct detection (IM/DD) technique: as Average secrecy capacity (ASC), secrecy outage probability (SOP), strictly positive secrecy capacity (SPSC), under different atmospheres turbulence conditions (weak to strong), zero boresight pointing errors and non-zero boresight pointing errors, and foggy weather conditions. To model the channel for all atmospheric turbulence conditions (weak, moderate, and strong), the generalized Malaga-M turbulence distribution for FSO communication links was used. The results indicate a deterioration of the secrecy performance with an increase in the severity of atmospheric turbulence and generalized pointing errors. The FSO communication achieved an ASC of 40 bit /s /Hz under weak turbulence in comparison with 10 bit /s/ Hz under moderate turbulence with low pointing errors of ψ = 6.7, and with the worst decrease in the performance of ASC reach to 2.5 bit/s/Hz under strong turbulence. The FSO communication gained about 21.2 dB when the turbulence shifted from moderate to weak under low pointing errors of ψ = 6.7 with SNR of wiretap channel of $\mu_{fso,E}$ = -10 dB and SOP of 10^{-5} , while the system gained 19.5 dB and 18 dB under the same condition with SNR of wiretap channel of $\mu_{fso,E}$ = 0 dB and 10 dB respectively. Under a low value of zero boresight pointing errors, the FSO communication achieves better performance in comparison with its high value. However, the effect of non-zero boresight pointing errors on the secrecy performance of the FSO communication is more deterioration than the effect of zero boresight pointing errors. In addition, the foggy weather conditions had a deeply negative impact

on the secrecy performance of the FSO communication. The increasing intensity of fog caused more reduction in the FSO communication secrecy performance.

Acknowledgments

Thanks and praise be to God. May he be exalted and glorified, who, thanks to him, his mercy, and his ability brought me to this stage of the study, through which I stood before prestigious academic and scholarly figures with pride and honor.

I extend my sincere thanks and gratitude to my supervisor, Dr. Wafaa Mohamed Ridha Shaker, who provided me with a helping hand and gave me enough knowledge, scientific, experience, and time to complete my letter in the required manner according to her continuous directives.

I also extend my thanks, appreciation, and respect to my university (Al- Furat Al-Awsat Technical University) and in particular to my college (Department of Communication Engineering, Engineering Technical College/Najaf) and all my dear professors.

TABLE OF CONTENTS

List of Tables

List of Figures

List of Abbreviations

Abbreviation	Description
AOD	Acousto-Optic Deflectors
ASC	Average secrecy capacity
AT	Atmospheric turbulence
AM	Amplitude Modulation
A	Alice
A.C	After Christ
AWGN	Additive White Gaussian Noise
BG	Bessel–Gaussian
B	Bob
B.C	Before Christ
CSI	Channel State Information
CV-QKD	Continuous-Variable-QKD
CDF	Cumulative Distribution Function
CAP-EX	Capital Expenditure
D	Destination
DFMT	Data Fragmentation Multipath Transmission
DES	Data Encryption Standard
DD	Direct Detection
E	Eavesdropper (Eve)

EGC	Equal Gain Combining
EGBMGF	Extended Generalized Bivariate Meijer G-Function
FSO	Free Space Optical
FM	Frequency Modulation
GG	Gamma-Gamma
GSM	Gaussian Schell-model
HD	heterodyne detection
HD	High Definition
IM	Intensity Modulation
IoT	Internet-of-things
IR	Infrared Radiation
IM/DD	Intensity Modulation/ Direct Detection
LED	Light Emitting Diode
LD	Laser Diode
LOS	Line-of-Sight
LN	Log-Normal
LG	Laguerre-Gaussian
MISO	Multiple-Input/Single-Output
NOMA	Non-Orthogonal Multiple Access
NLOS	Non- Line-of-Sight
OWC	Optical Wireless Communication
OOK	On-Off Keying

OLO	Optical Local Oscillator
OSI	Open Systems Interconnection
OAM	Orbital Angular Momentum
PDF	Probability Density Function
PD	Photo Detector
PM	Phase Modulation
PPM	Pulse Position Modulation
PLS	Physical Layer Security
PEs	Pointing Errors
QKD	Quantum Key Distribution
RF	Radio Frequency
SNR	Signal-to-Noise Ratio
S	Source
SKR	Secret Key Rates
SISO	Single Input-Single Output
SPSC	Strictly Positive Secrecy Capacity
SOP	Secrecy Outage Probability
TV	Television
Tbps	Terabyte per second
UV	Ultraviolet
VLC	Visible Light Communication
5G	Fifth Generation

List of Symbols

Symbol	Definition
μ_x	Zero Mean
h_{cs}	Received Irradiance
σ_x^2	Standard Deviation
$\Gamma(.)$	Gamma Function
$k_{a-m}(\cdot)$	Bessel Function of the Second Kind
$\mathcal{Y}$	Received Electrical Signal
η_{eff}	Efficiency Responsivity of the Photodetector
$\mathcal{X}$	Transmitted Optical Signal
h_{at}	Atmosphere Turbulence
h_{pe}	Pointing Errors
h_{fo}	Attenuation to the Foggy Weather
N	Additive White Gaussian Noise
α_{foggy}	Attenuation Coefficient
L	Link Length
λ	Wavelength
q	Related to the Particle Size Distribution
Tsr	Target Secrecy Rate
P	Probability
ζ	Non-Zero Boresight Pointing Errors
ρ	Scattering Power
Vis	Visibility
α	large-scale cells
β	Natural Number
$\boldsymbol{r}_b$	pointing errors vector
$w_{L,e(eq)}^2$	Equivalent Beam Width
r_b	Radial Distance

A_O	fraction of the collected power
erf (.)	Errors Function
$w_{L,e}$	Waist of the Beam's Gaussian
θ	Divergence Angle
$\sigma^2_{mod,pe}$	Estimated Jitter Variance
$G^{m,n}_{p,q}[\cdot]$	Meijer G -Function
$\gamma_{fso,g}$	Instantaneous SNR
$\mu_{fso,g}$	Average SNR
C_s	Secrecy Capacity Rate
W	Bandwidth
SOP_L	lower bound of the SOP
ψ	Zero Boresight pointing errors
dB	Decibel

CHAPTER ONE

INTRODUCTION

1.1 Background

The need for bandwidth to support wideband wireless services like mobile video phones, video conferencing, and high-speed internet access has extremely increased recently. Because of the widespread use of smart devices and the quick emergence of the fifth-generation (5G) and internet-of-things (IoT) applications, the need for adequate bandwidth is rapidly growing. Data transmission multimedia and a variety of radiofrequency (RF) technology-based wireless communication applications are among the technologies that can satisfy end-users communications demands in access networks. But due to RF spectrum limited capacity, highly regulated and congested spectrum, and limited accessibility to all, (RF) communication technologies will be unable to meet future demands as the worldwide need for bandwidth rises. Furthermore, these technologies are costly to license, have security vulnerabilities, and need a significant upfront investment. To increase the bandwidth available to their customers, network operators in several countries have built new optical fiber-based access networks. Although it is a popular misconception that optical fiber-based networks give infinite bandwidth, the architectural alternatives available, device and component compatibility, networking equipment performance restrictions, and system implementation all result in restricted capacity being supplied to end-users [1].

The spread of wireless communications is one of the most significant technological developments in history. Wireless technology has spread far faster than could have been predicted. As a result of the widespread deployment and usage of wireless RF devices and systems, the term "wireless" is now nearly synonymous with RF technology. With the increasing popularity of data-high wireless communications, demand for RF spectrum is outpacing supply. As a result, optical wireless communication (OWC) has emerged as a promising future alternative or supplement to existing RF networks for meeting expected traffic demand.

OWC stands for optical carrier transmission in unguided propagation mediums in the visible, infrared (IR), and ultraviolet (UV) spectral ranges. According to [2], depending on the transmission range, OWC systems can be categorized. In this way, different technologies can be studied such as (i) chip-to-chip communication for Ultra-short-range (ii) wireless personal area networks (WPANs) for Short-range, (iii) visible light communication (VLC) for wireless local area networks (WLANs), or indoor IR for Medium-range, (iv) FSO communication for Long-range, (v) deep space missions or inter-satellite links or ground-to-satellite/satellite-to-ground or inter-satellite link for Ultra-long-range, among others. The focus of this thesis is on terrestrial OWC links, often known as FSO links in the research and photonics community. Current terrestrial FSO links operate in the near-infrared (IR) wavelengths, i.e., at wavelengths of 850 nm to 1600 nm, which the wavelengths 850 and 1550 nm correspond to optical transmission windows, for wavelengths private 850, 1060, 1250, and 1550 nm, be attenuation of less than 0.2 dB/km [2].

The use of the optical band of the electromagnetic spectrum for wireless communication offers up new possibilities in areas that have hitherto been mostly untapped. Optical frequencies extend from 300 (GHz) to 300 petahertz (PHz), including infrared, visible, and ultraviolet bands a spectral range that dwarfs the RF band's 300 GHz. OWC systems have several technological and operational benefits, including greater bandwidth capacity, immunity to electromagnetic interference, inherent security, minimal power needs, and unrestricted spectrum. OWC may be used in a wide range of communication applications, from extremely short-range optical interconnects within integrated circuits (on the scale of millimeters) to outdoor inter-building linkages (on the order of kilometers) then to satellite communications (larger than 10,000 km) [3].

1.2 FSO Communication Systems

The FSO communication system is a communication system that uses a laser diode (LD) to transmit data through the free space. The FSO communication system is a promising technology to solve the expected increase in data transmission rates of the advanced generations, where the current RF system is not able to achieve. The FSO

communications have many advantages, i.e., unlicensed spectrum, high directivity, high data rate, and low cost [2]. Another distinguishing aspect of the FSO system is that transmission is only possible when the LOS component is present. In other words, if the LOS component is missing, the channel suffers from great deterioration [4].

FSO systems include some attractive applications such as satellite communications, inter-building connectivity, wireless video monitoring, backhaul for cellular networks, high-capacity backhaul network, broadcasting and disaster observation, last-mile problem solution, IoT , 5G, and security [5].

Despite its numerous benefits, the performance of FSO systems is impacted by unanticipated atmospheric conditions, which presents a significant challenge for FSO system decorators. In addition to the atmosphere turbulence impact. A misalignment between the transmitter and the legal receiver can cause pointing errors and increased the FSO system performance degradation. A mechanical error in the tracking system or mechanical vibrations in the system owing to winds or/and building movement [6], cause the misalignment. Thus, the displacement of the laser beam along with vertical (altitude) and horizontal (azimuth) directions, which are generally believed to be separate Gaussian random variables, causes pointing errors. The boresight and the jitter are the two major components of pointing errors [7]. To capture the effect of these drawbacks on the performance of the FSO systems, combined statistics of turbulence and pointing errors are essential. Significant attempts were reported in the literature for Gamma-Gamma (GG) distribution model in [8], the Log-Normal (LN) distribution model in [9], and the Rice-Nakagami distribution model in [10], all of which are considered special cases of the Malaga-M distribution model in [11]. Finding the combined effect of pointing errors, atmospheric turbulence, and weather conditions become a harder task when considering the general models of each.

1.3 Security Issues and Threats in FSO Communication Systems

FSO communication systems are considered to be inherently more secure than radio-frequency (RF) networks [12 – 15], owing to the high directivity of the optical beam transmitted from the laser source as previously mentioned. The eavesdropper's mission

of intercepting FSO communications becomes more difficult, yet not impossible. Because of a very narrow beam with a small divergence angle of 0.001 radians, the divergence region of the laser beam will be 1 m for the 1 km distance between the two legal peers [16]. In addition, the different channel conditions represent the factors affecting the optical signal transmitted through free space, which provides a chance for eavesdropping to obtain a version of the transmitted information. Thus, an eavesdropper can be defined as an unauthorized user who attempts to obtain confidential information that is sent to an authorized user [4].

Physical layer security (PLS) has emerged as a viable strategy for reducing the amount of information obtained by eavesdroppers through exploiting the randomization of noise, channel state information (CSI), and other resources (such as multi-antenna and cooperative nodes) [17, 18]. Typically, the physical layer of wireless networks is intended to enable reliable communication to authorized destinations, whereas the upper layers of wireless networks are used to protect and secure the communication data [19]. Wyner [20] proposed the secrecy capacity metric to evaluate system secrecy performance, and it was defined as the highest information rate that can be obtained at the legal destination while keeping the eavesdropper in the unaware.

The following are the advantages of using physical layer security approaches for FSO networks over cryptography approaches: physical layer security approaches do not rely on computing complexity. Unlike traditional encryption systems in the upper layers, no secret key is required in physical layer security, which makes use of the characteristics of fading channels to provide perfect secrecy [17]. Therefore, even if eavesdroppers (unauthorized smart devices) in FSO networks have strong computing equipment, secure and reliable communications may still be obtained. The security of computation-based encryption systems, on the other hand, will be compromised if the eavesdroppers' equipment has sufficient processing capacity to solve difficult mathematical problems. For all these motives, physical layer security in FSO systems is currently regarded as an open, challenging area by the research community.

The possible security threats scenarios for the FSO systems are illustrated in Figure 1.1 The legal transmitter or the source S (also known as Alice) wishes to send

confidential information to the legal receiver or destination D (also known as Bob) over the main channel (the FSO link between Alice and Bob). The illegal receiver or eavesdropper E (also known as Eve) attempts to intercept the information received signal by the eavesdropper channel (the FSO link between Alice and Eve). Depending on the position of the eavesdropper, the PLS analysis for FSO communications may be divided into three cases:

- **Case P1:** The illegal receiver (Eve) is close to the legal receiver (Bob).
  This is the most probable case for eavesdropping in FSO systems because the legal receiver acts as a point of reference for the eavesdropper in determining its direction and also because of the optical diffractions that cause the laser beam to diverge, locating Eve in the divergence region of the laser beam, it is considered one option for successful eavesdropping. On the one hand, the received irradiances at the legal receiver and illegal receiver will be affected by random fluctuations induced by turbulence both on eddies small-scale and large-scale [16, 21, 22].

- **Case P2:** The illegal receiver (Eve) is close to the legal transmitter (Alice).
  Confidential information sent through the atmosphere channel cannot be intercepted without partially blocking the LOS between the legal transmitter and receiver, so a sufficiently sophisticated device must be available to be able to pick up a small part of the laser beam towards Eve. Because of the short distance between Eve and Alice and the narrowness of the laser beam at Alice, the attenuation can be ignored in this case [12, 16].

- **Case P3:** Eavesdropper is not close to the legal transmitter and receiver.
  The Eve is not close to Alice or Bob, precisely aligning its location so that it may receive the irradiance from the laser beam towards the legal receiver is almost impossible, yet it is still feasible with the help of a drone [16].

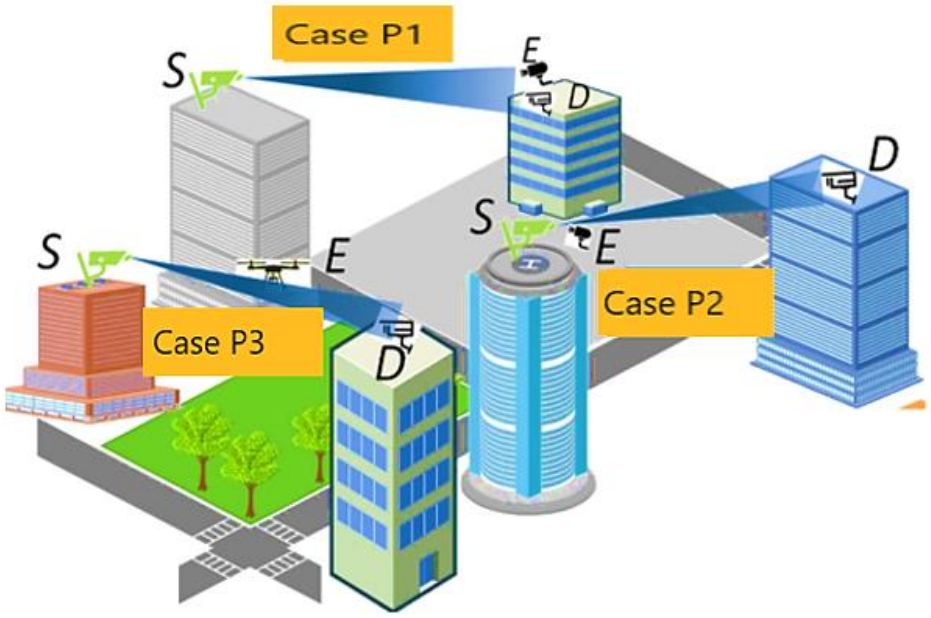

Figure 1.1. Security Threats in FSO Systems[16].

Unlike its RF counterparts, the PLS for FSO systems is not yet mature since its eavesdropping scenarios, which may be divided into active and passive eavesdropping, are still being debated. Eve might actively send jamming optical signals to Bob to make his receiver crowded with undesirable noises during active eavesdropping [23]. In the passive eavesdropping case, Eve is assumed to be passively intercepting the main channel near Alice's transmitter [12], in the middle of the communication link [13], and near Bob's receiver [12, 14, 24, 25]. This can also be expanded to mixed RF-FSO relaying networks where Eve is located near the Bob receiver in the FSO link [26, 27]. In practice, since the optical beam-width in FSO systems is very narrow and invisible, it is greatly challenging for Eve to intercept in the middle of the link. Therefore, it is practically reasonable to restrict Eve’s physical ability to tap the FSO channel, hence modeling it as an FSO-wiretap channel [28].

Specifically, Eve is assumed to be a fully passive eavesdropper situated somewhere on Bob’s reception plane or further behind and attempting to tap the side lobs of the diverging optical beams [28, 29]. This FSO wiretap channel model has been also applied for free-space quantum key distribution (QKD) systems in the pursuit of higher secret-key rates (SKRs) [104, 30]. It is worth while to mention that in the PLS evaluation, Eves and Bobs' channels are typically assumed to be independent of each other (i.e., both channels are separated at least half wavelength). Furthermore, the links

(i.e., Alice-to-Bob and Alice-to-Eve) that do not meet the aforementioned condition (i.e., correlated channels) are investigated in [12, 16].

1.4 Related and Previous Works

Increasing the security reliability of the FSO systems, while still exploiting their high data rate communications in wide unlicensed bandwidths, is a key requirement in the deployment of FSO-based systems. There are very few security techniques have been applied to mitigate the effects of channel impairments and adverse weather conditions to improve the security performance of the FSO communication systems. As a comparison of this work, it is clear from the papers [14, 41], the effect of generalized boresight pointing errors and foggy weather conditions have not been fully considered when evaluating the PLS of secrecy performance metrics analysis FSO communication system. In this section, some relevant work developed will be mentioned and discussed as in table 1.1 show.

Table 1.1 Summary of current research trends on PLS techniques in FSO systems.

System type and year	No of reference	The focus of the work	Contribution and research direction	Channel condition	Metrics
SISO-FSO 2014	[22]	Enhancing the data security in a terrestrial FSO system using an AOD with gratings of synthetic holographic	Formulating a transmissions beam setting by varying AOD's parameters is, which causes Gaussian beam changes to the secondary Gaussian Schell-model (GSM) beam with different parameters. The beam's radius and the intensity of the received beam at different beam paths affect directly the	Various AT	The intensity distribution of the secondary GSM beam at the transmitter.

			security of an FSO link.		
2015	[12]	Evaluating the FSO link security in presence of the eavesdropper.	This paper studies the mechanisms of eavesdropping based on the eavesdropper location and the effect of joint laser-beam divergence and random optical irradiance fluctuations on the probability of achieving a secure transmission.	Various AT	SPSC
2016	[25]	Emulating a typical scenario of PLS security of the real-field FSO link.	Tokyo FSO Testbed is used to gather the experimental data for various atmospheric conditions which meet real-life FSO links. Moreover, the real conditions influence on the instantaneous secrecy rate and the code lengths is analyzed.	Various AT	Secrecy rate, SOP, the code lengths
2016	[31]	Impact of eavesdropper's presence outside the transmit laser beam on a terrestrial FSO link security performance.	Formulating the security metrics considering the visibility of the link and different positions of eavesdropper taking into account two-dimensional space around the laser beam.	Various AT	ASC, SOP
2016	[32]	Secure communication over FSO links suffering from turbulence-induced fading.	The ASC of applying PLS to achieve security in an FSO link with binary-level OOK intensity modulation and	Various AT	ASC

			threshold detection based on a simple design principle for practical applications and yields a simpler ASC equation is derived. In conducting a special case of the correlated log-normal fading model, the authors analyze the impacts of fading and channel correlation on the system's ASC performance.		
2018	[33]	Secure FSO communications based on Bessel-Gaussian orbital angular momentum-carrying beams against eavesdropper's optical beam-splitting attacks over an atmospheric channel.	This paper provides a proved of the superiority of Bessel-Gaussian beams over the Laguerre-Gaussian beams in resilience to AT effects based on ASC comparison results of using computer simulations and experiments with spatial light modulators.	weak to medium AT	ASC
2018	[34]	Creating an experiment to emulate an optical wiretap channel to extend Wyner’s wiretap channel model to the FSO channels.	Obtain a positive secrecy capacity even when Alice and Bob do not use a shared key for communications over noisy and degraded channel conditions.	Various AT	ASC
2018	[35]	Enhancing the security of FSO link based on data fragmentation multipath transmission (DFMT) scheme to benefit from that	A field experiment of the FSO link between two buildings has been undertaken to experimentally prove the	In Lab AT	Intercept possibility

		incomplete data transmitted through the single atmospheric channel.	feasibility of the DFMT scheme.		
2018	[36]	Analyzing the ASC over GG AT affected by non-zero boresight PEs.	To reduce the losses produced by attacks, the greater normalized beam width is required in the high Signal-to-noise ratio (SNR).	AT with PE	ASC
2019	[37]	Proposing a misalignment errors model to consider a non-orthogonal optical beam concerning the photodetector plane at the eavesdroppers.	A two-axis pointing errors effect is modeled and the effect of such types of errors is investigated on the security performance of the FSO link.	AT with PE	SOP, SPSC
2019	[38]	Develop a novel model for the analysis of the SOP and SPSC in FSO systems over GG fading channels with nonzero boresight pointing errors.	Including the eavesdropper's location in the pointing errors model corresponding to the wiretap channel model is a step forward in PLS for FSO communication.	AT with PE	SOP, SPSC
2020	[39]	A new framework has been created to secrecy performance analysis of the FSO terrestrial links under different atmospheric channel conditions and impact of the eavesdropping location.	By PDF applied, all combined effects of the AT, transceiver misalignments, receiver noises, and the eavesdropper's location have been analyzed, for the PLS and IM/DD free-space continuous-variable-QKD (CV-QKD) systems.	AT with PE	SOP

2020	[40]	Enhancing the ASC in FSO links via MISO systems.	Employment spatial diversity techniques at the transmitter to mitigate the fading effects in FSO channels.	Generalized misalignment and AT	ASC
2020	[16]	Study the PLS of FSO communication under different eavesdropping scenarios.	Comprehensively analyze the secrecy performance of FSO communication under different realistic scenarios based on the positions of the eavesdropper, a evaluate impact of correlation on the secrecy performance metrics such as ASC and SOP for FSO communication.	Various AT	ASC,SOP

It is noteworthy that, in the context of the FSO system, there has been no such research that has addressed the generalized security performance of such a system to date. To the best of our knowledge, no research has been conducted on the generalized security performance of the FSO systems from the perspective of secrecy performance analysis. Motivated by the preceding discussion, We investigate the impact of secrecy performance of the FSO systems under the generalized atmospheric turbulence/pointing errors, power received by Eve, FSO link length, and weather conditions considering ASC,SOP, and SPSC secrecy performance metrics.

1.5 Applications of FSO Communication Systems

FSO communication systems have a wide range of applications, from short-range communications under 1 km to long-range and space communications. It connects end-users to the backbone by providing a broadband solution (high data speeds without cabling). In urban locations where burying cables is problematic, the short-range

application provides last-mile access by linking multiple towers, buildings, and other structures. When underground optical fiber communication is too expensive or impossible to implement, FSO systems can be a viable option. The following are a few of the more interesting applications of FSO systems [5, 56].

1- Inter-building (e.g.,universities, apartment complexes, and institutions) connectivity.
2- Observation using video.
3- Broadcasting and catastrophe observation.
4- IoT and 5G.
5- Satellite communications.

1.6 Problem Statement

In 5G technology, communication systems need ultra-high bandwidth, on another hand, wireless communications need to be highly secure. Consequently, using the high data rate FSO systems becomes essential. Although FSO communication is more secure than the broadcasting nature of RF communication due to the highly directional optical beam, the FSO is extremely susceptible to atmospheric challenges. Thus, general security analysis of the FSO communication systems suffers from many problems such as the presence of eavesdroppers, atmospheric turbulence, pointing errors, and weather conditions. This work aims to analyze the secrecy performance of an FSO system from a physical layer security point of view. Indeed, regardless of many FSO investigations in the performance analysis field, general physical layer security setups (e.g., generalized atmospheric turbulence, pointing errors, weather conditions, power received by an eavesdropper, and the FSO link's distance) have not been fully examined yet in the literature due to the analytical approaches' complexities.

1.7 Thesis Objectives

The main objectives of this thesis are two-folded:

- To fill the existent gap in the literature concerning the secrecy performance analysis of the FSO system, by investigating the secrecy performance of the system under the different channel and system conditions (e.g., atmospheric turbulence/generalized pointing error, weather conditions, power received by Eve, FSO link length) with the presence of an eavesdropper.

- Our other key objective in this thesis is the derivation of analytical closed-form expressions of the secrecy performance analysis of the FSO system over the Malaga-M turbulence channel. Several performance metrics including the SOP, ASC, and SPSC will be investigated.

1.8 Thesis Motivation

Despite the FSO system's considerable potential as an excellent candidate for future network backhaul and a variety of other applications, the secrecy performance of the FSO systems has not been widely examined in the open literature, considering all of the system and channel conditions. In contrast to earlier secrecy performance study efforts on comparable systems [14, 16], we analyzed the generalized secrecy performance of the FSO system under the difference of most of the system and channel parameters, considering the Malaga-M distribution model to describe atmospheric turbulence. The channel model would make it easy to track how different systems and channel parameters affect these systems' security performance. To the best of our knowledge, no comprehensive examination of overall security performance for FSO systems from the standpoint of PLS technology has been conducted.

1.9 Research Contribution

The main contributions of this thesis are cleared in the following points:

1- We first evaluate both the probability density function (PDF) and cumulative distribution function (CDF) of the FSO system using the IM/DD detection technique with the Malaga-M distributions. The major impairments and features of the FSO links are taken into account to make this study more realistic (e.g., atmospheric turbulence, foggy weather, the power received by eavesdropper terminal, distance of the FSO link, and the generalized pointing errors for the FSO links).

2- The exact analytical expressions of the ASC, SOP, and SPSC for the FSO system are obtained in presence of a single eavesdropper.

3- These expressions are used to generate numerical results with specified figures.

1.10 Thesis Organization

Chapter 2: This chapter provides a comprehensive overview of the free-space optical communication system and then presents the basic structure of the considered system. Moreover, it presents the distribution models adopted in the literature, and atmosphere channel losses Finally, the FSO system applications provide in addition to the physical layer security technology for wireless communication.

Chapter 3: This chapter provides an accurate analysis of the secrecy performance metrics of the FSO communication system.

Chapter 4: This chapter presents simulation results of the FSO system by implementing the system in the MATLAB program, and their discussion.

Chapter 5: This chapter presents conclusions of the thesis and proposed future works

CHAPTER TWO

FREE SPACE OPTICAL COMMUNICATION SYSTEM

2.1 Introduction and History of the FSO Communication Systems

FSO communication also called optical wireless communication or laser com (i.e. laser communications), is a resurgent technology that uses modulated optical beams to transmit data over short, medium, and long distances. The majority of emphasis on FSO communication systems was first boosted by military goals, and the technology's earliest development was devoted to solving challenges linked to defense applications. Specifically, because of the 300 THz high carrier frequency thus high bandwidth, the major notable benefits of FSO links communication systems may be their [42].

i. The ability to deliver extremely high data speeds of several gigabits per second (up to 40 gigabits per second in the future).
ii. Immunity.
   - Electromagnetic interference.
   - Jamming.
   - Eavesdropping.

And others, make FSO attractive for applications such as airborne, and satellite communication, also employ of solving the last mile problem [43].

The unique benefit FSO is the only wireless technology that can provide a bandwidth of up to several gigabits per second. The low initial capital expenditure (CAP-EX) requirement, the inherent high-level data protection, and security, as well as the system's remarkable flexibility and great scalability, are factors that prompted the interest in this technology. As a result, FSO's prospective applications now cover a broad range [44].

With all of the benefits of the FSO communication technology mentioned, it also comes with its own set of problems, including [45].

i. Geometric loss.
ii. Ambient light.
iii. Sources disruption.
iv. Misalignment.
v. Severe atmospheric conditions,
vi. Different weather conditions

Although FSO communication is traditionally regarded as an information secure technology, it suffers from security risks [12]. The security problem has to be studied due to the huge application potential of FSO communications. When an eavesdropper is within the laser beam as the intended receiver, for example, the eavesdropper intentionally blocks the beam to cut the intended receiver's (LOS). Or when the diverging optical laser beams footprint is large enough at the receiving end to encompass both the intended receiver and the eavesdropper [24]. Also, when the eavesdropper is outside the transmitted laser beam, it may detectable optical signals through a non-line-of-sight (NLOS) scattering channel created by atmospheric particles in the medium [31].

Physical layer security, which protects data secrecy via information-theoretic methods has recently attracted a lot of academic attention. The basic concept of the physical layer security relies on the transmission channel's inherent randomness to secure communication [46].

The history of the world of communication goes back to the fourth century B.C. Where it appeared reports by Enea il Tattico, of the hydraulic telegraph that may have been invented by the Carthaginians. During the Roman and Greek eras, "fire towers" were erected in strategic locations to be activated in the event of security breaches or border incursions, was extremely prevalent in the sixteenth and seventeenth centuries A.C. in the center-south of Italy, in particular [47].

Claude Chappe was the first to employ mechanical methods to build optical wireless networks in 1792 [49]. Chappe invents the "optical telegraph" in France. Although Bell's Photophone was not ever It was a commercial success, it demonstrated the fundamentals of optical communications. Thus, starting from this point, the

importance of wireless optical communications has increased with time, which enhances research all over the world.

The wireless optical experiments may categorize into three main groups based on their time duration: (i) laser concepts arise in the 1960s, bringing with them the concept of wireless communications, (ii) ground-to-satellite and satellite-to-ground laser communications in the 1990s, still employing red and green sources, become prominent, (iii) Free Space Optical technologies the boom after the year 2000 has resulted in civil and military applications ranging from standard telecommunications to inter-satellite and inter-planets studies, with wavelengths ranging from 1 to 10 microns. As a result, practically every aspect of today's FSO communications systems has been studied in recent years, initially for defense considerations and then for civil purposes. By overcoming the major engineering difficulties of FSO, this aerospace/defense operation laid a firm foundation for today's commercial FSO systems [44].

2.2 Structure of the FSO Communication Systems

As mentioned earlier in this thesis, the FSO communication system works correctly only with the presence of a line-of-sight FSO between the transmitter and the legal receiver to transmit the optical signal from one point to another through the free space. The FSO wireless optical communication technology like any classic communication technology, consists of three main stages such as transmitter stage, channel stage, and receiver stage, where each stage where performs its work sequentially to complete the communication process correctly and as shown in Figure 2.1.

Since the environment of the FSO system proposed is outdoors, it is preferred to use the LD due to the LOS transmission needs, larger transmission span, and higher data speeds in an outdoor environment. In addition, other components such as lenses and equipment are included in the transmitter as well. In beamforming and collimation of the laser output, positioning the LD at the focal length of a lens is a popular procedure [50]. The created optical beam is transmitted into the receiver.

The FSO links that depend on using (IM/DD) detection technology are better suited to more cost-effective modular systems [2, 51-54]. In the IM/DD technique, which is based on information data, only the intensity of the light is modulated. Whereas external modulation and coherence detection are methods of modulating and detecting light in which both the intensity and phase/frequency of the light can be altered, counter unlike IM/DD [55]. They are less popular than IM/DD which depends on systems because of the cost and complexity of practical implementation, particularly the stability and synchronization of laser sources at the transmitter and receiver [2].

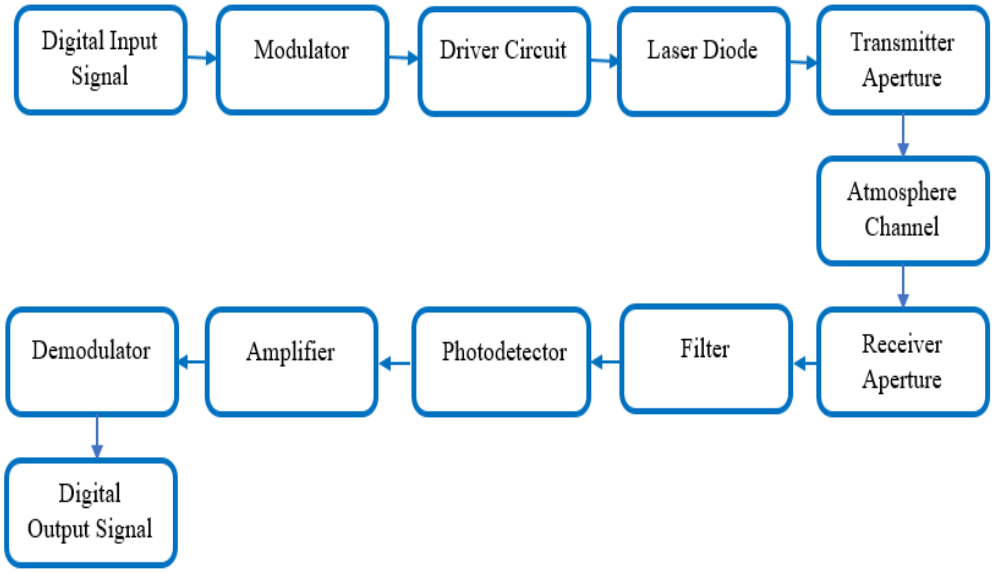

Figure 2.1. The general block diagram of the FSO communication systems.

2.2.1 Transmission Stage

In particular, as illustrated in Figure 2.1. The transmission stage of the FSO system includes a set of units necessary to complete the process of sending the optical signal to the intended destination through the atmosphere channel. The size, power, and beam quality are key aspects of the free-space optical transmitter system because they determine laser intensity and the lowest divergence available through the system.

i. **Modulator unit:** The modulator aid in the conversion of low-frequency information streams onto high-frequency optical carriers for long-distance communication [56].

To modulate the input information signal or the digital signal [0,1]on the electromagnetic wave carrier, amplitude modulation (AM), frequency modulation (FM), or phase modulation are utilized (PM). Another mostly used modulation method for the optical carrier is intensity modulation (IM). The flow energy per unit area per unit time stated in (W/m^2) is defined as the intensity, which is proportional to the square of the field's amplitude. The light fields from laser sources produce a collimated beam after traveling through beam-forming lenses. This process is similar to creating antenna gain in RF systems [57].

The on-off key (OOK) is the most often used modulation technique in IM/DD of the FSO systems, due to its efficient bandwidth usage and resistance to timing errors, despite its lower power efficiency than PPM. As shown in Figure 2.2 the schematic block diagram of the ideal maximum likelihood (ML) (i.e., a matched filter) based receiver for OOK. The digital input bits are sent to a transmitter filter has a unit-amplitude rectangular impulse response $P(t)$, with a duration of one-bit T_b. The following scaling through the peak detected signal photocurrent $2P_r$, as well as the inclusion of the photodetector responsivity R and the noise $n(t)$ of the regenerated electrical signal (t) , the regenerated electrical signal $i(t)$ is passed through a continuous-time filter with an impulse response $r(t)$ that is matched to $P(t)$. The output of $r(t)$ is sampled followed by a threshold detector in order to regenerate the estimated version of the digital transmitted data (e.g $\hat{a_i} \approx a_i$). Note that here sampling is at a rate of $1/T_b$ and is taken just before the peak of the integrator (i.e., matched filter output), and the threshold detector is set midway between expected 1 and 0 levels. [1].

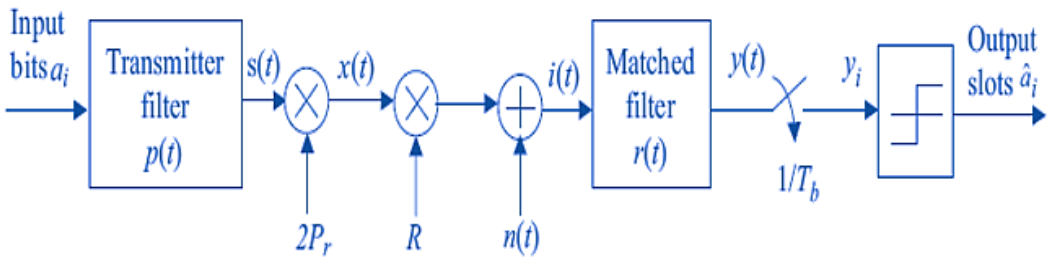

Figure 2.2. The block diagram of OOK modulation [1].

ii. **Driver Circuit unit :** The deiver circuit receives the modulator signal and performs the process of stabilizing the optical radiation against temperature changes[56].

iii. **Laser Diode Sourse:** The entire commercial FSO industry is focused on using semiconductor lasers because of their relatively small size, high power, and cost-efficiency. In addition, because the laser beam has a wavelength in the micrometer range, and not in the traditional electro -magnetic radio spectrum (meter - millimeter), there is no need for FCC or municipal license approvals. As a consequence, FSO links and FSO networks can be set up and be deployed rapidly, in a matter of few days as compared with years for a new fiber network. Thus, laser diode send optical signal to the transmitter aperture (transmitter lenses) [56, 86].

iv. **Transmitter aperture (transmitter lenses) :** The transmitter lenses collimates, and directs the optical radiations toward the receiver via the atmospheric channel [56].

2.2.2 Atmosphere Channel Stage

The atmosphere channel stage is considered the biggest challenge for FSO communication systems and includes several environmental factors .These factors do not have fixed characteristics and cause attenuation and deterioration of the received signal.

i. **Atmosphere Turbulence**: The atmospheric channel is the optical radiation propagation medium for the FSO system. Because of different atmospheric conditions, the received optical signal will be affected. As a result, it will deteriorate and get lost significantly. These conditions include different atmospheric turbulence conditions (weak to strong severity) where the laser beam is largely attenuated as a result of absorption and scattering by the atmosphere's component gases and particles.

So, atmospheric turbulence is the most significant factor affecting the performance of the FSO communication system negatively [58]. Atmospheric turbulence occurs due to the radiant solar energy received by the earth's surface, leading to a higher temperature of the air layer close to the earth's surface compared to the air layer relatively far from the earth's surface. The layer of air close to the surface of the earth with high temperature and reduced density rises to blend with the layered air of reduced temperature in a turbulent form, resulting in random fluctuations in temperature. Random fluctuations in temperature result in fluctuations in the air refractive index, fluctuations in the refractive index cause the beam to be refracted at different angles and result propagation of the optical beam occurs [59], as shown in Figure 2.3. Thus, the inhomogeneity of the medium leads to the formation of randomly distributed cells or eddies in the diffusion medium of different sizes, temperatures, and various refractive indexes. This difference in size results in negative effects, such as [60]:

1- The beam wanders effect occurs when the size of the atmospheric turbulence cell is greater than the width of the optical beam.

2- The scintillation effect occurs when the size of the atmospheric turbulence cell is smaller than the width of the optical beam.

The interaction of the laser beam with the turbulent route causes random phase and amplitude changes in the received signal referred to as fading, which causes intensity fluctuations resulting in FSO communication system performance degradation

[61]. In the following there are some of the known impacts of atmospheric turbulence on the receiver signal [62]:

- **Beam scintillation:** At the receiver plane, there are variations in the spatial power density. When compared to the high data rates of FSO transmission, the scintillation process is slow.

- **Beam spread:** Scattering causes increased beam divergence, which lowers the received power density.

- **Spatial coherence degradation:** Turbulence causes coherence losses across the beam phase foreheads; deterioration can be detrimental for photo-mixing as an incoherent receiver.

- **Beam steering:** The beam's angular departure from its main line of sight causes the optical beam to miss the receiver.

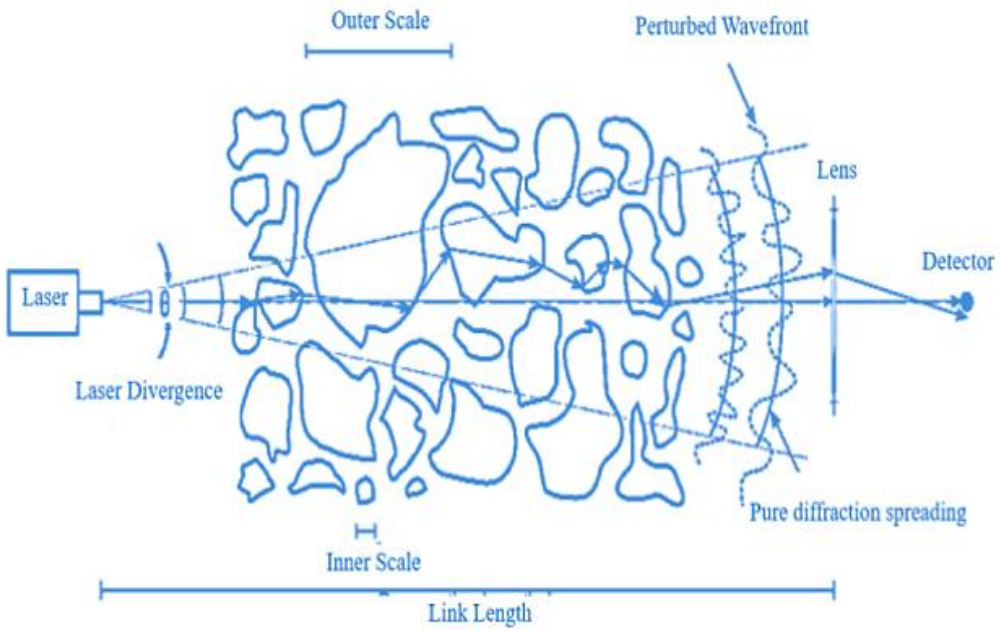

Figure 2.3. The effect of the atmospheric turbulence channel on the performance of the FSO communication system [63].

ii. **Pointing Errors:** Ideally, on the receiver side, an optical signal should be received without losses, but due to the occurrence of a phenomenon resulting from several diverse effects such as vibration, and movement of buildings installed on which the FSO components. In addition to the effect of the dispersal of the optical beam as a result of its spread through the atmosphere over long distances [64]. This phenomenon is called pointing errors or misalignment between the transmitter and legal receiver of the FSO system.

Consequently, losses and deterioration in FSO link performance occur as the receiving power decreases when the transmitted optical beam width is greater than the diameter of the receiver aperture. In addition, the pointing errors cause fluctuations in the amplitude of the receiving optical signal, which makes the detection process complicated [6]. Figure 2.4 shows the generally negative impact of pointing errors on the performance of the FSO system.

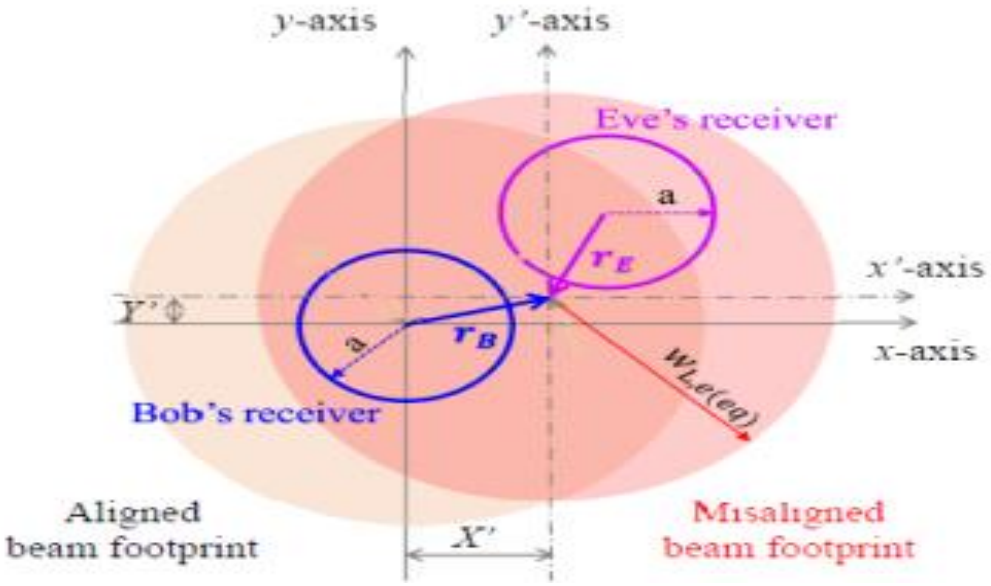

Figure 2.4. The effect of the components of pointing errors on FSO link performance [39].

iii. **Weather Conditions:** Different weather conditions such as (fog, rain, dust, and smoke) are a major reason for the attenuation of the optical beam propagating through the atmosphere. They have considered the phenomenon of absorption

of light energy by gas molecules suspended in the atmosphere and a phenomenon of directional redistribution of light energy known as scattering, contribution to atmospheric attenuation [65, 66].

Fundamentally, the visibility near the ground is reduced by fog molecules. Fog is defined by meteorologists as a reduction in visibility below 1 km. Varied forms of fog produce different amounts of optical losses, which are primarily determined by the distribution size, and position of fog molecules. Convection fog and marine/advection fog are two separate forms of fog described in the literature. Radiation or convection fog is produced when the earth cools due to radiation. In Figure 2.5 when the air becomes sufficiently cold and saturated, this fog emerges. Convection fog is most common at night and near the end of the day, with a particle size distribution of (1-3) μm and a liquid water concentration of (0.01-0.1) g/m^3. It mostly affects shorter wavelengths (first and second transmission windows), with the 10 μm transmission window scarcely impacted. This type of fog typically has a visibility range of 500 m [1].

The flow of moist and warm air masses above cooler marine or terrestrial surfaces causes advection fog. It has a liquid water concentration of more than (0.20) g/m^3 and a particle diameter close to 20 μm. For advection fog, a common visibility setting is 200 m [67]. Thus, for the two kinds of fog, any visibility setting between (0 - 1) km is acceptable [68-71].

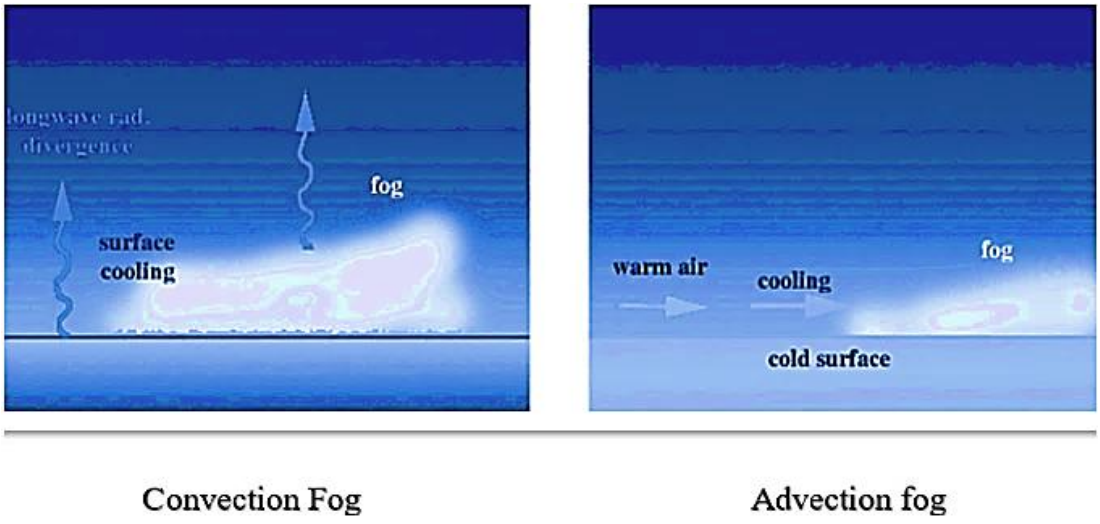

Figure 2.5. Illustration of the two types of fog formation (Data from Robert Tardif (2011)) [1].

In this thesis, we will focus on the largest atmospheric attenuation caused by the effect of fog particles in the air. We will also consider haze and different levels of fog (light fog, moderate fog, and heavy fog). Fog is the greater dominant factor in FSO communication systems.

The reason is that the fog particle size same as the wavelength of the FSO systems. FSO has a wavelength range of (780–1600) nm and can transmit data at speeds of up to 2.5 Gbps [72]. Thus, the scattering caused by the fog is known as Mie scattering. Therefore, the fog attenuation values can be predicted through the application of the Mie scattering theory, but this requires obtaining accurate information about the fog in addition to more complex calculations. The alternative approach depends on the visibility information that can be obtained from the meteorological over FSO link distances.

2.2.3 Receiver Stage

For the FSO receiver stage, the major goal is to retrieve data transmitted from incident optical radiation. The receiver stage consists of several components such as aperture receiver, optical filter, photodetector, amplifier, and demodulator [56].

i. **Receiver Aperture (Receiver Lens):** Using the receiver aperture incoming optical beam radiation is collected and focused onto the photodetector are gathered.

ii. **Optical Filter :** The optical filter reduces the level of background radiation and directs the signal on the photodetector and allows passing only the wavelength of the signal and blocks other radiations from the atmosphere [48].

iii. **Photodetector:** The Photodetector which turns the optical signal into an electrical signal, the photodetector output of which is amplified before being demodulated to retrieve the transmitted information signal [50]. There are two

main types of detecting systems that are extensively used in optical wireless communication such as coherent detection and direct detection.

- **Coherent Detection:** The information modulates the optical signal utilizing the amplitude, phase, and frequency of the lightwave carrier signal in coherent optical communications. The core concept of coherence detection is based on the product of electric fields of the received signal modulated light and the continuous-wave optical local oscillator (OLO) [73]. As a result, this possibility is responsible for the two forms of coherent detection: heterodyne and homodyne. The OLO frequency is nearly several gigahertz different from the optical frequency of the received optical signal in the coherent heterodyne detection system as illustrated in Figure 2.6. Thus, coherent detection is the most complex.

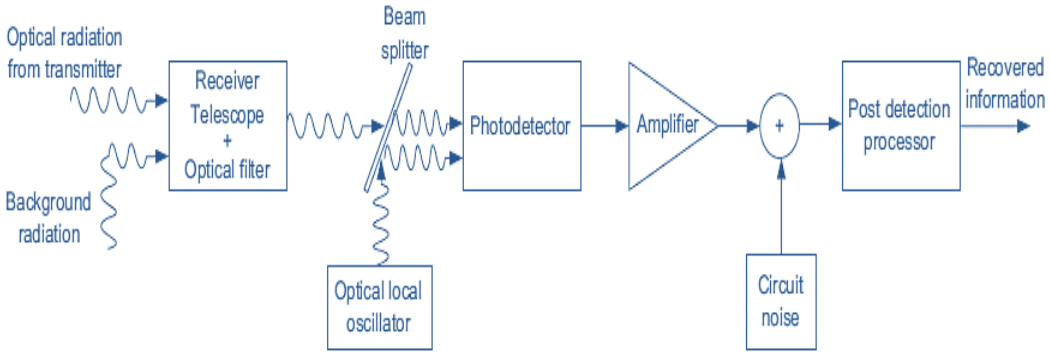

Figure 2.6. Block diagram of a coherent detection of the optical receiver [1].

- **Direct Detection:** The DD technique does not use a local oscillator in the detection process, the transmitted data must be correlated with the transmitted field's intensity fluctuation to recover the encoded data for this type of receiver as shown in Figure 2.7. Thus, IM/DD is the simplest and most extensively utilized in OWC systems [74].

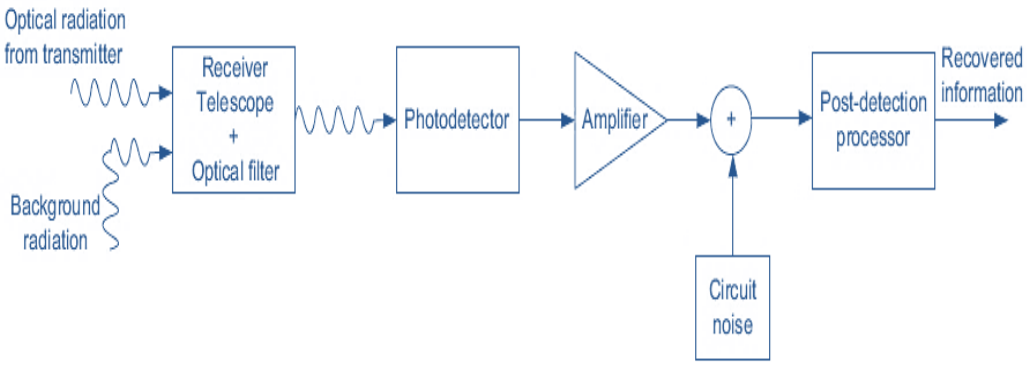

Figure 2.7. Block diagram of a direct detection of the optical receiver [1].

iv. **Amplifier:** Used amplifier to amplify the photodetector output (electrical signal).

v. **Demodulator:** After passing the de-modulator, the electrical output will contain the transmitted data.

2.3 FSO Atmospheric Turbulence Distribution Models

Several research studies led to the development of a mathematical model for the probability density function of the randomly fading receiver signal irradiance. These studies have resulted in several statistical models that may be used to characterize turbulence-induced fading in a variety of atmospheric conditions. Perhaps the most widely used of these models is the lognormal distribution model, Gamma-Gamma distribution model, and Malaga-M distribution model [56].

A. Log-normal (LN) Distribution Model

The optical turbulence may be expressed as a Lognormal distribution model when the optical channel is classified as a clear-sky atmospheric turbulence channel [75]. For weak turbulence conditions in [76], the authors proposed using the Lognormal PDF to describe the irradiance that is the optical beam's power density. The lognormal model is

used to calculate the irradiance statistics for weak turbulence. Because of its ease of mathematical computations [56]. The probability density function (PDF) in terms of received irradiance h_I of this model is given by [39]

$$f_{h_I}(h_I) = \frac{1}{h_I \sigma_x^2 \sqrt{8\pi}} \exp\left(- \frac{(ln(\, h_I) - \, 2\, \mu_x\,)^2}{8\sigma_x^2} \right) \tag{2.1}$$

where μ_x is the mean, whereas σ_x^2 is the standard deviation of the log-normal distribution.

Compared to experimental data, the lognormal PDF appears a large deviation as turbulence strength increases. As a result, in the case of significant fluctuation regimes, lognormal statistics are not a viable model [56].

B. Gamma- Gamma (GG) Distribution Model

The Gamma-Gamma distribution model, a newly suggested free space optical fading intensity model, is considered to be more appropriate to describe the turbulence-induced fading statistics of all atmospheric turbulence (weak to strong). The fading is considered to be two random operations, as small-scale atmospheric fluctuations and large-scale fluctuations; both types of atmospheric fluctuations are modeled as being gamma-distributed [77, 8]. The PDF of this model is calculated as

$$f_{h_I}(h_I) = \frac{2(\alpha\beta)^{(\alpha+\beta)/2}}{\Gamma(\alpha)\Gamma(\beta)} h_I^{(\alpha+\beta)/2-1} K_{(\alpha-\beta)}\left(2\sqrt{\alpha\beta h_I}\right) \qquad h_I \geq 0 \tag{2.2}$$

where α and β are the efficient number of atmospheric turbulence which represents the small scale and large scale, whereas represent h_I received irradiance, $\Gamma(.)$ is the gamma function, whereas $K_v(.)$ is the v th-order modified Bessel function of the second kind. Thus, under moderate irradiance variations, the lognormal model's range is limited. The gamma-gamma PDF, on the other hand, was recommended as a viable alternative to Beckmann's pdf due to its considerably more tractable mathematical model.

C. Malaga –M Distribution Model

The Malaga -M distribution describes how the irradiance fluctuates as an unbounded optical wavefront (plane or spherical waves) propagates over a turbulent medium for all irradiance conditions under inhomogeneous, isotropic turbulence [11]. As a special case, optical turbulence may be described as gamma-gamma distribution when the optical channel is viewed as a cloudy/foggy-sky atmospheric turbulence channel [3]. The Malaga-M distribution model is dependent on a physical model of scattering processes that are considered a continuation of the former work expanded by Churnside and Clifford [78].

Thus, the PDF of the received irradiance for the atmosphere turbulence h_{at} is given by [98]. For the FSO link adopts the (IM/DD) technique and follows the Malaga-M distribution turbulence model to describe the atmospheric turbulence.

$$f_{h_{at}}(h_{at}) = A \sum_{m=1}^{\beta} a_{mg}\ h_{at}\, k_{\alpha-m}\left(2\sqrt{\frac{\alpha\beta h_{at}}{\mathcal{S}\beta+\Omega'}}\right) \qquad h_{at>0} \qquad (2.3)$$

where

$$A \triangleq \frac{2\alpha^{\frac{\alpha}{2}}}{\mathcal{S}^{1+\frac{\alpha}{2}}\Gamma(\alpha)}\left(\frac{\mathcal{S}\beta}{\mathcal{S}\beta+\Omega'}\right)^{\beta+\frac{\alpha}{2}} \qquad (2.3\text{ a})$$

and

$$a_{mg} \triangleq \binom{\beta-1}{m-1}\frac{(\mathcal{S}\beta+\Omega')^{1-m/2}}{(m-1)!}\left(\frac{\Omega'}{\mathcal{S}}\right)^{m-1}\left(\frac{\alpha}{\beta}\right)^{m/2}\left(\frac{\alpha\beta}{\mathcal{S}\beta+\Omega'}\right)^{-\alpha+m/2} \qquad (2.3\text{ b})$$

where α is a positive parameter related to the effective number of large-scale cells of the scattering process, β is the amount of atmospheric turbulence-induced fading parameter which is a natural number, $\mathcal{S}$=$2b_0(1-\rho)$ is the average power of the scattering component received by off-axis eddies (U_S^G) which are related with both average power $2b_o$ of the total scatter components (U_S^C) and (U_S^G) and the parameter 0 $\leq$ ρ $\leq$1 that expresses the amount of scattering power coupled to the LOS component,

$\Omega' = \Omega + 2b_0\rho + 2\sqrt{2b_0\rho}\Omega \cos(\phi_A - \phi_B)$ is the average power from the coherent contributions, ϕ_A and ϕ_B is the scatter components of the deterministic phases of the LOS and the coupled to LOS paths, respectively. Whereas $\Gamma(\cdot)$ is the gamma function [99, Eq. (8.310.1)], and $k_{a-m}(\cdot)$ is the modified Bessel function of the second kind and order $(a - m)$ [8].

2.4 FSO Channel Conditions Losses

Since the FSO system is using an open medium (free space), the free space is less predictable in terms of atmospheric conditions. Controlling the transmission of optical signals over an open medium is significantly challenging due to unpredictability, this affects system availability and maximum design capacity. As known FSO is a line-of-sight technology, which implies that the interconnected points must be able to view each other without any obstructions. Thus, the optical signal propagates through the atmospheric channel in the FSO communication system, which is made up of different gases and other small particles floating in the atmosphere, such as aerosols, dust, smoke, and so on. The environment is characterized by heavy precipitation rain, haze, snow, and fog. Each of these atmospheric elements causes power level reduction, i.e., attenuation of the optical signal, because of a combination of factors such as light absorption by gas molecules, Rayleigh scattering, and Mie scattering. Thus, the optical beam travels through the atmospheric optical channel, it faces several losses [56, 86].

2.4.1 Foggy Weather Losses

Fog is for the visibility range lower than 500 m, haze for the visibility range higher than 1000 m, and a transitional zone called mist for the visibility range between 500 and 1000 m have been defined as three major forms of short-visibility weather [87]. Variations in observed particle size distributions and changes in the wavelength selectivity of recorded attenuation coefficients are used to create these zones. [88].Some of the foggy weather conditions are clarified below.

- Fog: Fog is made up of small water droplets suspended in the layered air close to the earth's surface. As a result of the presence of these droplets, light is scattered and visibility near the ground is reduced. Fog is described in meteorology as visibility is decreased to less than 1 km and the relative humidity of the air reaches a saturation level close to 100%. . Fog happens when water droplets of a few microns to a few tens of microns shape over the hazy particle nucleus during relative humidity is more than 95%.

- Haze: Haze is made up of microscopic fine dust or salt, as well as tiny droplets ranging from a few microns to a few tenths of a micron.

- Mist: Mist forms with the humidity rise to saturation during transitioning from haze to fog. This transitioning is usually swift because of the increase of (1-to 2 μm) micron droplets. As a result, the vision quickly deteriorates.

Among the different atmospheric conditions, the fog has the largest negative impact on optical signal propagation in FSO communication systems, because the size of fog's droplets is of the same order of magnitude as the wavelength of the optical beam, and their concentration is much larger than the rain or snow [89]. The attenuation foggy weather of the FSO link l_{fo} can be described by Beers law as [39]

$$l_{fo} = e^{-\alpha_{foggy} L} \tag{2.4}$$

where α_{foggy} $[dB/km]$ is the attenuation coefficient due to foggy weather conditions, and L is the link length of the FSO link.

The fog is responsible for the majority of the atmospheric attenuation, mainly due to absorption and scattering [90]. The atmosphere is an absorption medium relative to the Earth's surface. Any emitted photon is absorbed by a gaseous molecule and converted to kinetic energy, resulting in the heating of the atmosphere. Moreover, the wavelength plays a key role in the absorption process. For instance, at wavelengths below 200 nm, Oxygen (O_2) and Ozone (O_3) molecules can disrupt the transmission

of signals, but at visible wavelengths, they are less effective (i.e., 400 - 700 nm). Likewise, the signal transmission in the atmosphere is also susceptible to scattering, which is a function of wavelength. When atmosphere particles are smaller than the wavelength, Rayleigh scattering is examined. In addition, FSO transmission is essentially unaffected when the particles size is substantially larger than the wavelength, as in rain and snow [91]. On the other hand, when the particles are the same size as the wavelength, such as in fog and haze, Mie scattering is examined. In this situation, even across small distances, the signal might be greatly weakened. Experiments have demonstrated that moderate fog over a 50 m distance reduces transmission power by 90% [86]. Another experiment [92] done on the wavelength range of 785 to 1550 nm found that attenuation is wavelength-independent for foggy situations but not for haze. And when vision is less than 50 m in heavy fog, attenuation can exceed 350 decibels per km [93]. This indicates that the availability of the FSO link might be hampered. Very high power lasers combined with particular mitigation measures can help to enhance the odds of connection available in these situations. Because of their high transmitted power, the wavelength 1550 nm lasers are typically preferred during severe attenuation. Fog particles (1000 nm – 20000 nm) are smaller than haze particles (10nm – 1000nm), therefore haze does not affect light beam attenuation [92].

Thus, Mie scattering theory may be used to accurately estimate the optical attenuation of fog droplets. The fog attenuation is predicted using typical experimental models based on visibility range information. The visibility range Vis (km) is defined as the distance of a parallel bright beam that travels in the atmosphere before losing 2% of its original intensity. The wavelength (λ_O) of 550 nm is commonly used as reference wavelength for the visibility range. The attenuation coefficient obtained by popular experimental models for Mie scattering is defined by [94]

$$\alpha_{foggy} = \frac{3.91}{Vis}\left(\frac{\lambda}{\lambda_O}\right)^{-q} \tag{2.5}$$

where (λ =1550 nm) is the wavelength of a laser diode, q which is a parameter related to the particle size distribution in the atmosphere depending on the visibility. According to the Kim model, q is given by [92]

$$
\begin{aligned}
q &= 1.6 && Vis > 50\ km \\
&= 1.3 && 6\ km < Vis < 50\ km \\
&= 0.16\ Vis + 0.34 && 1km < Vis < 6\ km \\
&= Vis - 0.5 && 0.5\ km < Vis < 1\ km \\
&= 0 && Vis < 0.5\ km
\end{aligned} \tag{2.6}
$$

Thus, the visibility range for different foggy weather conditions can be shown in table 2.1.

Table 2.1. Visibility range versus both foggy weather conditions and various degrees of fog [95].

Different foggy weather conditions	Different Vis (Km)ranges.
Very Clear weather	Vis, larger of 50 Km
Clear weather	Vis, less of 50 Km
Haze weather	Vis, less of 6 Km
Fog weather	Vis, less of 1 Km and higher zero Km
Heavy fog	Vis, less of 0.05 Km
Moderate fog	Vis, less of 0. 5 Km
Light fog	Vis, less of 1 Km and higher 0.5 Km

2.4.2 Atmospheric Turbulence-induced Fading

The turbulence-induced fading is a significant impediment to high data rates speed and long-distance optical communications [76, 68]. Considering a fading is critical for measuring FSO communication systems performance. Thus, the atmosphere channel has several negative characteristics that can cause significant signal fading or even signal loss [96]. In this section, we present a statistical model of atmospheric turbulence

(h_{at}) to describe the receiver irradiance fluctuations of the optical signal propagating through the turbulence atmospheric channel. The Malaga-M distribution model related to the physical model has the benefit of being reduced to a simple closed-form analytical expression that applies to all turbulence regimes [97].

Thus, suppose the propagation of an electromagnetic wave in a turbulent environment with a random refractive index. As the wave travels through the turbulent medium, a fraction of the energy is dispersed, and the type of scattering determines the shape of the irradiance probability distribution. The physical model adopted by Malaga-M distribution consists of three components [11]. Thus, the Malaga-M turbulence model description is depicted in Figure 2.8.

i. LOS component (U_L) of the FSO link that experiences Malaga-M distribution turbulence, which is currently employed.

ii. Coupled-to-LOS component (U_S^C) is the component that is quasi-forward dispersed through eddies or cells on the propagation axis and coupled to the LOS component.

iii. Independent scatter component (U_S^G) is the component due to energy that is scattered to the receiver by off-axis eddies.

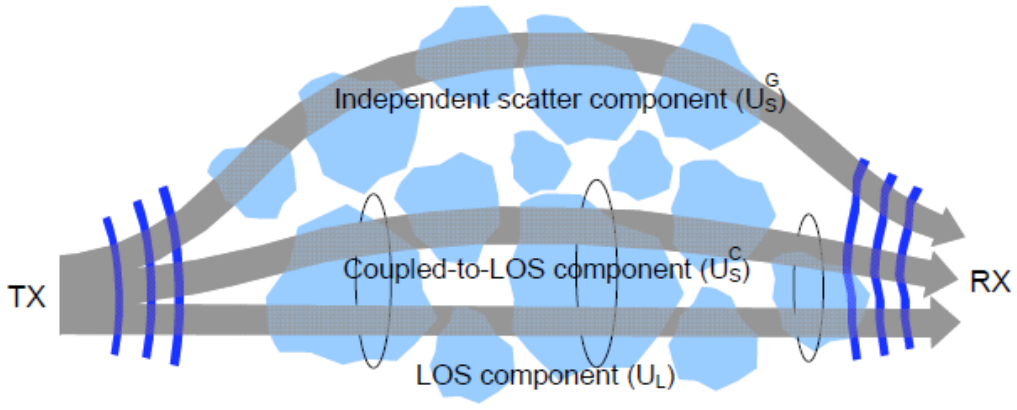

Figure 2.8. The propagation geometry for the optical laser beam in a generalized Malaga-M turbulence model to form the small-scale fluctuations [11].

2.4.3 Pointing Errors-Induced Fading

The pointing errors are made up of the key two components (Jitter and boresight), the jitter can be defined as the random displacement of the laser beam and the detector plane principally caused by building vibration. While boresight indicates the fixed displacement between the laser beam center and the detector center due to thermal expansion, the boresight can be (zero boresight pointing errors and non-zero boresight pointing errors) [7].

Thus, the pointing errors that occur between transmitter and legal receiver (h_{pe}) are analyzed by giving the normalized spatial distribution of the intensity of the divergent Gaussian at a distance L from the transmitter is given by $I_{beam}(\rho; L) = \frac{2}{\pi w_{L,e}^2} \exp\left(-\frac{2\|\boldsymbol{\rho}\|^2}{w_{L,e}^2}\right)$, where $\|\rho\|$ represents the radial vector from the beam center with the norm of a vector, $w_{L,e}$ is the beam waist at distance L [100]. The channel coefficient due to the geometric spread of the Gaussian beam with a pointing error vector $\boldsymbol{r}_b$ concerning the legal receiver can be expressed as $h_{pe}(\boldsymbol{r}_b; L) = \int_A I_{beam}(\rho - \boldsymbol{r}_b; L)\, d\rho$ indicating a fraction of the collected power at legal receiver with the detector area A. Because of the symmetry of the beam form and the size of the detector area, the end outcome $h_{pe}(\boldsymbol{r_b}; L)$ fraction of the collected power depends on the radial distance, written as $r_b = \|\boldsymbol{r}_b\| = \left\|\begin{bmatrix} X' \\ Y' \end{bmatrix}\right\|$, both X' and Y' represent the horizontal and vertical displacements along the propagation axes of the optical beam at the detector plane [85]. The fraction of collected power with a circular detection aperture of radius (a) at the legal receiver is therefore estimated as [100]

$$h_{pe}(\boldsymbol{r}_b; L) \cong A_O \exp\left(-\frac{2r_b^2}{w_{L,e(eq)}^2}\right) \qquad r_b \geq 0 \qquad (2.7)$$

where $A_O = [\mathrm{erf}(v)]^2$ represents the fraction of the collected power at $r_b = 0$, $v = \left(\frac{\sqrt{\pi}\, a}{\sqrt{2} w_{L,e}}\right)$, whereas $w_{L,e(eq)}^2$ is the equivalent beam width which can be given by $w_{L,e(eq)}^2 = w_{L,e}^2 \frac{\sqrt{\pi}\mathrm{erf}(v)}{2v \exp(v^2)}$, erf (.) denoting the errors function [99, Eq. (8.250.1)], $w_{L,e} \approx \theta\, L$ can be used to approximate the beam width value over comparatively long distances,

θ is the divergence angle of the transmit optical beam which represents the increase in beam radius with increasing the distance from the transmitter [61].

Due to the difficulty of solving the closed-form expression for the four-parameter Beckman distribution, the result in [85] is an accurate approximation of the four-parameter Beckman distribution by the Rayleigh distribution. Thus, at the receiver side, the radial displacement r_b, follows the Rayleigh distribution by taking into account separate equal Gaussian distributions for vertical and horizontal displacement (sway) as [85, 97]

$$f_{r_b}(r_b) = \frac{r_b}{\sigma^2_{mod,pe}} exp\left(-\frac{r_b^2}{2\sigma^2_{mod,pe}}\right) \qquad r_b \geq 0 \qquad (2.8)$$

where $\sigma^2_{mod,pe} = \left(\frac{3\mu_x^2\sigma_x^4+3\mu_y^2\sigma_y^4+\sigma_x^6+\sigma_y^6}{2}\right)^{1/3}$ is the estimated jitter variance of the misaligned beam.

For the legal receiver, and via combining the Equations (2.7), and (2.8), we can obtain the PDF for the received irradiance (h_{pe}) for the pointing errors based on the impact of the pointing errors with zero boresights by the following [100]

$$f_{h_{pe}}(h_{pe}) = \frac{\xi^2_{ra}}{A_G^{\xi^2_{ra}}} h_{pe}^{\xi^2_{ra}-1} \qquad 0 \leq h_{pe} \leq A_G \qquad (2.9)$$

ξ_{ra} $\in$ {zero boresight i.e., ψ, non-zero boresight i.e., ζ}, represents A_G=A_o=[erf(v)]^2, $\xi_{ra} = \frac{w_{L,e_{(eq)}}}{2\sigma_{s,pe}}$ is the ratio between the equivalent beam radius $w_{L,e_{(eq)}}$ and the standard deviation (jitter) at the receiver plane ($2\sigma_{s,pe}$). As a result of the radial displacement at the legal receiver of Rayleigh distribution, the random offset (jitter variances) equals ($\sigma_x = \sigma_y = \sigma_{s,pe}$), whereas fixed displacement (zero boresight pointing errors) equals ($\mu_x = \mu_y = 0$).

For the illegal receiver, The PDF for irradiance is affected by pointing errors $h_{pe}$with non-zero boresight can be given by [85]

$$f_{h_{pe}}(h_{pe}) = \frac{\xi_{ra}^2}{A_G^{\xi_{ra}^2}} h_{pe}^{\xi_{ra}^2-1} \qquad 0 \le h_{pe} \le A_G \qquad (2.10)$$

where $\mathrm{Q} = \exp\left(\frac{1}{\xi_{ra}^2} - \frac{1}{2\xi_{ra,x}^2} - \frac{1}{2\xi_{ra,y}^2} - \frac{\mu_x^2}{2\sigma_{x,pe}^2\xi_{ra,x}^2} - \frac{\mu_y^2}{2\sigma_{y,pe}^2\xi_{ra,y}^2}\right)$, $A_G = A_o\,\mathrm{Q}$, as for $\xi_{ra}^2 = \frac{w_{L,e(eq)}}{2\sigma_{mod,pe}}$, $\xi_{ra,x}^2 = \frac{w_{L,e\,(eq)}}{2\sigma_{x,pe}}$, $\xi_{ra,y}^2 = \frac{w_{L,e(eq)}}{2\sigma_{y,pe}}$, where the random offset (jitter variances) equals ($\sigma_{x,pe} = \sigma_{\,y,pe} = \sigma_{mod.pe}$), whereas fixed displacement (non-zero boresight pointing errors) equals ($s^2 = {\mu_x}^2 = {\mu_y}^2$) [7, 85, 101].

2.5 The Combined Effects of the FSO Links Channel Conditions Losses

It should be taken into account that both pointing errors and atmospheric turbulence effects are statistically independent, it is also known that the pointing errors are due to building sway. Thus, correlation time is within a few seconds, which is longer than the atmosphere turbulence correlation time (10-100 ms) [102]. The PDF of the receiver irradiance h_{cs}can be derived as [100]

$$f_{h_{cs}}(h_{cs}) = \int_{h_{cs}/(l_{fo}A_{G)}}^{\infty} f_{h_{cs}|h_{at}}\,(h_{cs}|h_{at})\, f_{h_{at}}\,(h_{at})\, dh_{at} \qquad (2.11)$$

where h_{cs} is the received irradiance for the FSO system consists of the three main components as $h_{cs} = h_{at}h_{pe}l_{fo}$. It is mentioned h_{at} represents the received irradiance for the atmosphere turbulence, h_{pe} represents the received irradiance for the pointing errors, and l_{fo} represents attenuation due to foggy weather condition effects, whereas $f_{h_{cs}|h_{at}}\,(h_{cs}|h_{at})$ is the conditional probability for a given a h_{at} state, and it's written as [102]

$$f_{h_{cs}|h_{at}}\,(h_{cs}|h_{at}) = \frac{1}{h_{at}l_{fo}} f_{h_{pe}}\left(\frac{h_{cs}}{h_{at}l_{fo}}\right)$$

$$= \frac{\xi_{ra}^2}{h_{at}l_{fo}A_G^{\xi_{ra}^2}}\left(\frac{h_{cs}}{h_{at}l_{fo}}\right)^{\xi_{ra}^2-1} \qquad (2.12)$$

For Malaga-M turbulence distribution model, Eq. (2.12) and Eq. (2.3) can be substituted into Eq. (2.11) as seen in the following Eq. (2.13)

$$f_{h_{cs}}(h_{cs}) = \int_{h_{cs}/(l_{fo}A_G)}^{\infty} \frac{\xi_{ra}^2}{h_{at} l_{fo} A_G^{\xi_{ra}^2}} \left(\frac{h_{cs}}{h_{at} l_{fo}}\right)^{\xi_{ra}^2 - 1} f_{h_{at}}(h_{at})\, dh_{at} \qquad (2.13)$$

Finally, we can obtain the PDF of the receiver irradiance (h_{cs}) under Malaga–M turbulence with the presence of the pointing errors given by [98]

$$f_{h_{cs}}(h_{cs}) = \frac{A\xi_{ra}^2}{2h_{cs}} \sum_{m_g=1}^{\beta_g} a_{mg}\; G_{1,3}^{3,0}\left[\frac{\alpha_g \beta_g}{(\mathcal{S}\beta_g + \Omega')} \frac{h_{cs}}{l_{fo} A_G} \middle| \begin{matrix} \xi_{ra}^2 + 1 \\ \xi_{ra}^2, \alpha_g, m_g \end{matrix}\right]. \qquad (2.14)$$

where $G_{p,q}^{m,n}[\cdot]$, is the Meijer G -function as defined in [99, Eq. (9.301)].

Thus, the PDF of the considered FSO system over Malaga-M turbulence channels with IM/DD detection technique in terms of SNR is given as [14]

$$f_{\gamma_{fso,g}}(\gamma_{fso,g}) = \frac{\xi_{ra}^2 A}{4\gamma_{fso,g}} \sum_{m_g=1}^{\beta_g} a_{m_g}\; G_{1,3}^{3,0}\left[\frac{\xi_{ra}^2(\mathcal{S} + \Omega')}{1 + \xi_{ra}^2}\left(\frac{\alpha_g \beta_g}{\mathcal{S}\beta_g + \Omega'}\right)\sqrt{\frac{\gamma_{fso,g}}{\mu_{fso,g}}} \middle| \begin{matrix} \xi_{ra}^2 + 1 \\ \xi_{ra}^2, \alpha_g, m_g \end{matrix}\right]. \qquad (2.15)$$

The $\gamma_{fso,g}$ represents instantaneous SNR of the considered FSO system that can be described as

$$\gamma_{fso,g} = \frac{\eta_{eff}^2\, h_{cs}^2}{N_o} \qquad (2.15\text{ a})$$

where the effective photoelectric conversion ratio η_{eff} is a number that represents the efficiency of converting light into electricity, the additive white Gaussian noise (AWGN) sample is denoted by the sign N_o, while the average SNR of the FSO link developsed can be described as

$$\mu_{fso.g} = \frac{\eta_{eff}^2 \mathbb{E}_{h_{cs}}^2[h_{cs}]}{N_o} \qquad (2.15\text{ b})$$

where $\mathbb{E}^2_{h_{cs}}[h_{cs}] = \left(l_{fo} A_G \xi^2_{ra}(\mathcal{S} + \Omega')\right)^2 / (1 + \xi^2_{ra})^2$, Eq. (2.15) can be rewritten in the following way

$$f_{\gamma_{fso,g}}\left(\gamma_{fso,g}\right) = \frac{\mathcal{B}_g \, \mathcal{L}_g}{\mu_{fso,g}} \sum_{m_g=1}^{\beta_g} a_{m_g} 2^{\alpha_g + m_g - 1} \, G^{6,0}_{2,6}\left[\frac{\gamma_{fso,g}}{\mu_{fso,g}} \mathcal{L}_g \, \middle| \begin{matrix} m_{\mathrm{g1}} - 1 \\ m_{\mathrm{g2}} - 1 \end{matrix}\right]. \quad (2.16)$$

The cumulative distribution function (CDF), after some simple algebraic operations and the use of [103, Eq. (07.34.21.0084.01)], the CDF of the considered Malaga-M distribution turbulence model in terms of $\gamma_{fso,g}$ can be obtained as [98] (3.15)

$$F_{\gamma_{fso,g}}(\gamma_{fso,g}) = \mathcal{B}_g \sum_{m_g=1}^{\beta_g} a_{m_g} 2^{\alpha_g + m_g - 1} G^{6,1}_{3,7}\left[\frac{\gamma_{fso,g}}{\mu_{fso,g}} \, \mathcal{L}_g \, \middle| \begin{matrix} 1, m_{g1} \\ m_{g2,} 0 \end{matrix}\right]. \quad (2.17)$$

2.6 PLS of Optical Wireless Communication

Because wireless networks are inherently open, which allows anybody inside a transmitter's coverage area to collect the transmitted signals, information security is one of the most problems significant and challenging in wireless networks. In the seven-layer Open Systems Interconnection (OSI) model of computer networking, shown in Figure 2.9 the information security is traditionally addressed above the physical layer, such as the commonly used encryption, which is generally utilized at the application layer presuming the physical layer has already established an errors-free link [79].

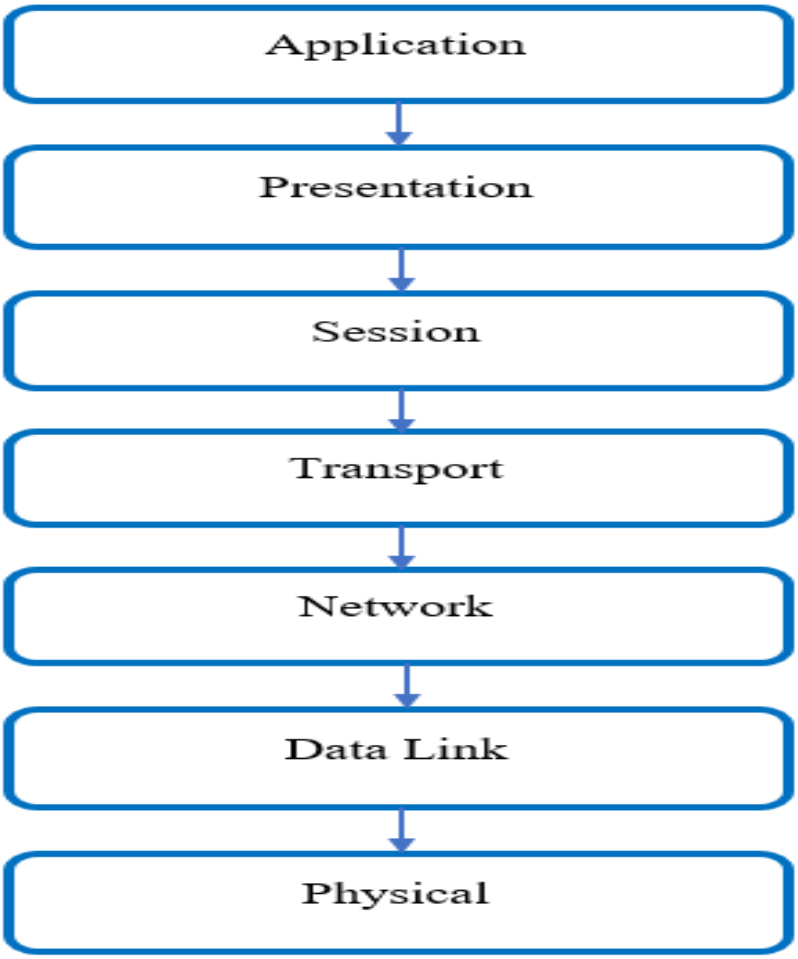

Figure 2.9. The Seven Layers of the OSI model.

Traditional cryptography encrypts plaintext messages with specific algorithms that are supposed to be computationally infeasible for the discount to decipher if the encryption keys are undisclosed to the discount. However, because of increasing development in computers and methods of penetration of encryption algorithms, there are fears that these security measures will no longer be enough, particularly for applications requiring a high level of security (as military networks). The Data Encryption Standard (DES) encryption technique, for example, was adopted as a standard by the US National Bureau of Standards in 1976 and uses a 56-bit key. However, in 1997, a DES cryptogram was publicly broken for the first time, and in 1998, the (Deep Crack device) broke a DES key in just 56 hours [80].

Physical layer security has recently been investigated as a possible method for delivering strong security for wireless networks. Unlike cryptography, which ignores differences in received signals between various receivers, the physical layer security is obtained by examining the differences between the physical features of signal channels to create unconditional security, i.e. security that is achieved regardless of the adversary's computational capabilities. As a result, physical layer security is sometimes referred to as information-theoretic security, which is now widely recognized as a more powerful concept than computational security. Information theory is generally concerned with conveying messages in the presence of noise, and it was established by Claude Shannon [81].

Because of the increasing expansion of wireless applications, services, and the wish for information secrecy. Physical layer security enjoys a shining future, both as a stand-alone security solution and as part of layered security schemes.

The Physical layer security improves secrecy by exploiting the physical medium's inherent unpredictability due to random (in a wireless channel, this might be caused to random electrical pulses in the atmosphere environment). However, the research into such potential physical layer security is still in its early stages [82, 83].

2.7 Wiretap Channel Model

The fundamental idea of physical layer security by showing a three-users (U1, U2, and U3) network where the communication channel from user U1 to U2 is called (main channel) being eavesdropped on by a third-party hostile user U3, whereas the communication channel from user U1 to U3 is called (eavesdropper channel) as in Figure 2.10 illustrated.

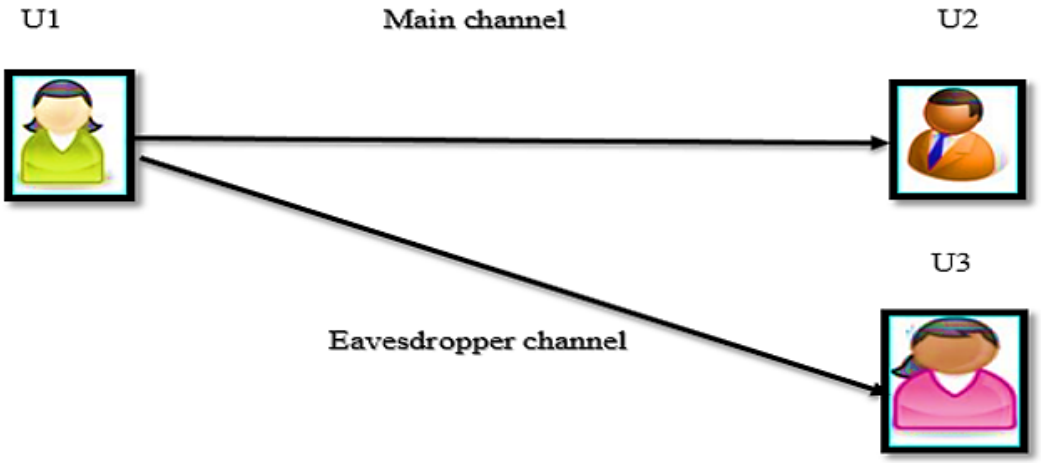

Figure 2.10. Illustration of the wiretap channel model.

The U1 encodes a sent data, represented by random variable (RV) $\in\mathcal{W} = \{1, \ldots, \mathcal{M}\}$, whereas in the codeword, can be represented by RV $\mathcal{X}_n \in X_n$, with the use of a stochastic encoder $fn(\cdot)$: $\mathcal{W} \rightarrow X_n$After then, the codeword X_n is sent over the main channel. The signal that U2 receives is symbolized by $\mathcal{Y}_n \in y_n$, whereas the U3 signal is signified by $\mathcal{Z}_n \in Z_n$. Following the reception of the signal, U2 attempts to decode it using a decoder $\varphi(\cdot)$: $y_n \rightarrow \mathcal{W}$. U2 guessed data is $\mathcal{W}$ indicated by $\hat{\mathcal{W}} = \varphi(\mathcal{Y}_n)$ as shown in Figure 2.11. $\mathcal{W}$, X, y, and Z represent the source, the channel input alphabet, the channel output alphabet of the main channel, and the channel output alphabet of the eavesdropper channel, respectively [82].

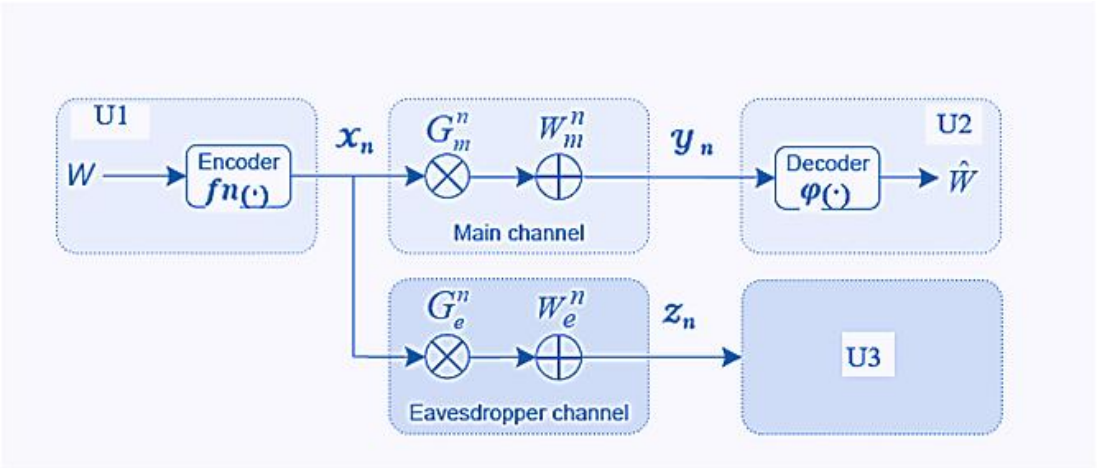

Figure 2.11. Fading wire-tap channel of the physical layer security [82].

The signals received by the two receivers U2 and U3 are generally different since they are positioned in separate areas [82]. The basic explanation is that the fading effects of the two channels through which signals flow are different. Fading may be divided into two types: small-scale fading and large-scale fading. Small scale fading, also known as multipath fading, is caused by surrounding scatters that reflect wavefront differently between the transmitter and legal receiver, and it may induce deep fades even over short distances.

However, large-scale fading is highly reliant on the location concerning obstacles. It's worth mentioning that these impacts change over time and are dependent on the environment. The physical layer security can be attained by investigating the following effects: When the main channel has better channel conditions than the eavesdropper channel, the system transmits secret messages; otherwise, transmissions will stop. It's worth mentioning that each system has a maximum allowable information rate, referred to as secrecy capacity. Secrecy capacity, like Shannon's capacity, sets the upper constraint on the quantity of data that can be securely conveyed without leaking any data.

2.8 Channel State Information (CSI)

Channel state information (CSI) refers to the channel properties of a communication link, such as channel gain, noise intensity, fading distribution, and spatial correlation, this term describes how a signal travels from a transmitter to a receiver. In terms of CSI, there are two types: instantaneous CSI and statistical CSI. The current channel conditions are indicated by the instantaneous CSI. Whereas the statistical CSI refers to the channel's statistical characterizations, which may be used to see if the instantaneous CSI is known or not. Instantaneous CSI allows transmissions to be adjusted to current channel conditions, which is critical for reliable communication, the statistical CSI, on the other hand, has no such benefit [82].

It is always feasible to obtain the CSI of the main channel since Bob can collaborate with Alice by giving backchannel estimates to her, but it is difficult to obtain

the CSI of the Eve's if he remains silent. However, there are conditions in which Alice can obtain Eve's CSI, or at the very least statistical CSI. For example, Eve is another active wireless network user who is not permitted to hear the secret messages, thus Alice may estimate Eve's channel based on Eve's previous transmissions.

In this thesis, our analysis is primarily focused on the scenario in which the transmitter has only partial CSI knowledge before transmission, in the sense that the transmitter knows the main channel's instantaneous CSI as well as the statistical CSI of both channels, but has no knowledge of the eavesdropper channel's instantaneous CSI.

CHAPTER THREE

SECRECY PERFORMANCE EVALUATION OF THE FSO CHANNEL

3.1 Introduction

In this chapter, we present an accurate analytical model of the FSO system under channel and system conditions such as (foggy weather, atmospheric turbulence, and pointing errors), Also, the chapter will present closed-form expressions to analyze the secrecy performance of the FSO system through ASC, SOP, and SPSC with the PDF and CDF in terms of SNR of the considered FSO system over Malaga-M turbulence channels with IM/DD detection technique.

3.2 FSO System Model

In this thesis, we consider an FSO communication system consisting of one transmitter is known as Alice (denoted A), the single legal receiver is known as Bob (denoted B), and the illegal receiver is known as Eve (denoted E). We will focus on the most potential scenario of eavesdropping where the eavesdropper is placed near to the legal receiver, this is mostly due to the fact of the dispersion of the laser beam through the atmosphere, and where the beam waist at the receiver becomes is much greater than the receiver's aperture size. As a result, when the eavesdropper is in the divergence zone of the received optical beam, a possible eavesdropping process will occur. As shown in Figure (3.1) the considered FSO system employ an (IM/DD) detection technology via Malaga-M distribution turbulence model for the optical link, under impact generalized atmospheric turbulence, pointing errors components, different foggy weather conditions, and distance between the transmitter and the legal receiver.

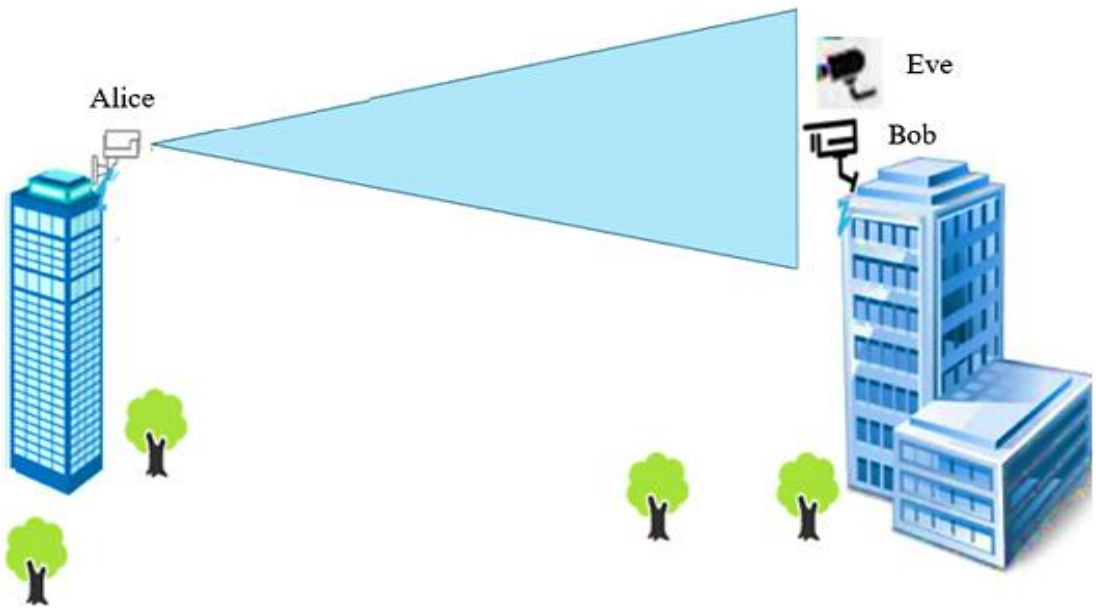

Figure 3.1. The free-space optical communication system in presence of an external eavesdropper.

In general, the received signal of the FSO communication system can be represented as

$$\mathcal{Y} = \eta \mathcal{X} h_{c_s} + N_o \tag{3.1}$$

where y denotes the received electrical signal by the photodetector of the FSO system receiver, η is the responsivity of the photodetector, $\mathcal{X} \in [0,1]$ is the digital input symbol, N_o represents the additive white Gaussian noise (AWGN) with zero mean and variance equals to $\sigma_n^2 = N_o/2$ of the receiver.

3.3 Secrecy Performance Metrics of the FSO System

In this section, a new mathematical framework is presented to investigate the secrecy performance of the FSO system, through the performance metrics such as ASC, SOP, and SPSC. The metrics are used to completely analyze the secrecy performance of physical layer security technology to realize secure and reliable information

transmission across the fading wiretap channel under atmospheric turbulence conditions (weak to strong), with pointing errors (jitter and zero boresight and non-zero), foggy weather conditions, and link length effect (distance between transmitter and legal receiver) onto secrecy outage probability, over Malaga-M distribution, using IM/DD detection technology. We utilized the following parameters in our analysis: $,\beta,\psi,\zeta$ ρ, b_o, Ω , and attenuation foggy weather values which are given in table 3.1. a,b,c The simulation results of this section were obtained using the MATLAB environment. As Figures 3.2 and 3.3 show the practical framework of the ASC and SOP metrics using the same environment**.**

Table 3.1 Channel conditions-dependent parameters of the FSO communication system.

Foggy weather a_{foggy} =Attenuation (dB/Km)	
Clear air	0.43
Haze	4.2
Light fog	20
Moderate fog	42.2
Heavy fog	125

(a)

Atmosphere turbulence parameters		
α	8	Weak turbulence
β	4	
α	4.2	Moderate turbulence
β	3	
α	2.296	Strong turbulence
β	2	
ρ		0.596
b_o		0.1079
Ω		1.3265

(b)

Pointing errors				
Zero boresight pointing errors with jitter pointing errors		Non-zero boresight pointing errors with jitter pointing errors		
ψ	1	ζ	2.52	Weak non-zero boresight pointing errors
ψ	6.7	ζ	1.3	Moderate non-zero boresight pointing errors
		ζ	0.59	Strong non-zero boresight pointing errors

(c)

3.3.1 ASC of the Considered FSO System

The ASC is a crucial security parameter for evaluating the secrecy performance of the FSO systems under the effect of the eavesdropping process. The average amount of information that can be securely transmitted across the atmosphere channel to the legal receiver while keeping the eavesdropper entirely unaware of the information is evaluated by the achievable secrecy capacity rater C_s which is the greatest rate that the transmitter can achieve, which is a crucial parameter in a communication system. The secrecy capacity rate of the wiretap model is defined as

$$C_s(\gamma_{fso,B}, \gamma_{fso,E}) = max[W\, ln(1 + c\gamma_{fso,B}) - W\, ln(1 + c\gamma_{fso,E}), 0]^+ \quad (3.2)$$

where the secrecy capacity rate of the wireless channel is defined as the difference between the capacity of the main channel $[\, ln(1 + c\gamma_{fso,\boldsymbol{B}})]$ and the capacity of the eavesdropping channel $[\, ln(1 + c\gamma_{fso,E)}]$, c=e/2π is a constant term, whereas W is the bandwidth of the FSO system. Now, and for the sake of simplicity considered W =1, then the (C_s) can be described as

$$C_s = \begin{cases} \ln(1 + c\gamma_{fso,B}) - \ln(1 + c\gamma_{fso,E}) & if\ \gamma_{fso,B} > \gamma_{fso,E} \\ 0 & if\ \gamma_{fso,B} \leq \gamma_{fso,E} \end{cases} \quad (3.3)$$

Thus, the ASC can be expressed by

$$ASC = \int_0^\infty \int_0^\infty C_s\,(\gamma_{fso,B}, \gamma_{fso,E})\, f_B(\gamma_{fso,B})\, f_E(\gamma_{fso,E}) d\gamma_{fso,B} d\gamma_{fso,E} \quad (3.4)$$

where $f_B(\gamma_{fso,B})$ and $f_E(\gamma_{fso,E})$ is the joint PDF for the γ_{fso} for the main and wiretap channels of the FSO system, so, we have

$$ASC = \frac{1}{ln2}[\int_0^{\infty} \ln(1 + c\gamma_{fso,B})\, f_B(\gamma_{fso,B}) \int_0^{\gamma_{fso,B}} f_E(\gamma_{fso,E}) d\gamma_{fso,E}\, d\gamma_{fso,B} - \int_0^{\infty} \ln(+c\gamma_{fso,E})\, f_E(\gamma_{fso,E}) \int_{\gamma_{fso,E}}^{\infty} f_B(\gamma_{fso,B}) d\gamma_{fso,B} d\gamma_{fso,E}] \quad (3.5)$$

After that, Eq. (3.5) might be rewritten as

$$ASC = \frac{1}{ln2}(T_1 + T_2 - T_3) \quad (3.6)$$

where

$$T_1 = \int_0^{\infty} ln(1 + c\gamma_{fso,B})\, f_B(\gamma_{fso,B})\, F_E\,(\gamma_{fso,B}) d\gamma_{fso,B} \quad (3.7)$$

$$T_2 = \int_0^{\infty} ln(1 + c\gamma_{fso,E})\, f_E(\gamma_{fs,E})\, F_B\,(\gamma_{fso,E}) d\gamma_{fso,E} \quad (3.8)$$

$$T_3 = \int_0^{\infty} ln(1 + c\gamma_{fso,E})\, f_E(\gamma_{fso,E})\, d\gamma_{fso,E} \quad (3.9)$$

The logarithm function in Eqs. (3.7), (3.8), and (3.9) may be expressed in the form of Meijer's G-function by

$$ln(1 + c\gamma_{fsog)} = G_{2,2}^{1,2}\left[c\gamma_{fso,g} \middle| \begin{matrix} 1,1 \\ 1,0 \end{matrix} \right] \quad (3.10)$$

By substituting Eqs. (2.16), (2.17), and (3.10) in Eq. (3.7), we can be obtaining the following

$$T_1 = \frac{\mathcal{B}_B \mathcal{B}_E \mathcal{L}_B}{\mu_{fso,B}} \sum_{m=1}^{\beta_B} \sum_{k=1}^{\beta_E} a_{Bm} a_{Ek} \int_0^{\infty} G_{2,2}^{1,2}\left[c\gamma_{fso,B} \middle| \begin{matrix} 1,1 \\ 1,0 \end{matrix} \right]$$

$$\times G_{2,6}^{6,0}\left[\frac{\gamma_{fso,B}}{\mu_{fso,B}} \mathcal{L}_B \middle| \begin{matrix} m_{1B} - 1 \\ m_{2B} - 1 \end{matrix} \right] \times G_{3,7}^{6,1}\left[\frac{\gamma_{fso,B}}{\mu_{fso,E}} \mathcal{L}_E \middle| \begin{matrix} 1, m_{1E} \\ m_{2E}, 0 \end{matrix} \right] d\gamma_{fso,B} \qquad (3.11)$$

where $\mathcal{B}_g = \frac{\xi_{ra}^2 A}{8\pi}$, $\mathcal{L}_g = \frac{\left(\frac{\xi_{ra}^2 (s+\Omega')}{1+\xi_{ra}^2} \frac{\alpha_g \beta_g}{s\beta_g + \Omega'} \right)^2}{16}$, $m_{g1} = \left\{ \frac{\xi_{ra}^2 + 1}{2} , \frac{\xi_{ra}^2 + 2}{2} \right\}$,

and $m_{g2} = \left\{ \frac{\xi_{ra}^2}{2}, \frac{\xi_{ra}^2 + 1}{2}, \frac{\alpha_g}{2}, \frac{\alpha_g + 1}{2}, \frac{m_g}{2} , \frac{m_g + 1}{2} \right\}$. where $g \in \{B, E\}$

Thus, extended generalized bivariate Meijer G-function (EGBMGF) can be used to express the product of three Meijer's G-functions by

$$T_1 = B_B B_E \sum_{m=1}^{\beta_B} \sum_{k=1}^{\beta_E} a_{Bm} a_{Ek} \, G_{6,2:3,7:2,2}^{6,0:6,1:1,2} \left[\begin{matrix} m_{2B} \\ m_{1B} \end{matrix} \middle| \begin{matrix} 1, m_{1E} \\ m_{2E}, 0 \end{matrix} \middle| \begin{matrix} 1,1 \\ 1,0 \end{matrix} \middle| \frac{\mathcal{L}_E \mu_{fso,B}}{\mathcal{L}_B \mu_{fso,E}}, \frac{c\mu_{fso,B}}{\mathcal{L}_B} \right] \qquad (3.12)$$

Thus, T_2 can be derived using the same method in Eq. (3.12) as

$$T_2 = \mathcal{B}_B \mathcal{B}_E \sum_{m=1}^{\beta_B} \sum_{k=1}^{\beta_E} a_{Bm} a_{Ek} \, G_{6,2:3,7:2,2}^{6,0:6,1:1,2} \left[\begin{matrix} m_{2E} \\ m_{1E} \end{matrix} \middle| \begin{matrix} 1, m_{1B} \\ m_{2B}, 0 \end{matrix} \middle| \begin{matrix} 1,1 \\ 1,0 \end{matrix} \middle| \frac{\mathcal{L}_B \mu_{fso,E}}{\mathcal{L}_E \mu_{fso,B}}, \frac{c\mu_{fso,E}}{\mathcal{L}_E} \right] \qquad (3.13)$$

Similarly can get

$$T_3 = \mathcal{B}_E \sum_{k=1}^{\beta_E} a_{Ek} \, G_{4,8}^{8,1} \left[\frac{\mathcal{L}_E}{c\mu_{fso,E}} \middle| \begin{matrix} 0,1, m_{1E} \\ m_{2E}, 0,0 \end{matrix} \right] \qquad (3.14)$$

Thus, the closed-form formula for ASC can be derived by substituting Eqs. (3.12), (3.13), and (3.29) into Eq. (3.6) and getting as follows.

$$ASC = \frac{1}{ln\,2}\,\mathcal{B}_B\,\mathcal{B}_E \sum_{m=1}^{\beta_B}\sum_{k-1}^{\beta_E} a_{Bm}a_{Ek}\,G_{6,2:3,7:2,2}^{6,0:6,1:1,2}\left[\begin{matrix} m_{2B} \\ m_{1B}\end{matrix}\middle|\begin{matrix}1, m_{1E}\\ m_{2E}, 0\end{matrix}\middle|\begin{matrix}1,1\\ 1,0\end{matrix}\middle|\frac{\mathcal{L}_E\mu_{fso,B}}{\mathcal{L}_B\mu_{fso,E}}, \frac{c\mu_B}{\mathcal{L}_B}\right]$$
$$+\,\mathcal{B}_B\mathcal{B}_E \sum_{m=1}^{\beta_B}\sum_{k-1}^{\beta_E} a_{Bm}a_{Ek}\,G_{6,2:3,7:2,2}^{6,0:6,1:1,2}\left[\begin{matrix} m_{2E} \\ m_{1B}\end{matrix}\middle|\begin{matrix}1, m_{1B}\\ m_{2B}, 0\end{matrix}\middle|\begin{matrix}1,1\\ 1,0\end{matrix}\middle|\frac{\mathcal{L}_B\mu_{fso,E}}{\mathcal{L}_E\mu_{fso,B}}, \frac{c\mu_E}{\mathcal{L}_E}\right]$$
$$-\,\mathcal{B}_E \sum_{k-1}^{\beta_E} a_{Ek}\,G_{4,8}^{8,1}\left[\frac{\mathcal{L}_E}{c\mu_{fso,E}}\middle|\begin{matrix}0,1, m_{1E}\\ m_{2E}, 0,0\end{matrix}\right] \tag{3.15}$$

3.3.2 SOP of the Considered FSO System

The ideal secrecy can be obtained when the CSI for the eavesdropping channel is fully known, where the secrecy rate (C_s) is greater than the target secrecy rate (Tsr) threshold. But it should be noted that wireless channels inherently fluctuate. So, it is therefore not possible to get a real-time CSI of wireless channels. Thus, this case can be considered unrealistic. While the case of unavailability of CSI of the eavesdropping channel, and a CSI that is only available for the main channel at the transmitter, is considered more realistic. Subsequently, this information can be employed by the transmitter and legal receiver to decide whether or not they should send secure messages. However, they may risk compromising the secrecy of secure information transmission. Therefore, the probability of the secrecy rate falling below the target secrecy rate is known as the secrecy outage probability, which is a basic measure of secrecy performance that is widely used to describe the physical layer security of an FSO link. The SOP can be given as

$$SOP = P\{C_s(\gamma_{fso,B}, \gamma_{fso,E}) \leq T_{sr}\} \tag{3.16}$$

where T_{sr}($T_{sr} \geq 0$) is the target secrecy rate threshold and $\vartheta = e^{T_{sr}} \geq 1$

$$SOP = P\{\gamma_{fso,B} \leq \vartheta\, \gamma_{fso,E} + \vartheta - 1\} \tag{3.17}$$

$$SOP = \int_0^{\infty} F_{\gamma_{fso,B}}\left(\vartheta\, \gamma_{fso,E} + \vartheta - 1\right) f_{\gamma_{fso,E}}(\gamma_{fso,E}) d\, \gamma_{fso,E} \tag{3.18}$$

when Eqs. (2.16) and (2.17) are substituted into Eq. (3.18), it is obvious that the resulting equation is difficult to solve mathematically since it involves an extremely complicated and polynomial integration. As a result, the lower bound of the SOP (SOP_L) is calculated as

$$SOP_L = P\{\gamma_{fso,B} \leq \vartheta\, \gamma_{fso,E} + \vartheta - 1\} \geq P\{\gamma_{fso,B} \leq \vartheta\, \gamma_{fso,E}\} \tag{3.19}$$

where $SOP_L \triangleq P\{\gamma_{fso,B} \leq \vartheta\, \gamma_{fso,E}\}$. Thus, SOP_L can be obtained as

$$SOP_L = \int_0^{\infty} F_{\gamma_{fso,B}}\left(\vartheta\, \gamma_{fso,E}\right) f_{\gamma_{fso,E}}\left(\gamma_{fso,E}\right) d\, \gamma_{fso,E} \tag{3.20}$$

we can obtain SOP_L by substituting Eqs. (2.16) and (2.17) in Eq. (3.20) by

(3.21)

$$SOP_L = \frac{\mathcal{B}_B \mathcal{B}_E \mathcal{L}_E}{\mu_{fso,E}} \sum_{m=1}^{\beta_B} \sum_{k=1}^{\beta_E} a_{Bm} a_{Em} \int_0^{\infty} G_{3,7}^{6,1}\left[\frac{\vartheta \mathcal{L}_B}{\mu_{fso,B}} \gamma_{fso.E} \middle| \begin{matrix} 1, m_{B1} \\ m_{B2}, 0 \end{matrix}\right] \times\; G_{2,6}^{6,0}\left[\frac{\gamma_{fso,E}}{\mu_{fso,E}} \mathcal{L}_E \middle| \begin{matrix} m_{E1}-1 \\ m_{E2}-1 \end{matrix}\right] d\gamma_{fso,E}$$

Thus, SOP_L can get as

$$SOP_L = \mathcal{B}_B \mathcal{B}_E \sum_{m=1}^{\beta_B} \sum_{k=1}^{\beta_E} a_{Bm} a_{Em}\; G_{9,9}^{7,6}\left[\frac{\mathcal{L}_E \mu_{fso,B}}{\vartheta \mathcal{L}_B \mu_{fso,E}} \middle| \begin{matrix} m_{3,B} \\ m_{4,E} \end{matrix}\right] \tag{3.22}$$

where $m_{g3} = \left\{\frac{2-\xi_{ra}^2}{2}, \frac{1-\xi_{ra}^2}{2}, \frac{2-\alpha_B}{2}, \frac{1-\alpha_B}{2}, \frac{2-m}{2}, \frac{1-m}{2}, 1, \frac{\xi_{ra}^2+1}{2}, \frac{\xi_{ra}^2+2}{2}\right\}$, and

$m_{g4} = \left\{\frac{\xi_{ra}^2}{2}, \frac{\xi_{ra}^2+1}{2}, \frac{\alpha_E}{2}, \frac{\alpha_E+1}{2}, \frac{m}{2}, \frac{m+1}{2}, 0, \frac{1-\xi_{ra}^2}{2}, -\frac{\xi_{ra}^2}{2}\right\}$

3.3.3 SPSC of the Considered FSO System

The C_s must be a positive number to ensure that the transmitted information is secure. The system's ability to maintain secrecy will be jeopardized otherwise. The SPSC may be defined mathematically as follows

$$\begin{aligned} SPSC &= P\{C_s(\gamma_{fso,B}, \gamma_{fso,E}) > 0\} \\ &= P\{\gamma_{fso,B} > \gamma_{fso,E}\} \\ &= 1 - SOP \\ &= 1 - \int_0^{\infty} F_{\gamma_{fso,B}}(\gamma_{fso,E})\, f_{\gamma_{fso,E}}(\gamma_{fso,E}) d\gamma_{fso,E} \end{aligned} \tag{3.23}$$

where $T_{sr} = 0$. Thus, we get SPSC by substituting Eqs. (2.16) and (2.17) into Eq. (3.23),

$$SPSC = 1 - \mathcal{B}_B \mathcal{B}_E \sum_{m=1}^{\beta_B} \sum_{k=1}^{\beta_E} a_{Bm} a_{Em}\; G_{9,9}^{7,6}\left[\frac{\mathcal{L}_E\, \mu_{fso,B}}{\vartheta \mathcal{L}_B\, \mu_{fso,E}} \middle| \begin{matrix} m_{3,B} \\ m_{4,E} \end{matrix} \right] \tag{3.24}$$

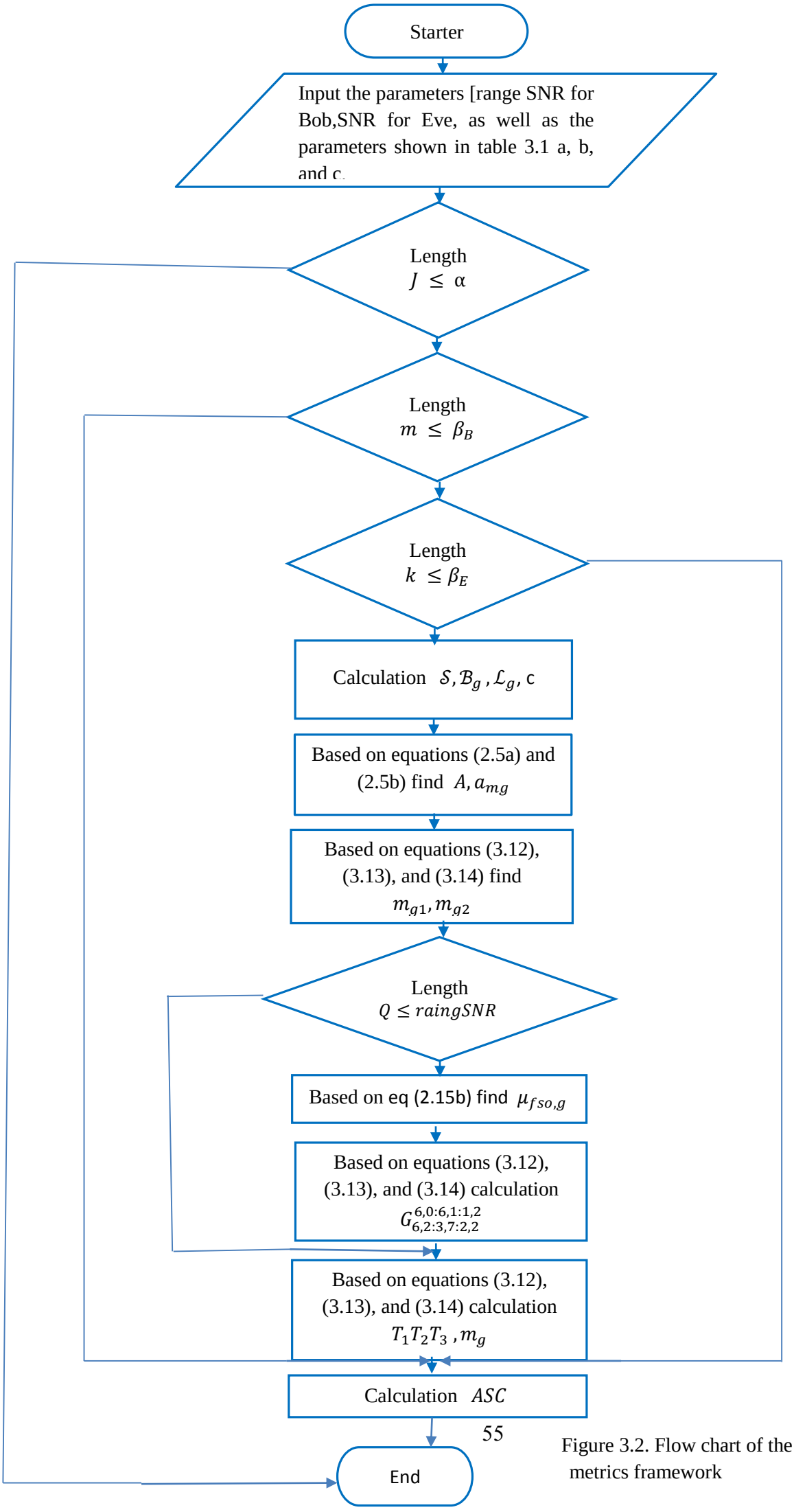

Figure 3.2. Flow chart of the ASC performance metrics framework

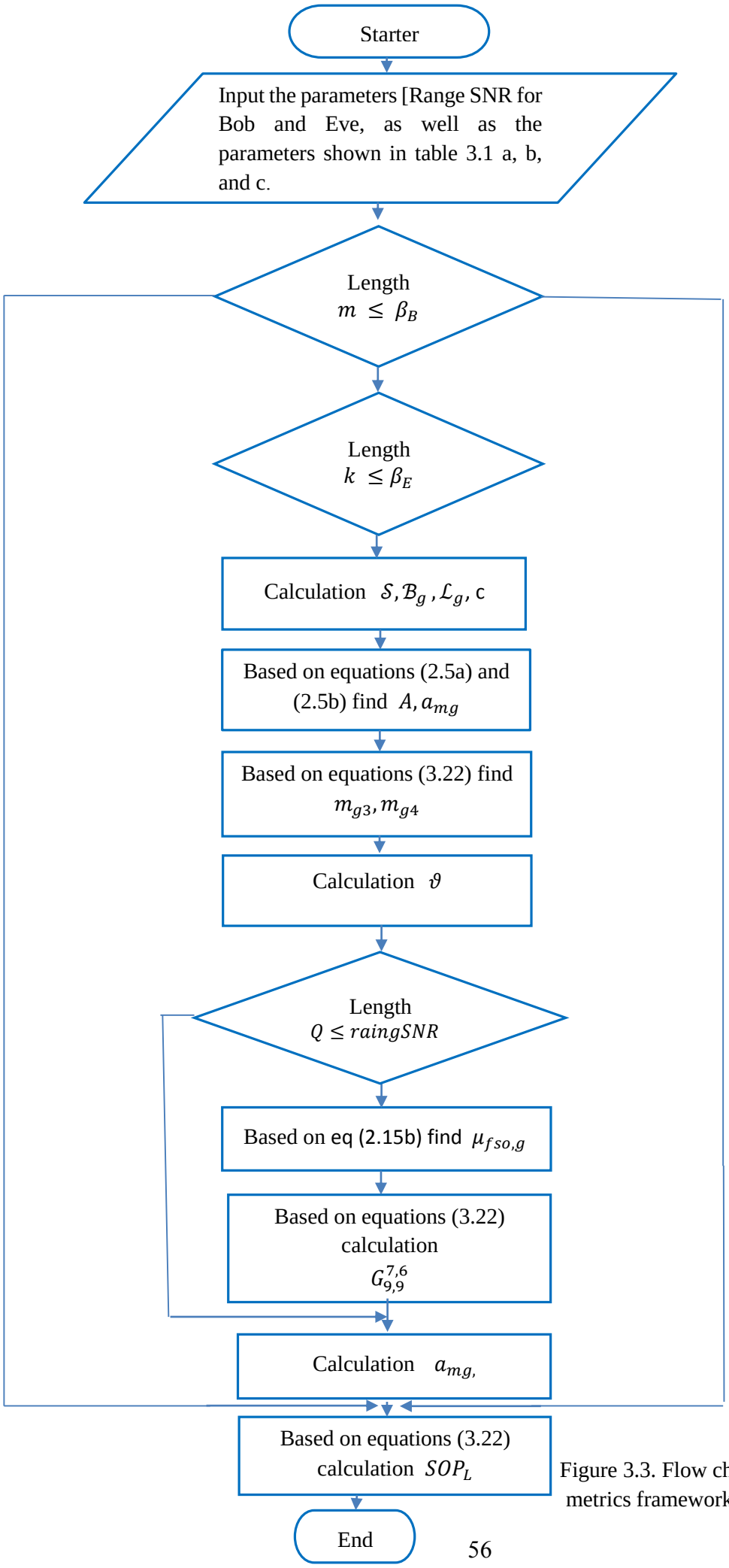

Figure 3.3. Flow chart of the SOP performance metrics framework

CHAPTER FOUR

SIMULATION RESULTS AND DISCUSSION

4.1 Introduction

In this chapter, the secrecy metrics, i.e., the ASC, SOP, and SPSC probability will be used to evaluate the secrecy performance of the FSO system. The FSO link length is assumed to be 1 Km with a wavelength of λ=1550 nm under varying atmosphere channel conditions in presence of an eavesdropper, it is assumed that the atmospheric turbulence conditions of the main channel and the eavesdropper channel are equal. Where parameters (α and β) represent atmospheric turbulence conditions (weak, moderate, and strong), the components of the pointing errors represented by the parameters (ψ and ζ), and the attenuation values due to the foggy weather provided in table 3.1 are also taken into account. The results are obtained by assuming IM/DD optical signal detection technique. Moreover, the target secrecy rate for information transmission is set to be 1 bit/s/Hz.

4.2 ASC Performance Analysis of the FSO System

In this section, we presented the ASC performance of the FSO system under different atmospheric turbulence conditions, pointing errors, and foggy weather conditions. the ASC performance as a function of the average SNR of the main channel (Bob) ($\mu_{fso,B}$) in Figures 4.1, 4.2, and 4.3 shown. With SNR values of the wiretap channel (Eve) ($\mu_{fso,E}$) are assumed as -10 dB, 0 dB, and 10 dB respectively, under different atmospheric turbulence effects, with fixed effect of pointing errors of ψ=6.7. From these figures, it can be seen that increasing the $\mu_{fso,B}$ enhances the overall ASC performance under all the atmosphere turbulence conditions as expected. On the other hand, increasing the $\mu_{fso,E}$ from -10 dB to 0 dB and then to 10 dB caused a deterioration in

ASC performance, which confirms the accuracy of our analytical expression of ASC that had been derived in section 3.3.1. The reason behind that is due to the improvement in eavesdropper link's quality with increasing in ($\mu_{fso,E}$) value. The ASC of the system is increased to 10 bit/s/Hz under moderate turbulence and raised to 40 bit/s/Hz under weak turbulence in comparison of 2.5 bit/s/Hz under strong turbulence and $\mu_{fso,E}$ =10 dB.

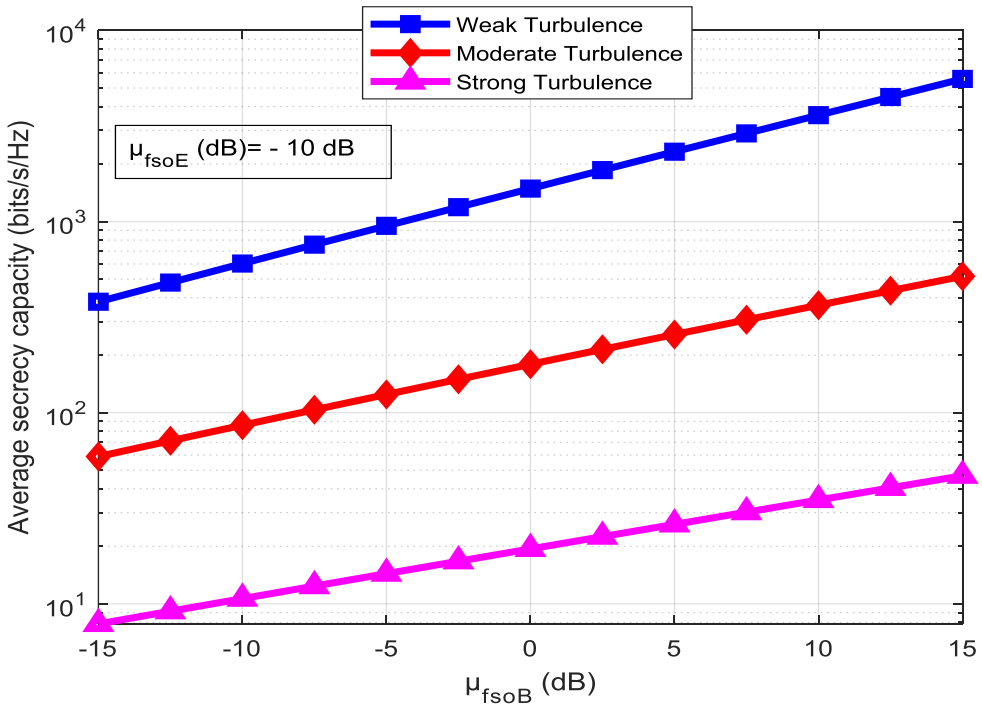

Figure 4.1. ASC vs. The average SNR of the Bob ($\mu_{fso,B}$) with SNR of the Eve ($\mu_{fso,E}$) = −10 dB.

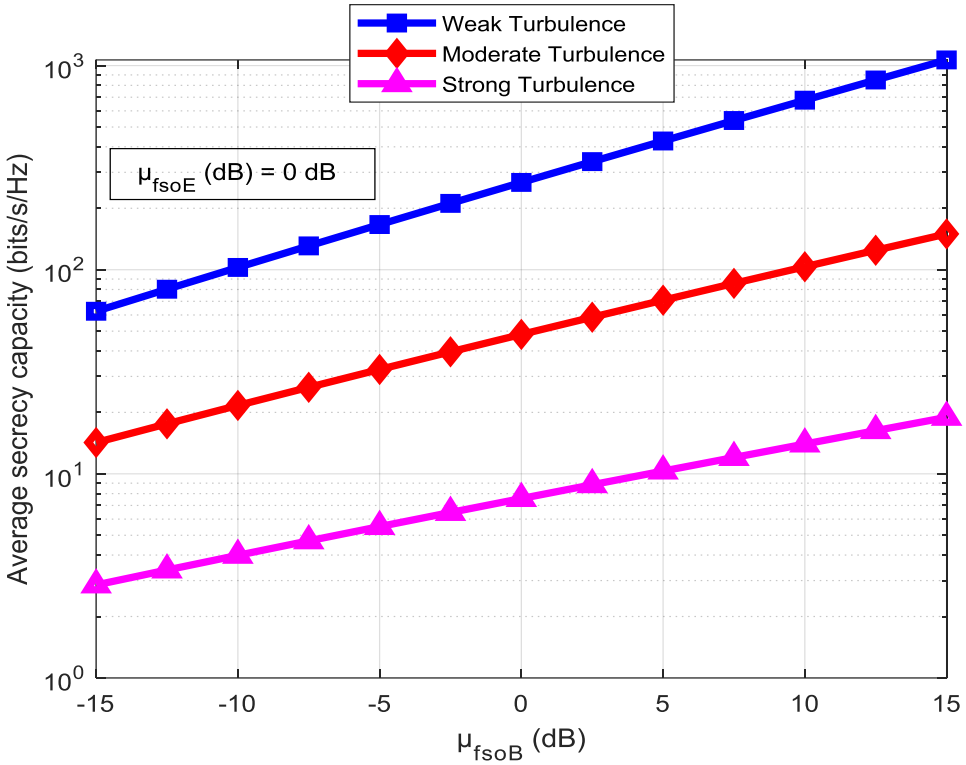

Figure 4.2. ASC Vs. The average SNR of the Bob ($\mu_{fso,B}$) with SNR of the Eve ($\mu_{fso,E}$) = 0 dB.

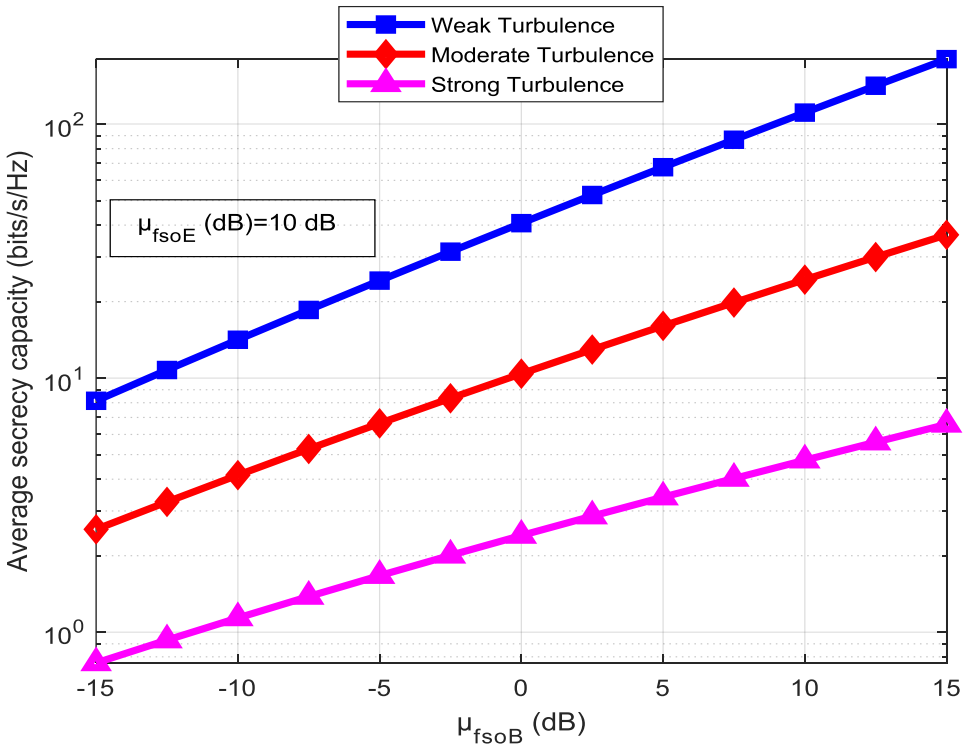

Figure 4.3. ASC Vs. The average SNR of the Bob ($\mu_{fso,B}$) with SNR of the Eve ($\mu_{fso,E}$)=10 dB.

The influence pointing errors (zero boresights with jitter) on the ASC performance under moderate turbulence conditions and varying pointing errors values of ψ=6.7 and ψ =1 respectively, as shown in Figures 4.4 and 4.5. It observes that the ASC performance improves when the effect of the pointing errors is reduced to the low value of ψ =6.7, thus the system has superior performance. Whereas the value of the pointing errors is high ψ=1, causing the ASC performance to be in the worst state. The reduced pointing errors influence is due to the small values of the random offset of the beam on the detector plane (jitter) when ψ is large.

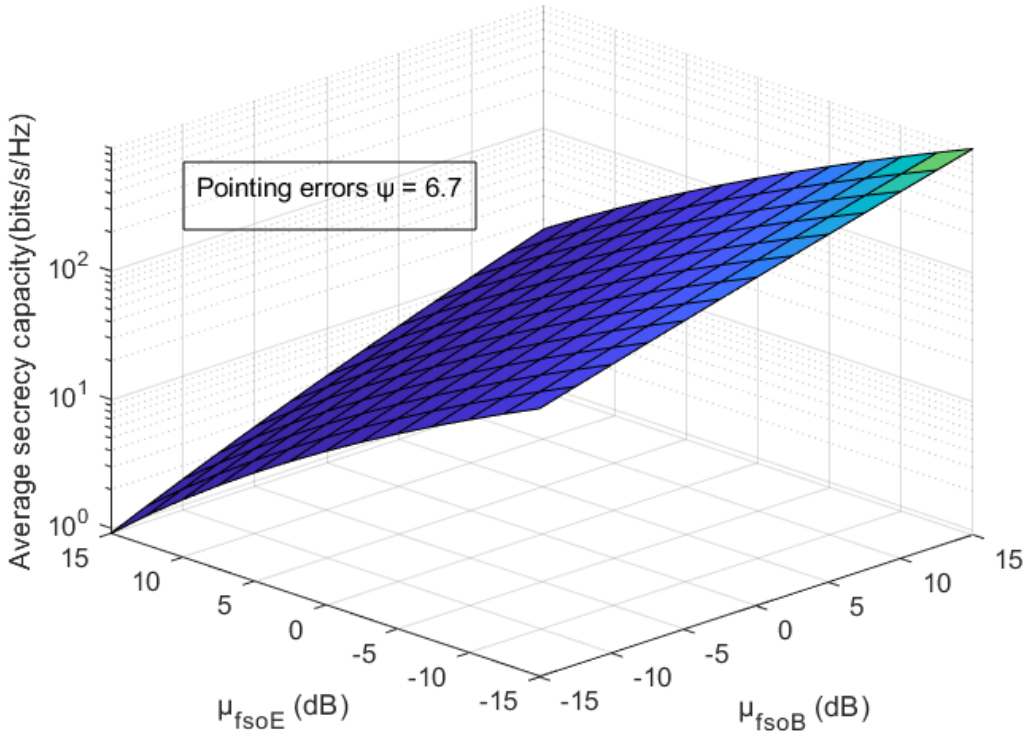

Figure 4.4. ASC Vs. The average SNR of the Bob ($\mu_{fso,B}$) and SNR of the Eve $(\mu_{fso,E})$ under effect ψ = 6.7.

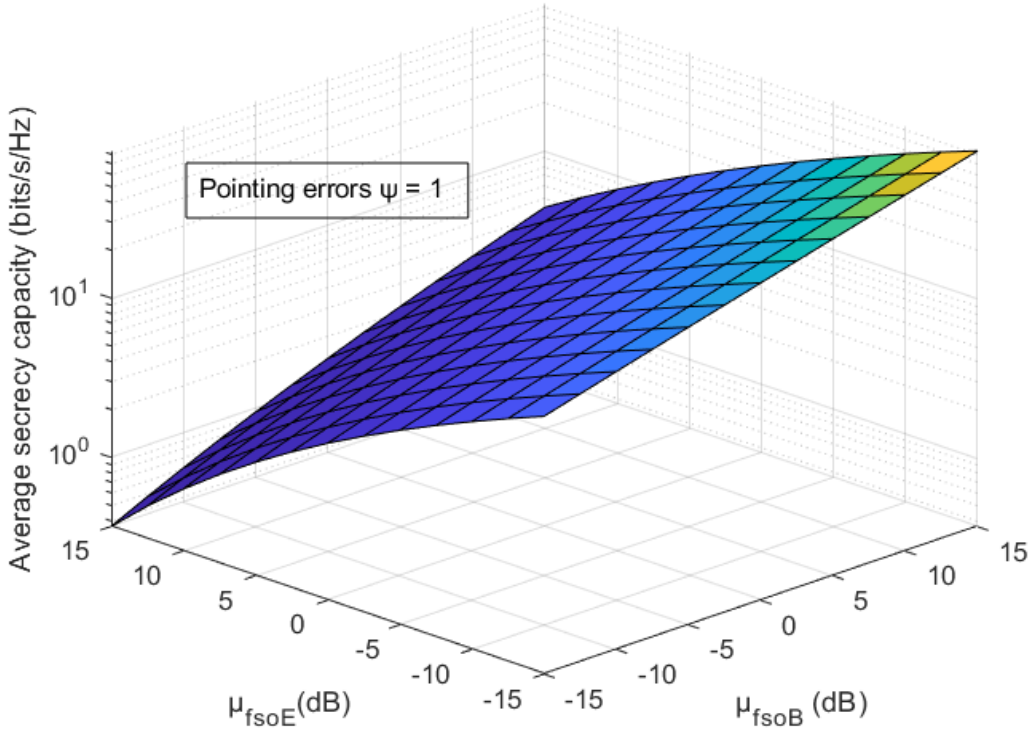

Figure 4.5. ASC The average SNR of the Bob ($\mu_{fso,B}$) and SNR of the Eve ($\mu_{fso,E}$) under effect ψ = 1.

The ASC performance versus the average SNR of the main channel with SNR of the wiretap channel of -10 dB and 10 dB respectively, as shown in Figures 4.6 and 4.7. In this case, we consider different atmospheric turbulence conditions under the effect of non-zero boresight pointing errors as ζ = (2.52, 1.3, 0.59) represented the weak, moderate, and strong pointing errors effect respectively. From the results, it has appeared that the impact of non-zero boresight on the ASC is more deteriorating in comparison with the effect of the zero boresight pointing errors. The reason behind that is due to the non-zero boresight pointing errors occurring in two dimensions X and Y, in comparison with the zero boresight pointing errors that occurs in one dimension either (X or Y).

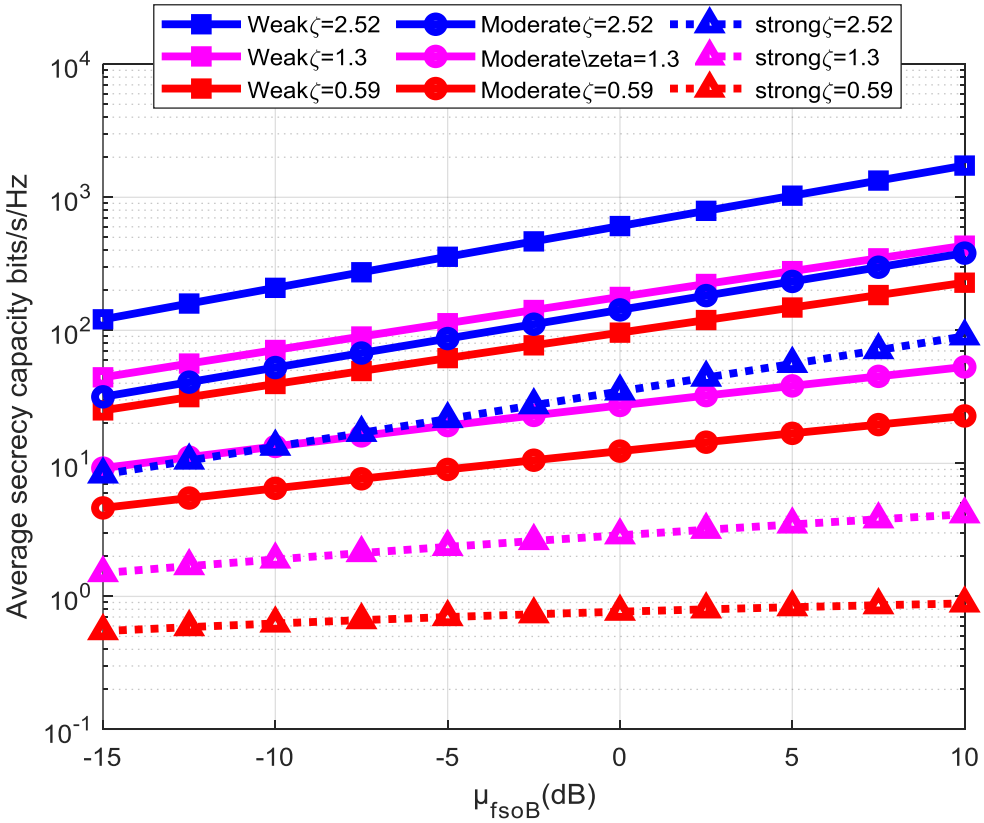

Figure 4.6. ASC under the effect of non-zero boresight with SNR of the Eve ($\mu_{fso,E}$)= −10 dB.

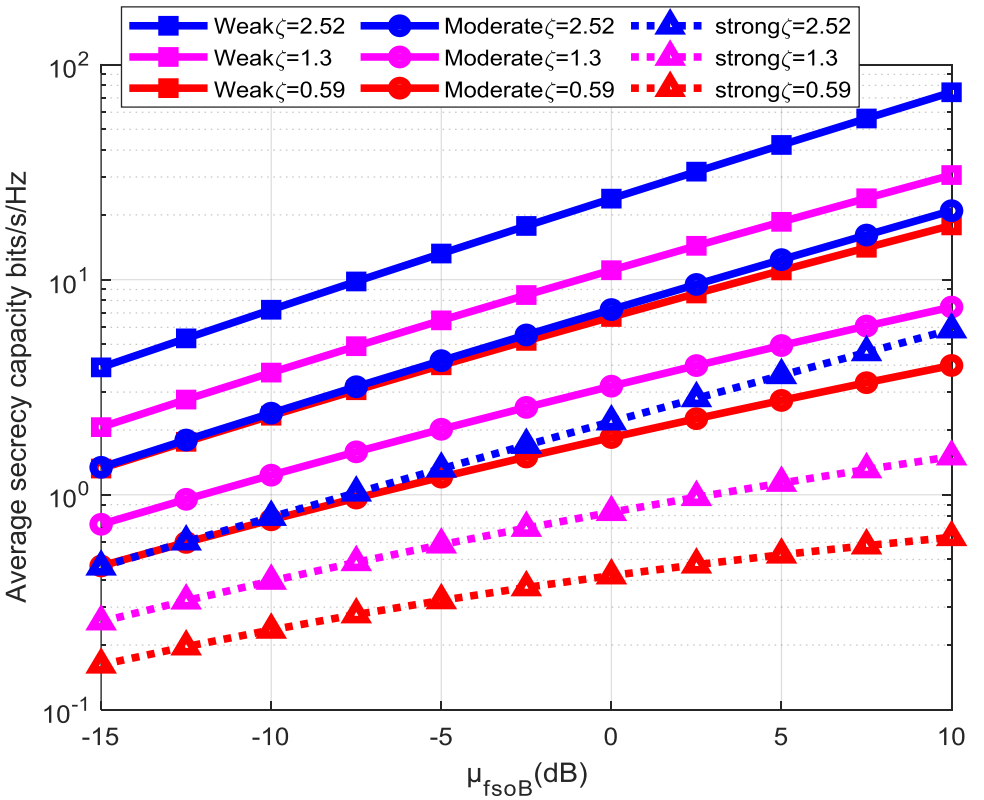

Figure 4.7. ASC under the effect of non-zero boresight with SNR of the Eve ($\mu_{fso,E}$)=10 dB.

The ASC as a function of the average SNR of the main channel in Figures 4.8, 4.9, 4.10, and 4.11, 4.12, 4.13 demonstrate with the selected value of the zero boresight pointing errors of ψ = 6.7 and ψ = 1 under different foggy weather conditions and different turbulence conditions (weak, moderate, strong) of the FSO system. The results show that when the attenuation of optical signal increased due to the severity of foggy weather, the ASC performance of the FSO links is degraded due to the decrease in the FSO link's visibility. This effect of fog is due to the size of droplets of fog which have the same wavelength size as the laser source used in optical systems.

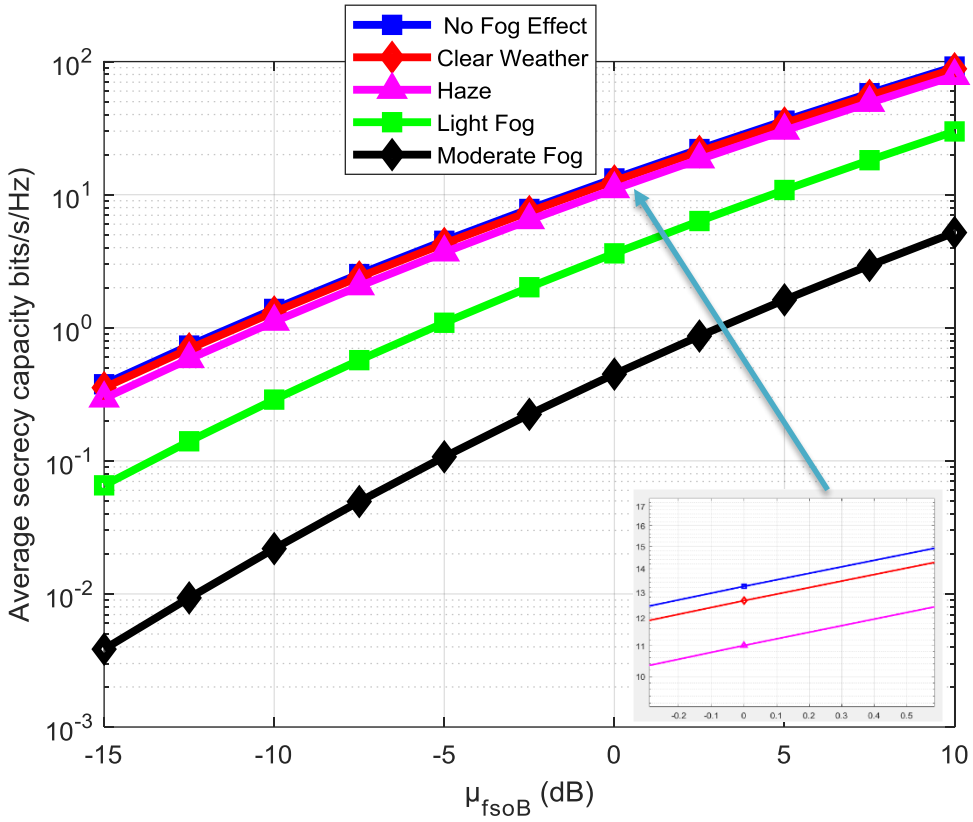

Figure 4.8. ASC under the influence of various foggy weather conditions with of ψ = 6.7, and weak turbulence.

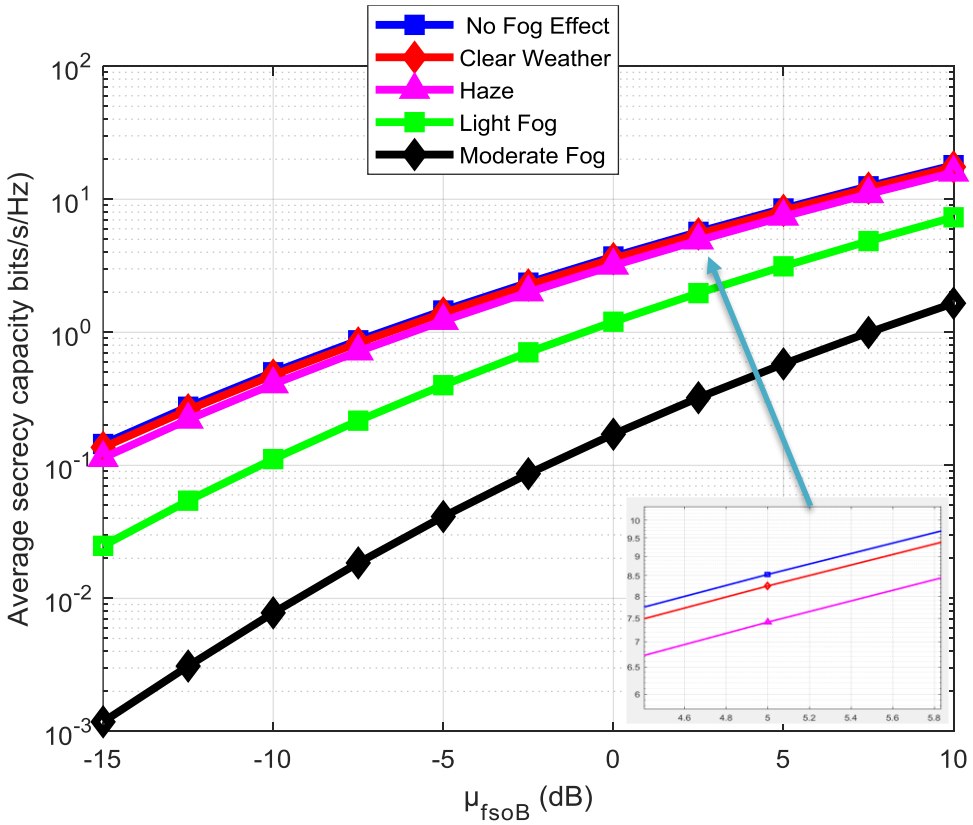

Figure 4.9. ASC under the influence of various foggy weather conditions with of ψ = 6.7, and moderate turbulence.

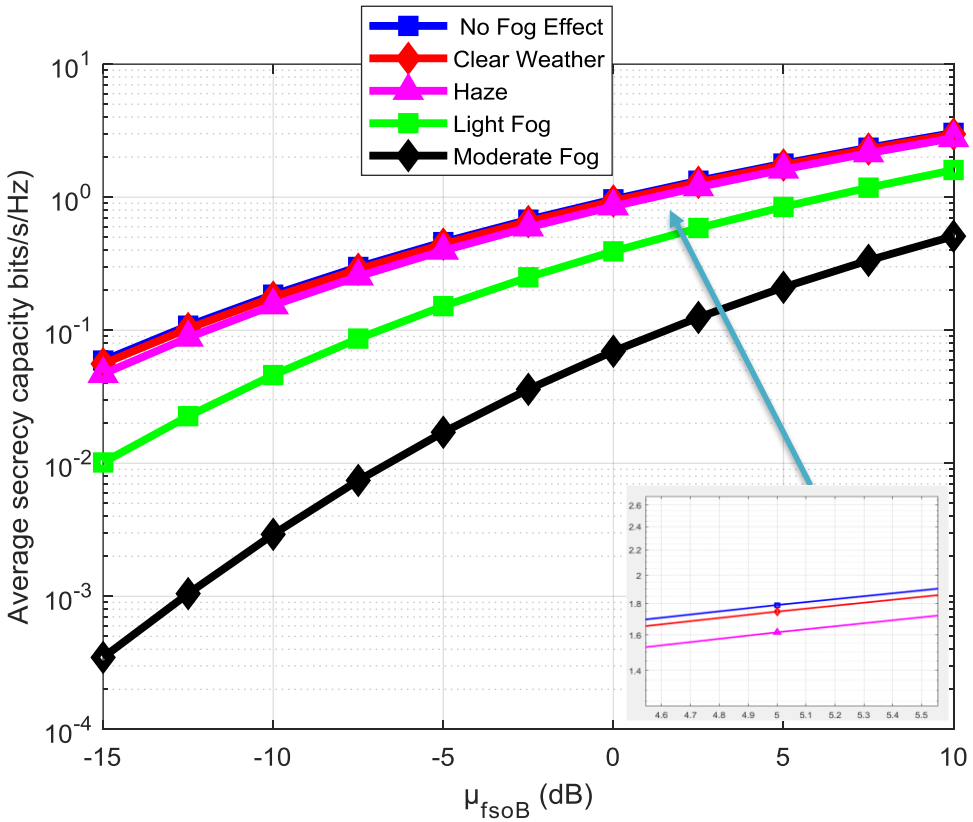

Figure 4.10. ASC under the influence of various foggy weather conditions with of ψ = 6.7, and strong turbulence.

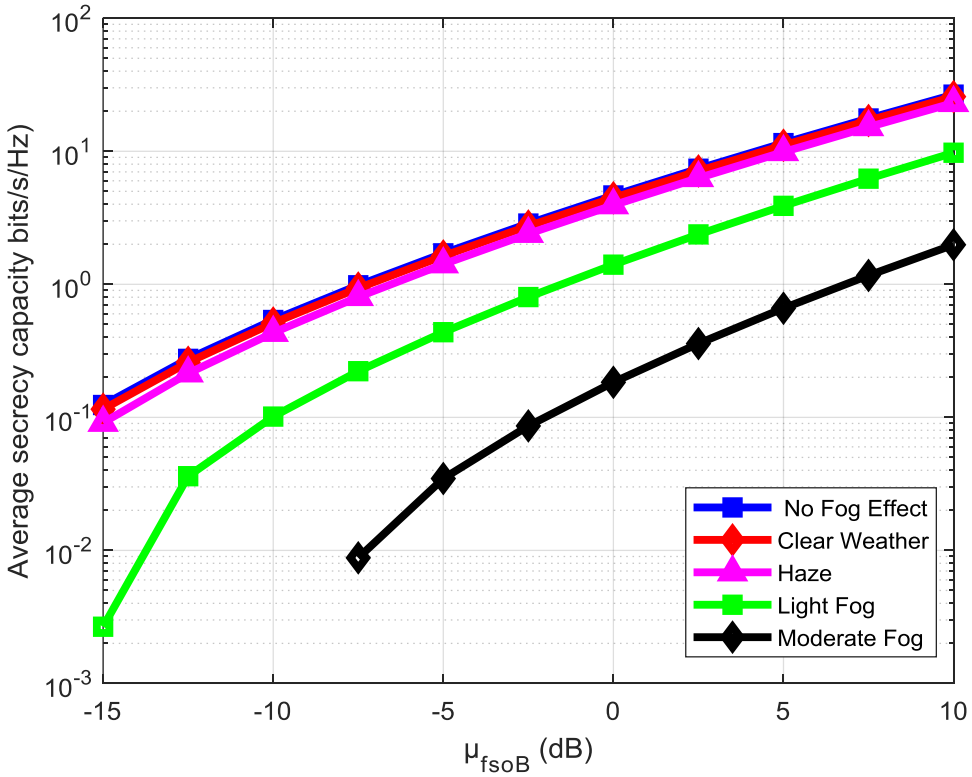

Figure 4.11. ASC under the influence of various foggy weather conditions with of ψ = 1, and weak turbulence.

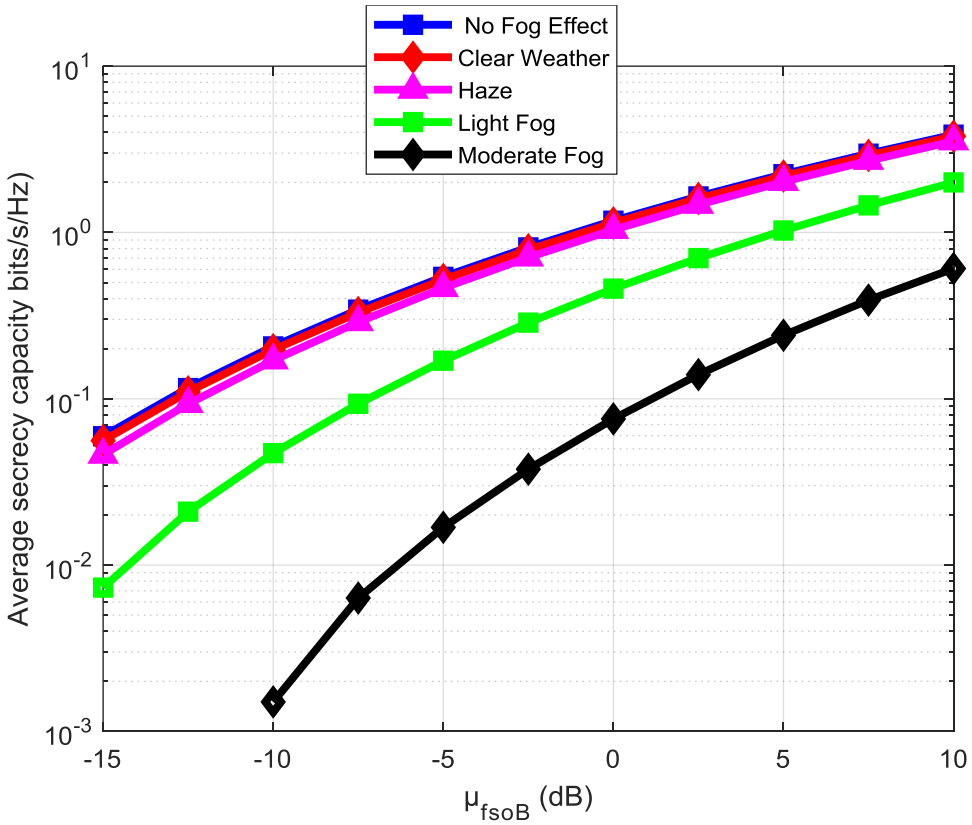

Figure 4.12. ASC under the influence of various foggy weather conditions with of ψ = 1, and moderate turbulence.

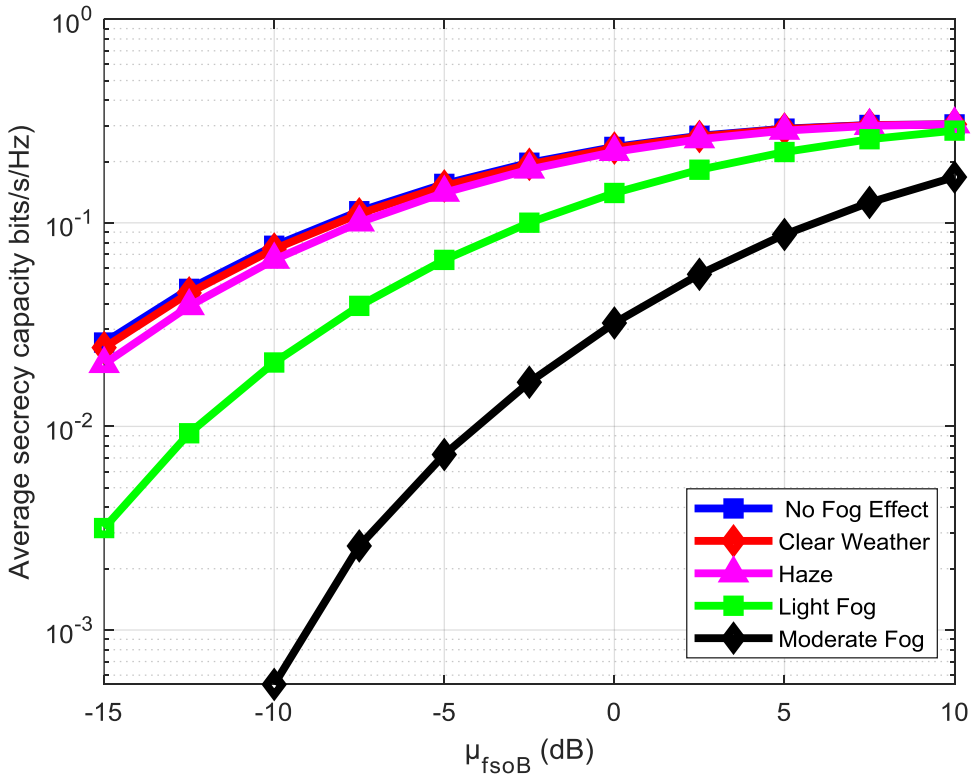

Figure 4.13. ASC under the influence of various foggy weather conditions with of ψ = 1, and strong turbulence.

4.3 SOP Performance Analysis of the FSO System

The SOP under high-value ψ=1 and low-value ψ=6.7 of pointing errors (zero boresights in this case) for various atmospheric turbulence conditions (weak to strong), as shown in Figures 4.14, 4.15, and 4.16 with selected values of the SNR of the wiretap channel of -10 dB, 0 dB, and 10 dB respectively. The results we obtained show that the increase in the SNR of the wiretap channel ($\mu_{fso,E}$) with the increased turbulence strength and effect of different pointing errors leads to further performance degradation of the FSO link, which led to an increase in the SOP of the FSO system. Whereas concerning the effect of the pointing errors, it is clear that the lower effect of pointing errors, the lower the SOP of the system. Thus, it improves the performance of the FSO system. From Figures 4.14, 4.15, and 4.16, it can be noticed that the FSO system gained 21.2 dB, 19.5 dB, 18 dB when the turbulence shifted from moderate to weak under negligible pointing

errors of ψ =6.7 with the SNR of the wiretap channel increased from -10 dB to 0 dB and then 10 dB, respectively, with SOP of 10^{-5}.

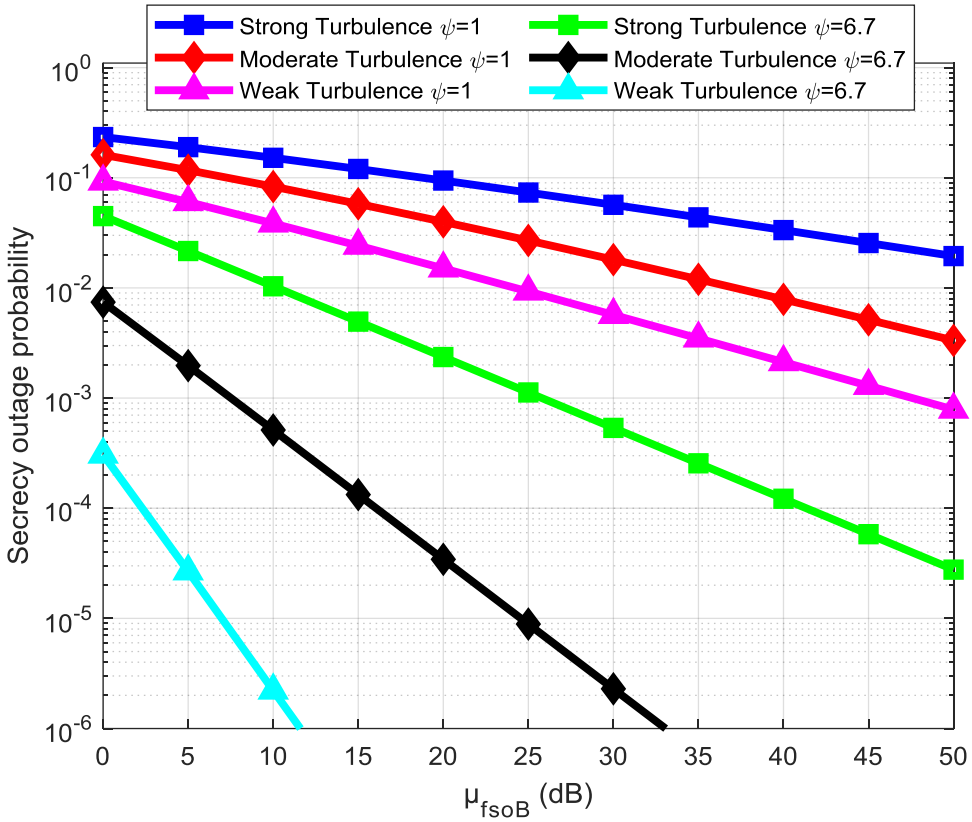

Figure 4.14. SOP Vs. The SNR of the Bob ($\mu_{fso,B}$) with a fixed SNR of the Eve ($\mu_{fso,E}$) $= -10$ dB, and $\psi = 1, \psi = 6.7$.

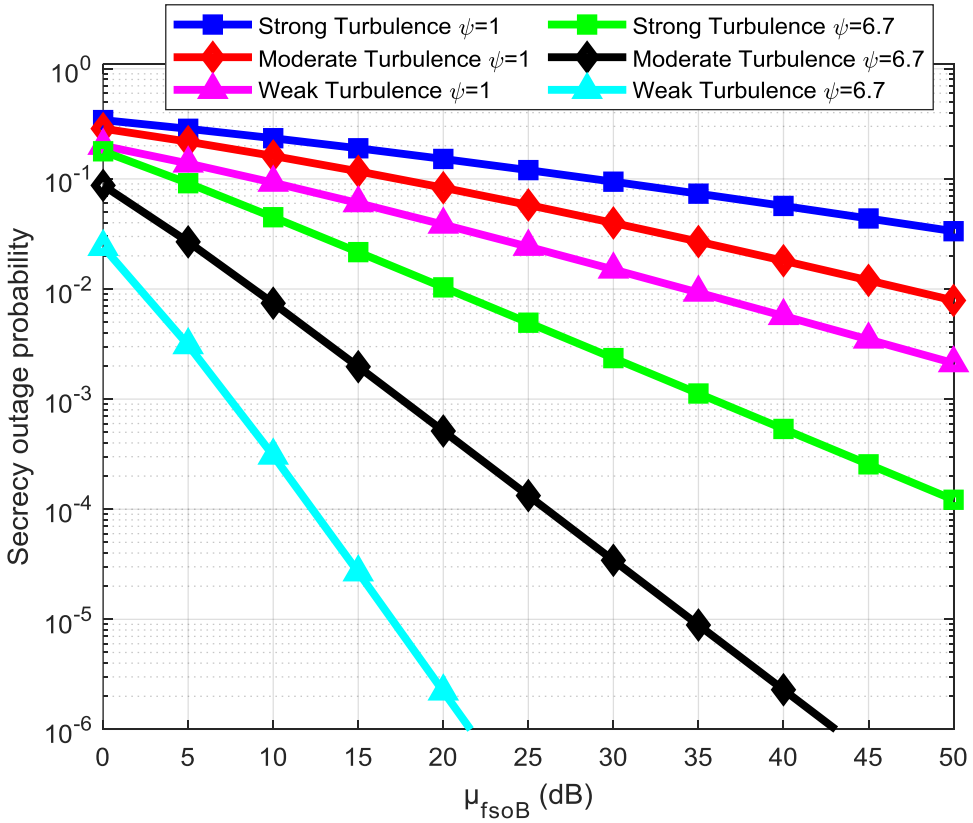

Figure 4.15. SOP Vs. The SNR of the Bob ($\mu_{fso,B}$) with a fixed SNR of the Eve ($\mu_{fso,E}$) = 0 dB, and $\psi = 1, \psi = 6.7$.

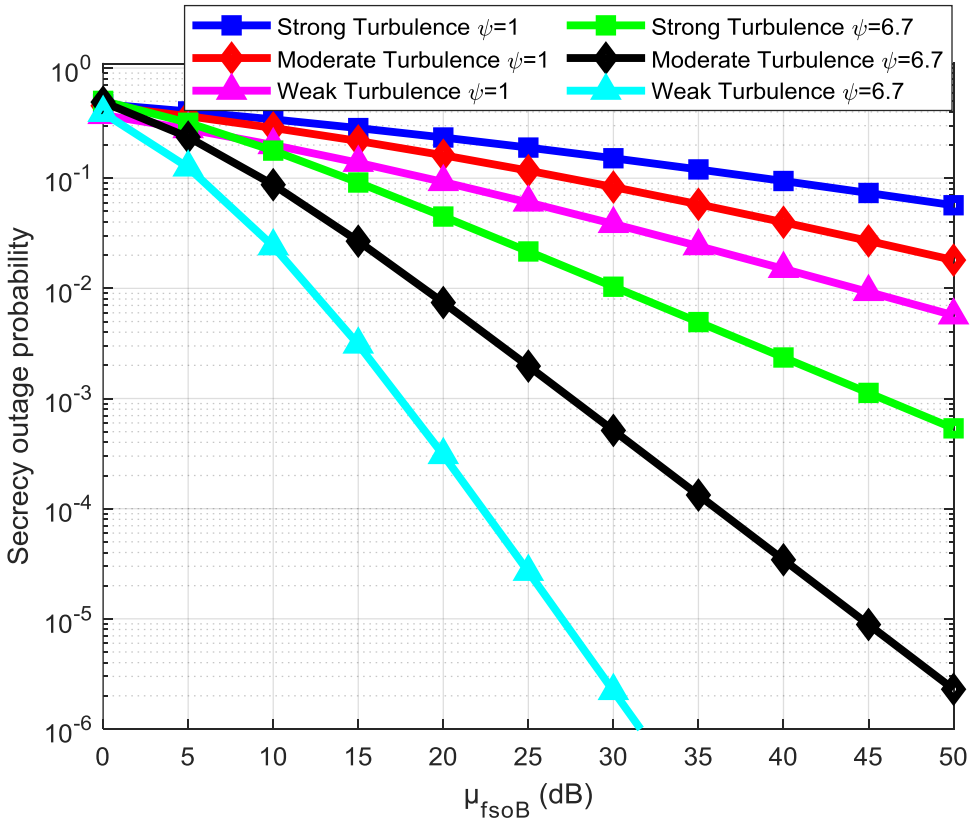

Figure 4.16. SOP Vs. The SNR of the Bob ($\mu_{fso,B}$) with a fixed SNR of the Eve ($\mu_{fso,E}$) = 10 dB, and $\psi = 1, \psi = 6.7$.

The effect of different pointing errors conditions on the SOP performance of the FSO system under moderate turbulence conditions in Figures 4.17 and 4.18 illustrate. In addition, the different SNR of the main and wiretap channel. Through the results, a significant improvement in system performance can be observed with the low pointing errors of ψ=6.7. On other hand, a significant deterioration in SOP performance is observed with the high pointing errors of ψ=1.

While the effect of different pointing errors conditions on SOP performance under strong turbulence conditions in Figures 4.19 and 4.20 show. In this case, the deterioration of the SOP performance is increased more as a result of two factors: the strong turbulence strength and the effect of high pointing errors. The reason behind that is the same as it was for the prior findings in Figure 4.4.

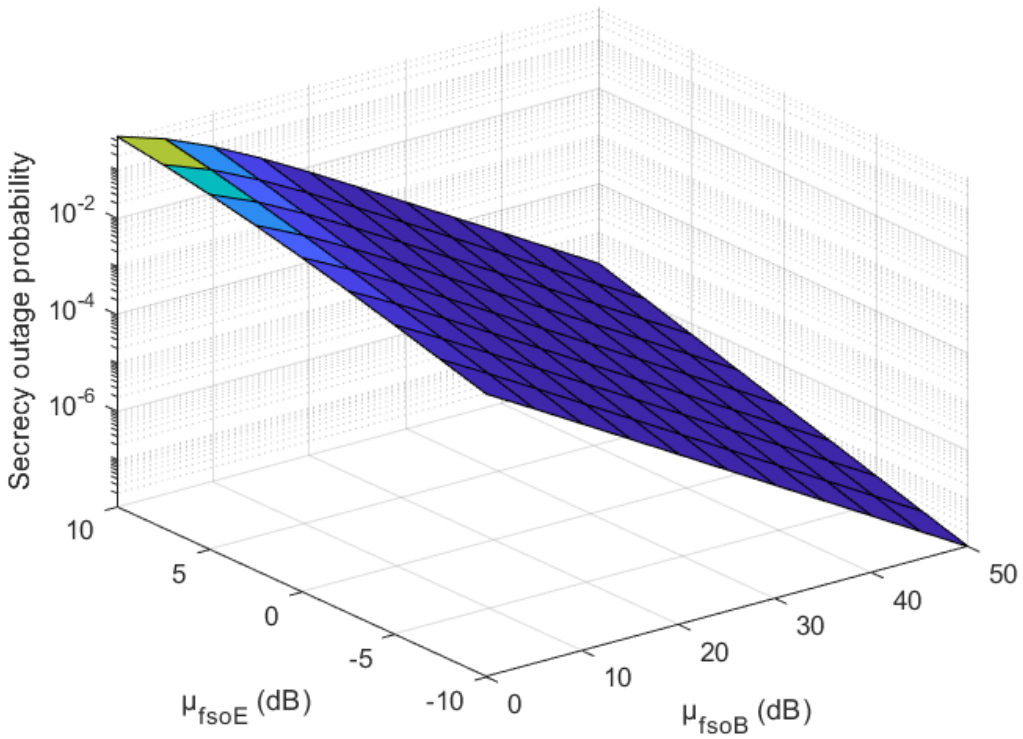

Figure 4.17. SOP Vs. The average SNR of the Bob ($\mu_{fso,B}$) and SNR of the Eve ($\mu_{fso,E}$) with the ψ = 6.7, under moderate turbulence.

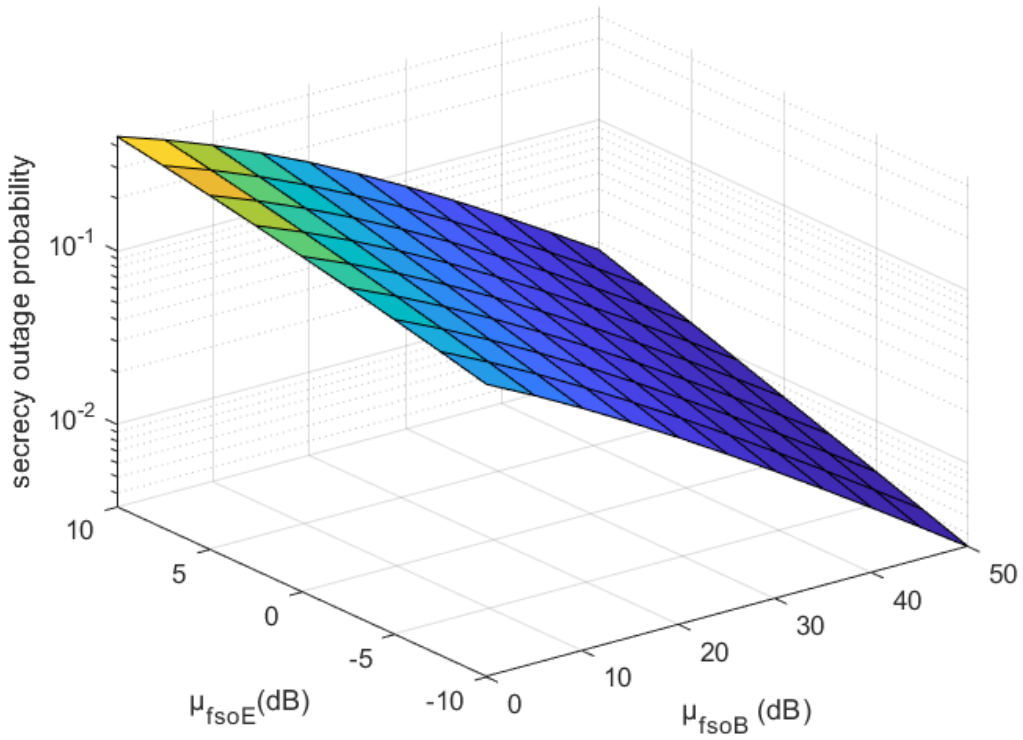

Figure 4.18. SOP Vs. The average SNR of the Bob ($\mu_{fso,B}$) and SNR of the Eve ($\mu_{fso,E}$) with the ψ = 1, under moderate turbulence.

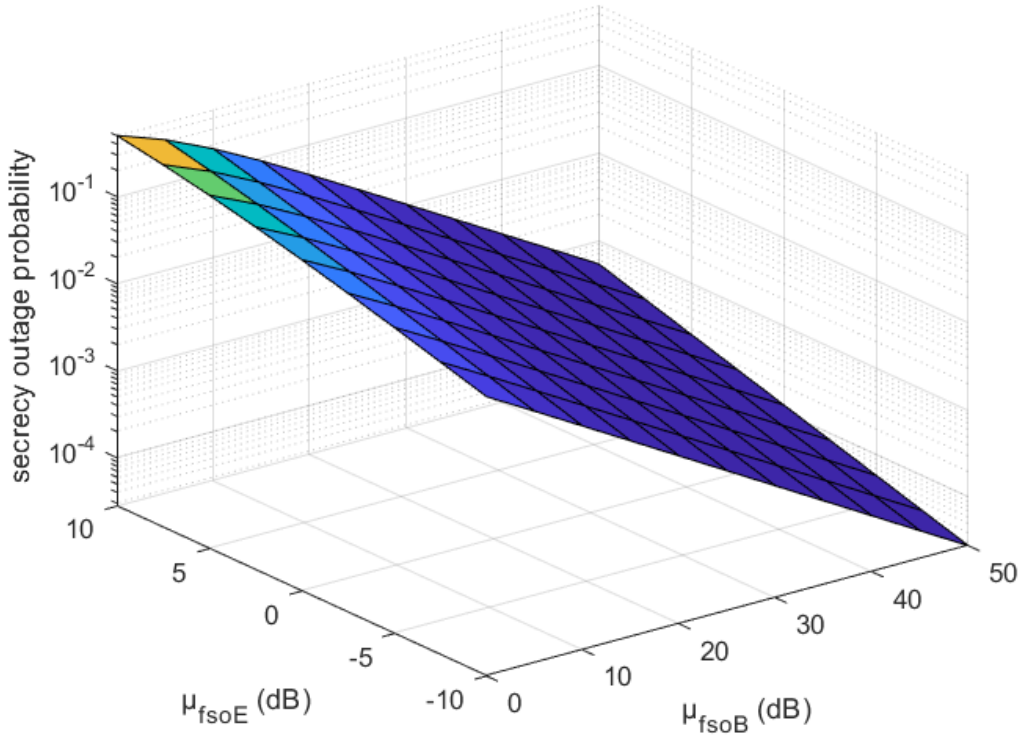

Figure 4.19. SOP Vs. The average SNR of the Bob ($\mu_{fso,B}$) and SNR of the Eve ($\mu_{fso,E}$) with the ψ = 6.7, under strong turbulence conditions.

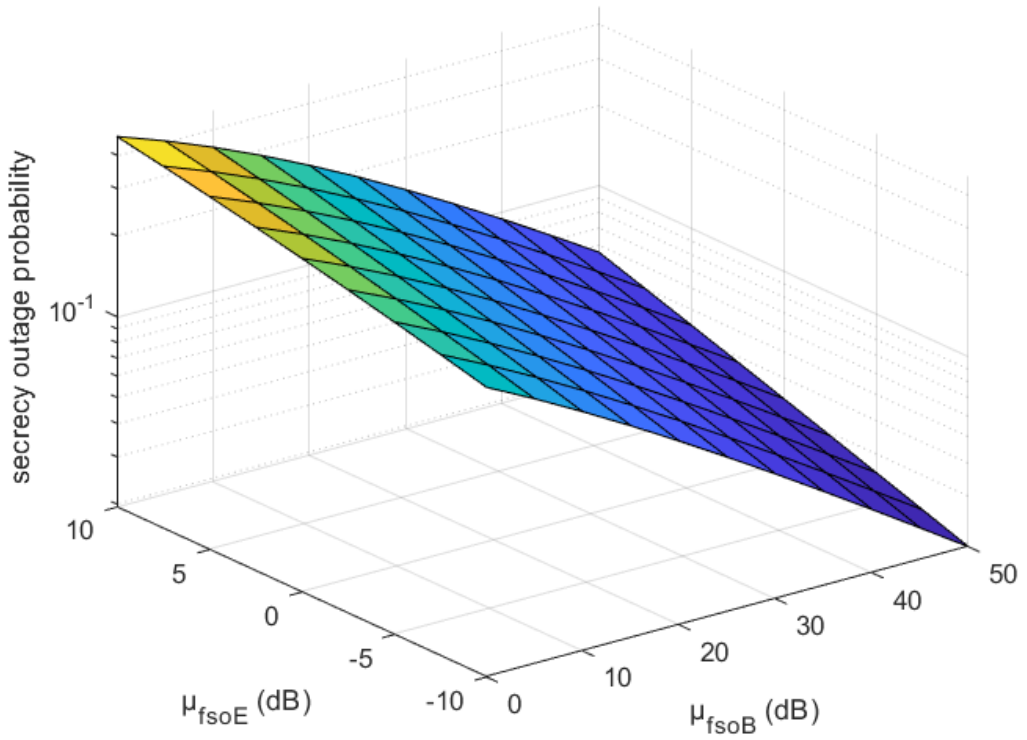

Figure 4.20. SOP Vs. The average SNR of the Bob ($\mu_{fso,B}$) and SNR of the Eve ($\mu_{fso,E}$) with the ψ = 1, under strong turbulence conditions.

The SOP performance under the effect of different turbulence conditions (weak to strong) in Figures 4.21, 4.22, and 4.23 illustrate, with varying non-zero boresight pointing errors conditions as ζ = (2.52, 1.3, 0.59), and SNR of the wiretap channel of -10 dB, 0 dB, and 10 dB, respectively. From the results, it can be observed that the effect of the non-zero boresight pointing errors is worse in comparison with the effect of zero boresight pointing errors. The reason was mentioned earlier, which in turn gives the eavesdropper a greater chance to eavesdrop on confidential information through the main link under severe pointing errors conditions.

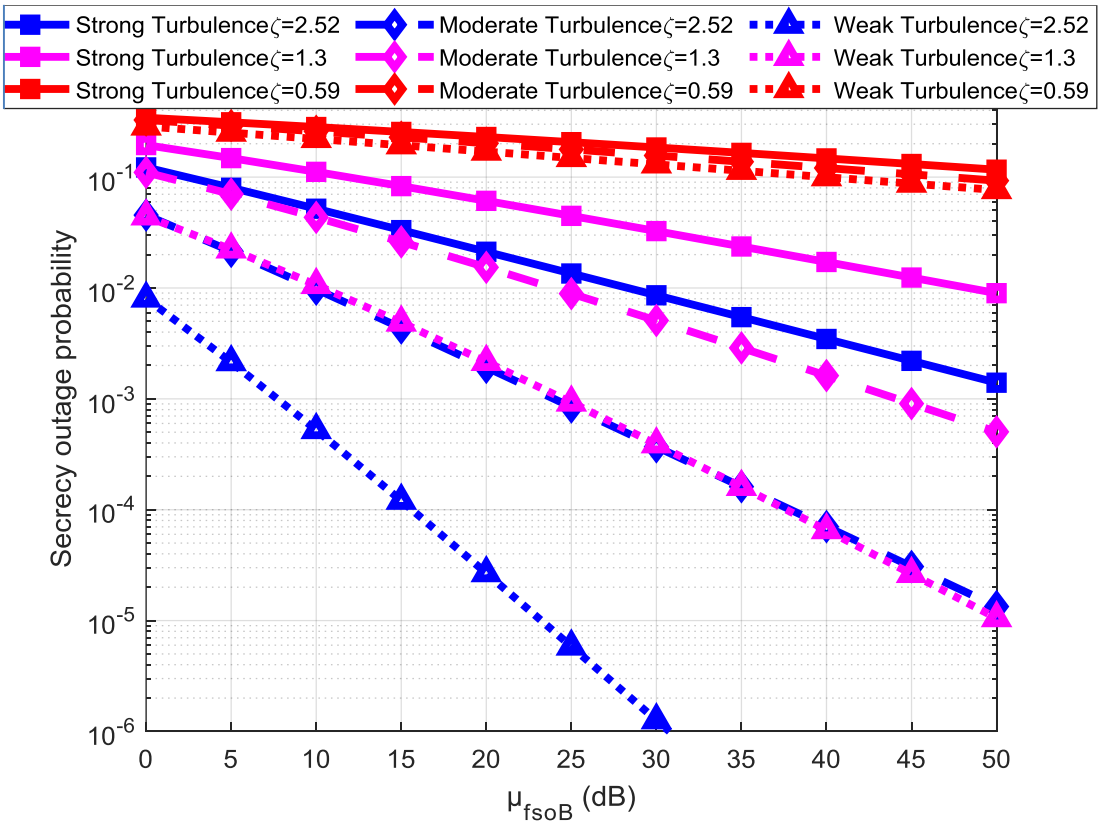

Figure 4.21. SOP Vs.The average SNR of the Bob ($\mu_{fso,B}$) with the SNR of the Eve ($\mu_{fso,E}$) = −10 dB.

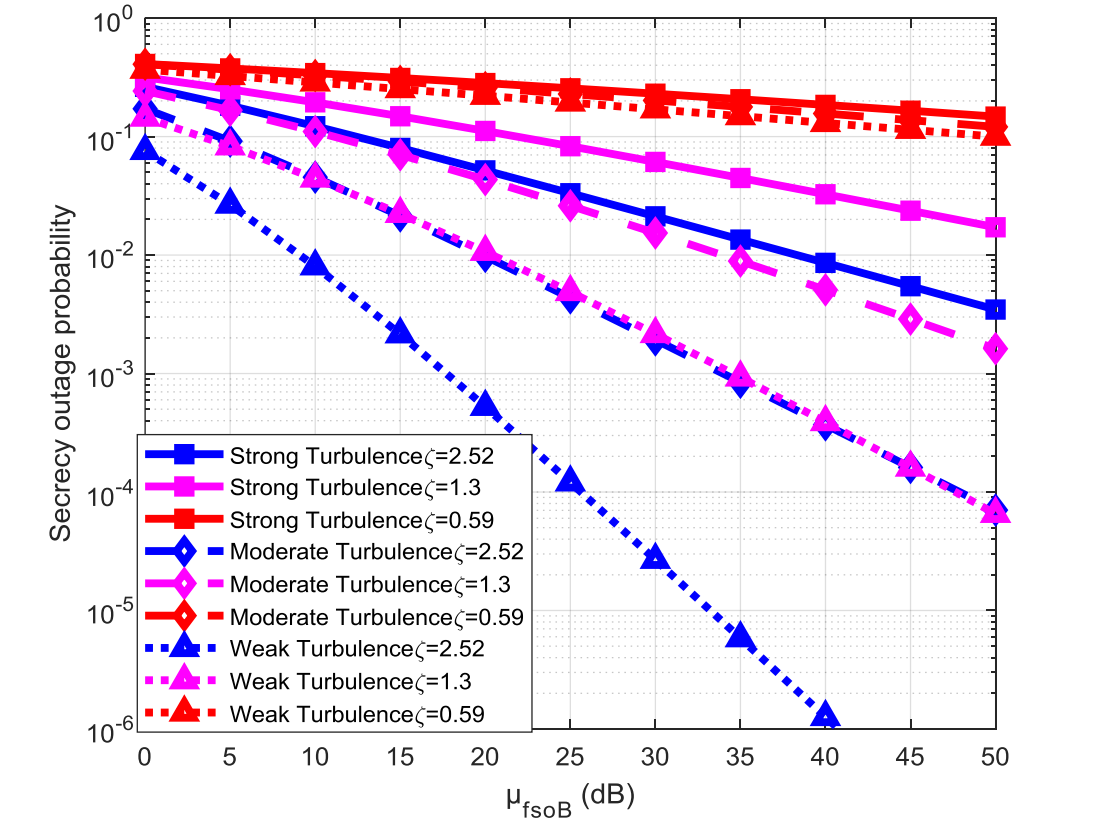

Figure 4.22. SOP Vs.The average SNR of the Bob ($\mu_{fso,B}$) with the SNR of the Eve ($\mu_{fso,E}$) = 0 dB.

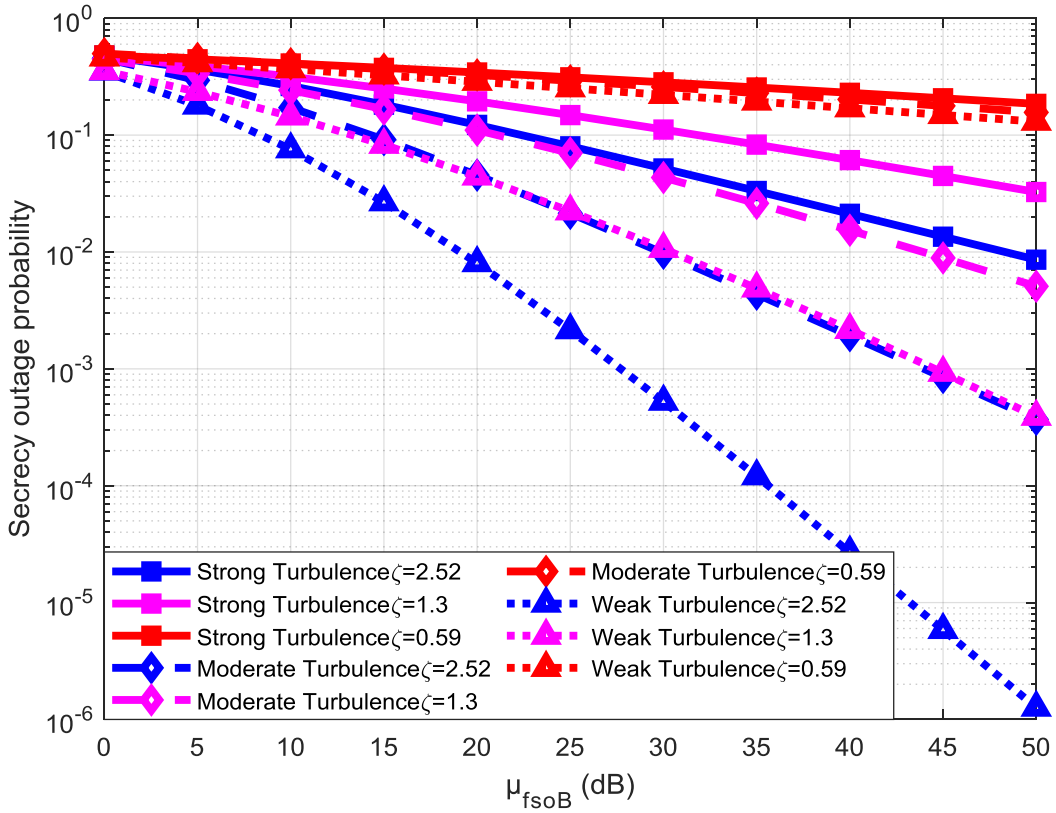

Figure 4.23. SOP Vs. The average SNR of the Bob ($\mu_{fso,B}$) with the SNR of theEve ($\mu_{fso,E}$) = 10 dB.

The SOP versus the average SNR of the main channel $\mu_{fso,B}$ for moderate turbulence conditions under different foggy weather conditions in Figure 4.24 show, with pointing errors of ψ=1 and ψ=6.7. From the results, the effect of fog can be observed, as the increased intensity of the fog leads to an increase in the attenuation intensity, and therefore the SOP of the FSO system is increased. However, the performance of the SOP of the FSO system is improved with the decreased intensity of the fog and the SNR of the main channel is increased underψ=6.7 due to the high power received by the FSO receiver. It can be shown that the FSO system lose about 0.5, 1, 8, and 16 dB when the foggy weather shifted from no fog to clear, haze, light, moderate, and heavy fog weather respectively with ψ=6.7 and SOP of 10^{-6}.

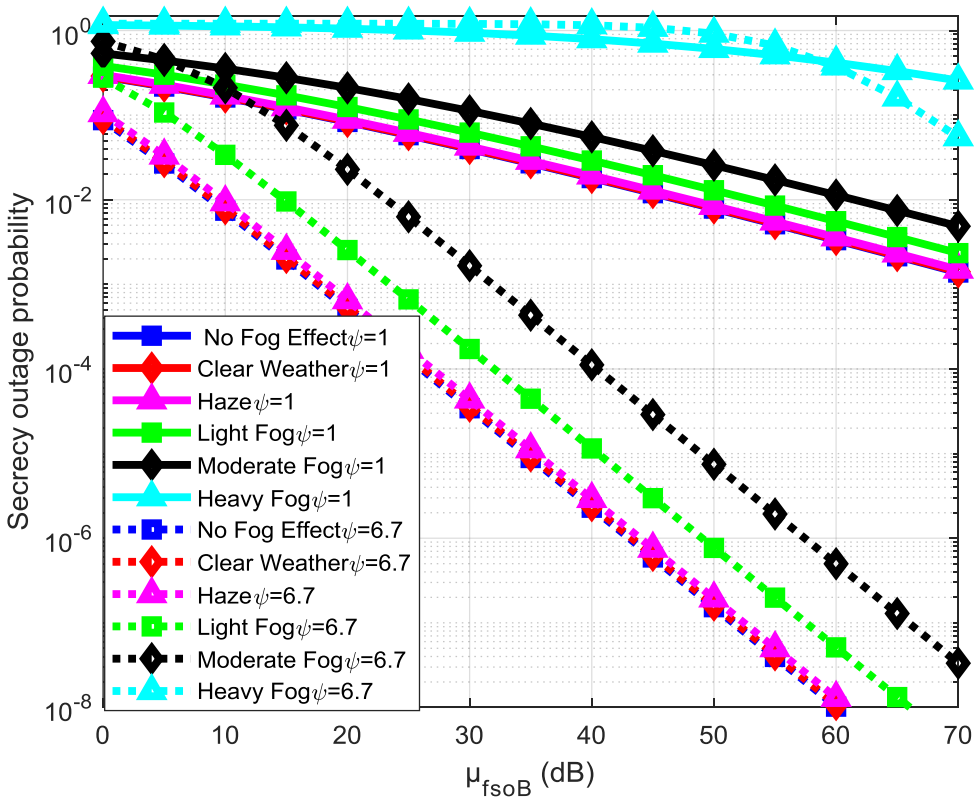

Figure 4.24. SOP under different foggy weather conditions , moderate turbulence, and ψ=6.7, ψ=1.

The SOP of the FSO system as a function of the distance between the transmitter and legal receiver of the FSO system in Figure 4.25 shows, under different foggy weather conditions with $\mu_{fso,E}$ =10 dB and pointing errors of ψ=6.7. From the results, it can be seen that the increase in the FSO link's distance with increased intensity of the fog, led to a decrease in the visibility of the link. Thus, an increased attenuation. However, the best SOP performance is obtained under no fog, clear weather and haze conditions across different distances as the range of vision are the best in these two cases, while under other foggy weather conditions the SOP performance is start to degrade. It is also can be noted the worse SOP performance observed is under heavy fog weather conditions as expected.

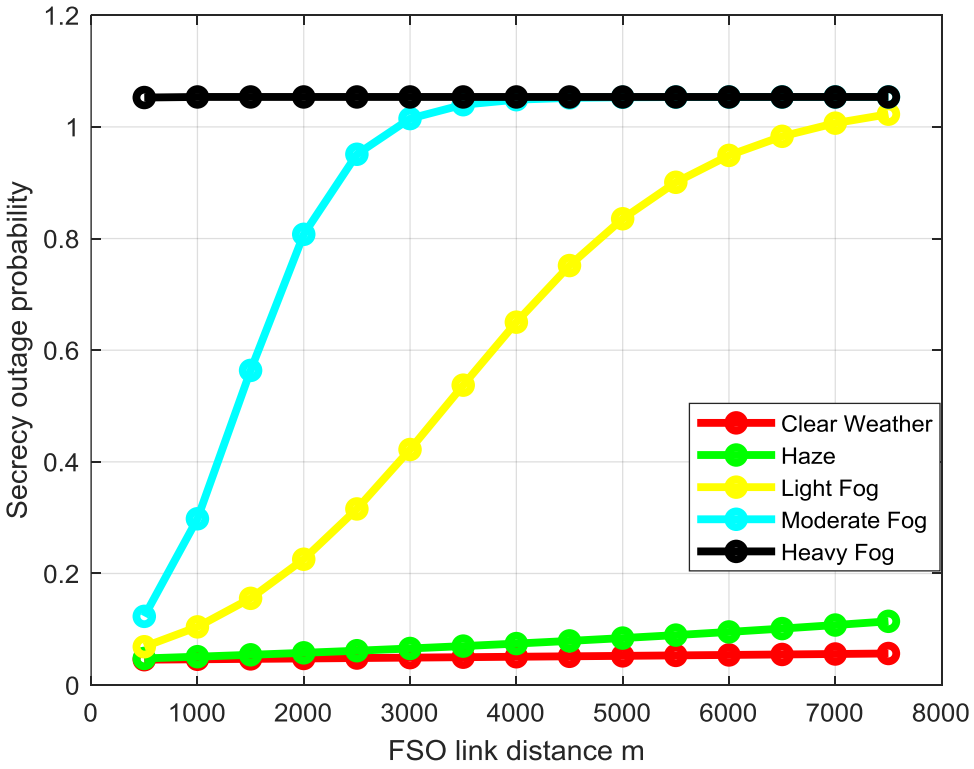

Figure 4.25. SOP Vs. The FSO link distance.

4.4 SPSC Performance Analysis of the FSO System

The SPSC performance as a function with SNR of the main channel under moderate turbulence and the effect of different values of the amount of scattering power coupled to the LOS component ρ, as in Figure 4.26 shown. We can be observed from the results that the SPSC performance improves with an increase in the scattering power values coupled to the LOS component where the turbulence intensity decreases.

While the SPSC performance under weak turbulence for scattering power of ρ= 0.99 as shown in Figures 4.27 and 4.28, a better secrecy performance can be achieved in comparison with the case of scattering power of ρ = 0.75. Thus, we can conclude that the decrease in scattering power coupled with the LOS component leads to a deterioration in general SPSC performance for the FSO system.

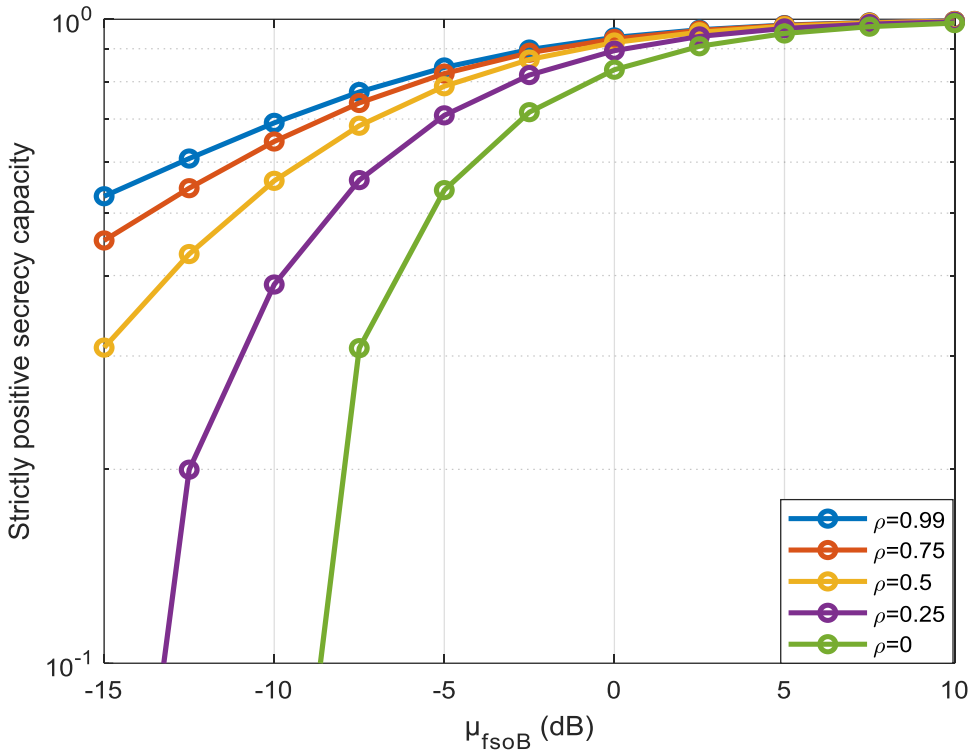

Figure 4.26. SPSC under different values of scattering power ρ.

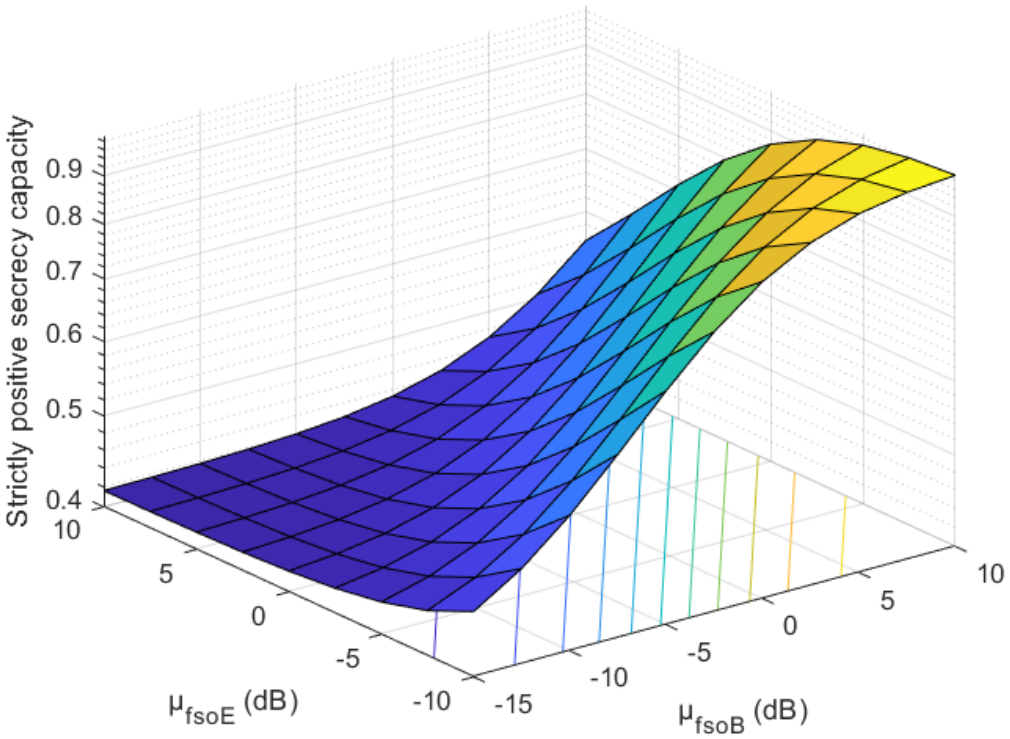

Figure 4.27. SPSC Vs. The average SNR of the Bob ($\mu_{fso,B}$)and SNR of the Eve ($\mu_{fso,E}$) with of ρ= 0.99.

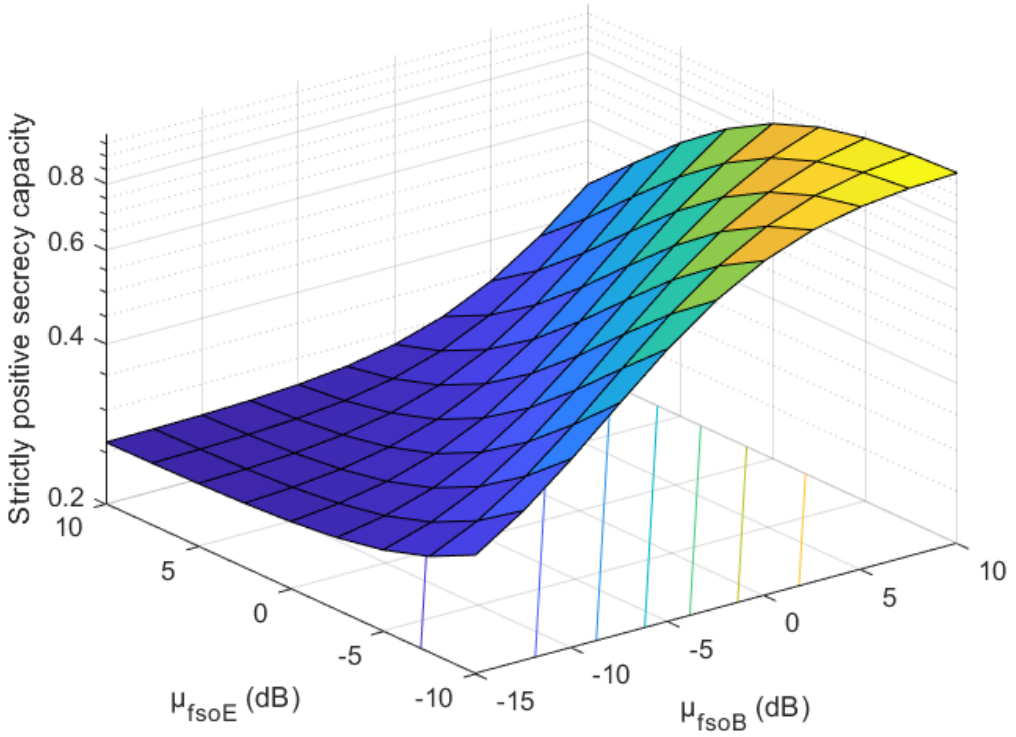

Figure 4.28. SPSC Vs. The average SNR of the Bob ($\mu_{fso,B}$) and SNR of the Eve ($\mu_{fso,E}$) with of ρ= 0.75.

The effect of different foggy weather conditions on the SPSC performance of the FSO system under weak turbulence with consideration of selected values of pointing errors as ψ =1 and ψ =6.7 as shown in Figure 4.29. Through the results, it can be seen that increasing the strength of foggy weather under high pointing errors of ψ =1 led to significant degradation in the SPSC performance of the FSO system. On the other hand, when the intensity of the fog decreased under low the effects of the pointing errors of ψ =6.7, better SPSC performance can be obtained in comparison with the case of ψ =1.

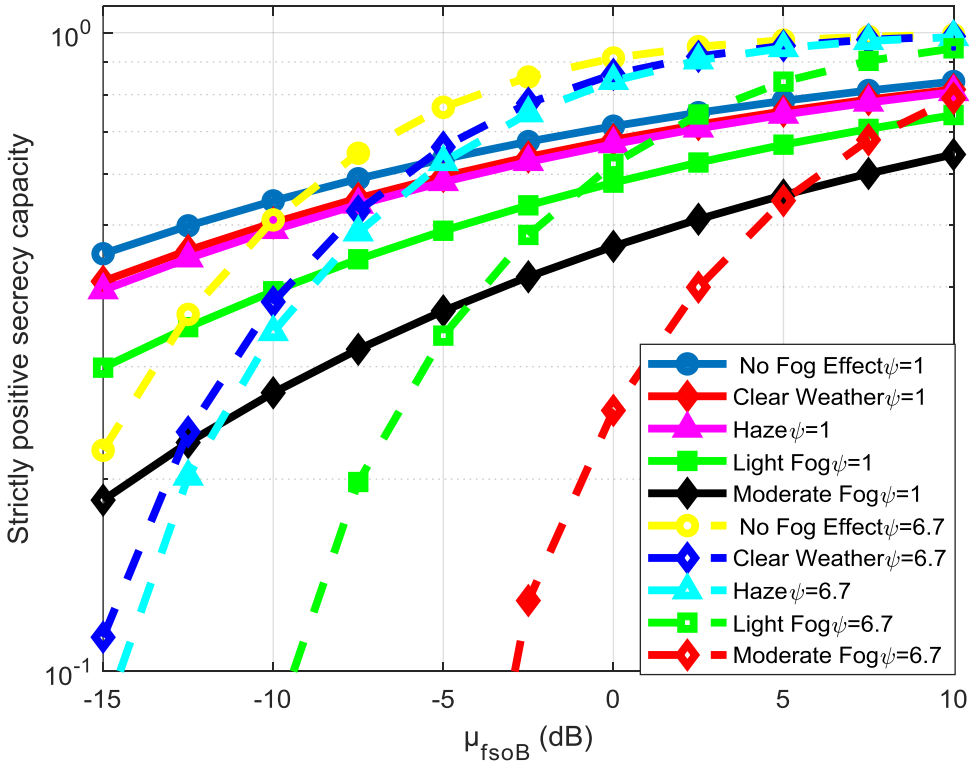

Figure 4.29. SPSC versus the SNR of the Bob ($\mu_{fso,B}$) under different conditions of foggy weather.

CHAPTER FIVE
CONCLUSION AND FUTURE WORKS

5.1 Conclusion

In this thesis, we presented closed-form expressions for the ASC, SOP, and SPSC secrecy performance metrics for FSO systems over a generalized Malaga–M distribution turbulence channel and using IM/DD detection technology. To provide an accurate and comprehensive analysis of the performance of the security properties for FSO communication systems, we evaluate the secrecy performance metrics under different atmospheric turbulence conditions, pointing errors components, and foggy weather conditions with the effect of different fog densities. It can be concluded from the results of this work that, the increasing of the atmospheric turbulence strengths and/or increasing the pointing errors degrade the secrecy performance of the considered FSO system in general. The reason behind that is due to the improvement of the eavesdropper link's quality with increasing of the value SNR for wiretap channel. The main conclusion of this work can be listed as follows:

1- The ASC of the system is improved with decreasing turbulence conditions where the ASC increased to 10 bit/s/Hz under moderate turbulence and raised to 40 bit/s/Hz under weak turbulence in comparison with 2.5 bit/s/Hz under strong turbulence .

2- The SOP performance of the considered system is increased with the increase of the SNR for the wiretap channel. It can be noticed that the FSO system gained 21.2 dB, 19.5 dB, 18 dB when the turbulence shifted from moderate to weak.

3- The performance of SPSC of the FSO system improved with the increase in the amount of scattering power coupled with LOS where SPSC is decreased to 0.3 under ρ = 0, then improves to 0.7 under ρ = 0.99.

4- In general, the non-zero boresight pointing errors had a more negative impact on the secrecy performance of the system in comparison with the zero boresight pointing errors.

5- The non-zero boresight pointing errors had a deeply negative impact on the ASC performance of the considered system. Whereat χ=2.52 the system achieved ASC of (23, 7, and 2 bit/s/Hz) under weak, moderate, and strong turbulence conditions respectively. Compared to a better performance of the ASC under the influence of zero boresight pointing errors.

6- In general, the SOP increased with the increase of the effect of the pointing errors, the non-zero boresight pointing errors had a significant deterioration on the secrecy performance of the FSO system. Where it can be noticed the FSO system gained 16 dB under weak turbulence with $\mu_{fso,E}$ =10 dB. While the system gained 17 dB and 18 dB with $\mu_{fso,E}$ = 0 dB and $\mu_{fso,E}$ = -10 dB respectively.

7-The foggy weather condition had the worst impact on the secrecy performance of the FSO system, like the following:

a. Foggy weather effect can be observed on the ASC performance, where the degradation begins slowly and then accelerates as the fog severity rises. Thus, the system achieves an ASC of up to (3.5 and 0.1 bit/s/Hz) for clear weather, and moderate fog, respectively. On the other hand, the

SOP increases and SPSC decrease with the increase in the severity of fog intensity.

b. Foggy weather effect can be observed on the SOP performance, where the FSO system loses about 0.5, 1, 8, and 16 dB when the foggy weather shifts from no fog to clear, haze, light fog, moderate fog, and heavy foggy weather respectively.

c. It appeared from the results that the increase in distance of the FSO link with increasing intensity of the fog led to deteriorating the SOP performance of the FSO system.

5.2 Future Works

We can propose the following recommendations for the open topics that will help in developing the physical layer security in FSO systems in this section:

1- This work proposes a secrecy performance evaluation of the hybrid (RF/FSO) system under various weather conditions, as well as variation distance between RF/FSO links

2- This work proposes to perform a comparison of our proposed system in this thesis with the same system and parameters, but experimentally on the ground to study the difference between the two systems.

3- Increasing the secrecy rate by optimizing the beamforming vectors at relays in mixed RF/FSO systems. The optimization problem may depend on the distribution of RF and the distribution of the legal users and eavesdroppers.

4- Investigating in the PLS of the hybrid RF/FSO systems, in which many eavesdroppers can target either the RF or the FSO link, or both links at the same time.

5- Securing the newly developing non-orthogonal multiple access (NOMA) techniques in FSO systems is still an open topic. We suggest the study PLS in NOMA-FSO based systems. Because of the specific characteristics of FSO systems, it is necessary to optimize and characterize the PLS in NOMA-FSO based systems.

REFERENCES

[1] Ghassemlooy, Z., Popoola, W., & Rajbhandari, S. (2019). *Optical wireless communications: system and channel modelling with Matlab®*. CRC press.

[2] Khalighi, M. A., & Uysal, M. (2014). Survey on free space optical communication: A communication theory perspective. *IEEE communications surveys & tutorials*, *16*(4), 2231-2258.

[3] Uysal, M., Capsoni, C., Ghassemlooy, Z., Boucouvalas, A., & Udvary, E. (2016). Optical wireless communications. *Switzerland: springer*, 107-122.

[4] Obeed, M., Salhab, A. M., Alouini, M. S., & Zummo, S. A. (2018, November). Survey on physical layer security in optical wireless communication systems. In *2018 Seventh International Conference on Communications and Networking (ComNet)* (pp. 1-5). IEEE.

[5] Jahid, A., Alsharif, M. H., & Hall, T. J. (2020). A Contemporary Survey on Free Space Optical Communication: Potential, Technical Challenges, Recent Advances and Research Direction. *arXiv preprint arXiv: 2012.00155*.

[6] Borah, D. K., & Voelz, D. G. (2009). Pointing error effects on free-space optical communication links in the presence of atmospheric turbulence. *Journal of Lightwave Technology*, *27*(18), 3965-3973.

[7] Yang, F., Cheng, J., & Tsiftsis, T. A. (2014). Free-space optical communication with nonzero boresight pointing errors. *IEEE Transactions on Communications*, *62*(2), 713-725.

[8] Al-Habash, A., Andrews, L. C., & Phillips, R. L. (2001). Mathematical model for the irradiance probability density function of a laser beam propagating through turbulent media. *Optical engineering*, *40*(8), 1554-1562.

[9] Zhu, X., & Kahn, J. M. (2002). Free-space optical communication through atmosphericturbulence channels. *IEEE Transactions on communications*, *50*(8), 1293-1300.

[10] Andrews, L. C., & Phillips, R. L. (1998). Laser Beam Propagation Through Random Media (Bellingham, WA: SPIE Optical Engineering Press).

[11] Jurado-Navas, A., Garrido-Balsells, J. M., Paris, J. F., Puerta-Notario, A., & Awrejcewicz, J. (2011). A unifying statistical model for atmospheric optical scintillation. *Numerical simulations of physical and engineering processes*, *181*(8), 181-205 ch 8.

[12] Lopez-Martinez, F. J., Gomez, G., & Garrido-Balsells, J. M. (2015). Physical-layer security in free-space optical communications. *IEEE Photonics Journal*, *7*(2), 1-14.

[13] Sun, X., & Djordjevic, I. B. (2016). Physical-layer security in orbital angular momentum multiplexing free-space optical communications. *IEEE Photonics Journal*, *8*(1), 1-10.

[14] Saber, M. J., & Sadough, S. M. S. (2017). On secure free-space optical communications over Málaga turbulence channels. *IEEE Wireless Communications Letters*, *6*(2), 274-277.

[15] Monteiro, M. E. P., Rebelatto, J. L., Souza, R. D., & Brante, G. (2018). Maximum secrecy throughput of MIMOME FSO communications with outage constraints. *IEEE Transactions on Wireless Communications*, *17*(5), 3487-3497.

[16] Ai, Y., Mathur, A., Verma, G. D., Kong, L., & Cheffena, M. (2020). Comprehensive physical layer security analysis of FSO communications over Málaga channels. *IEEE Photonics Journal*, *12*(6), 1-17.

[17] Zhou, X., Song, L., & Zhang, Y. (Eds.). (2013). *Physical layer security in wireless communications*. Crc Press.

[18] Obeed, M., & Mesbah, W. (2018). Efficient algorithms for physical layer security in two-way relay systems. *Physical Communication*, *28*, 78-88.

[19] Massey, J. L. (1988). An introduction to contemporary cryptology. *Proceedings of the IEEE*, *76*(5), 533-549.

[20] Wyner, A. D. (1975). The wire- tap channel. *Bell system technical journal*, *54*(8), 1355-1387.

[21] Andrews, L. C., Phillips, R. L., Hopen, C. Y., & Al-Habash, M. A. (1999). Theory of optical scintillation. *JOSA A*, *16*(6), 1417-1429.

[22] Eghbal, M., & Abouei, J. (2014). Security enhancement in free-space optics using acousto-optic deflectors. *Journal of Optical Communications and Networking*, *6*(8), 684-694.

[23] Paul, P., Bhatnagar, M. R., & Jaiswal, A. (2019). Jamming in free space optical systems: Mitigation and performance evaluation. *IEEE Transactions on Communications*, *68*(3), 1631-1647.

[24] Endo, H., Han, T. S., Aoki, T., & Sasaki, M. (2015). Numerical study on secrecy capacity and code length dependence of the performances in optical wiretap channels. *IEEE Photonics Journal*, *7*(5), 1-18.

[25] Endo, H., Fujiwara, M., Kitamura, M., Ito, T., Toyoshima, M., Takayama, Y., & Sasaki, M. (2016). Free-space optical channel estimation for physical layer security. *Optics express*, *24*(8), 8940-8955.

[26] Pan, X., Ran, H., Pan, G., Xie, Y., & Zhang, J. (2019). On secrecy analysis of DF based dual hop mixed RF-FSO systems. *IEEE Access*, *7*, 66725-66730.

[27] Pattanayak, D. R., Dwivedi, V. K., & Karwal, V. (2020). Physical layer security of a two way relay based mixed FSO/RF network in the presence of multiple eavesdroppers. *Optics Communications*, *463*, 125429.

[28] Fujiwara, M., Ito, T., Kitamura, M., Endo, H., Tsuzuki, O., Toyoshima, M., & Sasaki, M. (2018). Free-space optical wiretap channel and experimental secret key agreement in 7.8 km terrestrial link. *Optics express*, *26*(15), 19513-19523.

[29] Endo, H., Fujiwara, M., Kitamura, M., Tsuzuki, O., Ito, T., Shimizu, R., & Sasaki, M. (2018). Free space optical secret key agreement. *Optics express*, *26*(18), 23305-23332.

[30] Legre, M., Huttner, B., & SA, I. Q. (2017, September). Quantum-enhanced physical layer cryptography: A new paradigm for free-space key distribution. In *7th International Conference on Quantum Cryptography (QCRYPT)*.

[31] Zou, D., & Xu, Z. (2016). Information security risks outside the laser beam in terrestrial free-space optical communication. *IEEE Photonics Journal*, *8*(5),1-9.

[32] Zhu, J., Chen, Y., & Sasaki, M. (2016, January). Average secrecy capacity of free-space optical communication systems with on-off keying modulation and threshold detection. In *2016 International Symposium on Information Theory and Its Applications (ISITA)* (pp. 616-620). IEEE.

[33] Wang, T. L., Gariano, J. A., & Djordjevic, I. B. (2018). Employing Bessel-Gaussian beams to improve physical-layer security in free-space optical communications. *IEEE Photonics Journal*, *10*(5), 1-13.

[34] Wang, T. L., & Djordjevic, I. B. (2018). Physical-layer security of a binary data sequence transmitted with Bessel–Gaussian beams over an optical wiretap channel. *IEEE Photonics Journal*, *10*(6), 1-11.

[35] Huang, Q., Liu, D., Chen, Y., Wang, Y., Tan, J., Chen, W., & Zhu, N. (2018). Secure free-space optical communication system based on data fragmentation multipath transmission technology. *Optics express*, *26*(10), 13536-13542.

[36] Boluda-Ruiz, R., Castillo-Vázquez, C., Castillo-Vázquez, B., García-Zambrana, A., & Qaraqe, K. (2018, August). On the average secrecy capacity for FSO wiretap channels with nonzero boresight pointing errors. In *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)* (pp. 1-5). IEEE.

[37] Boluda-Ruiz, R., García-Zambrana, A., Castillo-Vázquez, B., & Qaraqe, K. (2019). Secure communication for FSO links in the presence of eavesdropper with generic location and orientation. *Optics express*, *27*(23), 34211-34229.

[38] Boluda-Ruiz, R., & Qaraqe, K. (2019, April). Effect of misalignment error on secrecy outage capacity of FSO communication links. In *2019 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 1-7). IEEE.

[39] Trinh, P. V., Carrasco-Casado, A., Pham, A. T., & Toyoshima, M. (2020). Secrecy analysis of FSO systems considering misalignments and eavesdropper's location. *IEEE Transactions on Communications*, *68*(12), 7810-7823.

[40] Boluda-Ruiz, R., Tokgoz, S. C., García-Zambrana, A., & Qaraqe, K. (2020). Enhancing Secrecy Capacity in FSO Links via MISO Systems Through Turbulence-Induced Fading Channels With Misalignment Errors. *IEEE Photonics Journal*, *12*(4), 1-13.

[41] Verma, G. D., Mathur, A., Ai, Y., & Cheffena, M. (2021). Secrecy performance of FSO communication systems with non- zero boresight pointing errors. *IET Communications*.

[42] Wells, J. (2009). Faster than fiber: The future of multi-G/s wireless. *IEEE microwave magazine*, *10*(3), 104-112.

[43] Stotts, L. B., Andrews, L. C., Cherry, P. C., Foshee, J. J., Kolodzy, P. J., McIntire, W. K., & Young, D. W. (2009). Hybrid optical RF airborne communications. *Proceedings of the IEEE*, *97*(6), 1109-1127.

[44] Forin, D. M., Teixeira, A. L. J., Geiger, B., Leitgeb, E., Nadeem, F., Incerti, G., & Andre, P. D. B. (2010). *Free space optical technologies* (p. 257). IntechOpen.

[45] Chan,V. W. (2006). Free-space optical communications. *Journal of Lightwave technology*, *24*(12), 4750-4762.

[46] Wu, Y., Khisti, A., Xiao, C., Caire, G., Wong, K. K., & Gao, X. (2018). A survey of physical layer security techniques for 5G wireless networks and challenges ahead. *IEEE Journal on Selected Areas in Communications*, *36*(4), 679-695.

[47] Agnello, G. (1963). Le torri costiere di Siracusa nella lotta anticorsara Archivio storico di Siracusa, Vol I-IV, p.25, Siracusa, Italy.

[48] Jagdishprasadsingh, K. A., Aggarwal, A. K., & Majumdar, A. K. (2016). Investigation on the Performance and Improvement of Free Space Optical Link in Atmospheric Turbulence (Doctoral dissertation, PhD thesis. Gujarat Technological University).

[49] Huurdeman, A. A. (2003). *The worldwide history of telecommunications*. John Wiley & Sons.

[50] Abadi, M. M. (2017). *A hybrid free space optics/radio frequency antenna-design and evaluation*. University of Northumbria at Newcastle (United Kingdom).

[51] Chaaban, A., Morvan, J. M., & Alouini, M. S. (2016). Free-space optical communications: Capacity bounds, approximations, and a new sphere-packing perspective. *IEEE Transactions on Communications*, *64*(3), 1176-1191.

[52] Bhatnagar, M. R., & Ghassemlooy, Z. (2016). Performance analysis of gamma–gamma fading FSO MIMO links with pointing errors. *Journal of Lightwave technology*, *34*(9), 2158-2169.

[53] Li, X., Bamiedakis, N., Guo, X., McKendry, J. J. D., Xie, E., Ferreira, R., & White, I. H. (2016). Wireless visible light communications employing feed-forward pre-equalization and PAM-4 modulation. *Journal of Lightwave Technology*, *34*(8), 2049-2055.

[54] Hamza, A. S., Deogun, J. S., & Alexander, D. R. (2016). Wireless communication in data centers: A survey. *IEEE communications surveys & tutorials*, *18*(3), 1572-1595.

[55] Park, J., Lee, E., Chae, C. B., & Yoon, G. (2015). Outage probability analysis of a coherent FSO amplify-and-forward relaying system. *IEEE Photonics Technology Letters*, *27*(11), 1204-1207.

[56] Kaushal, H., Jain, V. K., & Kar, S. (2017). *Free space optical communication* (p. 60). New Delhi: Springer india.

[57] Hossen, D.,& Alim, G. S. (2008). *Performane evaluation of the free space optical (FSO) communication with the effects of the atmospheric turbulances* (Doctoral dissertation, BRAC University).

[58] Li, F., Hou, Z., & Wu, Y. (2013). Experiment and numerical evaluation of bit error rate for free-space communication in turbulent atmosphere. *Optics and Laser Technology*, *45*, 104-109.

[59] Fadhil, H. A., Amphawan, A., Shamsuddin, H. A., Abd, T. H., Al-Khafaji, H. M., Aljunid, S. A., & Ahmed, N. (2013). Optimization of free space optics parameters: An optimum solution for bad weather conditions. *Optik*, *124*(19), 3969-3973.

[60] Malik, A., & Singh, P. (2015). Free space optics: current applications and future challenges. *International Journal of Optics*, *2015*.

[61] Varotsos, G. K., Nistazakis, H. E., Petkovic, M. I., Djordjevic, G. T.,& Tombras, G. S. (2017). SIMO optical wireless links with nonzero boresight pointing errors over M modeled turbulence channels. *Optics Communications*, *403*, 391-400.

[62] Majumdar, A. K. (2014). *Advanced free space optics (FSO): a systems approach* (Vol. 186). Springer.

[63] Barrios Porras, R. (2013). Exponentiated Weibull fading channel model in free-space optical communications under atmospheric turbulence.

[64] Bloom, S., Korevaar, E., Schuster, J., & Willebrand, H. (2003). Understanding the performance of free-space optics. *Journal of optical Networking*, *2*(6), 178-200.

[65] Ijaz, M., Ghassemlooy, Z., Pesek, J., Fiser, O., Le Minh, H., & Bentley, E. (2013). Modeling of fog and smoke attenuation in free space optical communications link under controlled laboratory conditions. *Journal of Lightwave Technology*, *31*(11), 1720-1726.

[66] Ijaz, M. (2013). *Experimental characterisation and modelling of atmospheric fog and turbulence in FSO*. University of Northumbria at Newcastle (United Kingdom).

[67] Al Naboulsi, M. C., Sizun, H., & de Fornel, F. (2004). Fog attenuation prediction for optical and infrared waves. *Optical Engineering*, *43*(2), 319-329.

[68] Ricklin, J. C., Hammel, S. M., Eaton, F. D., & Lachinova, S. L. (2006). Atmospheric channel effects on free-space laser communication. *Journal of Optical and Fiber Communications Reports*, *3*(2), 111-158.

[69] Awan, M. S., Leitgeb, E., Hillbrand, B., Nadeem, F., and Khan, M. S. (2009, September). Cloud attenuations for free-space optical links. In *2009 International Workshop on Satellite and Space Communications* (pp. 274-278). IEEE.

[70] Majumdar, A. K., & Ricklin, J. C. (Eds.). (2010). *Free-space laser communications: principles and advances* (Vol. 2). Springer Science and Business Media.

[71] Al Naboulsi, M. C., Sizun, H., & de Fornel, F. (2004, September). Wavelength selection for the free space optical telecommunication technology. In *Reliability of Optical Fiber Components, Devices, Systems, and Networks II* (Vol. 5465, pp. 168-179). International Society for Optics and Photonics.

[72] Lai, J. W. (2016). *Free space optical communication for tactical operations*. Naval Postgraduate School Monterey United States.

[73] Pratt, W. K. K. (1969). *Laser Communication Systems*, 1st ed. New York: John Wiley and Sons, Inc.

[74] Gagliardi, R. M., & Karp, S. (1976). Optical communications. *New York*.

[75] Niu, M., Cheng, J., & Holzman, J. F. (2012). Terrestrial coherent free-space optical communication systems. *Optical communication* ch8.

[76] Andrews, L. C., Phillips, R. L., & Hopen, C. Y. (2001). *Laser beam scintillation with applications* (Vol. 99). SPIE press.

[77] Uysal, M., Li, J., & Yu, M. (2006). Error rate performance analysis of coded free-space optical links over gamma-gamma atmospheric turbulence channels. *IEEE Transactions on wireless communications*, *5*(6), 1229-1233.

[78] Churnside, J. H., & Clifford, S. F. (1987). Log-normal Rician probability-density function of optical scintillations in the turbulent atmosphere. *JOSA A*, *4*(10), 1923-1930.

[79] Menezes, A. J., Vanstone, S. A., & Van Oorschot, P. C. (2010). Handbook of Applied Cryptography (Special Indian Edition.

[80] Foundation, E. F. (1998). Cracking DES: Secrets of encryption research, wiretap politics and chip design.

[81] Shannon, C. E. (1948). A mathematical theory of communication. *The Bell system technical journal*, *27*(3), 379-423.

[82] Zhu, J. (2014). Performance of physical layer security under correlated fading wire-tap channel.

[83] Chakravarty, J. J. (2020). *Physical Layer Security for Next Generation Wireless Systems* (Doctoral dissertation, University of Bristol).

[84] Dhasarathan, V., Singh, M., & Malhotra, J. (2020). Development of high-speed FSO transmission link for the implementation of 5G and Internet of Things. *Wireless Networks*, *26*(4), 2403-2412.

[85] Boluda-Ruiz, R., García-Zambrana, A., Castillo-Vázquez, C., & Castillo-Vázquez, B. (2016). Novel approximation of misalignment fading modeled by Beckmann distribution on free-space optical links. *Optics express*, *24*(20), 22635-22649.

[86] Willebrand, H., & Ghuman, B. S. (2002). *Free space optics: enabling optical connectivity in today's networks*. SAMS publishing.

[87] Eldridge, R. G. (1969). Mist—the transition from haze to fog. *Bulletin of the American Meteorological Society*, *50*(6), 422-427.

[88] Muhammad, S. S., Flecker, B., Leitgeb, E., & Gebhart, M. (2007). Characterization of fog attenuation in terrestrial free space optical links. *Optical engineering*, *46*(6), 066001.

[89] Shakir, W. M., & Mahdi, A. S. (2019, April). Errors rate analysis of the hybrid FSO/RF systems over foggy-weather fading-induced channel. In *2019 4th Scientific International Conference Najaf (SICN)* (pp. 156-160). IEEE.

[90] Kaushal, H., & Kaddoum, G. (2016). Optical communication in space: Challenges and mitigation techniques. *IEEE communications surveys & tutorials*, *19*(1), 57-96.

[91] Al-Quwaiee, H. (2016). *On the Performance Analysis of Free-Space Optical Links under Generalized Turbulence and Misalignment Models* (Doctoral dissertation).

[92] Kim, I. I., McArthur, B., & Korevaar, E. J. (2001, February). Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications. In *Optical Wireless Communications III* (Vol. 4214, pp. 26-37). International Society for Optics and Photonics.

[93] Nadeem, F., Javornik, T., Leitgeb, E., Kvicera, V., & Kandus, G. (2010). Continental fog attenuation empirical relationship from measured visibility data. *Radioengineering*, *19*(4), 596-600.

[94] Singh, M., Bhatia, S., & Kaushal, H. (2016). Performance evaluation of free space optical link under various weather conditions. In *Proceedings of the second international conference on computer and communication technologies* (pp. 329-342). Springer, New Delhi.

[95] Islam, M. N., & Bhuiyan, M. A. S. (2016). Effect of operating wavelengths and different weather conditions on performance of point-to-point free space optical link. *International Journal of Computer Networks and Communications*, *8*(2), 63-75.

[96] Majumdar, A. K. (2018). *Optical wireless communications for broadband global internet connectivity: fundamentals and potential applications*. Elsevier. Ch 4.

[97] Jurado-Navas, A., Garrido-Balsells, J. M., Paris, J. F., Castillo-Vázquez, M., & Puerta-Notario, A. (2012). Impact of pointing errors on the performance of generalized atmospheric optical channels. *Optics Express*, *20*(11), 12550-12562.

[98] Ansari, I. S., Yilmaz, F., & Alouini, M. S. (2015). Performance analysis of free-space optical links over Malaga (M) turbulence channels with pointing errors. *IEEE Transactions on Wireless Communications*, *15*(1), 91-102.

[99] Gradshteyn, I. S., & Ryzhik, I. M. (2000). Table of Integrals, Series, and Products, edited by A. *Jeffrey Academic, New York*, 658.

[100] Farid, A. A., & Hranilovic, S. (2007). Outage capacity optimization for free-space optical links with pointing errors. *Journal of Lightwave technology*, *25*(7), 1702-1710.

[101] Boluda-Ruiz, R., García-Zambrana, A., Castillo-Vázquez, B., & Castillo-Vázquez, C. (2016). Impact of nonzero boresight pointing error on ergodic capacity of MIMO FSO communication systems. *Optics express*, *24*(4), 3513-3534.

[102] Ruiz, R. B., & Zambrana, A. G. (2017). *On the performance of terrestrial free-space optical (fso) links under the presence of generalized pointing errors* (Doctoral dissertation, Ph. D. Thesis, University of Málaga).

[103] Research, W. (2010). Mathematica Edition: Version 8.0. *Champaign, Illinois: Wolfram Research Inc*.

[104] Trinh, P. V., Pham, T. V., Dang, N. T., Nguyen, H. V., Ng, S. X., & Pham, A. T. (2018). Design and security analysis of quantum key distribution protocol over free-space optics using dual-threshold direct-detection receiver. IEEE Access, 6, 4159-4175.

LIST OF PUBLICATIONS

Conferences

1-A Survey on Physical Layer Security for FSO Communication Systems.

Southern Technical University
International Multi-Disciplinary Conference Integrated Sciences and Technologies 2021
7-9 September 2021,

ACCEPTANCE LETTER

Date: 16 August 2021
Paper ID: 1570732199

Dear Wafaa Mohammed Ridha Shakir;and Ruwaida Abdulkareem,

On behalf of the organizing committee of the **International Multi-Disciplinary Conference Integrated Sciences and Technologies 2021**, we are pleased to inform you that your paper (**A Survey on Physical Layer Security for FSO Communication Systems**) has been accepted for presentation in the **conference**, which will be held on 7-9 September 2021.

Please note that All accepted papers will be published in **European Alliance for Innovation (EAI)** and submitted to **Scopus, WoS** and other indexing and abstracting databases including the conference proceeding and will be published with **ISBN number**. Moreover, a selected number of high-quality papers will be invited to two special issues of high impacts from **MDPI Journals**.

For more information please visit the conference website (*https://www.imdc-ist.org/*) or directly contact the conference secretary.

We truthfully appreciate your contribution and looking forward to meet you during the conference.

Best Regards,

Prof. Dr. Alaa F. Abdulahed
STU Vice President for Scientific Affairs
Chair of the Scientific Committee of IMDC-IST 2021

https://www.imdc-ist.org/ | | E-mail: *conf@stu.edu.iq*

2- On Secrecy Capacity Analysis of FSO Communication Systems Under Generalized Malaga-M Turbulence.

Scopus

Data: September 26, 2021
Paper ID: IICPS_223

LETTER OF ACCEPTANCE

Dear Authors,

On behalf of the IICPS -21 Committee, and based on the reviewers' evaluation after double blind peer review and Guest editors' approval we are pleased to inform you that your paper entitled:

" On Secrecy Capacity Analysis of FSO Communication Systems under Generalized Malaga-M turbulence "

Written By

Ruwaida Abdul Ameer Abdul Kareem and Wafaa Mohammed Ridha Shakir

Has been accepted and will be processed to publication in the IOP Journal of Physics (Online ISSN: 1742-6596, Print ISSN: 1742-6588, IICPS-2021). It is our pleasure to invite you to attend the Iraqi Academics Syndicate 2nd International Conference for Pure and Applied Sciences (IICPS), Babylon Branch, Babylon, Iraq at 14-15 November 2021 to present your paper. We congratulate you for your achievement, the technical details about the publication will be informed later. The publication of the accepted paper will be provided by the end of January 2022.

We Will encourage more quality submissions from you and your colleagues in future

Regards,

Prof. Dr. Shubham Sh. Sharma
Special Issue Guest Editor of IICPS

JOURNAL OF PHYSICS: CONFERENCE SERIES
IOP Publishing

Caution: This Acceptance Letter Made by IICPS Conference Guest Editors and All Approval Inquiries Should Addressed to Editorial Board Committee of IICPS .

Submitted

1- Secure Communications for FSO Systems over Generalized Malaga-M turbulence Channels.

الخلاصة

أدى التطور الهائل في مجالات تطبيق الجيل الخامس (5G) وما بعده من خدمات الاتصالات التي تتطلب معدلات نقل بيانات عالية إلى استخدام تقنية اتصال لاسلكي ضوئي تُعرف باسم تقنية الاتصالات البصريه في الفضاء الحر (FSO) ، والتي تستخدم الفضاء الحر كوسيلة لنقل المعلومات. في هذه الرساله ، يتم تحليل أداء سرية الاتصالات البصريه في الفضاء الحر في وجود متنصت يقع بالقرب من جهاز الاستقبال الشرعي من خلال تقديم تعبير مغلق الشكل لتحليل دقيق وشامل لمقاييس أداء السرية مثل متوسط سعة السرية (ASC) ، واحتمال انقطاع السرية (SOP) ، وسعة السرية الإيجابية الصارمة (SPSC), نظام الاتصالات البصريه في الفضاء الحر يستخدم تقنية الكثافة التعديل / الكشف المباشر (IM / DD), في ظل ظروف الاضطراب الجوي المختلفة (ضعيفة إلى قوية) ، وأخطاء توجيه التسديد الصفرية وغير -الصفري ، والطقس الضبابي. لنمذجة القناة لجميع ظروف الاضطرابات الجوية (ضعيفة ، معتدلة ، وقوية), تم استخدام التوزيع العام للاضطراب -Malaga M لوصلات الاتصالات البصريه في الفضاء الحر حيث تشير النتائج إلى تدهور أداء السرية مع زيادة شدة الاضطرابات الجوية وأخطاء التوجيه المعممه. تم تحقيق متوسط سعة السريه بمقدار 40 بت / ثانية / هرتز في ظل اضطراب ضعيف بالمقارنة مع 10 بت / ثانية / هرتز في ظل اضطراب معتدل مع أخطاء توجيه منخفضة تبلغ $\psi = 6.7$، وبأسوأ انخفاض يصل أداء متوسط سعة السريه إلى 2.5 بت / ثانية / هرتز في ظل اضطراب قوي. اكتسب نظام المساحه 21.2 dB عندما تحول الاضطراب من معتدل إلى ضعيف تحت أخطاء التوجيه المنخفضة $\psi = 6.7$ مع نسبة الاشاره الى الضوضاء SNR لقناة التنصت $\mu_{fso,E} = -10$ dB و SOP 10^{-5}، بينما حصل النظام على 19.5dB و 18 dB لنفس الحالة مع SNR لقناة التنصت $\mu_{fso,E} = 0$ dB و $\mu_{fso,E} = 10$ dB على التوالي. في ظل القيمة

المنخفضة لأخطاء توجيه التسديد الصفرية ، يحقق نظام الاتصالات البصري في الفضاء الحر أداءً أفضل مقارنةً بقيمته العالية. ومع ذلك ، فإن تأثير أخطاء توجيه خط التسديد غير الصفرية على أداء السرية لنظام الاتصالات البصري في الفضاء الحر هو أكثر تدهورًا من تأثير عدم وجود أخطاء في توجيه خط التسديد. بالإضافة إلى ذلك ، كان للظروف الجوية الضبابية تأثير سلبي عميق على أداء السرية لنظام الاتصالات البصري في الفضاء الحر أدت الكثافة المتزايدة للضباب إلى مزيد من التدهور في أداء سرية نظام الاتصالات البصري في القضاء الحر.

تحليل الأداء السري للرابط المساحه الحره البصريه (FSO) لأنظمة الاتصالات

الرسالة

مقدمة الى قسم هندسة تقنيات الاتصالات كجزء من متطلبات نيل درجة الماجستير

تقدم بها

رويده عبد الامير عبد الكريم

إشراف

الأستاذ المساعد الدكتورة

وفاء محمد رضا شاكر

2022

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة الفرات الاوسط التقنية
الكلية التقنية الهندسية- نجف

تحليل الأداء السري للرابط FSO لأنظمة الاتصالات

رويده عبد الامير عبد الكريم يوسف

بكالوريوس في هندسة تقنيات الاتصالات

2022