

PHYSICAL LAYER SECURITY OF WIRELESS TRANSMISSIONS OVER FADING
CHANNELS

by

Sadrac Blanc

A Thesis Submitted to the Faculty of
The College of Engineering and Computer Science
In Partial Fulfillment of the Requirements for the Degree of
Master of Science

Florida Atlantic University

Boca Raton, Florida

August 2016

Copyright by Sadrac Blanc 2016

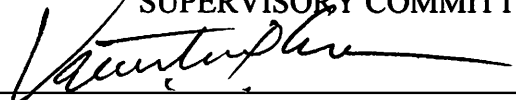
PHYSICAL LAYER SECURITY OF WIRELESS TRANSMISSIONS OVER FADING
CHANNELS


by


Sadrac Blanc


This thesis was prepared under the direction of the candidate's thesis advisor, Dr. Valentine Aalo, Department of Computer & Electrical Engineering and Computer Science, and has been approved by the members of his supervisory committee. It was submitted to the faculty of the College of Engineering and Computer Science and was accepted in partial fulfillment of the requirements for the degree of Master of Science.

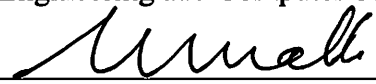
SUPERVISORY COMMITTEE:



Valentine Aalo, Ph.D.
Thesis Advisor

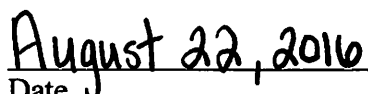

Ionut Cardei, PhD


Imad Mahgoub, PhD


Nurgun Erdol, Ph.D.
Chair, Department of Computer & Electrical
Engineering and Computer Science


Mohammad Ilyas, Ph.D.
Dean, College of Engineering and Computer Science


Deborah L. Floyd, Ed.D.
Dean, Graduate College


Date

ACKNOWLEDGEMENTS

The completion of this work would not be possible without the Almighty God. I thank Him for his love, and all the people who have invested in me. I have a long list of people who have helped me achieve this milestone in my life. I am grateful for their support, mentorship and all the help they have provided me throughout my studies. I want to express my sincere gratitude for all they have done for me; and their investment is not in vain.

First, I would like to thank my thesis supervisor, Dr. Valentine Aalo, whom I have known since I was a freshman. Throughout my research, Dr. Aalo has provided me with immense support, mentoring, compassion and guidance. I greatly appreciate all the time and feedback that he provided me during my research. I have benefited a lot from his expertise, and learned a lot in the field by the way he always pushed me to think outside of the box. His words of encouragement are amazing, and his remarks were significantly helpful during my research.

Secondly, I would like to thank the rest of my thesis committee, Dr. Ionut Cardei and Dr. Imad Mahgoub for their constructive suggestions and comments, which have improved the quality of this work.

I would also like to express my sincere gratitude to my mothers, Dr. Torrey Evelyn and Mary Davis, Harper Linda Smith and Noel Smith, Dr. Norman Kaufman, Dr. Herbert Shapiro, Richard Flick, and Rev. Charles Mory and his wife, Kathy Mory.

I cannot conclude this acknowledgement without expressing my gratitude and appreciation to Dr. Petrie for her mentorship and financial support through the LACCEI scholarship that helped me complete my studies.

I am grateful to my family, my church members, and all the friends who believe in me, and continue to support me throughout my education.

ABSTRACT

Author: Sadrac Blanc

Title: Physical Layer Security of Wireless Transmissions Over Fading Channels

Institution: Florida Atlantic University

Thesis Advisor: Dr. Valentine Aalo

Degree: Master of Science

Year: 2016

The open nature of the wireless medium makes the wireless communication susceptible to eavesdropping attacks. In addition, fading and shadowing significantly degrade the performance of the communication system in the wireless networks. A versatile approach to circumvent the issues of eavesdropping attacks while exploiting the physical properties of the wireless channel is the so-called physical layer-security. In this work, we consider a model in which two legitimate users communicate in the presence of an eavesdropper. We investigate the performance of the wireless network at the physical layer that is subject to a variety of fading environments that may be modeled by the Rayleigh, Nakagami-m, and Generalized-K distributions, to mention a few. We use the secrecy outage probability (SOP) as the standard performance metrics to study the performance of the wireless networks. We propose two different approaches to compute the secrecy outage probability, and derive explicit expressions for the secrecy outage

probability that allow us to characterize the performance of the wireless networks.

Specifically, we use a direct integration approach as well as a Taylor series base approach to evaluate the secrecy outage probability. Finally, we use computer simulations, based on MATLAB, to confirm the analytical results.

PHYSICAL LAYER SECURITY OF WIRELESS TRANSMISSIONS OVER FADING CHANNELS

LIST OF FIGURES	xi
LIST OF NOTATIONS	xv
LIST OF ACRONYMS	xvi
CHAPTER 1: INTRODUCTION	1
1.1 Overview	1
1.2 Outage Probability.....	2
1.3 Statement of the Problem	3
1.4 Methods of Solution	4
1.5 Thesis Objective.....	4
1.6 Thesis Organization.....	5
CHAPTER 2: SYSTEM MODELS	7
2.1 Introduction	7
2.2 Physical Layer Security in Wireless Communication.....	8
2.3 Evaluation of Secrecy Outage Probability	15
CHAPTER 3: CHANNELS FADING MODELS	17
3.1 Introduction	17
3.2 Multipath Fading.....	18
3.2.1 Rayleigh Fading.....	19
3.2.2 Nakagami.....	20
3.2.3 Generalized-Gamma.....	21
3.3 Shadowing.....	22
3.4 Composite.....	23
3.4.1 Generalized-K Channel Fading Model.....	24
3.5 G-Function Channels Fading Models	26

CHAPTER 4: DIRECT INTEGRATION METHOD.....	27
4.1 Introduction	27
4.2 Direct Integration Based Approach.....	28
4.3 Secrecy Outage Probability Using Integration Approach	28
4.3.1 Rayleigh Fading Case	28
4.3.2 Nakagami-m Fading Case	29
4.3.3 Generalized K-Fading Case.....	30
4.4 Approximation	31
CHAPTER 5: TAYLOR SERIES APPROACH	33
5.1 Introduction	33
5.2 Taylor Series	33
5.3 Application to Some Common Distributions	35
5.3.1 Case 1: Rayleigh.....	35
5.3.2 Nakagami-m	36
5.4 Application to G-Fading Channels.....	37
5.4.1 Derivation of nth Derivative.....	37
5.4.2 Derivation of nth Moment	39
5.4.3 The Generalized-K fading Channel Case	40
CHAPTER 6: ANALYTICAL AND COMPUTER SIMULATIONS RESULTS.....	41
6.1 Introduction	41
6.2 Rayleigh Fading	41
6.3 Nakagami-m Fading.....	42
6.4 Generalized-K Fading	44
CHAPTER 7: SUMMARY AND CONCLUSIONS	65
7.1 Summary of Main Results.....	65
7.2 Conclusion.....	67
7.3 Suggestions for Future Work	68
APPENDIX A	69
A.1 The Fox's H-function [42]	69
A.2 Meijer's G-function [48] - [69]	69
APPENDIX B	70
B. 1 Derivation of (4.8) and (4.9).....	70

REFERENCES	72
------------------	----

LIST OF FIGURES

Figure 2.1: System Model.....	8
Figure 2.2: SISO System. All the users are equipped with a single antenna [17]	10
Figure 2.3: A MIMO wireless system: the transmitter and the receiver are equipped with multiple antennas as well as the eavesdropper [17].....	11
Figure 2. 4: Simple Relay System [22].....	12
Figure 2.5: A cooperative diversity system where a transmitter communicates to a receiver with the help of M relays in the presence of an eavesdropper [17].	13
Figure 6.1: Secrecy Outage Probability versus $\overline{\gamma}_D$, in a Rayleigh fading environment, for selected values of $\overline{\gamma}_E$ with $t = 0.1$ bits/s/ Hz ($\theta = 2^{0.1}$).	45
Figure 6.2: Secrecy Outage Probability versus $\overline{\gamma}_D$, in a Rayleigh fading environment, for selected values of $\overline{\gamma}_E$ with $t = 0.75$ bits/s/Hz ($\theta = 2^{0.75}$).	46
Figure 6.3: Secrecy Outage Probability versus $\overline{\gamma}_D$, in a Rayleigh fading channel, for selected values of $\overline{\gamma}_E$ with $t = 1$ bits/s/Hz ($\theta = 2^1$).	47
Figure 6.4: Secrecy Outage Probability versus $\overline{\gamma}_D$, in a Rayleigh fading environment, for selected values of $\overline{\gamma}_E$ with $t = 1.45$ bits/s/Hz ($\theta = 2^{1.45}$).	48
Figure 6.5: Secrecy Outage Probability, in a Rayleigh fading environment, in terms of the average power ratio for selected values of the threshold when the average power at the eavesdropper $\overline{\gamma}_E$ is 5 dB.	49

Figure 6.6: Secrecy Outage Probability, in a Rayleigh fading environment, in terms of the average power ratio while varying the threshold values when the average power at the eavesdropper ($\overline{\gamma}_E$) is 20 dB.	50
Figure 6.7: Secrecy Outage Probability, in a Rayleigh fading environment, in terms of the average power while varying the threshold values when the average power at the eavesdropper is 5 dB.	51
Figure 6.8: Secrecy Outage Probability, in a Rayleigh fading environment, in terms of the average power while varying the threshold values when the average power at the eavesdropper is 20 dB.	52
Figure 6.9: Secrecy Outage Probability versus $\overline{\gamma}_D$, in a Nakagami-m fading environment, for selected values of $\overline{\gamma}_E$ with $t = 0.1$, bits/s/Hz ($\theta = 2^{0.1}$), $m_{\gamma_D} = m_{\gamma_E} = 1$	53
Figure 6.10: Secrecy Outage Probability versus $\overline{\gamma}_D$, in a Nakagami-m fading environment, for selected values of $\overline{\gamma}_E$, with $t = 0.5$ bits/s/Hz ($\theta = 2^{0.5}$) and the fading parameters $m_{\gamma_D} = 3$, $m_{\gamma_E} = 2$	54
Figure 6.11: Secrecy Outage Probability versus $\overline{\gamma}_D$, in a Nakagami-m fading environment, for selected values of $\overline{\gamma}_E$, with $t = 0.5$ bits/s/Hz ($\theta = 2^{0.5}$) and the fading parameters $m_{\gamma_D} = 4$, $m_{\gamma_E} = 2$	55
Figure 6.12: Secrecy Outage Probability versus $\overline{\gamma}_D$, in a Nakagami-m fading environment, for selected values of $\overline{\gamma}_E$, with $t = 0.5$ bits/s/Hz ($\theta = 2^{0.5}$) and the fading parameters $m_{\gamma_D} = 2$, $m_{\gamma_E} = 4$	56

Figure 6.13: Secrecy Outage Probability versus $\overline{\gamma_D}$, in a Nakagami-m fading environment, for selected values of $\overline{\gamma_E}$, with $t = 1$ bits/s/Hz ($\theta = 2^1$) and the fading parameters $m_{\gamma_D} = 3, m_{\gamma_E} = 2$	57
Figure 6.14: Secrecy Outage Probability versus $\overline{\gamma_D}$, in a Nakagami-m fading environment, for selected values of $\overline{\gamma_E}$, with $t = 1$ bits/s/Hz ($\theta = 2^1$) and the fading parameters $m_{\gamma_D} = 4, m_{\gamma_E} = 2$	58
Figure 6.15: Secrecy Outage Probability versus $\overline{\gamma_D}$, in a Nakagami-m fading environment, for selected values of $\overline{\gamma_E}$, with $t = 1$ bits/s/Hz ($\theta = 2^1$) and the fading parameters $m_{\gamma_D} = 2, m_{\gamma_E} = 4$	59
Figure 6.16: Secrecy Outage Probability versus $\overline{\gamma_D}$, in a Nakagami-m fading environment, for selected values of $\overline{\gamma_E}$, with $t = 0.5$ bits/s/Hz ($\theta = 2^{0.5}$) and the fading parameters $m_{\gamma_D} = m_{\gamma_E} = 4$	60
Figure 6.17: Secrecy Outage Probability versus $\overline{\gamma_D}$, in a Nakagami-m fading environment, for selected values of $\overline{\gamma_E}$, with $t = 1$ bits/s/Hz ($\theta = 2^1$) and the fading parameters $m_{\gamma_D} = m_{\gamma_E} = 4$	61
Figure 6.18: Secrecy Outage Probability versus $\overline{\gamma_D}$, in a Generalized-K fading environment, for selected values of $\overline{\gamma_E}$, with $t = 1$ bits/s/Hz ($\theta = 2^1$) and the fading parameters $m_D = m_E = 3, k_D = k_E = 4$	62
Figure 6.19: Secrecy Outage Probability versus $\overline{\gamma_D}$, in a Generalized-K fading environment, for selected values of $\overline{\gamma_E}$, with $t = 1$ bits/s/Hz ($\theta = 2^1$) and the fading parameters $m_D = m_E = 2, k_D = k_E = 4$	63

Figure 6.20: Secrecy Outage Probability versus $\overline{\gamma}_D$, in a Generalized-K fading environment, when the eavesdropper average power ($\overline{\gamma}_E$) is 10 dB, with $t = 1$ bits/s/Hz ($\theta = 2^1$) while varying the fading parameters..... 64

LIST OF NOTATIONS

γ_D	Instantaneous received signal at the desired receiver
γ_E	Instantaneous received signal at the eavesdropper
$f_\gamma(\gamma)$	Probabilty density function of random variable γ
$F_\gamma(\gamma)$	Cumulative distribution function of random variable γ
C_D	Channel capacity of main channel
C_E	Channel capacity of eavesdropper channel
t	Predefined threshold
$k_\nu(.)$	$\nu(.)$ order modified Bessel function of the second kind
α	Fading amplitude
σ	Standard deviation of log-normal
γ	Instantaneous received signal
Ω	Average SNR value
$\Gamma(.)$	Gamma function
m	Fading parameter
$\mathcal{G}(.,.)$	Lower incomplete Gamma function

μ	Mean of log normal
$f_{\gamma_D/\gamma_E}(\cdot \cdot)$	Conditional pdf for the received SNR
$p_{\gamma_D}(\cdot)$	Probability density function of the average signal power
$G_{p,q}^{m,n}(\cdot)$	Meijer's G function
$H_{p,q}^{m,n}(\cdot)$	Fox's H function

LIST OF ACRONYMS

AES	Advanced Encryption Standard
AWGN	Additive White Gaussian Noise
CDF	Cumulative density function
dB	Decibels
GG	Generalized Gamma
G-K	Generalized-K
ITS	Information-theoretic security
LOS	Line of sight
MGF	Moment generating function
MIMO	Multiple-input multiple-output
MISOME	Multiple-input single-output multiple-eavesdropper
OP	Outage probability
PC	Personal Communication
pdf	Probability density function
PHY	Physical layer Security

R-L	Rayleigh log-normal
RSA	Rivest-Shamir-Adleman
RVs	Random Variables
SIMOME	Single-input multiple-output multiple-eavesdropper
SINR	Signal-to-interference plus noise ratio
SISOSE	Single-input single-output single-eavesdropper
SNR	Signal-to-noise ratio

CHAPTER 1: INTRODUCTION

1.1 Overview

Wireless communication networks play a critical role in the transmission of information and how communication is done in today's world. Due to the high demand for information sharing and personal communication services (PCS), wireless networks will continue to widely expand in the field of communication. Several concerns on security and privacy have arisen in regards to wireless communication networks. Due to the broadcast nature of wireless networks, communications within these networks are susceptible to eavesdropping attacks [1]. The design and implementing of cryptographic algorithms are normally used to secure the information in the upper application layer of the wireless network using sophisticated encryption techniques. Common data encryption techniques include the Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) [2]. It has been shown that these encryption techniques are not uniquely adequate to provide perfect security in the communication channels [3]. In cases where the cryptographic design of the wireless systems fails, eavesdroppers can access the information in the network [67].

Over the last few decades, physical layer security has notably gained attention to overcome the challenges of privacy and security in the transmission over wireless channels. Several efforts have been made to solve the issues of privacy and security in wireless networks by strengthening the physical layer of the wireless network. A

versatile approach to study the security issues in wireless systems is the use of the notion of information-theoretic security (ITS) at the physical layer, which focuses on exploiting the characteristics and properties of the physical channel. The principle of information-theoretic security was first initiated by Shannon [4]. In his works, Shannon studied the condition to achieve perfect secrecy in discrete memoryless channel for reliable transmission over a wiretap channel. Other researchers have furthered the work of Shannon. For example, Wyner and Csiszar considered the broadcast wireless channel [5] while Korner, Leung, and Hellman studied the additive white Gaussian noise channel (AWGN) [6].

Unlike a wired network, wireless communication systems are susceptible to impairments such as multipath fading, shadowing, interferences, and noise. Several techniques may be used to improve the secrecy capacity of wireless communication systems. Among these techniques include the use of multiple antennas, cooperative relays, and multiple-input multiple-output (MIMO) and error control coding [7]- [8]- [9]. Our work focuses on the study of the physical layer to improve security over the wireless network, assuming that cryptographic protocols have already been established at the upper application layers.

1.2 Outage Probability

A performance measure that is commonly used to characterize a wireless communication system over fading channels is the outage probability (OP). Outage probability is defined as the probability that the desired instantaneous output signal falls below a pre-set threshold. In terms of the signal-to-noise ratio (SNR), the OP is the

probability that the instantaneous desired signal-to-interference plus noise ratio (SINR) falls below the threshold, ie.

$$O_P = \int_0^{\gamma_{th}} f_{\gamma}(\gamma) d\gamma \quad (1.1)$$

where $f_{\gamma}(\gamma)$ is the probability density function of γ . More explicitly, O_P is the cumulative distribution function (CDF) of γ , evaluated at γ_{th} .

1.3 Statement of the Problem

In wireless networks, the information between legitimate users can be overheard as long as the eavesdropper lies in the coverage area of the transmitter. Typically, the information security is addressed at the upper application layer using cryptographic techniques, while assuming that the physical layer has already provided an error-free-link. In the cryptographic approaches, information security is achieved by implementing complex algorithms such that is practically impossible for eavesdroppers to decode the message. Although cryptography provides secure communication, a limitation includes power-limitation in many wireless infrastructure network. In addition, in many complex wireless network structures, it is challenging to manage and implement higher layer key distribution to secure communication within the wireless networks. An approach to improve the reliability and enhance the security against eavesdropping attacks in a wireless environment is the so-called physical layer security. Unlike the cryptography that ignores the difference between the received signals at the receivers, physical layer security takes advantage of the physical characteristics of the wireless channel to avoid the eavesdropper from interfering with signal transmission to the desired destination. Due to the fading effect in such environments, the link performance evaluation depends

on many channel parameters. In this regard, several performance metrics are used to characterize the wireless channel; among these performance metrics include the secrecy capacity, the outage probability, and the secrecy outage probability.

1.4 Methods of Solution

In this work, we study the performance of wireless systems network over fading channels. We present two different approaches to compute the secrecy outage probability: Direct Integration approach and a Taylor Series approach. While the direct integration method may be used to compute the secrecy outage probability when the pdf of the signal-to-noise ratio (SNR) takes a simple form, the Taylor Series approach is new and constitutes the main contribution of our work.

1.5 Thesis Objective

The broadcast nature of wireless communications renders the transmitted signals susceptible to eavesdropping attacks, which poses serious concerns for privacy and security in wireless communications. An attractive approach has been the use of physical-layer techniques, which focus on the exploitation of physical properties (channel statistical properties) of the wireless channel such as fading, interference, and noise to guarantee both reliable and secure communication between legitimate users. As such, the performance of wireless communication systems over wireless channel depends on the fading environment, and parameters associated with the fading channel. The focus of this thesis is to study the reliability and physical layer security of wireless networks over fading channels using the secrecy outage probability as the principal performance metric.

1.6 Thesis Organization

In Chapter 2, we introduce the system model under consideration. Section 2.2 deals with the issues of physical layer security in wireless communications. In Section 2.3, we present the most common techniques used in the literature to solve the issues of security at the physical layer security in wireless system networks. The performance metrics are outlined in Section 2.4.

Chapter 3 covers the channel models. Section 3.1 briefly introduces the chapter. Section 3.2, Section 3.3, and Section 3.4 provide probability densities functions and their relationship with the study of fading channels due to impairments such as the effects of fading and shadowing. In Section 3.5, we present a more general fading channel: The G-function, to represent the fading channels.

In Chapter 4, we present the first approach, a Direct Integration method to evaluate the secrecy outage probability. In Section 4.1, we give an overview of the direct integration method. In Section 4.2, we express the secrecy outage probability in terms of the integration approach. In Section 4.3.1 and Section 4.3.2, we apply the integration method to compute the secrecy outage probability over some fading models, respectively the Rayleigh and Nakagami-m. In Section 4.3.3, we extend the integration approach to a more general fading environment: The Generalized-K distribution and we make use of the Meijer's G-function. In Section 4.4, we provide an approximation for evaluating the SOP for the Generalized-K fading channel based on the integration method.

In Chapter 5, we discuss the Taylor Series approach to compute the secrecy outage probability. Section 5.1 offers an introduction to the Taylor Series approach. In

Sections 5.2-5.3, we apply the Taylor series to compute the secrecy outage probability for the Rayleigh and Nakagami-m fading channels. In Section 5.4, we expand the Taylor Series to G-function fading channels. We derive the n th-moment and the n -th derivative required to compute the secrecy outage probability for G-functions channel models, respectively, in 5.4.1 and 5.4.2. In Section 5.4.3, we use the Taylor series approach to compute the secrecy outage probability for the Generalized-K fading channel in terms of its G-function form.

In Chapter 6, numerical results for the secrecy outage probability are presented. Graphs for each method are presented, and analysis are done to validate the numerical results for each method.

In Chapter 7, we offer a summary, conclusion and future research directions.

In the appendix, we include some of our derivations used throughout this work. The reference includes the technical papers, textbooks, and other resources that were used in the completion of the thesis.

CHAPTER 2: SYSTEM MODELS

2.1 Introduction

In wired networks, the information transmitted between users is physically connected through cables. On the other hand, communication in wireless networks is done in open air with no actual physical connection between the users. Because of the open nature of the wireless medium, wireless transmission is prone to eavesdropping attacks, where unauthorized users can intercept the communication between legitimate users. Additional security issues in wireless networks come from impairments such as multipath fading, interference and path-loss, making the wireless medium susceptible to interception from eavesdroppers. The conventional approach to addressing security issues in wireless systems is the use of cryptographic techniques to prevent an eavesdropper from accessing the information among legal users [1]- [2]. Recently, an alternative solution, called physical layer security (PHY), emerged to improve security and combat eavesdropping attacks in wireless networks. The idea behind the physical layer approach is based on the notion of information-theoretic-security (ITS) introduced by Shannon [4], and it consists of exploiting the physical characteristics such as multipath fading, interference, and path loss associated with the wireless channel. In this chapter, we outline several physical layer issues and discuss some corresponding techniques used to enhance the physical layer for secure wireless transmission.

2.2 Physical Layer Security in Wireless Communication

Physical layer security was first introduced by Wyner [5] who presented in his work a general noisy wiretap channel. Wyner presented a discrete memoryless wiretap channel for secure communications in the presence of an eavesdropper as the basis to protect information at the physical layer. The wiretap channel considered by Wyner consisted of two legitimate users communicating in the presence of an eavesdropper [5]. In his works, Wyner elaborated on the notion of channel capacity to characterize the physical layer security of the channel. Wyner proved that the transmission of information is perfectly guaranteed when the channel capacity of the main link (from a legitimate transmitter to legitimate receiver) is higher than that the channel capacity of the eavesdropper (from transmitter to eavesdropper) [5].

We consider a generic wireless communication system that involves three nodes: the transmitter, the receiver, and the eavesdropper. A legitimate transmitter (Alice) communicates to a legitimate transmitter (Bob) while there is a third party (Eve) eavesdropping on the transmissions. Figure 2.1 depicts the model for the system.

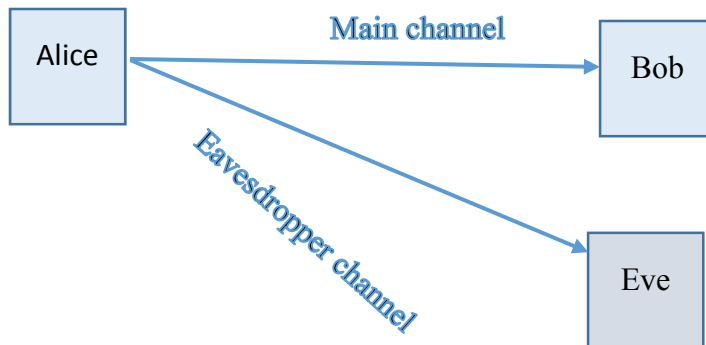


Figure 2.1: System Model

The link between Alice and Bob is the main channel; and Eve attempts to decode the message from the signal it receives through the eavesdropper channel. This is an

example of a three-node network, where the transmission between Alice and Bob is being eavesdropped by a maliciously third-party, Eve. We assume that the source (Alice) directly communicates its signal to the destination (Bob) without relays in the main channel. The eavesdropper (Eve) attempts to access the signal transmission from the transmitter to the receiver.

The general problem of secure transmission over wireless systems, due to its open-broadcast nature in combination with fading effects, has given rise to a variety of studies aimed at improving the transmission security against eavesdropping attacks. Researchers have extended the work initiated by Wyner through the investigation of some practical fading channels. For example, the authors in [6] and [11] considered the issues of security when both the main and eavesdropper channel undergo Rayleigh fading. In [12] and [13], Rice and Nakagami-m fading channels were investigated, respectively.

Several communication schemes and techniques such as the exploitation of multiple antenna [12]- [17]- [50] and cooperative relays [11]- [18]- [19] are among the most common techniques used to enhance transmission security in wireless networks. The simplest communication scheme is when the users (transmitter, receivers, and eavesdropper) are all equipped with a single antenna (see Figure 2.2). This communication scheme is called single-input single-output single eavesdropper (SISOSE) in existing literature [13].

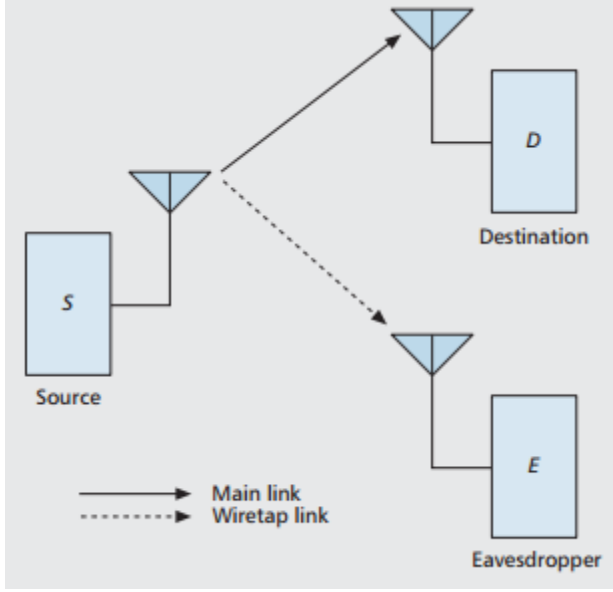


Figure 2.2: SISO System. All the users are equipped with a single antenna [17]

A second scenario is when the transmitter is equipped with a single antenna while the receiver is equipped with multiple antenna. This scenario is referred to as single-input multiple-output multiple-eavesdroppers (SIMOME) [14]. A third case involves the use of multiple antennas at the transmitter and a single antenna at the receiver. This scenario is referred to as multiple-input single-output multiple eavesdroppers (MISOME) [15]- [44]. The last scenario we consider is the multiple-input multiple-output setup which is widely used in many wireless networks. In a MIMO setup, each node in the network is equipped with multiple antennas [17].

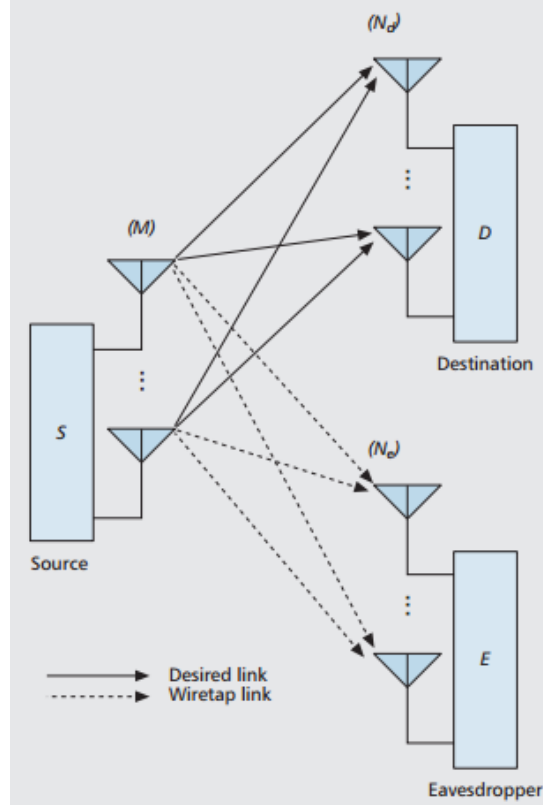


Figure 2.3: A MIMO wireless system: the transmitter and the receiver are equipped with multiple antennas as well as the eavesdropper [17]

Relaying is another technique that is widely used in physical layer security to improve the secrecy performance of wireless communications [18]- [19]- [34]. In a relaying setup, intermediate nodes are used to assist in the transmission of information from the source to the receiver. The authors of [19] have proved that user cooperation via relays can improve the reliability and throughput of wireless communications, and enhance the wireless security against eavesdropping attacks. In addition, the authors of [34] investigated the physical layer security in MIMO relay networks and showed that the

secrecy capacity considerably improves using MIMO relays. In Figure 2.4, we show a simple relay system and in Figure 2.5, we show a MIMO relay system.

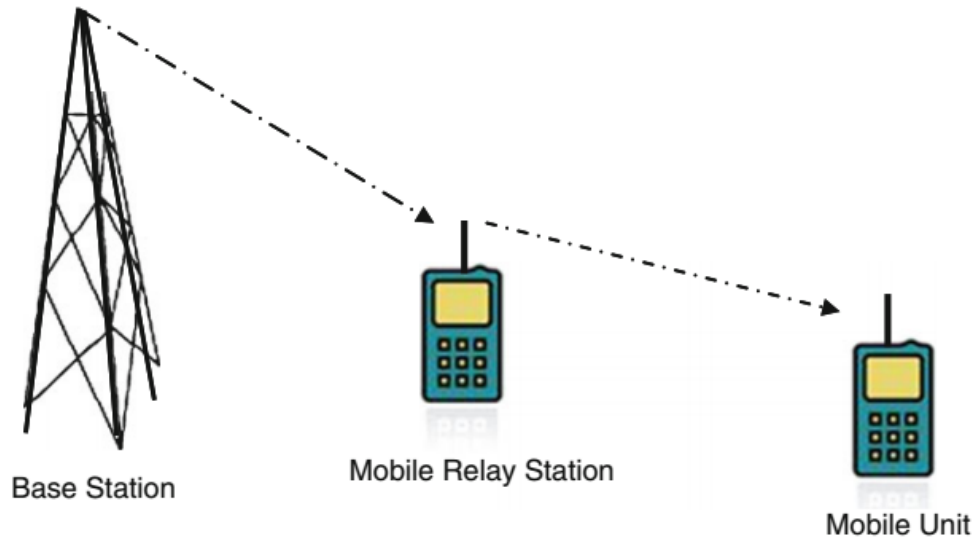


Figure 2. 4: Simple Relay System [22]

Figure 2.5 shows a cooperative wireless network in which a transmitter communicates to a receiver in the presence of an eavesdropper, and a number of relays are used in the transmission of the signal from the transmitter to the receiver. In this setup, the source first sends its information to the relays, and the relays process and forward their received signal to the destination. This type of relay protocol is called amplify-and-forward (AF) relay. In the AF protocol, a relay node amplifies and retransmits the received signal to the destination. Another type of relay protocol is the decode-and-forward relay (DF) in which the relay node first decodes the received signal before it retransmits the decoded signal to the destination node. The authors in [19] have shown that the security

performance of cooperative relay transmission considerably improves the physical-layer security against eavesdropping attacks. The secrecy performance of the cooperative decode-and-forward (DF) relaying networks was studied on [18]. The secrecy performance of the cooperative relaying networks with multiple amplify-and-forward (AF) relays was studied in [19].

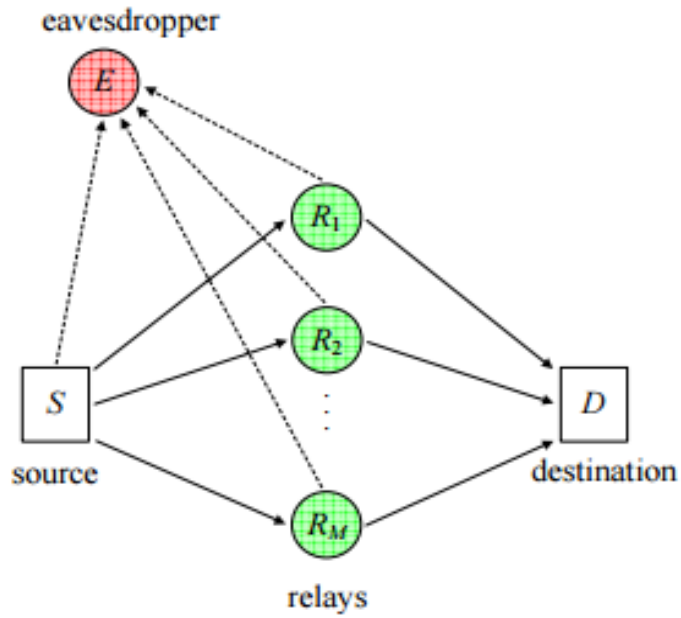


Figure 2.5: A cooperative diversity system where a transmitter communicates to a receiver with the help of M relays in the presence of an eavesdropper [17].

Physical-layer security is commonly characterized by achievable secrecy rates. The secrecy capacity was defined as the maximum transmission rate between the legitimate parties with the eavesdropper unable to obtain any information [20]- [46]. Several authors, have contributed in the characterization of the physical layer security using several performance metrics such as the secrecy outage probability (SOP) [32], the

secrecy capacity, the probability of strictly positive, and the ergodic secrecy capacity. Analytical results are available for the many common fading distributions such as Rayleigh, Nakagami-m, Rice, Log-normal, and Hoyt [36-41]. For their research, in [21-22], [45], closed-form expressions for the average capacity and outage probability over Rayleigh and Nakagami-m fading channels were studied, respectively. The secrecy performance over Rician and Nakagami-m fading channels were presented in [15]- [16]. Furthermore, several authors have shown that antenna selection can enhance the secrecy performance of wireless communications [22]- [23]. In a wireless system with multiple antennas at the transmitter, antenna selection can be used to exploit the fluctuation of fading channels among antennas. The effect of transmit antenna selection on the security of a multi-input single-output network was considered in [10]-[47]. Using the secrecy outage probability as performance metric, it has been shown that the transmit antenna selection can significantly improve the physical layer security. In addition, a multiple-input multi-output system was proposed in [16] to enhance the security of the wireless system. The performance of the system was given in terms of the secrecy outage probability. The authors in [14]-[57] investigated the impact of antenna correlation on secrecy performance of multiple-input multiple-output wiretap channels where the transmitter uses transmitter antenna selection while the receiver employs maximal-ratio combining with arbitrary correlation. In regards to relays, the authors in [23]- [34] explored the use of cooperative relays for improving the physical-layer security expressed in terms of the secrecy rate performance.

2.3 Evaluation of Secrecy Outage Probability

Secrecy capacity is defined as the difference between the capacities of the main channel (from source to destination) and the wiretap channel (from source to eavesdropper). Let the random variable γ_D be the instantaneous received signal (SNR) at the desired receiver and γ_E be the SNR of the eavesdropper. We assume that both the receiver and eavesdropper channels undergo similar and independent fading. We also assume that the random variables γ_D and γ_E have pdfs $f_{\gamma_D}(\gamma_D)$ and $f_{\gamma_E}(\gamma_E)$ respectively, and the corresponding CDF are given by $F_{\gamma_D}(\gamma_D)$ and $F_{\gamma_E}(\gamma_E)$.

The instantaneous channel capacity of the main link is given by:

$$C_D = \log_2(1 + \gamma_D) \quad (2.1)$$

Then the corresponding channel capacity of the eavesdropper is given by:

$$C_E = \log_2(1 + \gamma_E) \quad (2.2)$$

The instantaneous secrecy capacity is defined as:

$$C_S = \begin{cases} \log_2(1 + \gamma_D) - \log_2(1 + \gamma_E), & \text{if } \gamma_D > \gamma_E \\ 0 & \text{if } \gamma_D \leq \gamma_E \end{cases} \quad (2.3)$$

The secrecy outage probability (SOP) is defined as the probability that the instantaneous secrecy capacity falls below a predefined threshold. Mathematically, it can be expressed as:

$$\begin{aligned} P_O &= \Pr\{C_S < t\} \\ &= \Pr\{\log_2(1 + \gamma_D) - \log_2(1 + \gamma_E) \leq t\} \end{aligned}$$

$$\begin{aligned}
&= Pr \left\{ \log_2 \left(\frac{1+\gamma_D}{1+\gamma_E} \right) \leq t \right\} \\
&= Pr \left\{ \frac{1+\gamma_D}{1+\gamma_E} \leq 2^t \right\} \\
&= Pr \{ \gamma_D \leq (1 + \gamma_E) \theta - 1 \} , \quad \text{where } \theta = 2^t \\
&= F_{\gamma_D} \{ (1 + \gamma_E) \theta - 1 \} \\
P_O &= \int_0^\infty F_{\gamma_D} (\theta \gamma_E + \theta - 1) f_{\gamma_E} (\gamma_E) d\gamma_E \tag{2.4}
\end{aligned}$$

Equation (2.4) is an important result that will be used throughout this work.

CHAPTER 3: CHANNELS FADING MODELS

3.1 Introduction

The performance of wireless systems depends on using accurate statistical model to characterize the propagation channel. Depending on the environment, the propagation channel is susceptible to several physical problems such as path loss, interference, multipath and shadow fading. For example, in a typical communication system, the effects of fading cause the received signal to fluctuate rapidly around its mean. Models that describe the effects of multipath fading are known as short-term fading, whereas models that describe the effects of shadow fading are called long-term fading. In many real world scenarios, the effects of both multipath and shadow fading are present in the system. Models that combine the effects of short and long term fading are known as composite fading models.

Furthermore, in the transmission of a signal, the direct propagation path between a transmitter and a receiver may not always be present. The transmission path between the transmitter and the receiver can be severely hindered by tall buildings, trees, mountains, and foliage; and the signal propagating in the wireless link results from scattering, diffraction, and reflection. These three propagation mechanisms affect the communication within the wireless medium.

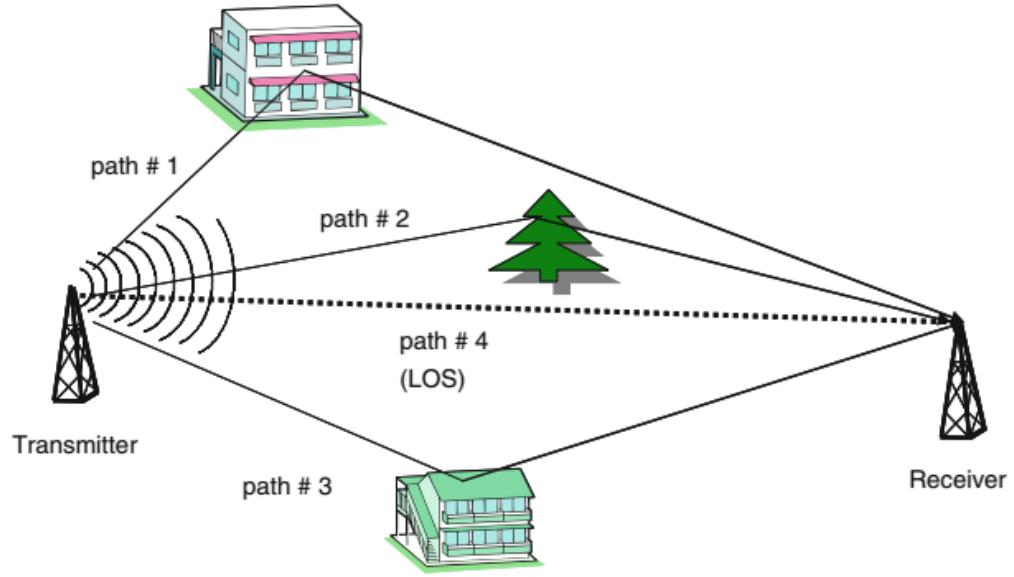


Figure 3.1: Multipath phenomenon transmission [52]

Unlike a wired system that is stationary and predictable, wireless channels are random and require suitable statistical distributions to characterize the channel propagation. It is important to identify models that describe the physical problems at the background of multipath and shadow fading effects in order to comprehend and analyze the usefulness of wireless communication systems. In this chapter, we present models that are used to characterize the effects of multipath fading, shadowing and multipath/shadowing on wireless communication channel.

3.2 Multipath Fading

A signal passing through a medium encounters several obstacles such as tall buildings, trees or a train passing by that disturb the signal and cause the signal to undergo variations. Such variations include random delayed, reflection, scattering, and diffraction of the signal components. The signal that gets to the receiver is a combination of the variations of the transmitted signal coming from different directions. These

multiple versions of the transmitted signal that arrive at the receiver vary in phase and in amplitude. The phase difference occurs due to the fact that the signals have traveled different distances along different routes. Since the phases of the incoming signals change rapidly, the received signal amplitude experiences rapid fluctuations, and can be distorted or faded. In addition, the fluctuations caused by the signals occur rapidly over a short period or travel distance create rapid fluctuations at the receiver, and thus multipath fading is considered to be short-term fading. Because the signals that get to the receiver are random, the received power at the receiver is also random. Depending on the particular propagation environment, several models are used to describe the behavior of multipath fading. The most common distributions used to describe short term fading include the Rayleigh, Nakagami, Weibul models; and we discuss each of these distributions in the next section.

3.2.1 Rayleigh Fading

The Rayleigh fading model is one of the simplest and most commonly used distribution to model short term-fading. It is used to model multipath fading when there is no direct line of sight (LOS) between the transmitter and the receiver, and the resultant signal at the receiver will be the sum of all the reflected and scattered waves. The Rayleigh fading model is characterized by a single parameter. The pdf of the channel fading amplitude α , in a Rayleigh fading environment is given by:

$$f_{\alpha}(\alpha) = \frac{2\alpha}{\Omega} \exp(-\alpha^2/\Omega), \quad \alpha \geq 0 \quad (3.1)$$

In the presence of fading, the amplitude of the received signal is attenuated by the fading amplitude α , which is a random variable (RV) with mean-square value Ω . The

probability density function depends on the propagation environment of the signal. The corresponding instantaneous SNR per bit and the average SNR per bit can be defined, respectively, by the following equations:

$$\gamma = \alpha^2 \frac{E_b}{N_o} \quad (3.2)$$

$$\Omega = \overline{\alpha^2} \frac{E_b}{N_o} \quad (3.3)$$

Since we are interested in conducting the performance analysis in terms of the average SNR, by making a change of variables in eq. (3.1), the pdf of the instantaneous SNR has the exponential pdf given by:

$$f_\gamma(\gamma) = \frac{1}{\Omega} \exp\left(-\frac{\gamma}{\Omega}\right), \quad \gamma \geq 0 \quad (3.4)$$

3.2.2 Nakagami

The Nakagami distribution is another common distribution that can be used to model the statistics of short term fading. The Rayleigh distribution does not provide a good fit to measured data in many practical fading environments. One limitation of the Rayleigh distribution is that its pdf of the power is a single parameter, which makes the model less flexible. The Rayleigh distribution is thus inadequate to model all fading conditions in some wireless channels, and researchers have introduced other models to describe fading effects that cannot be characterized by the Rayleigh fading channel model. The Nakagami-m fading model can be used to model fading conditions which are either more or less severe than Rayleigh fading distribution [24]; and it provides more accurate fit in many experimental tests than the Rayleigh distribution [25]- [53]. It has also been shown in several works that the Nakagami-m distribution provides the best fit

to land-mobile [24 -26] and indoor-mobile [27]- [54]. The amplitude of the received signal envelope, in a Nakagami- m fading environment, can be expressed as:

$$f_{\alpha}(\alpha) = \frac{2m^m \alpha^{2m-1}}{\Omega^m \Gamma(m)} \exp\left(-\frac{m\alpha^2}{\Omega}\right), \alpha \geq 0 \quad (3.5)$$

where $\Gamma(c) = \int_0^{\infty} t^{c-1} e^{-t} dt$ is the well-known gamma function [48-49] and m is the Nakagami- m fading parameter which characterizes the fading severity and takes values in the interval from $1/2$ to ∞ .

Unlike the Rayleigh distribution, the parameters in the Nakagami- m distribution can be tweaked to obtain other distributions used to model fading channels. In equation (3.5), by adjusting the fading parameter m , other distributions are obtained from the Nakagami- m distribution. The Nakagami- m distribution reduces to the Rayleigh distribution when $m = 1$, and it equivalent to the one-sided Gaussian channel when $m = 1/2$ [65]. The corresponding pdf of the instantaneous power is distributed according to a gamma distribution given as:

$$f_{\gamma}(\gamma) = \frac{m^m \gamma^{m-1}}{\Omega^m \Gamma(m)} \exp\left(-\frac{m\gamma}{\Omega}\right), \gamma \geq 0 \quad (3.6)$$

3.2.3 Generalized-Gamma

The three-parameter Generalized Gamma (GG) distribution was first introduced by Stacy [62] as a generalization of the gamma distribution. Later on, Yacoub rewrote the GG distribution in a more compact form in terms of two parameters, which depend on the physical properties of the transmission medium [29]. Griffiths and McGeehan [59] then presented the GG distribution as a more general gamma distribution that can be used to model radio-wave propagation. In [58]- [61], the probability density function of the

received signal envelope, in a Generalized-Gamma fading environment, may be written in terms of three parameters. As such, the GG is flexible and is easy to mathematically manipulated. The parameters in the GG distribution can be varied to obtain other fading type distributions. These distributions include the gamma, Nakagami-m, exponential, Weibul, and Rayleigh distributions. The pdf of the envelope α of the received signal in a GG fading environment is given by [31]:

$$f_{\alpha}(\alpha) = \frac{2v\alpha^{2vm-1}}{\Gamma(m)\Omega^m} \exp\left(-\left(\frac{m}{\Omega}\right)\alpha^{2v}\right), \quad \alpha > 0, m > 0 \quad (3.7)$$

where m is the fading parameter, and v is the shape parameter. For example, when $m = 1, v = 1$, we obtain the Rayleigh distribution; the Nakagami-m is obtained when $v = 1$. Other special cases of the Generalized-Gamma distribution are the Weibull distribution for which is obtained when $m = 1$, and the lognormal distribution which is obtained when $m \rightarrow \infty, v \rightarrow 0$. The probability density function of the signal-to-noise-ratio for the GG is given by:

$$f_{\gamma}(\gamma) = \frac{v\beta^{mv}\gamma^{vm-1}}{\Gamma(m)\Omega^{mv}} \exp\left(-\left(\frac{\beta\gamma}{\Omega}\right)^v\right) \quad (3.8)$$

In (3.8), the Nakagami-m fading distribution is obtained when $v = 1$, and we have $\beta = m$.

3.3 Shadowing

In terrestrial and satellite land-mobile systems, the link quality of the receiver suffers from shadowing caused by slow variation associated with large scale environmental obstacles such as tall buildings, terrains, and trees. As such, the local mean power varies randomly from place to place within a specified geographical

location. Several studies in the literature based on empirical measurement have argued that the local mean power has a log-normal distribution in both indoor and outdoor environments [28] given by:

$$f_{\gamma}(\gamma) = \frac{\zeta}{\sqrt{2\pi}\sigma\gamma} \exp\left[-\frac{(10\log_{10}\gamma - \mu)^2}{2\sigma^2}\right] \quad (3.9)$$

where $\zeta = 10/\ln 10$ and μ and σ are, respectively, the mean and the standard deviation of $10\log_{10}\gamma$, both expressed in dB units.

3.4 Composite

In many situations, a signal propagating in a wireless medium is subject to both short term-fading and long term-fading. Typically, this type of situation occurs in congested city areas with slow traffic and slow-moving pedestrians [23]. Due to the presence of multipath fading superimposed on log-normal shadowing, the average power of the received signal is random in a composite fading environment. Therefore, it is impractical for the receiver to average out the envelope fading due to multipath. As such, the receiver is to react to the instantaneous composite multipath/shadowed signal.

Two approaches are commonly used in the literature for modeling a composite distribution. One approach is to express the square envelope as a conditional density and integrating over the density of the condition. In the presence of both multipath and shadow fading, the composite pdf for the received signal power of two fading random distributions with respectively SNR γ_D and γ_E can mathematically be expressed as follows:

$$f_{\gamma_D}(\gamma_D) = \int_0^{\infty} f_{\gamma_D|\gamma_E}(\gamma_D|\gamma_E) f_{\gamma_E}(\gamma_E) d\gamma_E \quad (3.10)$$

where $f_{\gamma_D|\gamma_E}(\cdot|\cdot)$ is the conditional pdf for the received SNR power, given the average signal power γ_D and $p_{\gamma_D}(\cdot)$ is the pdf of the average signal power.

Several models have been used in the literature to model the simultaneous effect of fading and shadowing on the received signal [63]. Among the well-known composite statistical models that are used to model multipath fading and shadowing include the Nakagami-Lognormal and the Rayleigh-log-normal (Suzuki) distributions [55]. Nevertheless, closed-form expressions do not exist for these distributions; and thus make it difficult to evaluate system performances with these distributions [56]. Other distributions such as the gamma distribution was proposed to model shadow fading because the gamma distribution is mathematically easy to handle as compared to both the Nakagami-Lognormal and the Suzuki distributions [56]. For example, the gamma distribution was proposed instead of the log-normal distribution to model shadow fading; and it was proved that the gamma distribution fits well the analytical and experimental data compared to the log-normal distribution [56]. Other classes distributions have derived from the gamma distribution and proven to be good fit for modeling shadow fading. These classes of distributions include the K-distribution, the Generalized-K distribution, and the General-Extended-K distribution.

3.4.1 Generalized-K Channel Fading Model

The Generalized-K (GK) distribution is used to model the effects of both fading and shadowing in wireless communication systems. The GK distribution is a general model with adjustable parameters; in which other fading distributions such as the K-

distribution is a special case [30] and the Rayleigh-Lognormal and Nakagami-Lognormal distributions are accurately approximated by the GK [25]. The probability density function of the received signal envelope, in a Generalized-K fading environment, is given by [33]:

$$f_{\alpha}(\alpha) = \frac{4\alpha^{m+k-1}}{\Gamma(m)\Gamma(k)} \left(\frac{m}{\Omega}\right)^{\frac{k+m}{2}} K_{k-m} \left(2 \left(\frac{m}{\Omega}\right)^{1/2} \alpha\right) \quad \alpha \geq 0 \quad (3.11)$$

Let $\beta = k + m - 1$ and $\omega = k - m$, then

$$f_{\alpha}(\alpha) = \frac{4m^{(\beta+1)/2}}{\Gamma(m)\Gamma(k)\Omega^{(\beta+1)/2}} \alpha^{\beta} K_{\omega} \left(2 \left(\frac{m}{\Omega}\right)^{1/2} \alpha\right) \quad \alpha \geq 0 \quad (3.12)$$

where k, m are the shaping parameters of the distribution. $K_v(\cdot)$ is the v th order modified Bessel function of the second kind [48, eq. (8.407.1)]. The two parameters m and k can be adjusted in the Generalized-K distribution to obtain other fading distributions. For example, when $k \rightarrow \infty$, the Generalized-K approximates to the Nakagami-m distribution [22]. For $m = 1$, the Generalized-K corresponds with the K-distribution, and when $m \rightarrow \infty$ and $k \rightarrow \infty$, the Generalized-K approximates to the R-L fading condition [64]-[65]. The pdf of the SNR for the Generalized-K distribution is expressed in the following form:

$$f_{\gamma}(\gamma) = \frac{2}{\Gamma(m)\Gamma(k)} \left(\frac{km}{\Omega}\right)^{\frac{m+k}{2}} \gamma^{\frac{k+m}{2}-1} K_{k-m} \left(2 \sqrt{\frac{km\gamma}{\Omega}}\right), \quad i \in \{D, E\} \quad (3.13)$$

We note in eq. (3.13), for $m = 1$, the Generalized-K distribution reduces to the Suzuki distribution [25], which approximates accurately the Rayleigh-lognormal distribution.

Because of the modified Bessel functions present in eq. (3.13), it is very difficult to obtain closed-form expression in the evaluation of performance metrics when using eq.

(3.13). In [68-70], the authors have shown that the sum of independent (GK) can be approximated by another GK distribution. Therefore, the pdf of SNR of the Generalized-K can be expressed by [43]:

$$f_{\gamma_i}(\gamma) = \frac{2\Xi^{\frac{\beta_i+1}{2}}}{\Gamma(m_i)\Gamma(k_i)} \gamma^{\frac{\beta_i-1}{2}-1} K_{\eta_i}(\sqrt{\Xi\gamma 2}), i \in \{D, E\} \quad (3.14)$$

where $m_i, i \in \{D, E\}$ and $k_i \in \{D, E\}$ are the fading parameters of the random variables that model the main and eavesdropper channels, respectively, and $\Xi = \frac{km}{\bar{\gamma}}$.

3.5 G-Function Channels Fading Models

Most common distributions in wireless communication can be expressed in terms of the Meijer G-function [48]- [66]. The Meijer G-function is a very useful mathematical function that possesses some nice properties, and it is widely used in the performance evaluation of wireless networks. Meijer G-function can be computed in Wolfram or MATLAB via the Mupad function. We assume that the channel distributions can be expressed in terms of the Meijer G-function as follows:

$$f_{\gamma}(\gamma) = G_{p,q}^{m,n} \left(A\gamma \middle| b_q^{a_p} \right), \gamma \geq 0 \quad (3.15)$$

where $G(.)$ is the Meijer's G-function and a_p and b_q are the parameters of the G-function.

CHAPTER 4: DIRECT INTEGRATION METHOD

4.1 Introduction

There is extensive literature on the use of the direct integration to evaluate the performance metrics such as the average secrecy capacity, the outage probability and the secrecy outage probability for wireless networks. The integration approach works well for channel models for which closed-form expressions for the performance metrics can be easily obtained such as the Rayleigh and Nakagami-m channels. In these cases, the integration approach is convenient and provides accurate results especially as those integrals do not carry much complexity in their evaluation. However, in many practical applications in wireless system networks, the fading environment is characterized by a complicated channel model other than the simple Rayleigh and Nakagami-m. More specifically, in generalized fading environments, the pdf of the SNR may not exist in simple and canonical form. Therefore, the computation of performance metrics requires the evaluation of several integrals which can be cumbersome. The direct integration presents some inconvenience for the generalized fading environments and the sophisticated diversity techniques; yet it is still a very useful tool for the analysis of performance of wireless networks. In this chapter we present the direct integration method to allow the computation of the secrecy outage probability for channel models in which the integration can be handled.

4.2 Direct Integration Based Approach

The secrecy outage probability was defined in Section 2.4 as:

$$P_O = \int_0^\infty F_{\gamma_D}(\theta\gamma_E + \theta - 1) f_{\gamma_E}(\gamma_E) d\gamma_E \quad (4.1)$$

The integrant in the above expression is the product of two terms. Using integration by parts, we have:

$$P_O = \int_0^\infty \underbrace{F_{\gamma_D}(\theta\gamma_E + \theta - 1)}_U \underbrace{f_{\gamma_E}(\gamma_E)}_{dV} d\gamma_E$$

Let $V = F_{\gamma_E}(\gamma_E)$, $dU = \theta f_{\gamma_D}(\theta\gamma_E + \theta - 1) d\gamma_E$, we obtain:

$$\begin{aligned} P_O &= F_{\gamma_D}(\theta\gamma_E + \theta - 1) F_{\gamma_E}(\gamma_E) \Big|_0^\infty - \theta \int_0^\infty f_{\gamma_D}(\theta\gamma_D + \theta - 1) F_{\gamma_E}(\gamma_E) d\gamma_E \\ &= 1 - \theta \int_0^\infty f_{\gamma_D}(\theta\gamma_E + \theta - 1) F_{\gamma_E}(\gamma_E) d\gamma_E . \end{aligned} \quad (4.2)$$

4.3 Secrecy Outage Probability Using Integration Approach

In this section, we use the integration method to compute the secrecy outage probability for the Rayleigh, Nakagami-m, and the Generalized-K fading channels. Equation (4.1) follows from the model depicted in Section 2.1, where the signal-to-noise ratio of the main and the eavesdropper channels are given respectively by γ_D and γ_E . From (4.1), the computation of the secrecy outage probability requires the CDF of the main channel and the pdf of the eavesdropper channel.

4.3.1 Rayleigh Fading Case

For the Rayleigh fading environment, the pdf of the received SNR is given in (3.4). The corresponding cumulative distribution function (CDF) of the channel is given by:

$$F_\gamma(\gamma) = 1 - \exp\left(-\frac{\gamma}{\Omega}\right) \quad (4.3)$$

Substituting (3.4) and (4.3) in (4.1) gives:

$$\begin{aligned}
P_O &= \int_0^\infty \left\{ 1 - \exp\left(-\frac{(\theta\gamma_E + \theta - 1)}{\Omega_{\gamma_D}}\right) \right\} \frac{1}{\Omega_{\gamma_E}} \exp\left(-\frac{\gamma_E}{\Omega_{\gamma_E}}\right) d\gamma_E \\
&= 1 - \frac{1}{\Omega_{\gamma_E}} \exp\left(-\frac{(\theta - 1)}{\Omega_{\gamma_D}}\right) \int_0^\infty \exp\left(-\gamma_E \left[\frac{\theta}{\Omega_{\gamma_D}} + \frac{1}{\Omega_{\gamma_E}}\right]\right) d\gamma_E \\
&= 1 - \left(\frac{\Omega_{\gamma_D}}{\Omega_{\gamma_E}\theta + \Omega_{\gamma_D}}\right) \exp\left(-\frac{(\theta - 1)}{\Omega_{\gamma_D}}\right).
\end{aligned} \tag{4.4}$$

4.3.2 Nakagami-m Fading Case

The pdf of the SNR in a Nakagami-m fading channel is given in (3.6). The corresponding CDF is given:

$$F_\gamma(\gamma) = \frac{1}{\Gamma(m)} \mathcal{G}\left(m, \frac{m}{\Omega} \gamma\right) \tag{4.5}$$

where $\mathcal{G}(v, x) = \int_0^x t^{v-1} \exp(-t) dt$ is the lower incomplete gamma function [48]. It is important to note that when the Nakagami fading parameter m is an integer, the CDF may be expressed as:

$$F_\gamma(\gamma) = 1 - \exp\left(-\frac{m\gamma}{\Omega}\right) \sum_{k=0}^{m-1} \frac{\left(\frac{m\gamma}{\Omega}\right)^k}{k!} \tag{4.6}$$

Then, the secrecy outage probability is given by:

$$\begin{aligned}
P_O &= \int_0^\infty F_{\gamma_D}(\theta\gamma_E + \theta - 1) f_{\gamma_E}(\gamma_E) d\gamma_E \\
&= \frac{1}{\theta} \int_0^\infty F_{\gamma_D}(\gamma_E + \theta - 1) f_{\gamma_E}(\gamma_E/\theta) d\gamma_E \\
&= 1 - \left(\frac{m_{\gamma_E}}{\Omega_{\gamma_E}\theta}\right)^{m_{\gamma_E}} \frac{1}{\Gamma(m_{\gamma_E})} \times \exp\left(-\frac{m_{\gamma_D}}{\Omega_{\gamma_D}}(\theta - 1)\right) \sum_{k=0}^{m_{\gamma_D}-1} \frac{1}{k!} \left(\frac{m_{\gamma_D}}{\Omega_{\gamma_D}}\right)^k \int_0^\infty \exp\left(-\gamma_E \left\{\frac{m_{\gamma_D}}{\Omega_{\gamma_D}} + \frac{m_{\gamma_E}}{\theta\Omega_{\gamma_E}}\right\}\right) (\gamma_E + \theta - 1)^k \gamma_E^{m_{\gamma_E}-1} d\gamma_E
\end{aligned}$$

$$\begin{aligned}
P_O = 1 - \left(\frac{m_{\gamma_E}}{\Omega_{\gamma_E} \theta} \right)^{m_{\gamma_E}} \exp \left(- \frac{m_{\gamma_D}}{\Omega_{\gamma_D}} (\theta - 1) \right) \\
\times \sum_{k=0}^{m_{\gamma_D}-1} \frac{1}{k!} \left(\frac{m_{\gamma_D}}{\Omega_{\gamma_D}} \right)^k \sum_{i=0}^k \binom{k}{i} \frac{\Gamma(m_{\gamma_E}+i)}{\Gamma(m_{\gamma_E})} \frac{(\theta-1)^{k-i}}{\left(\frac{m_{\gamma_D}}{\Omega_{\gamma_D}} + \frac{m_{\gamma_E}}{\Omega_{\gamma_E} \theta} \right)^{m_{\gamma_E}+i}} . \quad (4.7)
\end{aligned}$$

4.3.3 Generalized K-Fading Case

In the case of the Generalized-K fading channel, for simplicity, we will express the GK in terms of the Meijer G-function, defined in section (3.4), and then perform the integration. For the Generalized-K fading environment, the pdf of the received SNR, in terms of the Meijer G-function (See Appendix B for details) is given by:

$$f_{\gamma}(\gamma) = \frac{\Xi^{\frac{\beta+1}{2}} \gamma^{\frac{\beta+1}{2}-1}}{\Gamma(m)\Gamma(k)} G_{0,2}^{2,0} \left(\Xi \gamma \left| \frac{\omega}{2}, -\frac{\omega}{2} \right. \right) \quad (4.8)$$

The corresponding CDF of the Generalized-K distribution is given by:

$$F_{\gamma}(\gamma) = \frac{1}{\Gamma(m)\Gamma(k)} G_{1,3}^{2,1} \left(\Xi \gamma \left| \frac{\omega+\beta+1}{2}, \frac{\beta-\omega+1}{2}, 0 \right. \right) \quad (4.9)$$

Substituting (4.8) and (4.9) by their respective expression in (4.1) gives:

$$\begin{aligned}
P_O = \frac{(\Xi_E)^{\frac{\beta_E+1}{2}}}{\Gamma(m_D)\Gamma(k_D)\Gamma(m_E)\Gamma(k_E)} \int_0^{\infty} \gamma_E^{\frac{\beta_E+1}{2}-1} G_{0,2}^{2,0} \left(\Xi_E \gamma_E \left| \frac{\omega_E}{2}, -\frac{\omega_E}{2} \right. \right) \\
\times G_{1,3}^{2,1} \left(\Xi_D (\theta \gamma_E + \theta - 1) \left| \frac{\omega_D+\beta_D+1}{2}, \frac{\beta_D-\omega_D+1}{2}, 0 \right. \right) d\gamma_E \quad (4.10)
\end{aligned}$$

Let $t = \Xi_D \theta \gamma_E$, $dt = \Xi_D \theta d\gamma_E$, $\gamma_E = \frac{t}{\Xi_D \theta}$, we have:

$$P_O = \frac{(\Xi_E)^{\frac{\beta_E+1}{2}} (\Xi_D \theta)^{-\frac{\beta_E+1}{2}}}{\Gamma(m_D)\Gamma(k_D)\Gamma(m_E)\Gamma(k_E)} \int_0^{\infty} t^{\frac{\beta_E+1}{2}-1} G_{0,2}^{2,0} \left(\frac{\Xi_E}{\Xi_D \theta} t \left| \frac{\omega_E}{2}, -\frac{\omega_E}{2} \right. \right) dt$$

$$\times G_{1,3}^{2,1} \left(t + \frac{\theta-1}{\varepsilon_D \theta} \left| \frac{\omega_D + \beta_D + 1}{2}, \frac{\beta_D - \omega_D + 1}{2}, 0 \right. \right) dt \quad (4.11)$$

Using [71, eq. (0.7.34.21.0082.01)], we have:

$$\begin{aligned} P_O &= \frac{\theta^{-\left(\frac{\beta_E+1}{2}\right)}}{\Gamma(m_D)\Gamma(k_D)\Gamma(m_E)\Gamma(k_E)} \sum_{n=0}^{\infty} \frac{(-1)^n}{n!} \left(\frac{\theta-1}{\varepsilon_D \theta} \right)^n \\ &\quad \times G_{4,4}^{3,3} \left(\frac{\varepsilon_E}{\varepsilon_D \theta} \left| \frac{1-\beta_E}{2}, n - \frac{\beta_E + \omega_D + \beta_D}{2}, n - \frac{\beta_E - \omega_D + \beta_D}{2}, n - \frac{\beta_E - 1}{2} \right. \right. \\ &\quad \left. \left. \frac{\omega_E}{2}, \frac{-\omega_E}{2}, n - \frac{\beta_E + 1}{2}, n - \frac{\beta_E - 1}{2} \right. \right). \end{aligned} \quad (4.12)$$

When $\theta = 1$, (4.12) reduces to:

$$\begin{aligned} P_O &= \frac{1}{\Gamma(m_D)\Gamma(k_D)\Gamma(m_E)\Gamma(k_E)} G_{4,4}^{3,3} \left(\frac{\varepsilon_E}{\varepsilon_D} \left| \frac{1-\beta_E}{2}, -\frac{\beta_E + \omega_D + \beta_D}{2}, -\frac{\beta_E - \omega_D + \beta_D}{2}, \frac{1-\beta_E}{2} \right. \right. \\ &\quad \left. \left. \frac{\omega_E}{2}, \frac{-\omega_E}{2}, -\frac{\beta_E + 1}{2}, \frac{1-\beta_E}{2} \right. \right) \\ &= \frac{1}{\Gamma(m_D)\Gamma(k_D)\Gamma(m_E)\Gamma(k_E)} G_{3,3}^{3,2} \left(\frac{\varepsilon_E}{\varepsilon_D} \left| -\frac{\beta_E + \omega_D + \beta_D}{2}, -\frac{\beta_E - \omega_D + \beta_D}{2}, \frac{1-\beta_E}{2} \right. \right. \\ &\quad \left. \left. \frac{\omega_E}{2}, \frac{-\omega_E}{2}, -\frac{\beta_E + 1}{2} \right. \right). \end{aligned} \quad (4.13)$$

4.4 Approximation

In this section, we present an approximation of the direct integration method for the Generalized-K distribution. This approximation is based on the assumption that

$\frac{(1+x)}{(1+y)} \simeq x/y$; the authors in [72] - [73] used this approximation. In addition, the effect of

approximation error can be ignored in the high SNR region. It holds that:

$$\frac{1+SNR^D}{1+SNR^E} \simeq \frac{SNR^D}{SNR^E}$$

We have, based on the model described in Chapter 2:

$$\begin{aligned}
P_O &= Pr\left\{\frac{1+\gamma_D}{1+\gamma_E} \leq 2^t\right\}, \text{ where } \theta = 2^t \\
&\approx Pr\left\{\frac{\gamma_D}{\gamma_E} \leq \theta\right\} \\
&= \int_0^\infty F_{\gamma_D}(\theta\gamma_E) f_{\gamma_E}(\gamma_E) d\gamma_E
\end{aligned} \tag{4.14}$$

$$\begin{aligned}
P_O &\cong \frac{(\varepsilon_E)^{\frac{\beta_E+1}{2}}}{\Gamma(m_D)\Gamma(k_D)\Gamma(m_E)\Gamma(k_E)} \int_0^\infty \gamma_E^{\frac{\beta_E+1}{2}-1} G_{0,2}^{2,0}\left(\varepsilon_E\gamma_E \left| \frac{\omega_E}{2}, \frac{-\omega_E}{2} \right.\right) \\
&\quad \times G_{1,3}^{2,1}\left(\varepsilon_D\theta\gamma_E \left| \frac{\omega_D+\beta_D+1}{2}, \frac{\beta_D-\omega_D+1}{2}, 0 \right.\right) d\gamma_E
\end{aligned} \tag{4.15}$$

From [71, eq. (0.7.34.21.0011.01)], we have:

$$P_0 \cong \frac{1}{\Gamma(m_D)\Gamma(k_D)\Gamma(m_E)\Gamma(k_E)} G_{3,3}^{2,3}\left(\frac{\varepsilon_D\theta}{\varepsilon_E} \left| \frac{1, \frac{1-\beta_E-\omega_E}{2}, \frac{1-\beta_E+\omega_E}{2}}{\frac{\omega_D+\beta_D+1}{2}, \frac{\beta_D-\omega_D+1}{2}, 0} \right.\right). \tag{4.16}$$

CHAPTER 5: TAYLOR SERIES APPROACH

5.1 Introduction

In the previous section we used the direct integration method to compute the secrecy outage probability. The direct integration method may present difficulties for systems that require evaluation of several integrals or expressions that involve series. Thus, the evaluation of the outage probability using the direct integration method can be cumbersome and tedious. An alternative approach to circumvent the computation of difficult integral is the use of the Taylor series approach, which is the main contribution of our work. Contrary to the direct integration method that works well for some restricted simple cases by finding the pdf of the random variables, the Taylor series-expansion approach is a general method that can be applied to any fading environment with arbitrary parameters.

5.2 Taylor Series

Taylor Series is broadly used in Mathematics; engineers have borrowed and used it in several fields of engineering. In many engineering applications, sometimes it is difficult to obtain exact results and approximations are just good enough in several cases. Taylor series is a very useful tool because it allows us to express a function as an infinite sum of terms. In this section, we present the Taylor Series expansion to compute the

secrecy outage probability for any arbitrary fading channels distribution. By definition, the Taylor series can be written in the following form:

$$f(\gamma) = \sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!} (\gamma - a)^n \quad (5.1)$$

$$f(\gamma + a) = \sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!} \gamma^n \quad (5.2)$$

where $f^{(n)}(a)$ denotes the n th derivative of f , evaluated at the point a . Based on the system model that was defined in Section (2.2), the secrecy outage probability (SOP) was given in (2.2) by:

$$P_O = \int_0^{\infty} F_{\gamma_D}(\theta\gamma_E + \theta - 1) f_{\gamma_E}(\gamma_E) d\gamma_E \quad (5.3)$$

By applying (5.2), the expression for the secrecy outage probability in (5.3) becomes:

$$F_{\gamma_D}(\theta\gamma_E + \theta - 1) = \sum_{n=0}^{\infty} \frac{[F_{\gamma_D}^{(n)}(\theta-1)]}{n!} (\theta\gamma_E)^n \quad (5.4)$$

By substituting (4.4) in the above equation, we obtain:

$$P_O = \sum_{n=0}^{\infty} \frac{[F_{\gamma_D}^{(n)}(\theta-1)]\theta^n}{n!} \int_0^{\infty} \gamma_E^n f_{\gamma_E}(\gamma_E) d\gamma_E$$

$$P_O = \sum_{n=0}^{\infty} \frac{[F_{\gamma_D}^{(n)}(\theta-1)]\theta^n}{n!} E(\gamma_E^n) \quad (5.5)$$

Equation (5.5) is the main result to compute the secrecy outage probability for any arbitrary fading channel distributions of two random variables. From (5.5), to compute the secrecy outage probability, we only need to find the n th derivative of the CDF of the direct channel and the n th moment of the pdf of the eavesdropper channel. Additionally, (5.5) requires to evaluate the CDF at the zero order which is the CDF itself, and $(\theta - 1)^0$ and $0!$ are defined to be 1.

5.3 Application to Some Common Distributions

In this section, we compute the secrecy outage probability for two common fading distributions, respectively; the Rayleigh and Nakagami-m distributions.

5.3.1 Case 1: Rayleigh

By definition, for any arbitrary random variable γ , the k -th moment is defined by:

$$E(\gamma^k) = \int_0^{\infty} \gamma^k f(\gamma) d\gamma \quad (5.6)$$

Equation (4.5) requires the n -th moment of the distribution of γ_E . We assume that both the main channel and eavesdropper channel undergo the same distribution; therefore, the eavesdropper channel is modeled by another Rayleigh distribution.

For a Rayleigh fading distribution with the pdf of the SNR is given in (3.4), the n th-moment is given by:

$$E(\gamma_E^n) = \frac{1}{\Omega_{\gamma_E}} \int_0^{\infty} \gamma_E^n \exp\left(-\frac{\gamma_E}{\Omega_{\gamma_E}}\right) d\gamma_E = (\Omega_{\gamma_E})^n n! \quad (5.7)$$

The n -th derivative of the CDF of the Rayleigh distribution can be computed as:

$$\frac{d^n}{d\gamma_D^n} \left\{ 1 - \exp\left(-\frac{\gamma_D}{\Omega_{\gamma_D}}\right) \right\} = \frac{(-1)^{n-1}}{\Omega_{\gamma_D}^n} \exp\left(-\frac{\gamma_D}{\Omega_{\gamma_D}}\right) \quad (5.8)$$

Substituting (5.7) and (5.8) into (5.5), we have:

$$\begin{aligned} P_O &= \sum_{n=0}^{\infty} \frac{[F_{\gamma_D}^{(n)}(\theta-1)]\theta^n}{n!} E(\gamma_E^n) \\ &= F_{\gamma_D}(\theta-1) + \sum_{n=1}^{\infty} \frac{[F_{\gamma_D}^{(n)}(\theta-1)]\theta^n}{n!} E(\gamma_E^n) \\ &= 1 - \exp\left(-\frac{\theta-1}{\Omega_{\gamma_D}}\right) + \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n!\Omega_{\gamma_D}^n} \exp\left(-\frac{(\theta-1)}{\Omega_{\gamma_D}}\right) (\Omega_{\gamma_E}\theta)^n n! \\ &= 1 - \exp\left(-\frac{\theta-1}{\Omega_{\gamma_D}}\right) + \exp\left(-\frac{(\theta-1)}{\Omega_{\gamma_D}}\right) \sum_{n=1}^{\infty} (-1)^{n-1} \left(\frac{\Omega_{\gamma_E}\theta}{\Omega_{\gamma_D}}\right)^n; \end{aligned}$$

Making the change of variable $k = n - 1$, the result becomes:

$$\begin{aligned} P_O &= 1 - \exp\left(-\frac{\theta-1}{\Omega_{\gamma_D}}\right) + \left(\frac{\Omega_{\gamma_E}\theta}{\Omega_{\gamma_D}}\right) \exp\left(-\frac{(\theta-1)}{\Omega_{\gamma_D}}\right) \sum_{k=0}^{\infty} \left(-\frac{\Omega_{\gamma_E}\theta}{\Omega_{\gamma_D}}\right)^k \\ &= 1 - \exp\left(-\frac{\theta-1}{\Omega_{\gamma_D}}\right) + \left(\frac{\Omega_{\gamma_E}\theta}{\Omega_{\gamma_D}}\right) \exp\left(-\frac{(\theta-1)}{\Omega_{\gamma_D}}\right) \left(\frac{\Omega_{\gamma_D}}{\Omega_{\gamma_E}\theta + \Omega_{\gamma_D}}\right) \\ &= 1 - \exp\left(-\frac{\theta-1}{\Omega_{\gamma_D}}\right) + \left(\frac{\Omega_{\gamma_E}\theta}{\theta\Omega_{\gamma_E} + \Omega_{\gamma_D}}\right) \exp\left(-\frac{(\theta-1)}{\Omega_{\gamma_D}}\right) \\ P_O &= 1 - \left(\frac{\Omega_{\gamma_D}}{\theta\Omega_{\gamma_E} + \Omega_{\gamma_D}}\right) \exp\left(-\frac{(\theta-1)}{\Omega_{\gamma_D}}\right). \end{aligned} \quad (5.9)$$

5.3.2 Nakagami-m

The pdf of the SNR at the eavesdropper is given as:

$$f_{\gamma_E}(\gamma_E) = \left(\frac{m_{\gamma_E}}{\Omega_{\gamma_E}}\right)^{m_{\gamma_E}} \frac{\gamma_E^{m_{\gamma_E}-1}}{\Gamma(m_{\gamma_E})} \exp\left(-\frac{m_{\gamma_E}}{\Omega_{\gamma_E}}\gamma_E\right) u(\gamma) \quad (5.10)$$

with n-th moment given by:

$$\begin{aligned}
E(\gamma_E^n) &= \frac{1}{\Gamma(m_{\gamma_E})} \left(\frac{m_{\gamma_E}}{\Omega_{\gamma_E}} \right)^{m_{\gamma_E}} \int_0^\infty \gamma_E^{m_{\gamma_E}+n-1} \exp\left(-\frac{m_{\gamma_E}}{\Omega_{\gamma_E}} \gamma_E\right) d\gamma_E \\
&= \frac{1}{\Gamma(m_{\gamma_E})} \left(\frac{m_{\gamma_E}}{\Omega_{\gamma_E}} \right)^{m_{\gamma_E}} \frac{\Gamma(m_{\gamma_E}+n)}{\left(\frac{m_{\gamma_E}}{\Omega_{\gamma_E}} \right)^{m_{\gamma_E}+n}} = \frac{\Gamma(m_{\gamma_E}+n)}{\Gamma(m_{\gamma_E})} \left(\frac{\Omega_{\gamma_E}}{m_{\gamma_E}} \right)^n
\end{aligned} \tag{5.11}$$

Putting (5.10) and (5.11) into (5.5), the SOP becomes:

$$\begin{aligned}
P_O &= F_{\gamma_D}(\theta - 1) + \sum_{n=1}^\infty \frac{[F_{\gamma_D}^{(n)}(\theta-1)]\theta^n}{n!} E(\gamma_E^n) \\
&= 1 - \sum_{k=0}^{m_{\gamma_D}-1} \frac{1}{k!} \left(\frac{m_{\gamma_D}}{\Omega_{\gamma_D}} (\theta - 1) \right)^k \exp\left(-\frac{m_{\gamma_D}}{\Omega_{\gamma_D}} (\theta - 1)\right) \\
&+ \exp\left(-\frac{(\theta-1)}{\Omega_{\gamma_D}}\right) \sum_{n=1}^\infty \frac{\Gamma(m_{\gamma_E}+n)}{n! \Gamma(m_{\gamma_E})} \left(\frac{\Omega_{\gamma_E} \theta}{m_{\gamma_E}} \right)^n \frac{d^n}{d\gamma_D^n} \left\{ \frac{1}{\Gamma(m_{\gamma_D})} \gamma \left(m_{\gamma_D}, \frac{m_{\gamma_D}}{\Omega_{\gamma_D}} \gamma_D \right) \right\} \Big|_{\gamma_D=\theta-1}. \tag{5.12}
\end{aligned}$$

5.4 Application to G-Fading Channels

In this section, we apply the Taylor series approach to the more general fading channel: The G-Fading channels. We proceed by finding the nth derivative and the nth moment for the G-fading channels with pdf given by:

$$f_\gamma(\gamma) = A\gamma^{-1} G_{p,q}^{m,n} \left(B\gamma^v \middle| \begin{matrix} a_p \\ b_q \end{matrix} \right) \tag{5.13}$$

5.4.1 Derivation of nth Derivative

The Meijer G-function is a special case of the Fox's H-function for which the parameter a_p is unity in the definition of the H-function (See Appendix A for details).

We derive the nth-derivative here by starting with the H-function and then convert the H-function to the G-function. We start with

$$\frac{d^n}{d\gamma^n} \left[H_{p,q}^{m,n} \left(a\gamma^\sigma \left| \begin{matrix} (a_p, A_p) \\ (b_q, B_q) \end{matrix} \right. \right) \right] = \gamma^{-n} H_{p+1,q+1}^{m,n+1} \left(a\gamma^\sigma \left| \begin{matrix} (0, \sigma), (a_p, A_p) \\ (b_q, B_q), (n, \sigma) \end{matrix} \right. \right) \quad (5.14)$$

Let $A_p = B_q = 1$

$$\begin{aligned} \frac{d^n}{d\gamma^n} \left[H_{p,q}^{m,n} \left(a\gamma^\sigma \left| \begin{matrix} (a_p, 1) \\ (b_q, 1) \end{matrix} \right. \right) \right] &= \frac{d^n}{d\gamma^n} \left[G_{p,q}^{m,n} \left(a\gamma^\sigma \left| \begin{matrix} (a_p) \\ (b_q) \end{matrix} \right. \right) \right] \\ &= \gamma^{-n} H_{p+1,q+1}^{m,n+1} \left(a\gamma^\sigma \left| \begin{matrix} (0, \sigma), (a_p, 1) \\ (b_q, 1), (n, \sigma) \end{matrix} \right. \right) \end{aligned} \quad (5.15)$$

$$= \gamma^{-n} \frac{1}{2\pi j} \oint_{\mathcal{C}} \frac{\Gamma(1-\sigma s) \prod_{k=1}^m \Gamma(b_k+s) \prod_{k=1}^n \Gamma(1-a_k-s)}{\Gamma(1-n-\sigma s) \prod_{k=m+1}^q \Gamma(1-b_k-s) \prod_{k=n+1}^p \Gamma(a_k+s)} (a\gamma^\sigma)^{-s} ds \quad (5.16)$$

where we have used the definition of the H-function to obtain (5.16). Using the gamma multiplication formula [48], we can write:

$$\begin{aligned} \frac{\Gamma(1-\sigma s)}{\Gamma(1-n-\sigma s)} &= \frac{\Gamma\left[\sigma\left(\frac{1}{\sigma}-s\right)\right]}{\Gamma\left[\sigma\left(\frac{1-n}{\sigma}-s\right)\right]} = \frac{(2\pi)^{\frac{1-\sigma}{2}} \sigma^{1-\sigma s - \frac{1}{2}} \prod_{k=0}^{\sigma-1} \Gamma\left(\frac{1}{\sigma}-s+\frac{k}{\sigma}\right)}{(2\pi)^{\frac{1-\sigma}{2}} \sigma^{1-n-\sigma s - \frac{1}{2}} \prod_{k=0}^{\sigma-1} \Gamma\left(\frac{1-n}{\sigma}-s+\frac{k}{\sigma}\right)} \\ &= \sigma^n \frac{\prod_{k=0}^{\sigma-1} \Gamma\left(\frac{1+k}{\sigma}-s\right)}{\prod_{k=0}^{\sigma-1} \Gamma\left(\frac{1-n+k}{\sigma}-s\right)} = \sigma^n \frac{\prod_{k=0}^{\sigma-1} \Gamma\left(1-\frac{\sigma-1-k}{\sigma}-s\right)}{\prod_{k=0}^{\sigma-1} \Gamma\left(1-\frac{\sigma-1+n-k}{\sigma}-s\right)}; \end{aligned} \quad (5.17)$$

Note that:

$$\begin{aligned} \left(\frac{\sigma-1-k}{\sigma}\right) &\rightarrow \left(\frac{\sigma-1}{\sigma}\right), \left(\frac{\sigma-2}{\sigma}\right), \left(\frac{\sigma-3}{\sigma}\right), \dots, \left(\frac{1}{\sigma}\right), \left(\frac{0}{\sigma}\right) \rightarrow \Delta(0, \sigma) \\ \left(\frac{\sigma-1+n-k}{\sigma}\right) &\rightarrow \left(\frac{\sigma-1+n}{\sigma}\right), \left(\frac{\sigma+n-2}{\sigma}\right), \left(\frac{\sigma+n-3}{\sigma}\right), \dots, \left(\frac{n+1}{\sigma}\right), \left(\frac{n}{\sigma}\right) \rightarrow \Delta(n, \sigma) \end{aligned}$$

The right hand side of (5.16) then becomes:

$$\text{RHS} = \gamma^{-n} \frac{1}{2\pi j} \oint_{\mathcal{C}} \sigma^n \frac{\prod_{k=1}^m \Gamma(b_k+s) \prod_{k=1}^n \Gamma(1-a_k-s) \prod_{k=0}^{\sigma-1} \Gamma\left(\frac{1+k}{\sigma}-s\right)}{\prod_{k=m+1}^q \Gamma(1-b_k-s) \prod_{k=n+1}^p \Gamma(a_k+s) \prod_{k=0}^{\sigma-1} \Gamma\left(\frac{1-n+k}{\sigma}-s\right)} (a\gamma^\sigma)^{-s} ds$$

$$= \gamma^{-n} \frac{1}{2\pi j} \oint_C \sigma^n \frac{\prod_{k=1}^m \Gamma(b_k+s) \prod_{k=1}^n \Gamma(1-a_k-s) \prod_{k=0}^{\sigma-1} \Gamma\left(1-\frac{\sigma-1-k}{\sigma}-s\right)}{\prod_{k=m+1}^q \Gamma(1-b_k-s) \prod_{k=n+1}^p \Gamma(a_k+s) \prod_{k=0}^{\sigma-1} \Gamma\left(1-\frac{\sigma-1+n-k}{\sigma}-s\right)} (a\gamma^\sigma)^{-s} ds.$$

Therefore, we have

$$\frac{d^k}{d\gamma^k} \left[G_{p,q}^{m,n} \left(a\gamma^\sigma \left| \begin{matrix} (a_p) \\ (b_q) \end{matrix} \right. \right) \right] = \gamma^{-n} G_{p+\sigma, q+\sigma}^{m, n+\sigma} \left(a\gamma^\sigma \left| \begin{matrix} \Delta(0, \sigma), (a_p) \\ (b_q), \Delta(n, \sigma) \end{matrix} \right. \right) \quad (5.18)$$

5.4.2 Derivation of nth Moment

For the G-fading channel expressed in (5.13), the nth moment is defined as:

$$E(\gamma^k) = \int_0^\infty A \gamma^{k-1} G_{p,q}^{m,n} \left(B\gamma^v \left| \begin{matrix} (a_p) \\ (b_q) \end{matrix} \right. \right) d\gamma$$

Let $t = \gamma^v$, $dt = v\gamma^{v-1}d\gamma$

$$\begin{aligned} E(\gamma^k) &= \int_0^\infty A (t^{1/v})^{k-1} G_{p,q}^{m,n} \left(B(t^{1/v})^v \left| \begin{matrix} (a_p) \\ (b_q) \end{matrix} \right. \right) \frac{dt}{vt^{v-1/v}} \\ &= \int_0^\infty A t^{k-1/v} G_{p,q}^{m,n} \left(Bt \left| \begin{matrix} (a_p) \\ (b_q) \end{matrix} \right. \right) v^{-1} t^{-(\frac{v-1}{v})} dt \\ &= \int_0^\infty t^{\frac{k}{v}-1} v^{-1} G_{p,q}^{m,n} \left(Bt \left| \begin{matrix} (a_p) \\ (b_q) \end{matrix} \right. \right) dt \\ &= \frac{A}{v} \int_{-\infty}^\infty t^{\frac{k}{v}-1} G_{p,q}^{m,n} \left(Bt \left| \begin{matrix} (a_p) \\ (b_q) \end{matrix} \right. \right) dt \\ E(\gamma^k) &= \frac{A}{v} \left[\frac{\prod_{k=1}^m \Gamma\left(\frac{k}{v}+b_k\right) \prod_{k=1}^n \Gamma\left(1-\frac{k}{v}-a_k\right)}{\prod_{k=n+1}^p \Gamma\left(\frac{k}{v}+a_k\right) \prod_{k=m+1}^q \Gamma\left(1-\frac{k}{v}-b_k\right)} B^{-\frac{k}{v}} \right] \end{aligned} \quad (5.19)$$

5.4.3 The Generalized-K fading Channel Case

Using the results found in (5.18) and (5.19), the n th derivative and the n th moment of the pdf of the Generalized-k (GK) fading channels are given as follow:

$$\begin{aligned} & \frac{d^n}{d\gamma_D^n} \left[\frac{1}{\Gamma(m_D)\Gamma(k_D)} G_{1,3}^{2,1} \left(\Xi_D \gamma_D \left| \frac{\omega_D + \beta_D + 1}{2}, \frac{\beta_D - \omega_D + 1}{2}, 0 \right. \right) \right] \\ &= \frac{(\Xi_D)^{2n}}{\Gamma(m_D)\Gamma(k_D)} G_{2,4}^{2,2} \left(\Xi_D (\theta - 1) \left| \frac{\omega_D + \beta_D + 1}{2} - n, \frac{\beta_D - \omega_D + 1}{2} - n, -n, 0 \right. \right) \end{aligned} \quad (5.20)$$

$$\begin{aligned} E(\gamma_E^n) &= \frac{(\Xi_E)^{\frac{\beta_E + 1}{2}}}{\Gamma(m_E)\Gamma(k_E)} \int_0^\infty \gamma_E^{\frac{\beta_E + 1}{2} + n - 1} G_{0,2}^{2,0} \left(\Xi_E \gamma_E \left| \frac{\omega_E}{2}, \frac{-\omega_E}{2} \right. \right) d\gamma_E \\ &= \frac{\Gamma\left(\frac{\beta_E + \omega_E + 1}{2} + n\right) \Gamma\left(\frac{\beta_E - \omega_E + 1}{2} + n\right)}{\Gamma(m_E)\Gamma(k_E)(\Xi_E)^n} \end{aligned} \quad (5.21)$$

Replacing (5.20) and (5.21) into (5.5), we obtain:

$$\begin{aligned} P_O &= \frac{1}{\Gamma(m_D)\Gamma(k_D)\Gamma(m_E)\Gamma(k_E)} \sum_{n=0}^\infty \left(\frac{(\Xi_D)^2 \theta}{\Xi_E} \right)^n \frac{\Gamma\left(\frac{\beta_E + \omega_E + 1}{2} + n\right) \Gamma\left(\frac{\beta_E - \omega_E + 1}{2} + n\right)}{n!} \\ &\quad \times G_{2,4}^{2,2} \left(\Xi_D (\theta - 1) \left| \frac{\omega_D + \beta_D + 1}{2}, \frac{\beta_D - \omega_D + 1}{2}, 0, n \right. \right). \end{aligned} \quad (5.22)$$

CHAPTER 6: ANALYTICAL AND COMPUTER SIMULATIONS RESULTS

6.1 Introduction

In this chapter, we present some numerical results to illustrate the analysis and provide MATLAB results to validate our derivations for the secrecy outage probability. We compare the secrecy outage probability for three different fading channels, namely; the Rayleigh, Nakagami-m and the Generalized-K fading channels. For each fading distribution, the required system parameters were carefully chosen and varied to provide more insight about the performance of the fading channel model.

6.2 Rayleigh Fading

In this section, we present plots for the secrecy outage probability for the Rayleigh fading environment under different conditions. We provide several plots for the secrecy outage probability versus the average power ($\overline{\gamma_D}$) and the average power ratio ($\lambda = \frac{\overline{\gamma_D}}{\overline{\gamma_E}}$) for the Rayleigh fading channel. We also provide plots for the secrecy outage probability for selected values of the average power at the eavesdropper ($\overline{\gamma_E}$) under a fixed threshold value ($\theta = 2^t$). Figures 6.1, 6.2, 6.3, and 6.4 illustrate that, the secrecy outage probability improves as the average power of the main channel increases. In addition, we observe that as the average power of the main link increases more than the average power of the eavesdropper's link, the secrecy outage probability decreases. As the average power of the eavesdropper's link increases, the secrecy outage probability increases as well. Figures 6.1, 6.2, 6.3 and 6.4 also show the relationship between

the secrecy outage probability with the threshold. It is seen that as the threshold increases, for selected values of $\overline{\gamma}_E$, the secrecy outage probability increases as well.

In Figures 6.5 and 6.6, we investigate the effect of the outage threshold on the secrecy outage probability. We plot the secrecy outage probability versus of the ratio of the average power of the direct link to the average power of the eavesdropper link (i. e., $\lambda = \frac{\overline{\gamma}_D}{\overline{\gamma}_E}$) under different values of the threshold. We observe that the secrecy outage probability for a lower θ outperforms that at a higher θ . We also note that the SOP converges to zero as the average power increases asymptotically. In Figures 6.7 and 6.8, we plot the secrecy outage probability vs $\overline{\gamma}_D$, for fixed values of the threshold, respectively, for $\overline{\gamma}_E = 5$ dB and $\overline{\gamma}_E = 20$ dB. We observe that the SOP converges faster to zero when the average power at the eavesdropper channel is smaller, and specifically, the SOP converges faster for $\overline{\gamma}_E = 5$ dB than for $\overline{\gamma}_E = 20$ dB. From these plots, we conclude that the SOP improves as the average power ratio increases; that is, when as expected, the main channel is better than the eavesdropper channel.

6.3 Nakagami-m Fading

In this section, we provide several plots for the secrecy outage probability for the Nakagami- m fading channel. We plot the secrecy outage probability versus $\overline{\gamma}_D$, for selected values of $\overline{\gamma}_E$ under different values of the threshold. The first scenario we consider is when the fading parameter for both the main and eavesdropper channels suffer Rayleigh fading (i.e., $m_{\gamma_D} = m_{\gamma_E} = 1$). MATLAB simulations confirm the analytical results in equations (4.7) and (5.16), that the Nakagami- m fading environment corresponds to the Rayleigh fading environment when the fading parameter is equal to 1. Figure 6.9 agrees with Figure 6.1 as expected. In the Nakagami- m fading distribution, the parameter m corresponds to the fading

severity and smaller values of m implies more severe fading channel conditions. We consider cases where the Nakagami fading parameter of the main channel is larger than that of the eavesdropper channel. In Figures 6.10 and 6.11, we plot the SOP, respectively, for $(m_{\gamma_D}, m_{\gamma_E}) = (3, 2)$ and $(4, 2)$ for a fixed threshold of $\vartheta = 2^{0.5}$. We observe that the secrecy outage probability for lower $\overline{\gamma_E}$ values outperforms those for larger $\overline{\gamma_E}$ values. We also note that the SOP decreases as the average power at the main channel increases. We observe that the secrecy outage probability decreases as the fading parameter of the main link increases (that, as the quality of the main channel improves). For example, the secrecy outage probability for $(m_{\gamma_D} = 4, m_{\gamma_E} = 2)$ is better than that for $(m_{\gamma_D} = 3, m_{\gamma_E} = 2)$.

In Figures 6.12, we plot the secrecy outage probability when the fading parameter of the eavesdropper channel is larger than the fading parameter of the main channel, $(m_{\gamma_D} = 2, m_{\gamma_E} = 4)$. We observe the same trend; the SOP performance improves as $\overline{\gamma_E}$ decreases. However, the performance of the wireless communication system deteriorates when m_{γ_D} is smaller than m_{γ_E} .

Next we increase the threshold to $\theta = 2^1$ under similar conditions as in Figure 12 in Figures 6.13 and 6.14. We also observe that the SOP for smaller $\overline{\gamma_E}$ outperforms the ones for larger $\overline{\gamma_E}$. However, by comparing Figures 6.13 and 6.14 to Figures 6.10 and 6.11, we notice that the SOP increases as the threshold increases. It is clear that, as the threshold increases, that the performance of the wireless system deteriorates with increasing threshold values. We also notice that the average power gap between the plots decreases as the threshold increases. In Figure 6.15, we plot the SOP for $\theta = 2^1$ when the eavesdropper link is better than the main link, $(m_{\gamma_D} = 2, m_{\gamma_E} = 4)$. The figure shows that the performance of the wireless communication system

deteriorates as the threshold increases, and also its performance degrades when there is more severe fading in the main link than the eavesdropper link. In Figures 6.16 and 6.17, we plot the SOP when both the main and eavesdropper channel undergo identical fading severity (i.e., $m_{\gamma_D} = m_{\gamma_E} = 4$), respectively for $\theta = 2^{0.5}$ and $\theta = 2^{1.0}$. We observe that the secrecy outage probability is smaller for the case when the threshold is smaller ($\theta = 2^{0.5}$). In conclusion, we observe that for both the Rayleigh and Nakagami-m fading channels, the SOP approaches a constant and converges to zero when the average SNR of the main link is asymptotically high.

6.4 Generalized-K Fading

We plot the secrecy outage probability versus $\overline{\gamma_D}$ for the Generalized-K fading distribution in Figures 6.18 and 6.19. From these figures, we see that the secrecy outage probability decreases as the average signal power of the main channel increases. In addition, we also notice that the security performance improves while decreasing the average power of the eavesdropper channel. Furthermore, we see that the secrecy outage probability decreases as the fading factors (k_d, k_E, m_D, m_E) of the GK channel increases. In Figure 6.20, we investigate the effect of the fading parameters on the performance of the wireless communication network. We observe that when the average power at the main link is better than the average power at the eavesdropper link, the secrecy outage probability decreases as the fading parameters increase.

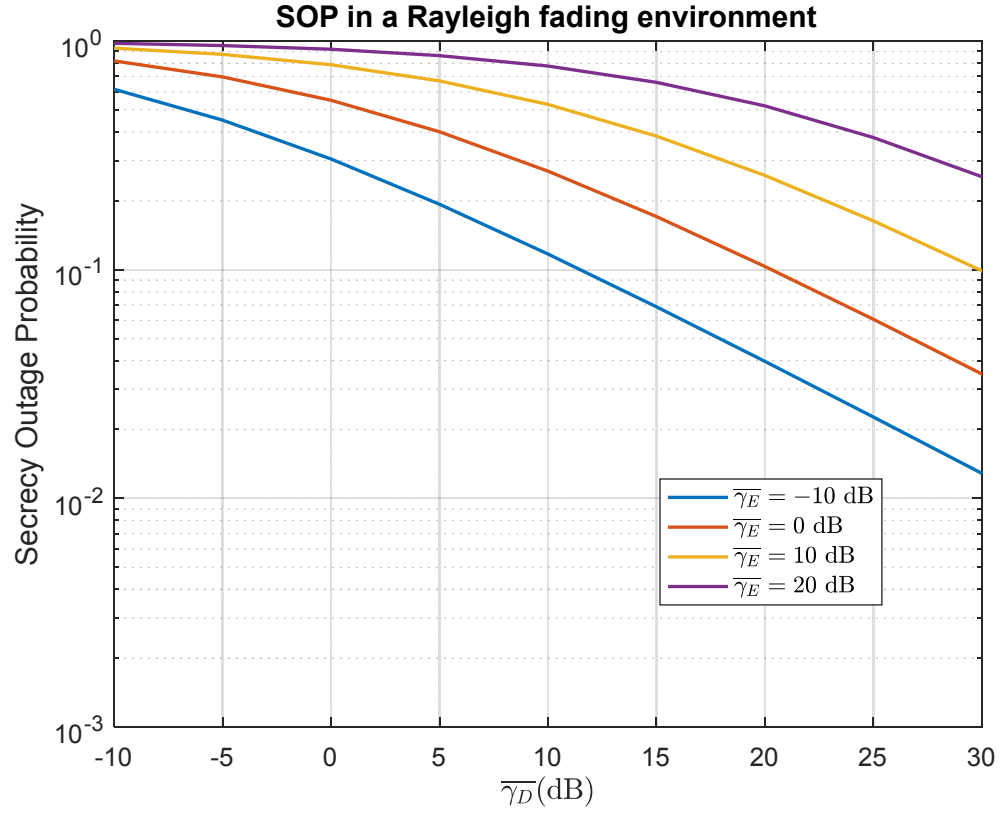


Figure 6.1: Secrecy Outage Probability versus $\bar{\gamma}_D$, in a Rayleigh fading environment, for selected values of $\bar{\gamma}_E$ with $t = 0.1$ bits/s/ Hz ($\theta = 2^{0.1}$).

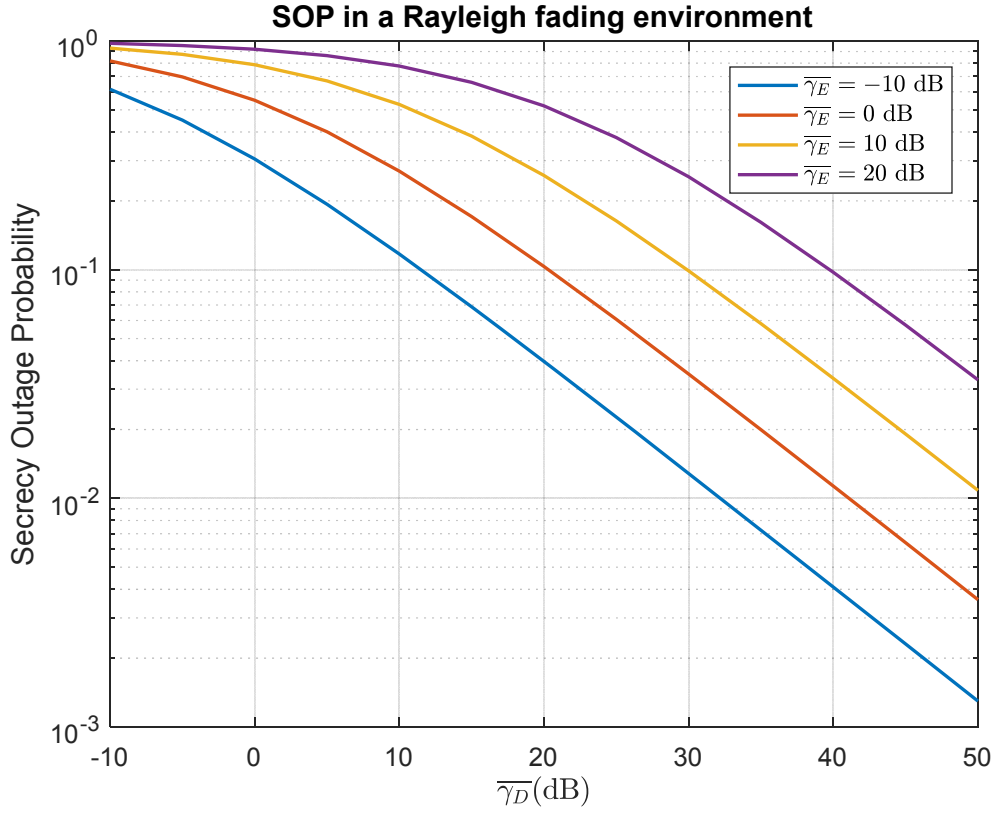


Figure 6.2: Secrecy Outage Probability versus $\overline{\gamma}_D$, in a Rayleigh fading environment, for selected values of $\overline{\gamma}_E$ with $t = 0.75$ bits/s/Hz ($\theta = 2^{0.75}$).

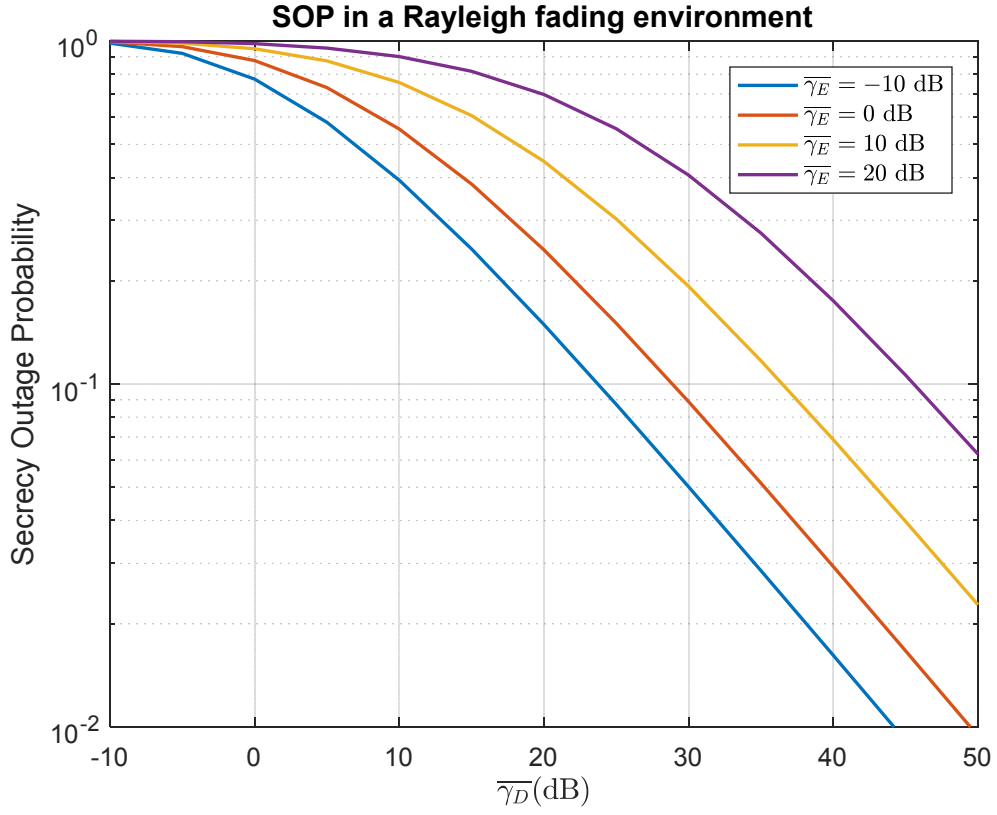


Figure 6.3: Secrecy Outage Probability versus $\bar{\gamma}_D$, in a Rayleigh fading channel, for selected values of $\bar{\gamma}_E$ with $t = 1 \text{ bits/s/Hz}$ ($\theta = 2^1$).

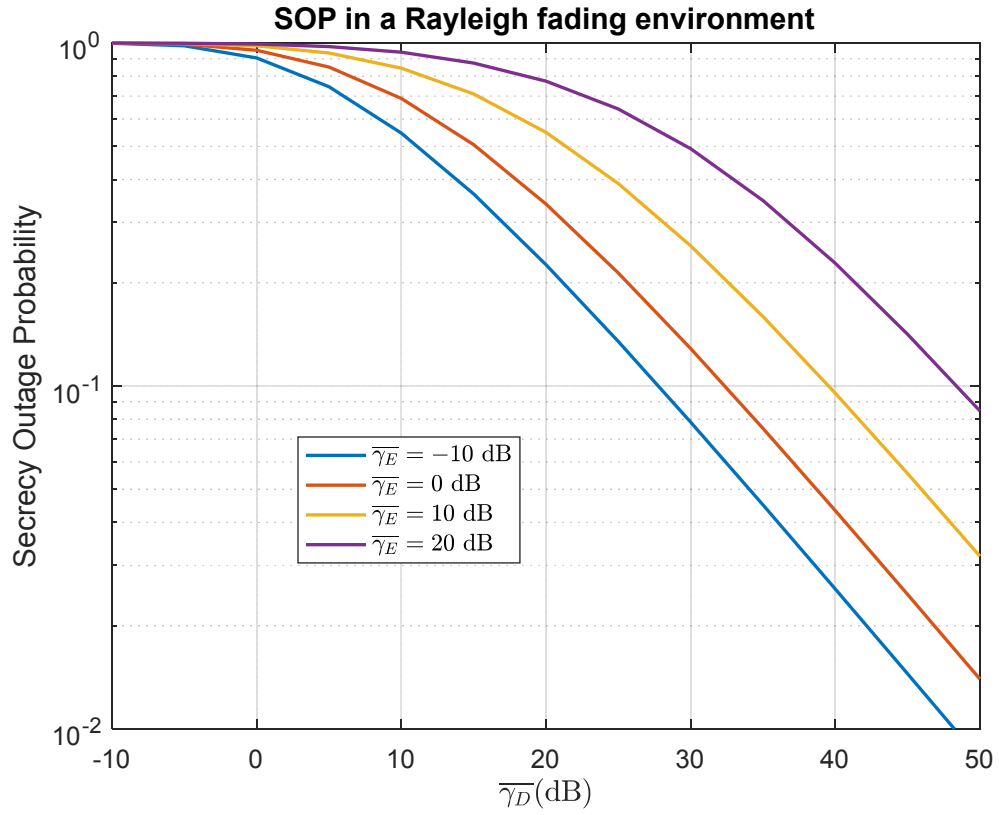


Figure 6.4: Secrecy Outage Probability versus $\bar{\gamma}_D$, in a Rayleigh fading environment, for selected values of $\bar{\gamma}_E$ with $t = 1.45$ bits/s/Hz ($\theta = 2^{1.45}$).

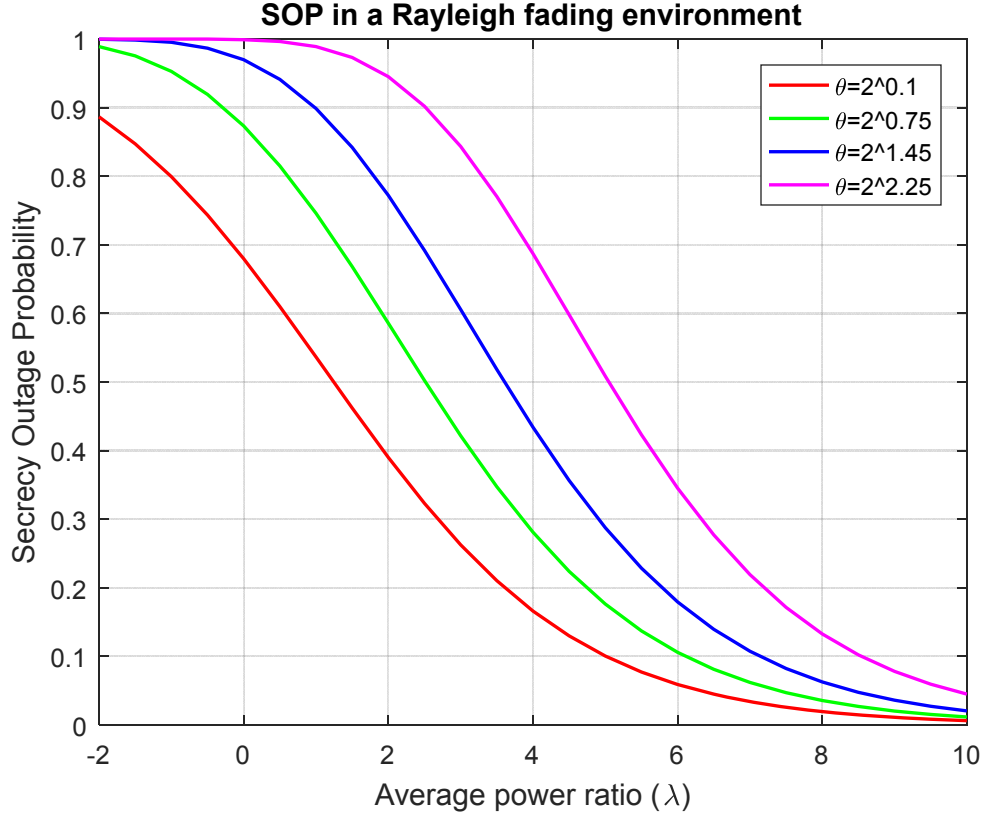


Figure 6.5: Secrecy Outage Probability, in a Rayleigh fading environment, in terms of the average power ratio for selected values of the threshold when the average power at the eavesdropper ($\overline{\gamma}_E$) is 5 dB.

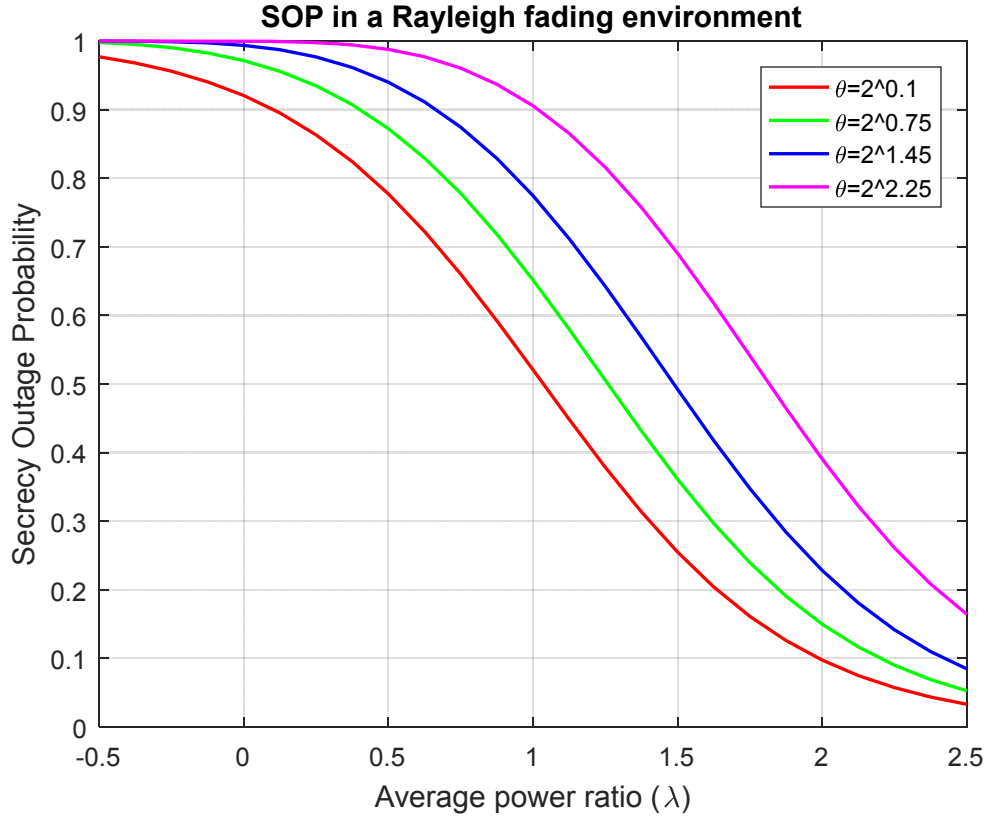


Figure 6.6: Secrecy Outage Probability, in a Rayleigh fading environment, in terms of the average power ratio while varying the threshold values when the average power at the eavesdropper ($\overline{\gamma}_E$) is 20 dB.

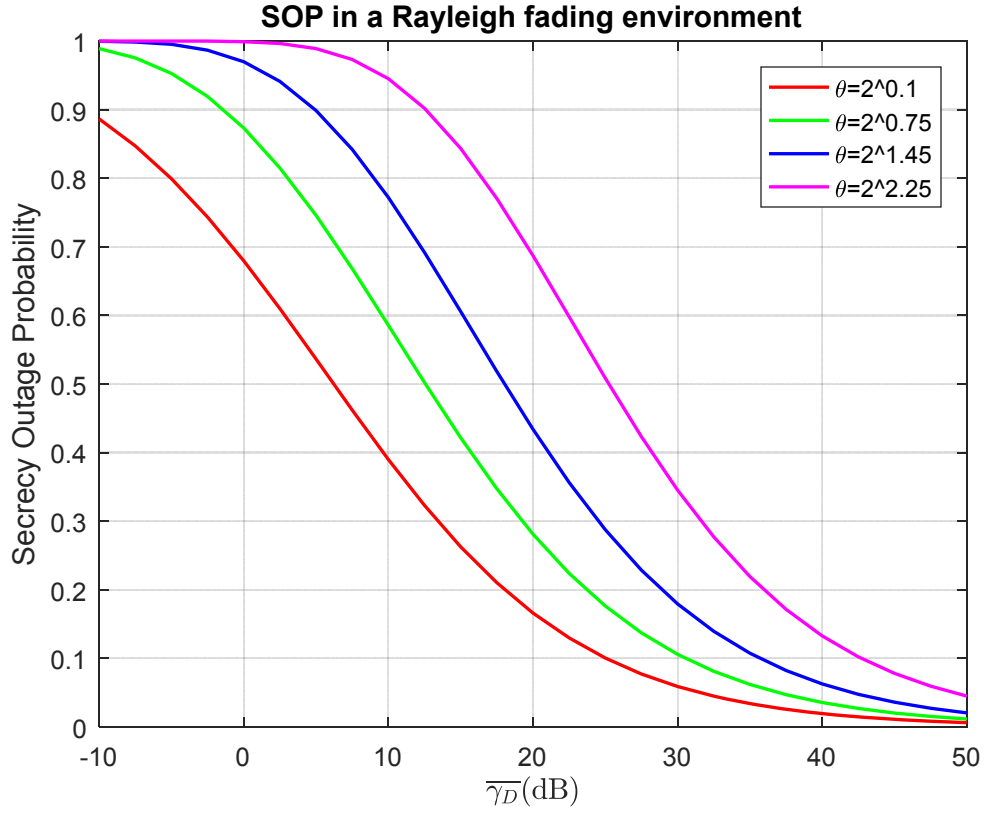


Figure 6.7: Secrecy Outage Probability, in a Rayleigh fading environment, in terms of the average power while varying the threshold values when the average power at the eavesdropper is 5 dB.

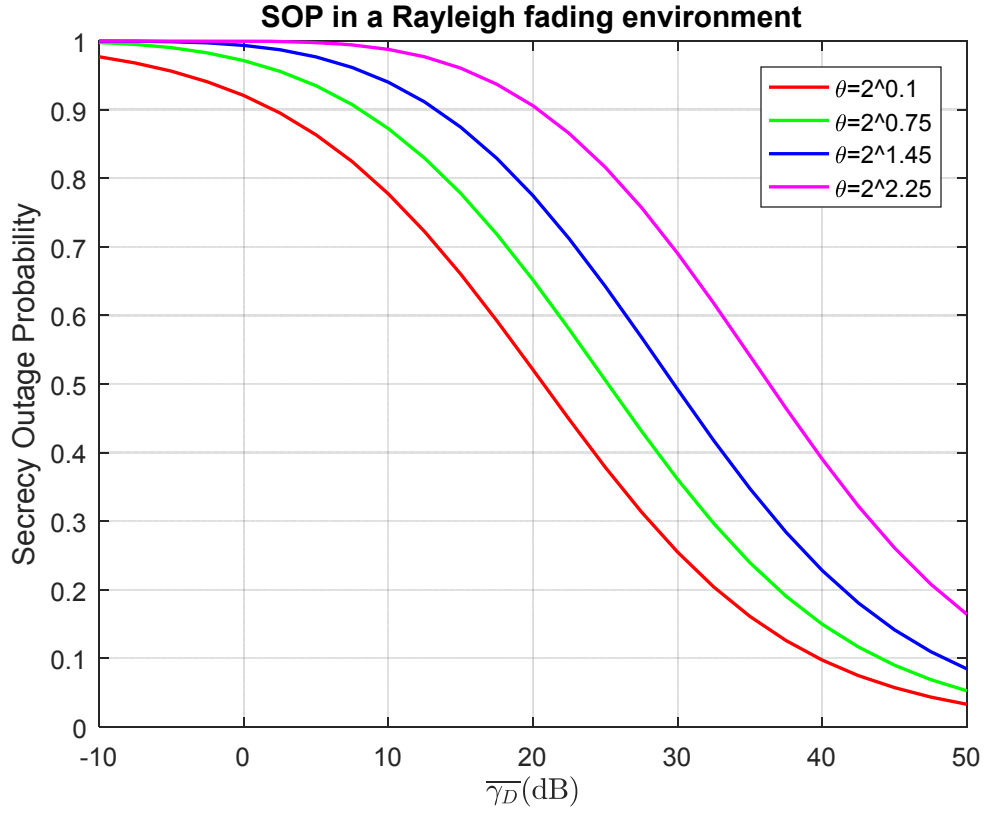


Figure 6.8: Secrecy Outage Probability, in a Rayleigh fading environment, in terms of the average power while varying the threshold values when the average power at the eavesdropper is 20 dB.

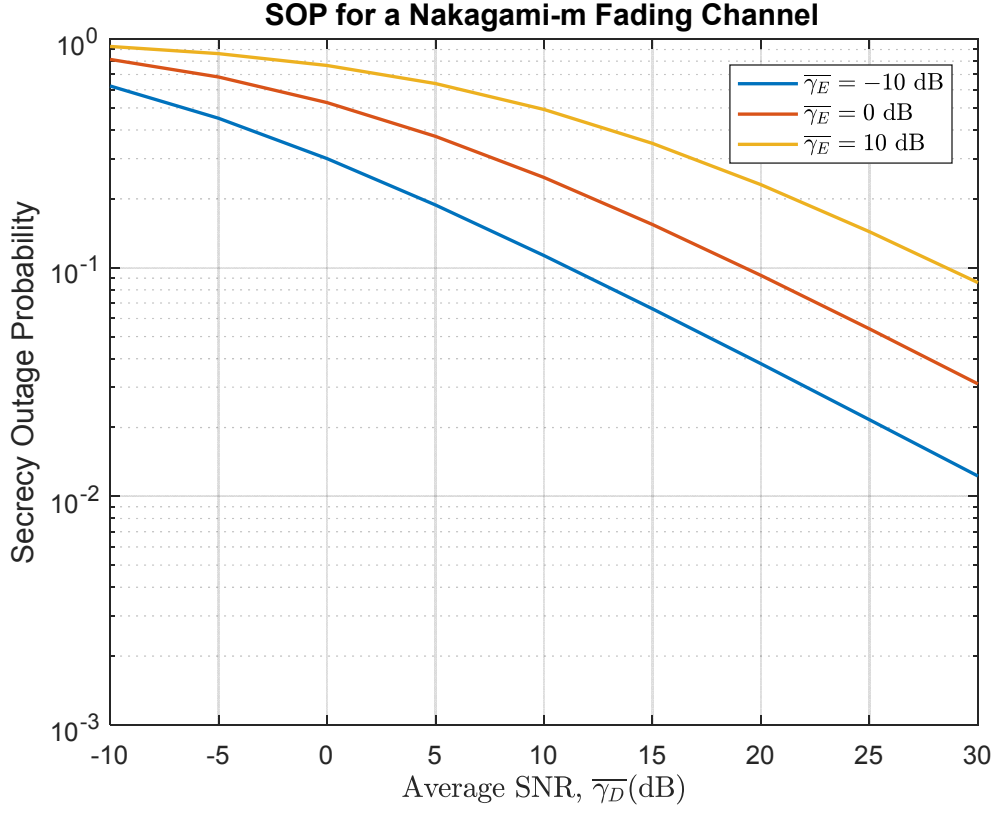


Figure 6.9: Secrecy Outage Probability versus $\bar{\gamma}_D$, in a Nakagami- m fading environment, for selected values of $\bar{\gamma}_E$ with $t = 0.1$, bits/s/Hz ($\theta = 2^{0.1}$), $m_{\gamma_D} = m_{\gamma_E} = 1$.

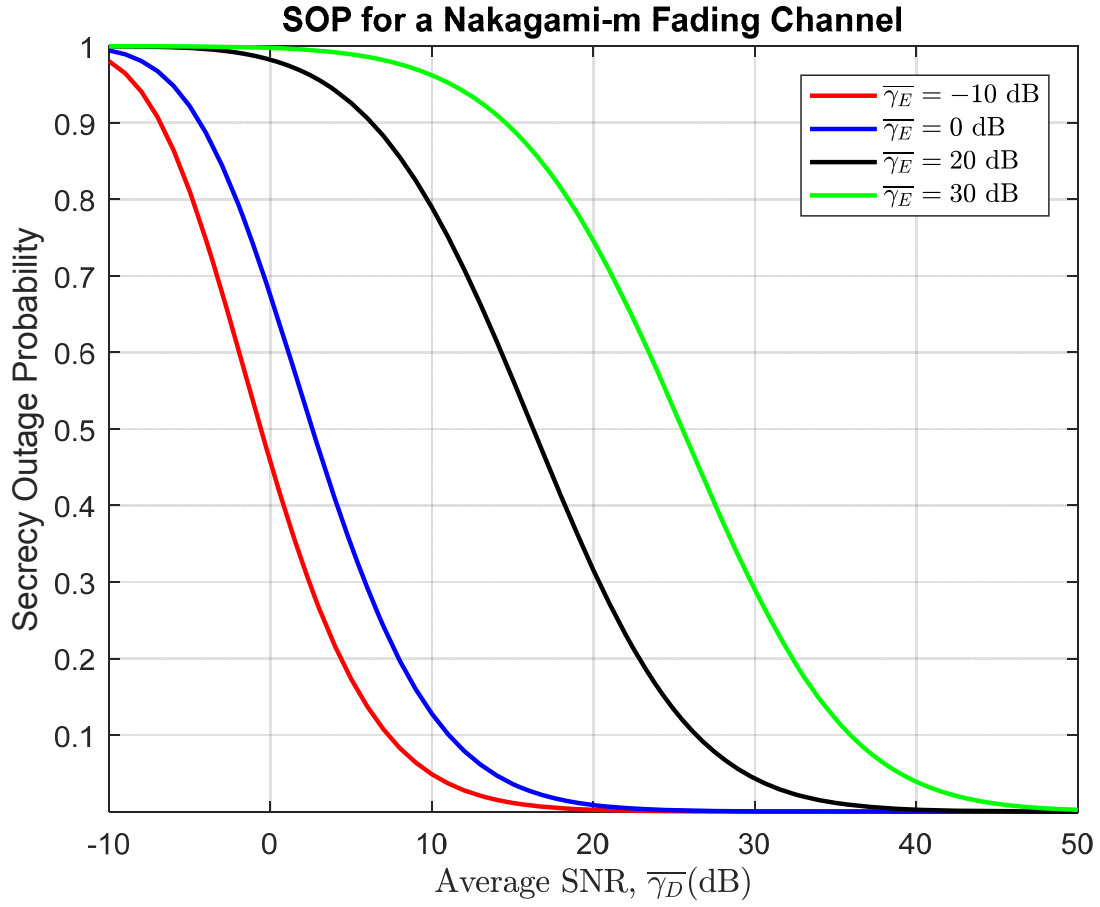


Figure 6.10: Secrecy Outage Probability versus $\bar{\gamma}_D$, in a Nakagami- m fading environment, for selected values of $\bar{\gamma}_E$, with $t = 0.5$ bits/s/Hz ($\theta = 2^{0.5}$) and the fading parameters $m_{\gamma_D} = 3$, $m_{\gamma_E} = 2$.

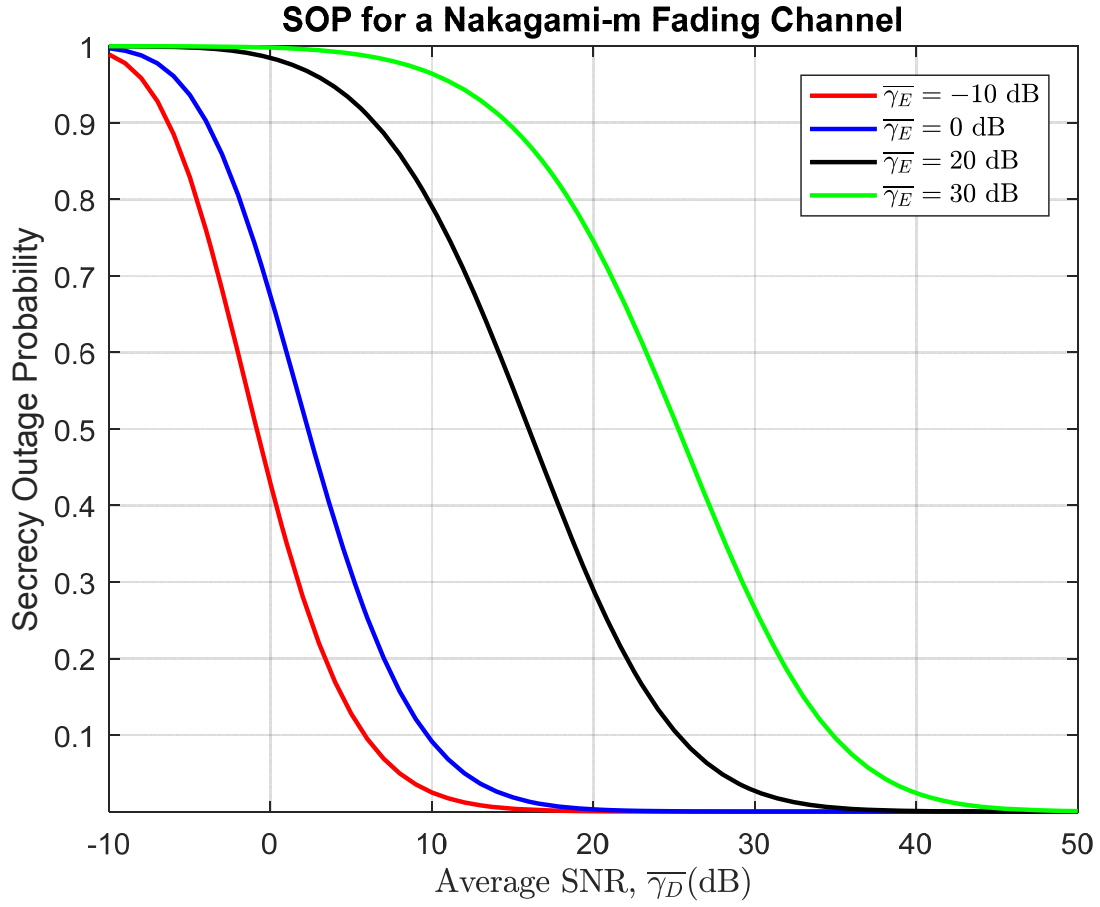


Figure 6.11: Secrecy Outage Probability versus $\bar{\gamma}_D$, in a Nakagami- m fading environment, for selected values of $\bar{\gamma}_E$, with $t = 0.5$ bits/s/Hz ($\theta = 2^{0.5}$) and the fading parameters $m_{\gamma_D} = 4$, $m_{\gamma_E} = 2$.

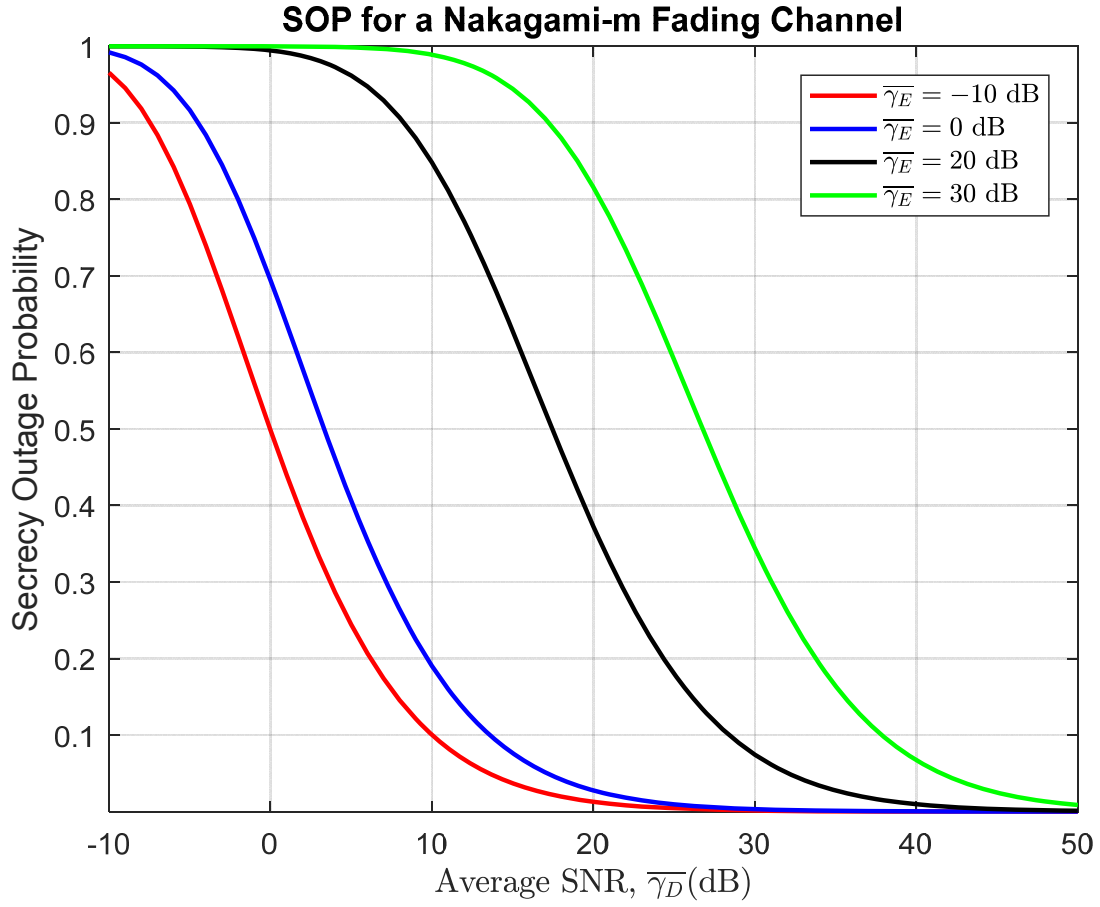


Figure 6.12: Secrecy Outage Probability versus $\bar{\gamma}_D$, in a Nakagami- m fading environment, for selected values of $\bar{\gamma}_E$, with $t = 0.5$ bits/s/Hz ($\theta = 2^{0.5}$) and the fading parameters $m_{\gamma_D} = 2$, $m_{\gamma_E} = 4$.

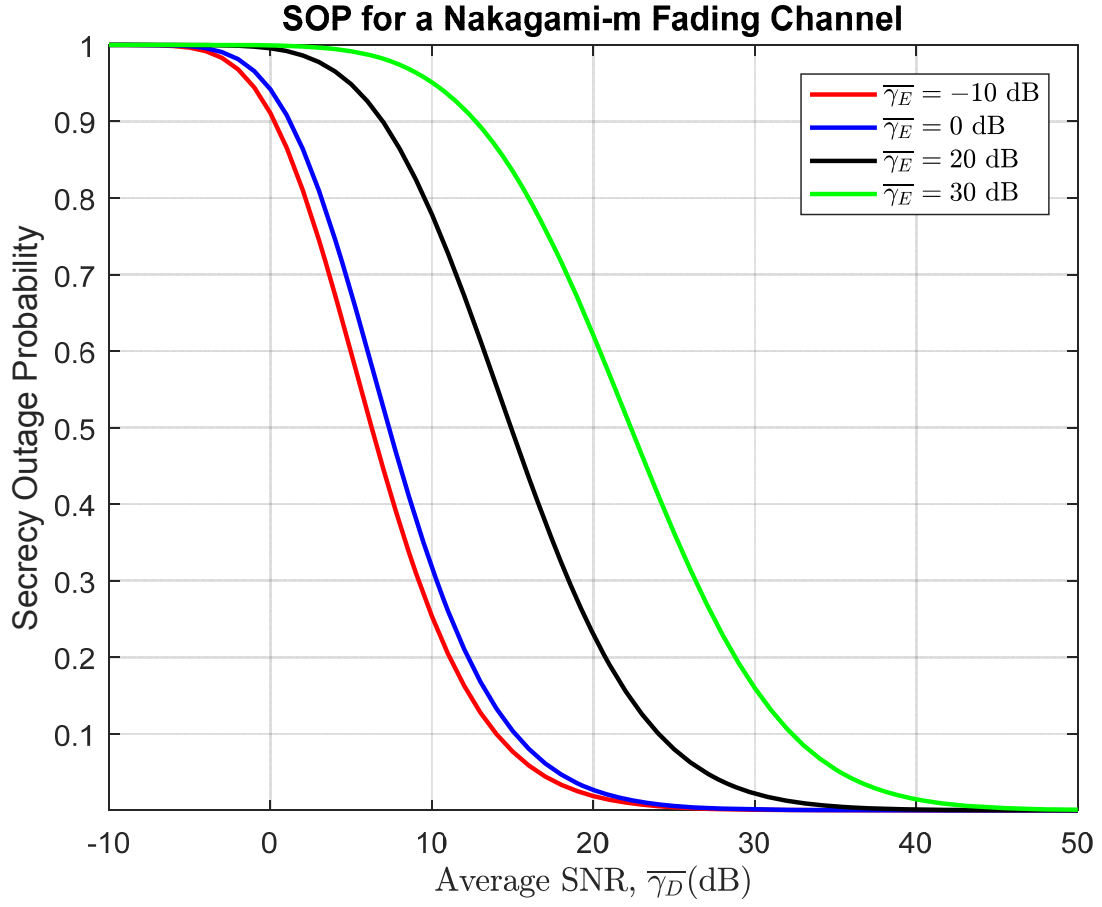


Figure 6.13: Secrecy Outage Probability versus $\bar{\gamma}_D$, in a Nakagami- m fading environment, for selected values of $\bar{\gamma}_E$, with $t = 1$ bits/s/Hz ($\theta = 2^1$) and the fading parameters $m_{\gamma_D} = 3$, $m_{\gamma_E} =$

2.

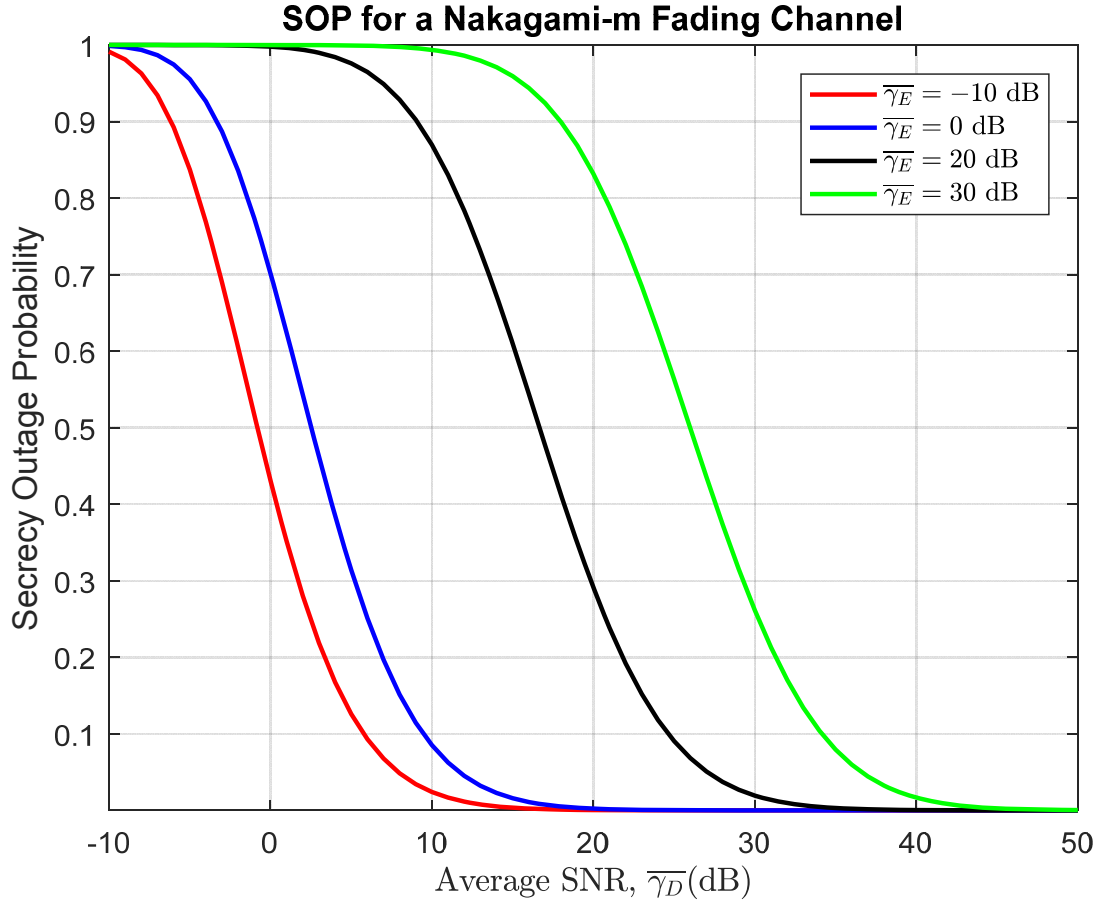


Figure 6.14: Secrecy Outage Probability versus $\bar{\gamma}_D$, in a Nakagami- m fading environment, for selected values of $\bar{\gamma}_E$, with $t = 1$ bits/s/Hz ($\theta = 2^1$) and the fading parameters $m_{\gamma_D} = 4$, $m_{\gamma_E} = 2$.

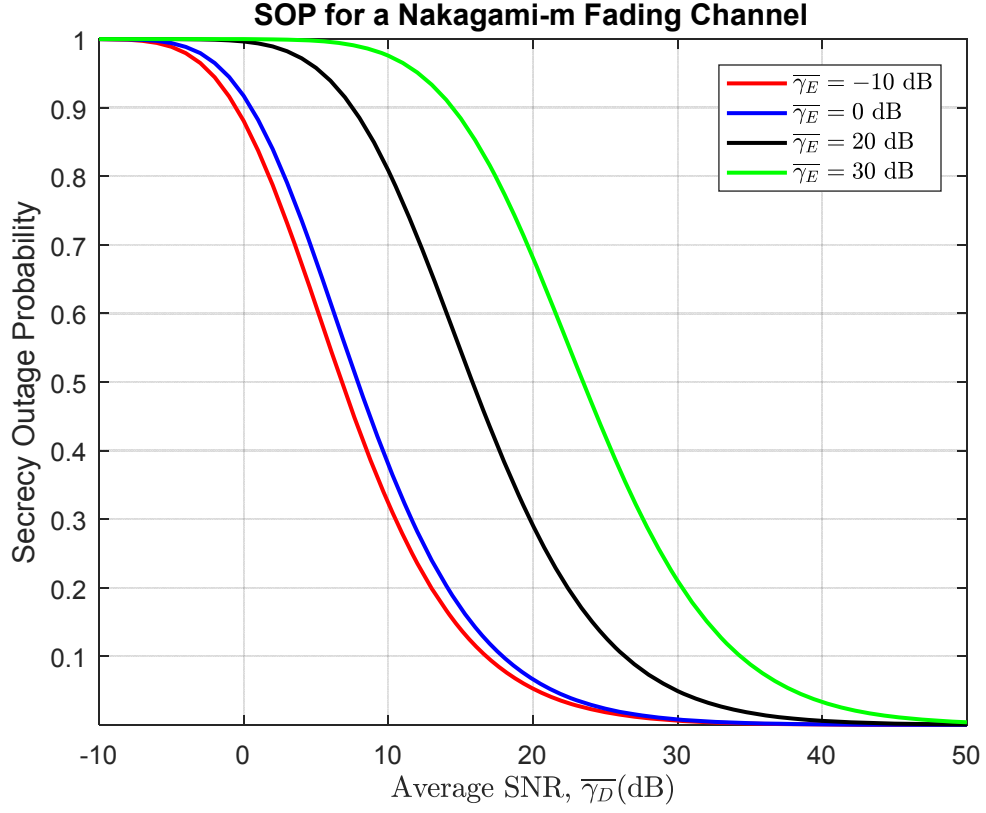


Figure 6.15: Secrecy Outage Probability versus $\bar{\gamma}_D$, in a Nakagami- m fading environment, for selected values of $\bar{\gamma}_E$, with $t = 1$ bits/s/Hz ($\theta = 2^1$) and the fading parameters $m_{\gamma_D} = 2$, $m_{\gamma_E} = 4$.

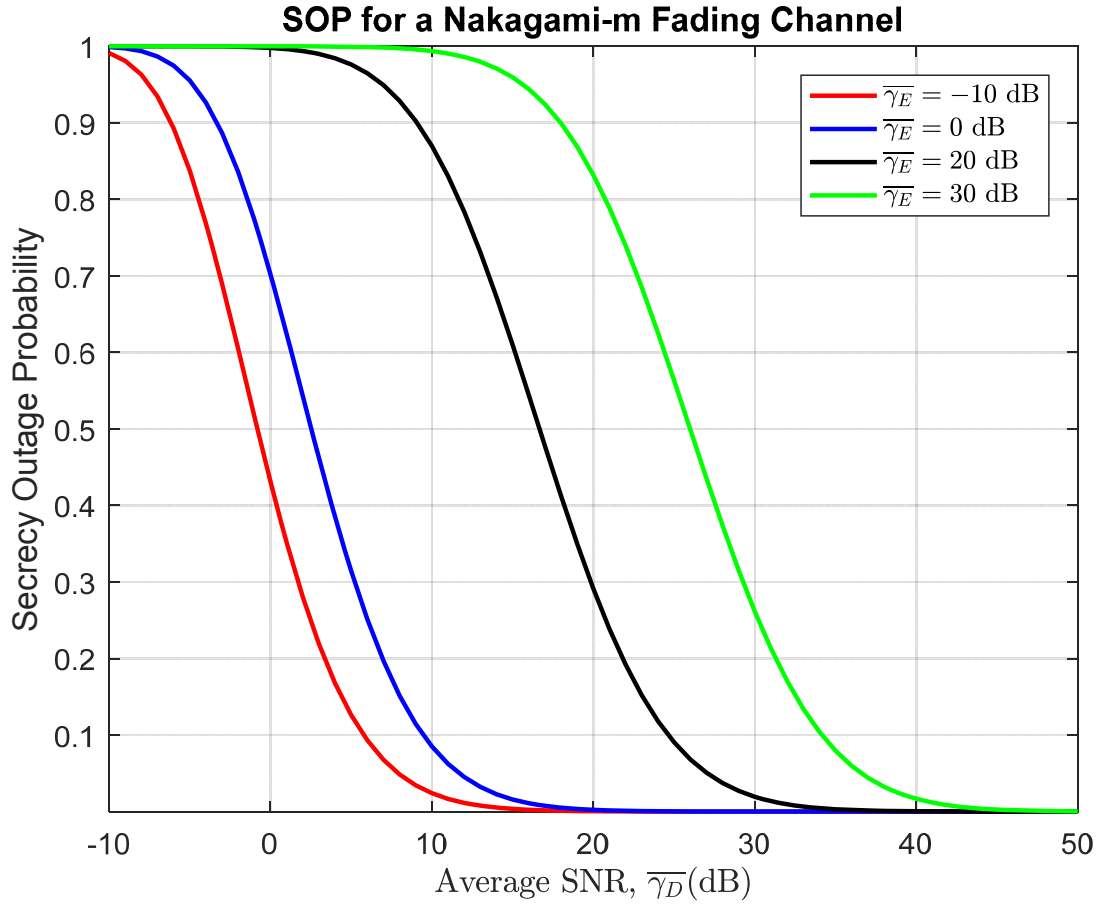


Figure 6.16: Secrecy Outage Probability versus $\bar{\gamma}_D$, in a Nakagami- m fading environment, for selected values of $\bar{\gamma}_E$, with $t = 0.5$ bits/s/Hz ($\theta = 2^{0.5}$) and the fading parameters $m_{\gamma_D} = m_{\gamma_E} = 4$.

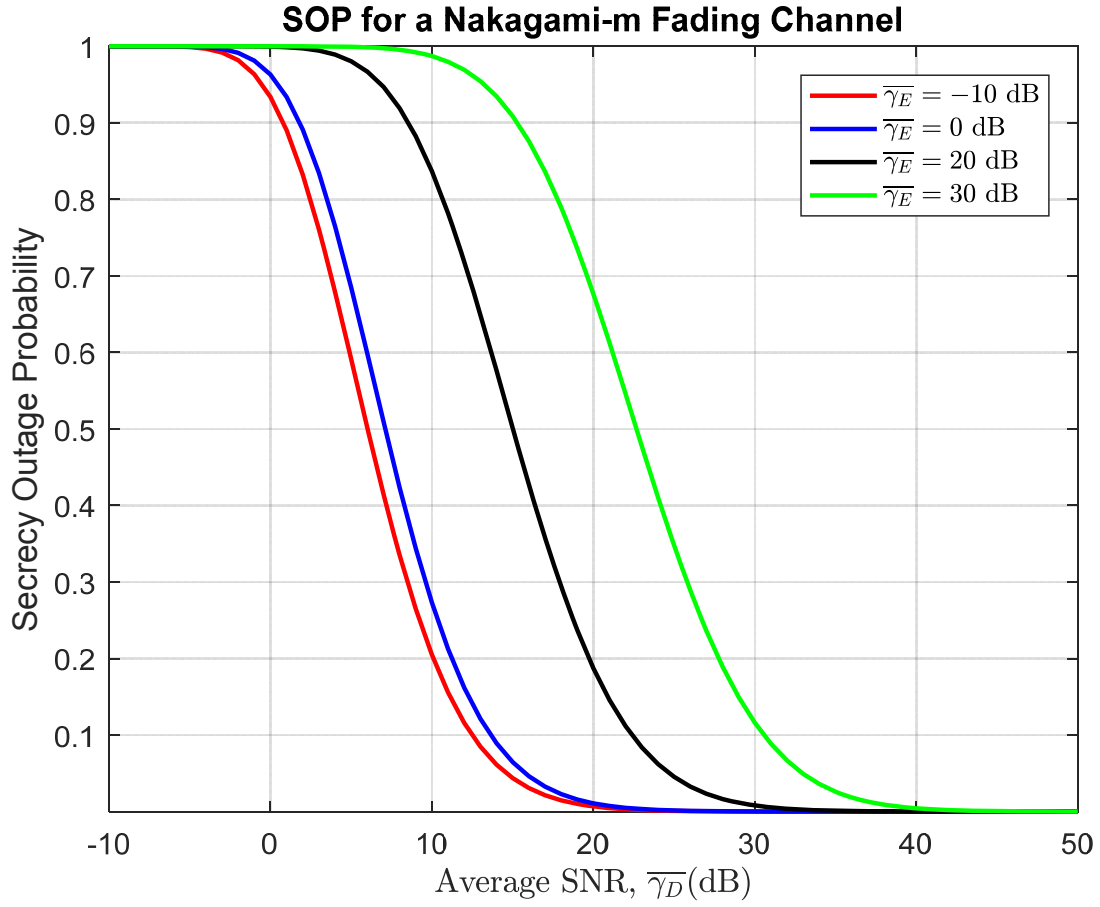


Figure 6.17: Secrecy Outage Probability versus $\bar{\gamma}_D$, in a Nakagami- m fading environment, for selected values of $\bar{\gamma}_E$, with $t = 1$ bits/s/Hz ($\theta = 2^1$) and the fading parameters $m_{\gamma_D} = m_{\gamma_E} = 4$.

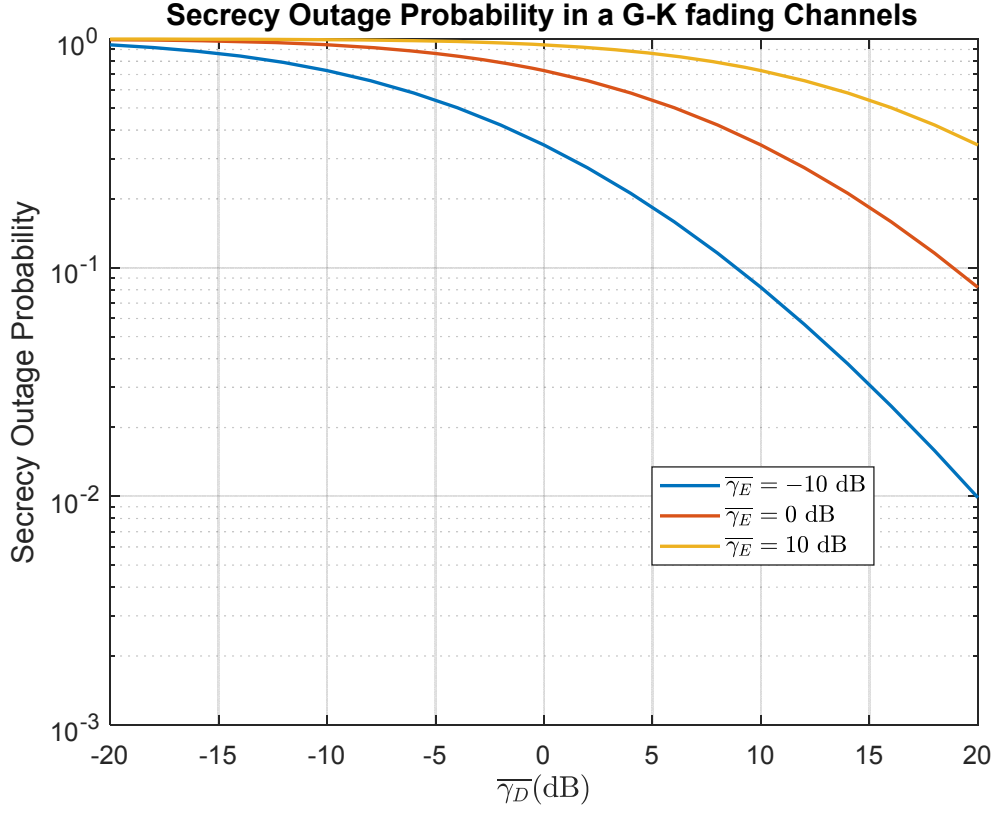


Figure 6.18: Secrecy Outage Probability versus $\bar{\gamma}_D$, in a Generalized-K fading environment, for selected values of $\bar{\gamma}_E$, with $t = 1$ bits/s/Hz ($\theta = 2^1$) and the fading parameters $m_D = m_E = 3$, $k_D = k_E = 4$.

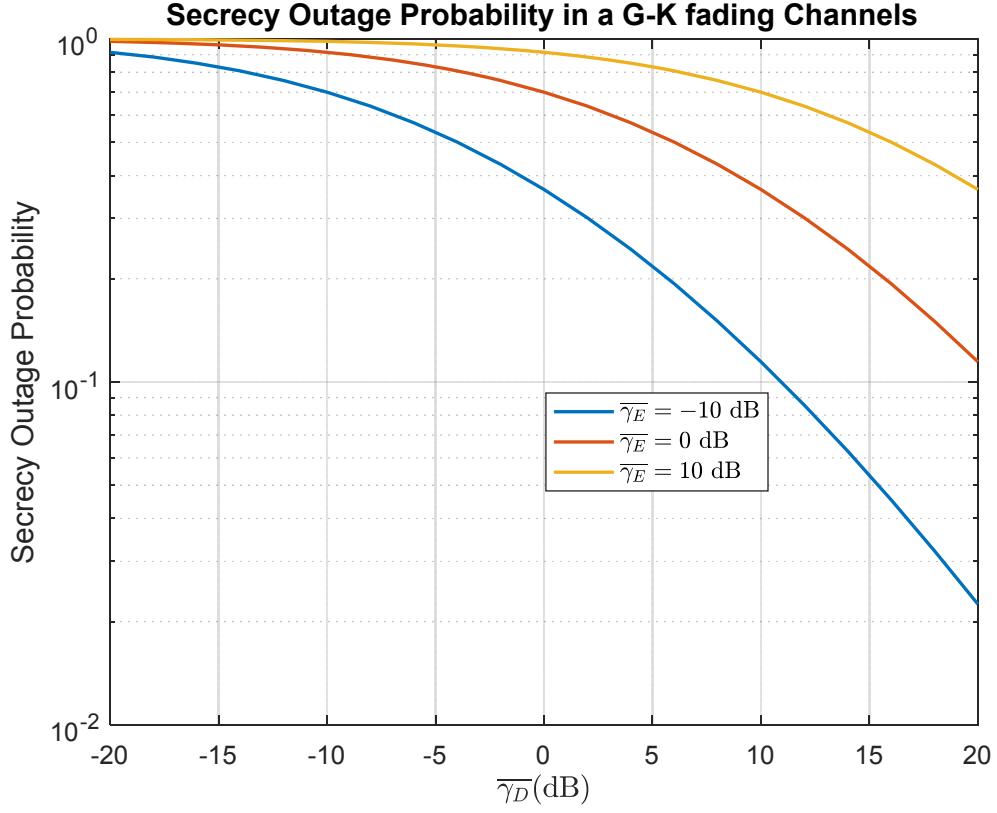


Figure 6.19: Secrecy Outage Probability versus $\bar{\gamma}_D$, in a Generalized-K fading environment, for selected values of $\bar{\gamma}_E$, with $t = 1$ bits/s/Hz ($\theta = 2^1$) and the fading parameters $m_D = m_E = 2$, $k_D = k_E = 4$.

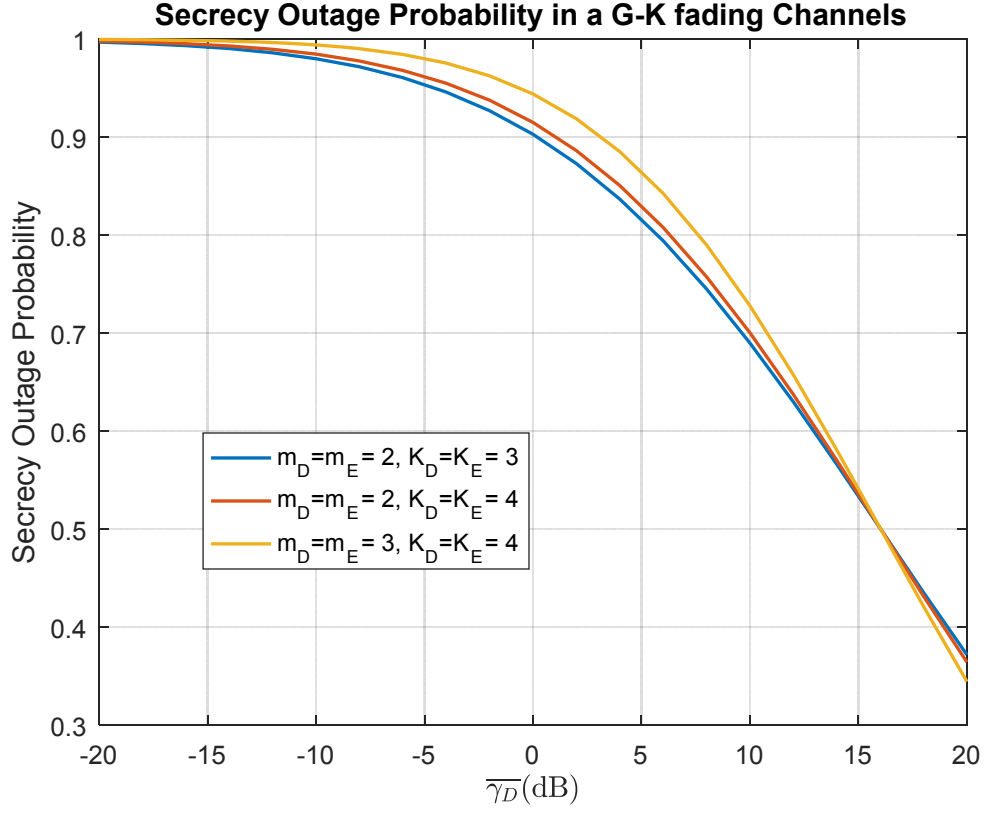


Figure 6.20: Secrecy Outage Probability versus $\bar{\gamma}_D$, in a Generalized-K fading environment, when the eavesdropper average power $\bar{\gamma}_E$ is 10 dB, with $t = 1$ bits/s/Hz ($\theta = 2^1$) while varying the fading parameters.

CHAPTER 7: SUMMARY AND CONCLUSIONS

7.1 Summary of Main Results

In this chapter, a summary of the main results obtained in this thesis for the secrecy outage probability for the Rayleigh, Nakagami- m , and the Generalized-K fading channels are presented. In Chapter 1, we started with a discussion of the issues in wireless system networks and introduced the so-called physical layer security in wireless networks, which was the motivation behind our work. In Chapter 2, we elaborated on the system model for wireless communications where two legitimate users communicate in the presence of a malicious third-party eavesdropping on the communication. We also presented in Chapter 2 several techniques that are applied at the physical layer to improve reliability and security of wireless networks. At the end of Chapter 2, we presented the secrecy outage probability as a performance metric to characterize the performance of the wireless channel. In chapter 3, we discussed the effects of fading and shadowing in wireless channels, and presented several techniques such as MIMO, relaying, and diversity combining that can be applied at the physical layer to improve security in wireless networks. In Chapter 4, we proposed the Direct Integration approach to evaluate the secrecy outage probability over the fading channels outlined in Chapter 3. The Direct Integration approach was used to evaluate the secrecy outage probability over three different fading channels. Firstly, we derived closed-form expression for the secrecy outage probability over the Rayleigh fading channel. Secondly, we used the direct

integration approach to evaluate the secrecy outage probability for Nakagami-m fading environment. To simplify the analysis, we restricted our analysis to the Nakagami fading channel with integer fading parameters, and we were able to obtain closed-form expression for the secrecy outage probability. Thirdly, we applied the direct integration method to a composite fading channel: the Generalized-K fading, which captures many other fading models as special cases. In this section, we expressed the Generalized-K in terms of the Meijer G-function presented in Chapter 3. We evaluated the secrecy outage probability for the Generalized-K by integrating its Meijer G-function form. For the Generalized-K fading environment, we provided an expression for the secrecy outage probability for the exact distribution and we also provided an expression for an approximation of the distribution. In Chapter 5, we discussed the Taylor series approach. We first introduced the Taylor series as general approach that can be used for any fading channel environment. We derived closed-form expressions for the secrecy outage probability using the Taylor series approach in a Rayleigh fading environment. We obtained closed-form expressions for the secrecy outage probability in a Rayleigh fading environment using the Taylor-series approach. We showed that the direct integration and Taylor series approaches yielded the same closed-form results in the Rayleigh fading channel. Secondly, we derived expression for the secrecy outage probability over the Nakagami-m fading channel. Using the Taylor series approach, we were not able to find closed-form expressions for the Nakagami-m fading environment. However, the expression found can be easily evaluated numerically. Thirdly, we used the Taylor series approach to evaluate the secrecy outage probability for the Generalized-K fading environment based on the Meijer G-function. Closed form-expressions for the secrecy

outage probability was derived for the Generalized-K fading channel. Extreme care was taken to ensure that the numerical computations in MATLAB were accurate since the series involved G-functions with alternating signs.

In Chapter 6, we presented the computer results using MATLAB. We provided plots for the secrecy outage probability for the Rayleigh, Nakagami-m, and the Generalized-K fading environments. For each fading environment, we provided several plots to illustrate the secrecy outage probability by varying the parameters associated with the fading models under different conditions. The analytical results match well with the MATLAB simulation results. The computer results show that the secrecy outage probability for a higher average power at the main channel outperform the ones for a lower average power at the eavesdropper channel for all three fading models discussed in this work.

7.2 Conclusion

The main contributions of this thesis may be summarized as follow:

- 1) We investigated the issue of physical layer security as an attractive approach to combatting eavesdropping in wireless networks by focusing on the exploitation of the physical characteristics of the fading channels.
- 2) We discussed the effects of fading and shadowing in wireless network, and described several distributions that can be used to model the effects of fading and shadowing in practical scenarios.

- 3) We derived closed-form expressions for the secrecy outage probability using the direct integration method for the Rayleigh, Nakagami-m and the Generalized-K fading environments.
- 4) We presented the Taylor Series approach as a general technique to evaluate the performance of wireless system network over any fading channel. The Taylor series approach is an attractive because it simply requires the n th moment and n th derivative for any arbitrary fading environment.

7.3 Suggestions for Future Work

A frequency domain approach may also be used to evaluate the secrecy outage probability. Such approach requires knowledge of either the moment generating function (MGF) or characteristic function (CH) of the fading distributions. Contrary to the direct integration method that can be cumbersome, the frequency domain approach is somewhat more flexible and efficient, especially, in cases where the direct integration method may involve multi-fold integration, and thus may be difficult to evaluate. Since the computation of an L - fold integral is tedious; a Laplace Transform (LT) approach may provide an alternative way to evaluate the secrecy outage probability in situations where the direct integration method may seem impractical. A unified communications-theoretic framework for evaluating the secrecy capacity and secrecy outage capacity based on Parseval's theorem was recently proposed in [74]. Following this approach, a Laplace Transform-based method can be used to numerically evaluate the outage secrecy capacity with considerable numerical accuracy. Such analysis can be extended to other fading distributions such as Rice, Weibull and, more general, the Meijer's G -fading channels.

APPENDIX A

A.1 The Fox's H-function [42]

The H-function was first introduced by Fox [42] as a generalization function of many of the special functions of mathematics and physics, including the Meijer's G-function, the hypergeometric function, etc. The Fox's H function is defined as follows:

$$H_{p,q}^{m,n} \left(z \left| \begin{matrix} (a_1, \omega_1), \dots, (a_p, \omega_p) \\ (b_1, \beta_1), \dots, (b_q, \beta_q) \end{matrix} \right. \right) = \frac{1}{2\pi i} \oint \frac{\prod_{j=1}^m \Gamma(b_j - \beta_j s) \prod_{j=1}^n \Gamma(1 - a_j + \omega_j s)}{\prod_{j=m+1}^q \Gamma(1 - b_j + \beta_j s) \prod_{j=n+1}^p \Gamma(a_j - \omega_j s)} z^s ds \quad (\text{A.1})$$

wheren $0 \leq m \leq q$, $0 \leq n \leq q$; $\omega_j > 0$, for $j = 1, 2, \dots, p$; $\beta_j > 0$, for $j = 1, 2, \dots, q$.

A.2 Meijer's G-function [48] - [69]

The Meijer's G-function is a special case of the Fox-H function that results by substituting $w_p = \beta_q = 1$, in (A.1). The Meijer G function is defined by the integral:

$$G_{p,q}^{m,n} \left(z \left| \begin{matrix} a_1, \dots, a_p \\ b_1, \dots, b_q \end{matrix} \right. \right) = G_{p,q}^{m,n} \left(z \left| \begin{matrix} a_p \\ b_q \end{matrix} \right. \right) = \frac{1}{2\pi i} \oint \frac{\prod_{j=1}^m \Gamma(b_j - s) \prod_{j=1}^n \Gamma(1 - a_j + s) z^s ds}{\prod_{j=m+1}^q \Gamma(1 - b_j + s) \prod_{j=n+1}^p \Gamma(a_j - s)} \quad (\text{A.2})$$

APPENDIX B

B. 1 Derivation of (4.8) and (4.9)

$$f_Y(\gamma) = \frac{2\Xi^{\frac{\beta+1}{2}} \gamma^{\frac{\beta-1}{2}}}{\Gamma(m)\Gamma(k)} K_\omega(2\sqrt{\Xi\gamma}) ; \gamma \geq 0 \quad (\text{B.1})$$

From [46, eq. (8.4. 23.1)], we can express the modified Bessel function in terms of the Meijer's G function as:

$$K_{k-m}(2\sqrt{\Xi\gamma}) = \frac{1}{2} G_{0,2}^{2,0} \left(\Xi\gamma \middle| \frac{\omega}{2}, -\frac{\omega}{2} \right) \quad (\text{B.2})$$

Now using [45, eq. (9.31.5)], we have:

$$\begin{aligned} f_Y(\gamma) &= \frac{2\Xi^{\frac{\beta+1}{2}}}{\Gamma(m)\Gamma(k)} \gamma^{\frac{\beta-1}{2}} \frac{1}{2} G_{0,2}^{2,0} \left(\Xi\gamma \middle| \frac{\omega}{2}, -\frac{\omega}{2} \right) \\ &= \frac{\Xi^{\frac{\beta+1}{2}} \gamma^{\frac{\beta+1}{2}-1}}{\Gamma(m)\Gamma(k)} G_{0,2}^{2,0} \left(\Xi\gamma \middle| \omega/2, -\omega/2 \right) \end{aligned} \quad (\text{B.3})$$

The corresponding CDF follows by integrating the pdf as

$$F_Y(\gamma) = \frac{\Xi^{\frac{\beta+1}{2}}}{\Gamma(m)\Gamma(k)} \int_0^\gamma t^{\frac{\beta+1}{2}-1} G_{0,2}^{2,0} \left(\Xi t \middle| \frac{\omega}{2}, -\frac{\omega}{2} \right) dt \quad (\text{B.4})$$

Using the definition of Meijer's function (A.2), we obtain:

$$\begin{aligned} F_Y(\gamma) &= \frac{\Xi^{\frac{\beta+1}{2}}}{\Gamma(m)\Gamma(k)} \int_0^\gamma t^{\frac{\beta+1}{2}-1} \left[\frac{1}{2\pi i} \oint \Gamma\left(s + \frac{\omega}{2}\right) \Gamma\left(s - \frac{\omega}{2}\right) (\Xi t)^{-s} ds \right] dt \\ &= \frac{\Xi^{\frac{\beta+1}{2}}}{\Gamma(m)\Gamma(k)} \frac{1}{2\pi i} \oint \Gamma\left(s + \frac{\omega}{2}\right) \Gamma\left(s - \frac{\omega}{2}\right) \Xi^{-s} \int_0^\gamma t^{\left(\frac{\beta+1}{2}-s\right)-1} dt ds \end{aligned} \quad (\text{B.5})$$

$$\begin{aligned}
&= \frac{\Xi^{\frac{\beta+1}{2}}}{\Gamma(m)\Gamma(k)} \frac{1}{2\pi i} \oint \Gamma\left(s + \frac{\omega}{2}\right) \Gamma\left(s - \frac{\omega}{2}\right) \Xi^{-s} \left(\frac{\frac{\beta+1}{2}-s}{\left(\frac{\beta+1}{2}-s\right)} \right) \Big|_0^\gamma ds \\
&= \frac{\Xi^{\frac{\beta+1}{2}}}{\Gamma(m)\Gamma(k)} \frac{1}{2\pi i} \oint \Gamma\left(s + \frac{\omega}{2}\right) \Gamma\left(s - \frac{\omega}{2}\right) (\Xi\gamma)^{-s} \frac{\gamma^{\frac{\beta+1}{2}}}{\left(\frac{\beta+1}{2}-s\right)} ds \\
&= \frac{\Xi^{\frac{\beta+1}{2}}}{\Gamma(m)\Gamma(k)} \frac{1}{2\pi i} \gamma^{\frac{\beta+1}{2}} \oint \Gamma\left(s + \frac{\omega}{2}\right) \Gamma\left(s - \frac{\omega}{2}\right) (\Xi\gamma)^{-s} \frac{1}{\left(\frac{\beta+1}{2}-s\right)} ds \tag{B.6}
\end{aligned}$$

$$\text{Let } \frac{1}{q-s} = \frac{\Gamma(q-s)}{(q-s)\Gamma(q-s)} = \frac{\Gamma(q-s)}{\Gamma(q-s+1)},$$

$$\text{we have } \frac{1}{\left(\frac{\beta+1}{2}-s\right)} = \frac{\Gamma\left(\frac{\beta+1}{2}-s\right)}{\left(\frac{\beta+1}{2}-s\right)\Gamma\left(\frac{\beta+1}{2}-s\right)}.$$

Consequently, the CDF becomes

$$\begin{aligned}
F_\gamma(\gamma) &= \frac{\Xi^{\frac{\beta+1}{2}}}{\Gamma(m)\Gamma(k)} \gamma^{\frac{\beta+1}{2}} \frac{1}{2\pi i} \oint_C \frac{\Gamma\left(s+\frac{\omega}{2}\right)\Gamma\left(s-\frac{\omega}{2}\right)\Gamma\left(\frac{\beta+1}{2}-s\right)}{\Gamma\left(\frac{\beta+1}{2}+1-s\right)} (\Xi\gamma)^{-s} ds \\
&= \frac{\Xi^{\frac{\beta+1}{2}}}{\Gamma(m)\Gamma(k)} \gamma^{\frac{\beta+1}{2}} G_{1,3}^{2,1} \left(\Xi\gamma \left| \begin{matrix} 1 - \frac{\beta+1}{2} \\ \omega/2, -\omega/2, -\frac{\beta+1}{2} \end{matrix} \right. \right) \tag{B.7}
\end{aligned}$$

REFERENCES

- [1] Y.S. Shiu, S. Y. Chang, H.-C. Wu, S. C-Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," IEEE Communications Magazine., vol. 18, no 2, pp. 66-74, April 2011.
- [2] M. E. Hellman, "An overview of Public Key Cryptography," IEEE Communications Magazine, vol. 16, no. 6, May 2002, pp. 42-49.
- [3] S. S. V. Kartalopoulos, "A primer on Cryptography in Communications," IEEE Communications Magazine, vol. 20, no. 4, April 2006, pp. 146-51.
- [4] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Technical Journal, vol. 29, pp. 656-715, 1949.
- [5] A. D. Wyner, "The wire-tap channel, Bell System Technical Journal," vol. 54, pp. 1355-1387, 1975.
- [6] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," IEEE Transactions on Information Theory, vol. IT-24, no.3, pp. 339-348, May 1978.
- [7] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," IEEE Transactions on Information Theory, vol. 55, no.6, pp.2547-2553, June 2009.
- [8] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wire-tap channel," IEEE Transactions Information Theory, vol.57, no. 8, pp. 4961-4972, August 2011.
- [9] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," IEEE Transactions on Wireless Communications, vol. 10, no. 2, pp. 425-430, February 2011.

- [10] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-part I: The MISOME wire-tap channel," *IEEE Transactions on Information Theory*, vol.56, no.7, pp. 3088, July 2010.
- [11] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, A.A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Communications*, vol. 6, pp. 2676-2687, June 2012.
- [12] J. li and A. P. Petropulu, "Ergodic secrecy rate for multiple-antenna wiretap channels with Rician fading," *IEEE Transactions on Information Forensics Security*, vol. 6, no. 3, pp.861-867, September 2011.
- [13] M. Z. I. Sarkar and T. Ratnarajah, "Secure communication through Nakagami-m fading MISO channel," in *IEEE ICC*, Kyoto, Japan, 2011, pp.1-5.
- [14] V. Prabhu and M. Rodrigues, "On wireless channels with M-antenna eavesdroppers: Characterization of the outage probability and ϵ -outage secrecy capacity," *IEEE Transactions on Information Forensics Security*, vol. 6, pp.853-860, September 2011.
- [15] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Communications Letters*, vol. 15, pp.509-511, May 2011.
- [16] Yulong Zou, Jia Zhu, Xianbin Wang, and victor C.M. Leung, "Improving Physical-layer Security Wireless Communications Using Diversity Techniques," *IEEE Networks*, January/February 2015.
- [17] Y. Zhou, Y. D. Yao, and B. Zheng, "Opportunistic Distributed Space-Time Coding for Decode-And-Forward Cooperation Systems," *IEEE Transactions on Signal Processing*, vol. 60, no. 4, April 2012, pp. 1766-83.
- [18] Y. Zou, X. Wang, and W. Shen, "Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks," *IEEE JSAC*, vol. 31, no. 10, October 2013, pp. 2099-2111.
- [19] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp.4687-4698, October 2008.

- [20] M. Bloch and J. Barros, "Physical-layer security: from information theory to security engineering," Cambridge University Press, 2011.
- [21] Z. Rezki and M.-S Alouini, "On the capacity of Nakagami-m fading channels with full channel state information at low SNR," IEEE Wireless on Communications Letters, vol.1, no. 3, pp. 253-256, June 2012.
- [22] N. Yang, P.L Yeoh, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," IEEE on Signal Processing Letters, vol.19, no. 6, pp. 372-375, June 2012.
- [23] W. R. Braun and U. Dersch, "A physical mobile radio channel," IEEE Transactions on Vehicular Technology, vol. VT-40, May 1991, pp. 472-482.
- [24] A. U. Sheikh, M. Handfrth, and M. Abdi, "Indoor mobile radio channel at 946 MHz: measurements and modeling," IEEE Proceedings on Vehicular Technology Conference, Secaucus, NJ, May 1993, pp. 73-76.
- [25] H. Suzuki, "A statistical model for urban multipath propagation," IEEE Transactions on Communications, vol. 25, July 1977, pp. 673-680.
- [26] H. Hashemi, "Impulse response modeling of indoor radio propagation channels," IEE Journal on Selected areas in Communications, vol.7, no.7, September 1993.
- [27] W. Y. Luo, L.Jin, K. Z. Zhong, "User selection and resource allocation for secure multiuser MISO-OFDMA SYSTEMS," Electron. Letters, vol.47, no 15, pp. 884-886, July 2011.
- [28] P. Gaofeng, T. Chaoqing, X. Zhang, T. Li, et al., "Physical-layer Security Over Non-Small-Scale Fading Channels," IEEE Transactions On Vehicular Technology, vol. 65, No. 3, March 2016.
- [29] M. D. Yacoub, "The $\alpha - \mu$ Distribution: A Physical Model for the Stacy Distribution," IEEE Transactions on Vehicular Technology, vol. 56, no.1, January 2007.
- [30] P. S. Bithas, N.C. Sagias, P.T Mathiopoulos, G.K Karagiannidis, and A.A. Rontogiannis, "On the performance analysis of digital communication over Generalized-K fading channels," IEEE Communications Letters, vol. 10, no.5, pp. 353-355, Jan. 2006.

- [31] H. Lei, C. Gao, Y. Guo, et al, "On Physical Layer Security Over Generalized Gamma Fading Channels," IEEE on Communications Letters, vol. 19, no.7, July 2015.
- [32] X. Zhou, M. R. McKay, B. Maham, A. H. Jorungnes, "Rethinking the Secrecy Outage Formulation: A Secure Transmisson Design Perspective," IEEE on Communication Letters, vol. 15, no.3, March 2011.
- [33] V. K. Dwivedi and G. Singh, "A novel MGF Based Analysis of Channel Capacity of Generalized-K fading with Maximal-Ratio Combining Diversity," Progress in Electromagnetics Research C, vol. 26, 153-165, 2012.
- [34] L. Fan, X. Lei, T. Q. Duong, M. El Kashlan, and G. K. Karagiannidis, "Secure multiuser Communications in Multiple Amplify-and-Forward Relay Networks," IEEE Transactions on Communications, vol. 62, no. 9, September 2014.
- [35] J. Barros and M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels, "ISIT 2006, Seattle, USA, July 9-14, 2006.
- [36] X. Liu, "Strictly Positive Secrecy Capacity of Log-Normal Fading Channel with Multiple Eavesdroppers," IEEE 2014, Communication and information Systems Security Symposium.
- [37] X. Liu, "Probability of Strictly Positive Secrecy Capacity of the Rician-Rician Fading Channel," IEEE Wireless Communications Letters, vol. 2, no.1, February 2013.
- [38] O. Takahashi, X. Jiang, Y. Nakamura, et al., "Outage Secrecy Capacity Over Correlated Fading Channels at High SNR," ICMU 2012.
- [39] X. Sun, J. Wang, Wei Xu, and C. Zhao, "Performance of Secure Communications Over Correlated Fading Channels," IEEE on Signal Processing Letters, vol.19, no.8, August 2012.
- [40] L. Kong, G. Kaddoum, M. Taha, "Performance Analysis of Physical Layer Security of Chaos-based Modulation Schemes," International Workshop on Selected Topics in Mobile and Wireless Computing, IEEE, 2015.
- [41] G. Gomez, F. J. Lopez-Martinez, D. Morales-Jimenez, and M. R. McKay, "On the Equivalence between Interference and Eavesdropping in Wireless Communications, IEEE 2014" SIAM J. Appl. Math, vol.33, no.4, December 1977.

- [42] B. D. Carter and D. Melvin, "The Distribution of products, Quotients and powers of Independent H-Function Variates".
- [43] H. Lei, H. Zhang, I. S. Ansari, et al. "Performance Analysis of Physical Layer Security over Generalized-K Fading Channels Using a Mixture Gamma Distribution, IEEE on Communication Letters, 2015.
- [44] P. Wang, G. Yu, and Z. Zhang, "On the Secrecy Capacity of Fading Wireless Channel with Multiple Eavesdroppers," ISIT 2007, Nice, France, June 24-June 29, 2007.
- [45] M. Z. I Sarkar, T. Ratnarajah, and M. Sellathurai, "Secrecy capacity of Nakagami-m fading wireless channels in the presence of multi-eavesdroppers," in 43rd Asilomar Conf. on Signals, Systems and Computers, pp. 829-833, 2009.
- [46] M. Block, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," IEEE Transactions on Information Theory, vol. 54, no.6, pp. 2515-2534, June.
- [47] W. Y. Luo, L. Jin, K. Z. Zhong, "User selection and resource allocation for secure multiuser MISO-OFDMA SYSTEMS," Electronics Letters, vol.47, no 15, pp.884-886, July 2011
- [48] I. Gradshteyn and I. M. Ryzhik, Table of Integrals, series, and products, 7th Edition, Academic, New York, 2007.
- [49] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, "Integrals and series: More special functions," vol. 3, New York: CRC Press, 1992.
- [50] G. J. Foschini and M. J. Gans, "On limits of Wireless Communications in a Fading Environment when Using Multiple Antennas," Wireless Personal Communications, vol. 6, no. 3, March 1998, pp. 311-35.
- [51] D. Ha, P. T. Van, and T. T. Vu, "Physical Layer Secrecy Performance Analysis over Rayleigh/Nakagami Fading Channels," WCES 2014, 22-24, October 2014, San Francisco, USA.
- [52] M. K Simon and M.-S. Alouini, Digital Communication over Fading Channels, 2nd edition, John Wiley & Sons, New York, 2005.

- [53] W. R. Braun and U. Dersch, "A physical mobile radio channel," IEEE Transactions on Vehicular Technology, vol. VT-40, May 1991, pp. 472-482.
- [54] G. L. Turin, F. D. Clapp, T.L. Johnston, et al., "A statistical model of urban multipath propagation," IEEE Transactions on Vehicular Technology, vol. VT-21, February 1972, pp. 1-9.
- [55] S. Atapattu, C. Tellambura and H. Jiang, "A Mixture Gamma Distribution to model the SNR of Wireless Channels," IEEE Transactions on Wireless Communications, vol.10, pp. 4193-4203, 2011.
- [56] A. Abdi and M. Kaveh, "On the utility of gamma PDF in modeling shadow fading (slow fading)," in IEEE 49th Vehicular Technology Conference, 1999, pp. 2308-2312 "IEEE J. Sel. Areas Communications, vol. SAC-11, September 1993, pp.967-978.
- [57] P. Shankar," Performance Analysis of Diversity Combining Algorithms in Shadowing Fading Channels," Wireless Personal Communications, vol. 37, pp.61-72, 2006.
- [58] A. J. Coulson, A. G. Williamson, and R. G. Vaughan, "Improved fading distribution for mobile radio," IEEE Proceedings F-Communications, vol. 145, pp. 197-202, June 1998.
- [59] J. Griffiths and J. P. McGeehan, "Interrelationship between some statistical distributions used in radio-wave propagation," IEEE Proceedings F-Communications, vol. 129, pp. 411-417, Dec. 1982.
- [60] P. M. Shankar, "Ultrasonic tissue characterization using a generalized Nakagami model," IEEE Transactions Ultrasonic, vol. 48, pp. 1716-1720, November 2001.
- [61] I. M. Kostic, "Analytical approach to performance analysis for channel subject to shadowing and fading," IEEE Proceedings Communications, vol. 152, pp. 821-827, 2005.
- [62] E. W. Stacy, "A generalization of the Gamma Distribution," The Annals of Mathematics Statistics, vol. 33, pp. 1187-1192, September 1962.
- [63] P. Shankar, "Statistical Models for Fading and Shadowed Fading Channels in Wireless Systems: A pedagogical perspective," Wireless Personal Communications, vol. 60, pp. 191-213, 2011.

- [64] P. M. Shankar, "Error rates in generalized shadowed fading channels," *Wireless Personal Communications*, vol. 28, no. 4, pp. 233-238, February 2004.
- [65] A. Abdi and M. Kaveh, "K distribution: An appropriate substitute for Rayleigh-lognormal distribution in fading-shadowing wireless channels," *Electronics Letters*, vol. 34, no. 9, pp. 851-852, April 1998.
- [66] A. M. Mathai, *A Handbook of Generalized Special Functions for Statistical and Physical Sciences*, Oxford University Press, Oxford, UK, 1993.
- [67] B. Schneier, "Cryptographic design vulnerabilities," *Computer*, vol. 31, no.9, pp.29-33, September 1998.
- [68] N. D. Chatzidiamantis, G. K. Karagiannidis, and D. S. Michalopoulos, "On the distribution of the sum of gamma-gamma variates and application in MIMO optical wireless systems," in *Proc. GLOBECOM'09*, Nov. 2009, pp. 1-6.
- [69] N. D. Chatzidiamantis, G. K. Karagiannidis, "On the distribution of the sum of gamma-gamma variates and applications in RF and optical wireless communications," *IEEE Transactions on Communications*, vol. 59, no. 5, pp. 1298-1308, May 2011.
- [70] S. Al-Ahmadi and H. Yanikomeroglu, "On the approximation of the PDF of the sum of independent Generalized-K RVs by another Generalized-K PDF with applications to distributed antenna systems," in *Proc. WCNC'10*, Sydney, Australia, April 2010, pp. 1-6.
- [71] "The Wolfram function website", [online], available at <http://functions.wolfram.com/pdf/MeijerG.pdf>.
- [72] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Communications*, vol. 4, no. 15, pp. 1787-1791, Oct. 2010.
- [73] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Transactions of Wireless Communications*, vol.8, no.10, pp. 5003-5011, Oct. 2009.

[74] K. P. Peppas, N.C. Sagias, and A. Maras, "Physical layer security for multi-antenna systems: A unified approach," *IEEE Transactions on Communications*, vol. 64, no. 1, pp. 314-328, January 2016.