PHYSICAL LAYER SECURITY ANALYSIS AND IMPROVEMENT OVER GENERALIZED GAMMA FADING CHANNELS

by

Youssef Mohamed Abdelfattah Eldokmak

A Thesis presented to the Faculty of the
American University of Sharjah
College of Engineering
In Partial Fulfilment
of the Requirements
for the Degree of

Master of Science in
Electrical Engineering

Sharjah, United Arab Emirates

November 2022

Declaration of Authorship

I declare that this thesis is my own work and, to the best of my knowledge and belief, it does not contain material published or written by a third party, except where permission has been obtained and/or appropriately cited through full and accurate referencing.

Signed Youssef Mohamed Abdelfattah Eldokmak

Date 16/11/2022

The Author controls copyright for this report.

Material should not be reused without the consent of the author. Due acknowledgement should be made where appropriate.

© Year 2022

Youssef Mohamed Abdelfattah Eldokmak

ALL RIGHTS RESERVED

Approval Signatures

We, the undersigned, approve the Master's Thesis of Youssef Mohamed Abdelfattah Eldokmak

Thesis Title: Wireless Networks Physical Layer Security Analysis and Improvement

Date of Defence: 28/11/2022

Name, Title and Affiliation **Signature**

Dr. Mahmoud H. Ismail
Professor, Department of Electrical Engineering
Thesis Advisor

Dr. Mohamed Hassan
Professor, Department of Electrical Engineering
Thesis Co-Advisor

Dr. Hasan Mir
Professor, Department of Electrical Engineering
Thesis Committee Member

Dr. Taha Landolsi
Professor, Department of Computer Science and Engineering
Thesis Committee Member

Dr. Mostafa Shaaban
Interim Head of Department
Department of Electrical Engineering

Dr. Lotfi Romdhane
Associate Dean for Graduate Affairs and Research
College of Engineering

Dr. Fadi Aloul
Dean
College of Engineering

Dr. Mohamed El-Tarhuni
Vice Provost for Research and Graduate Studies
Office of Research and Graduate Studies

Acknowledgements

I would like to thank my advisors Dr. Mahmoud Ibrahim and Dr. Mohamed Hassan for providing knowledge, guidance, support, and motivation throughout my research stages. I'm deeply beholden for their great assistance, worthy discussion, and suggestions.

I would like to thank the professors of the Electrical Engineering department who taught me the master level courses with mighty teaching methods and skills. I really appreciate their dignified advice and motivation.

I would like to acknowledge the American University of Sharjah for providing me with research and teaching assistantships throughout the period of my master degree.

Dedication

Optional, for example

To my family…

Abstract

With the recent advancements in computational power, traditional security techniques are being challenged since it is now easier for an eavesdropper to decode messages previously deemed to be practically impossible to decode. That is why physical layer security is becoming an important research field that is gaining much attention among the research community. Studying the physical layer security for a wireless network enables us to find different important secrecy performance metrics such as the average secrecy capacity, the secrecy outage probability and the probability of non-zero secrecy capacity. These different metrics can be used to assess the network properly and to know what data rates could be transmitted to a legitimate receiver without an eavesdropper decoding it. As a consequence, studying secrecy performance over different fading channels and under various case scenarios depending on the application has been extensively addressed in the literature. In addition, as much as secrecy performance analysis is important, developing techniques to improve the secrecy performance is as important in order to ensure reliable and secure data transmission. In this thesis, we focus on analysing the secrecy performance over general fading/shadowing channels that have not yet been studied in the literature. Specifically, we focus on the analysis of two cases of the generalized gamma channels. In the first, the signal to noise ratio follows a composite generalized gamma log-normal distribution and in the second, the channels of the legitimate and eavesdropper receivers follow a correlated generalized gamma distribution. These fading models can be used to represent a wide range of channels that are encountered in many practical applications. We finally address how artificial noise could be used in secrecy performance improvement.

Keywords: Physical layer security; Composite fading; Gamma distribution; Lognormal distribution; Correlated Channels; Artificial noise.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

5G	Fifth Generation Mobile Networks
AN	Artificial Noise
ASC	Average Secrecy Capacity
CDF	Cumulative Distribution Function
D2D	Device to Device Network
GG	Generalized Gamma
GH	Gauss-Hermite Approximation
M2M	Mobile to Mobile Network
MIMO	Multiple Input Multiple Output
MRC	Maximum Ratio Combining
OSI	Open Systems Interconnection
PDF	Probability Density Function
PLS	Physical Layer Security
PNSC	Probability on Non-zero Secrecy Capacity
SC	Selection Combining
SNR	Signal to Noise Ratio
SOP	Secrecy Outage Probability
V2V	Vehicle to Vehicle Network

Chapter 1. Introduction

1.1. Introduction

In this chapter, we provide a short introduction about wireless networks and the different layers used in modelling wireless networks. We then discuss the motive for studying secrecy based on the physical layer of a wireless network. Then, we present the problem investigated in this study as well as the thesis contribution. Finally, general organization of the thesis is presented.

1.2. Overview

Wireless communications had significantly grown over the past decades and became integral to in our daily lives with numerous applications, this led to the development of a conceptual model known as Open Systems Interconnection (OSI) model which is important for interoperation of different communication systems. The OSI model divides the flow of data over seven different layers which in Figure 1-1.

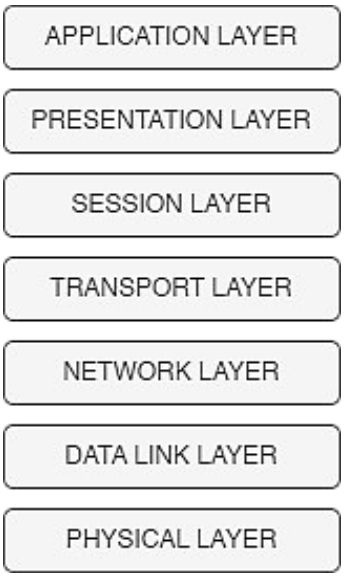

Figure 1-1: OSI Model.

With the increased importance and benefits of wireless communications, a very important issue has to be addressed, which is the security of the information being transmitted. One of the main attacks, which the wireless networks are prone to, is eavesdropping in which unintended personnel tries to intercept the information being sent. This is possible due to the broadcasting nature of radio propagation. For a long time, the solution for the eavesdropping had been cryptography where decoding the

data would be almost impossible since it could require millions of years [1]. However, with the exponential growth of computational capabilities especially with quantum computers, cryptography could start to lose its advantages [2]. Therefore, a stricter form of securing the wireless networks had to be addressed. This gave rise to the notion of security over the physical layer, the lowest layer of the OSI model, as opposed to cryptography where security is addressed at higher layers of the OSI model. The main idea for PLS is to make use the imperfections in the channels to ensure secure communication between the transmitter and the intended receiver and that any information that is captured by the eavesdropper cannot be decoded into anything meaningful even with unlimited computational power. This is referred to in the literature as information theoretic security, as the basis that ensure the secrecy of the information being transmitted is based on information theory concepts [3].

Another important motive for the analysis and study of physical layer security (PLS) is eliminating the need of secure key distribution which is one of the issues that have to be considered in systems with large number of established connections such as in 5G with the MIMO implementation or an ad-hoc network, where a user is constantly communicating with different users [4, 5].

In the analysis of physical layer security, there are some metrics that are evaluated in order to study the performance of the system at hand. One of these metrics is the Average Secrecy Capacity (ASC), which is defined as the average capacity at which the transmitter can communicate with the legitimate receiver without the eavesdropper being able to decode any useful information [6, 7]. Another metric is the probability of non-zero secrecy capacity (PNSC), which is the probability that the instantaneous secrecy capacity is more than zero [8, 9]. Finally, Secrecy Outage Probability (SOP) is also used, which is the probability that the instantaneous secrecy capacity falls below a predetermined threshold value [7, 8].

1.3. Thesis Objectives

The aim of the thesis is analysing and improving the physical layer security performance of a different GG fading channels. The GG model is chosen due to its flexibility as mentioned earlier and the fact that it subsumes many of the other commonly used fading models. To the best of our knowledge, the physical layer security performance of communication channels involving variations of the GG fading

channels has several research gaps in the literature which are to be addressed. We start by analysing a composite fading channel where the small-scale multipath component is superimposed on large-scale lognormal shadowing [7]. The small-scale fading component is modelled using a GG distribution and the legitimate and eavesdropper channels are assumed independent. We derive expressions for ASC at high SNR, PNSC and a lower bound on SOP and Monte Carlo simulations are used to confirm the avidity of the obtained expressions. The thesis also aims at suggesting and evaluating secrecy improvement techniques.

1.4. Research Contribution

The contributions of this research work can be summarized as follows:

- Physical layer security analysis over general channel models that encompass various channels and cases that can arise in wireless networks. The main focus is the generalized gamma distribution which can be used to represent various fading channels. We consider two cases for our generalized gamma distribution model. The first model is assuming the SNR of the channels follow an independent composite generalized gamma – lognormal distribution and the other case was assuming the fading channels to follow a correlated generalized gamma distribution. In both cases the metrics were evaluated and verified by the use of Monte-Carlo simulation.
- Using artificial noise to improve the secrecy performance of a wireless network is addressed and simulations were done to show the improvement in secrecy performance.

1.5. Thesis Organization

The rest of the thesis is organized as follows: Chapter 2 provides background and literature review for the work done regarding physical layer security analysis and improvement. Moreover, related works to this research are discussed. The model used is discussed in Chapter 3 along with the derivation for the probability density functions and cumulative distribution functions for the channels that we base our analysis upon. Chapter 4 provides detailed analysis of the channels under study as well as the implemented improvement technique. The simulation and results supporting our

analysis are then discussed in Chapter 5. Finally, Chapter 6 concludes the thesis and outlines the future work.

Chapter 2. Background and Literature Review

In this chapter, we discuss the fundamentals of physical layer security and the system model used as well as the different metrics used to evaluate the secrecy performance along with their definitions. We also discuss different works in the literature that analyse the secrecy performance over different fading channels. We also review several works in the literature that address how could the secrecy performance be improved.

2.1. Background

2.1.1. System model

A system model that is considered in several works that analyse physical layer security is the fading wiretap model as described by Wyner [10]. The legitimate channel is the channel between Alice and Bob and the eavesdropper channel is the channel between Alice and Eve and as shown in Figure 2-1.

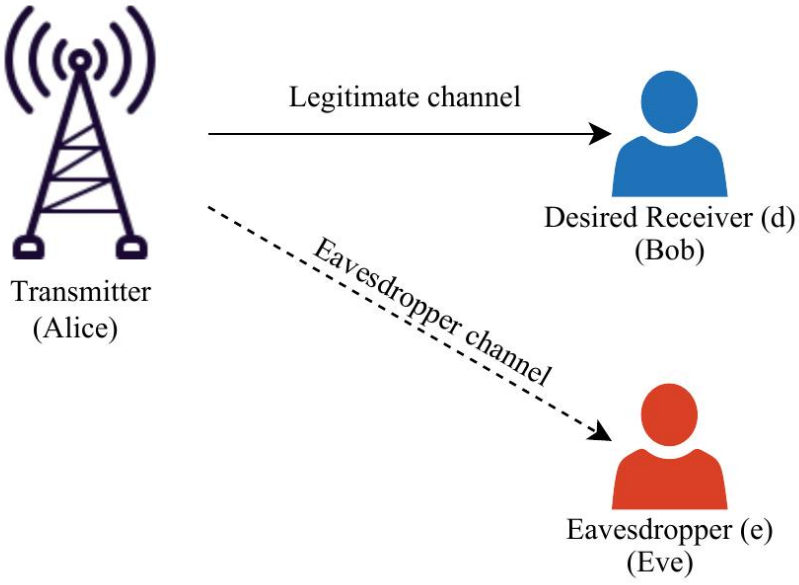

Figure 2-1: The wiretap channel model.

The received signals at Bob and Eve are given, respectively, by

$$y_d = \sqrt{P_t} h_d s + n_d, \quad (1a)$$

$$y_e = \sqrt{P_t} h_e s + n_e, \quad (1b)$$

where P_t represents the average transmitted power, h_d and h_e are the legitimate and eavesdropper channel gains, respectively, s is the transmitted signal from Alice and n_k,

$k \in d, e$ is complex a Gaussian noise with zero mean and variance w_k^2, $k \in \{d, e\}$ [8, 9].

Based on the model above, the instantaneous SNR of the legitimate channel is given by $\gamma_d = P_t|h_d|^2/w_d^2$ and for the eavesdropper channel is given by $\gamma_e = P_t|h_e|^2/w_e^2$. For the sake of simplicity and throughout the rest of the paper, the transmitted signal power is going to be assumed equal to 1, i.e., $P_t = 1$ and the noise is assumed to have unit variance, i.e., $w_k^2 = 1$, $k \in \{d, e\}$. This simplifies the expressions for the SNRs to become $x_d = |h_d|^2$ and $x_e = |h_e|^2$. In this Thesis, a quasi-static channel is going to be assumed and thus, h_k, $k \in \{d, e\}$ are assumed to follow the same distribution with the same parameters with respect to time.

In the analysis of physical layer security, there are some metrics that are evaluated in order to study the secrecy performance of the wireless network system at hand. Some of the metrics that are widely used to evaluate the secrecy performance are Average Secrecy Capacity (ASC), probability of non-zero secrecy capacity (PNSC) and Secrecy Outage Probability (SOP).

2.1.2. Average secrecy capacity

Average Secrecy Capacity (ASC) is defined as the average capacity at which the transmitter can communicate with the legitimate receiver without the eavesdropper being able to decode any useful information [6, 7]. In order to define ASC, we first introduce the instantaneous secrecy capacity, which is defined as the difference between the capacity of the legitimate and the eavesdropper channels [11], which can be expressed as follows

$$C_s(x_d, x_e) = \max\{\ln(1 + x_d) - \ln(1 + x_e), 0\}. \quad (2)$$

The ASC is therefore given by [7]

$$\overline{C}_s = \mathrm{E}[C_s(x_d, x_e)] = \int_0^\infty \int_0^\infty C_s(x_d, x_e) f(x_d, x_e)\, \mathrm{d}x_d\, \mathrm{d}x_e, \quad (3)$$

where $\mathrm{E}(\cdot)$ is the expectation operator and $f(x_d, x_e)$ is the joint probability density function (PDF) of the SNRs of the legitimate and eavesdropper channels x_d and x_e. This expression can be then simplified further depending on the channel that is being studied.

2.1.3. Probability of non-zero secrecy capacity

Probability of non-zero secrecy capacity (PNSC), which is the probability that the instantaneous secrecy capacity is more than zero [8]. For the instantaneous secrecy capacity to have a value greater than zero, the capacity of the legitimate channel must be more than the capacity of the eavesdropper channel. In order for this to happen, the SNR of the legitimate channel should be higher than the SNR of the eavesdropper channel. Therefore, the PNSC can be expressed as the probability that the SNR of the main channel is higher than that of the eavesdropper which is as expressed as shown by the expression below [7]

$$\mathrm{P}(C_s > 0) = \mathrm{P}(x_d > x_e) = \int_0^{\infty} \int_0^{x_d} f(x_d, xe)\ \mathrm{d}x_e\, \mathrm{d}x_d, \tag{4}$$

2.1.4. Secrecy outage probability

Secrecy Outage Probability (SOP) is also an important metric to be considered. SOP is defined as the probability that the instantaneous secrecy capacity falls below a predetermined threshold value [7, 8]. The SOP is given by $\mathrm{P}_{out}(R_{th}) = \mathrm{P}(C_s < R_{th})$ and by using the total law of probability, it can be expressed as follows [12]:

$$\begin{aligned} \mathrm{P}_{out}(R_{th}) &= \mathrm{P}(C_s < R_{th}) \\ &= \mathrm{P}(\ln(1+\gamma_d) - \ln(1+\gamma_e) < R_{th}) \\ &= \mathrm{P}(\gamma_d < \mathrm{e}^{R_{th}}(1+\gamma_e) - 1), \end{aligned} \tag{5}$$

where R_{th} is the threshold secrecy capacity that we need to maintain in order to consider a transmission a success and any transmission with secrecy capacity that is below the threshold value is considered to be an outage in our transmission.

2.2. Related Work

This section investigates the different works in the literature that address the topics of physical layer security analysis and improvement. We start by reviewing the different works of physical layer security analysis and the different variations that can be done in the analysis and this helps us in determining the research gap and thus in deciding on the channels that we performed the analysis on.

2.2.1. PLS over Rayleigh shadowing

Rayleigh fading channels would present a good starting point for the literature review and getting insight to the field of secrecy performance analysis. This is because fading

channels are commonly modelled using the Rayleigh distribution. It is common for cases where there is multipath fading and absence of line of sight between the transmission and receiver to be represented using a Rayleigh distribution [13]. Another advantage for the Rayleigh distribution is the simplicity of the PDF and thus it can be manipulated easily to derive the different expressions for the secrecy performance metrics.

In [8] secrecy performance is analysed for a transmitter sending data to a single receiver over a quasi-static Rayleigh fading channel, while the eavesdropper observes the transmissions over an independent quasi-static Rayleigh fading channel. A quasi-static channel indicates that the fading coefficients of a channel are constant over time. In this paper it is assumed that CSI for the legitimate channel is known at the transmitter and the legitimate receiver; however, no information is available about the wiretap channel. Similarly, the eavesdropper has knowledge of the wiretap channel. The authors derive exact expression for both PNSC and SOP which are then verified by Monte Carlo simulations.

In [14], the authors extended the work on Rayleigh fading channel by assuming the main and the eavesdropper channels are correlated which is usually due to the spatial proximity of the eavesdropper and the legitimate receiver and thus, would have relatively similar channels. The paper assumes correlated Rayleigh fading channels and it studies how the average secrecy capacity is affected by the correlation between the legitimate and eavesdropper channels. The paper studies the asymptotic behaviour of the secrecy capacity assuming a high SNR case. The results of the paper analysis show that the increased correlation between the channels degrades the secrecy performance of the network, that is illustrated by the results that for the same channel parameters, the higher the correlation, the lower the ASC become, These results matches with what could have been expected as correlated channels leave less room for randomness in the SNR levels at the legitimate and eavesdropper receivers and thus, degradation of the secrecy performance.

In [6] correlated Rayleigh fading channels were addressed again; however, the authors did not impose any limitations on the SNR levels. In order to be able to derive expressions for the ASC and SOP to analyse the secrecy performance, an infinite series was used to represent the Bessel function term in the joint PDF of the SNRs at the

legitimate and eavesdropper receivers, this enables the authors to manipulate the PDF expressions and thus, be able to derive terms for both the ASC and SOP, which would also have infinite summations. The paper also shows that truncating the infinite series at a reasonable number of terms still gives accurate results which are verified by simulations.

2.2.2. PLS over lognormal shadowing

Shadowing that is also known as large scale fading is important to consider for a wireless network [15] that usually indicates the average signal power attenuation due to large distance between the transmitter and the receiver, lognormal is usually used to model large scale fading.

A detailed study of physical layer security over non-small scale fading channels was presented in [7]. The authors focused on three different scenarios in which the main and eavesdropper channels are experiencing, independent lognormal fading or, correlated lognormal fading or, independent composite fading. In the case of composite fading, it is assumed that a Rayleigh distribution is superimposed on a lognormal distribution to represent both fading and shadowing. For all three cases, a quasi-static channel is assumed. For the different scenarios, the authors were able to derives expressions for the metrics ASC, PNSC and SOP, some of the derived expressions were based on approximations as the lognormal distribution can be present some difficulties when manipulating it. The authors then present Monte Carlo simulations that verify the accuracy of the derived expressions and thus, it verifies the approximations that the authors used in their analysis.

2.2.3. PLS over Weibull fading channels

In [16], the authors represented the mm Wave quasi-static channel by a composite fading channel where the SNR follows a Weibull-lognormal distribution. The paper aimed at deriving expressions for ASC, PNSC and SOP considering a maximum ratio combining (MRC) reception diversity technique for the eavesdropper receivers. In order to be able to analyse the secrecy performance, the authors had to define an expression for the PDF of the SNR following the composite fading channel as it was not available in the literature and thus, the authors had to propose a valid PDF and derive an expression for it. This was done be taking the channel coefficients to be following the Weibull distribution with dependence on the lognormal distribution. This

considers both small scale (Weibull) and large scale (lognormal) fading. Gauss-Hermite (GH) approximation was used in order to evaluate that PDF as it presents a method to approximate complex integrals following a certain form that the authors face in the PDF derivation. Using the derived expressions, the authors manage to evaluate expressions for the secrecy performance metrics; however, an exact expression for the SOP deemed very complex to evaluate and thus, the authors decided to find an expression for a lower bound on the SOP. The authors then verify their results by running Monte Carlo simulations which demonstrate the accuracy of the evaluated expressions especially the lower bound taken for the SOP.

Another work that addresses Weibull fading channels is [17] in which the authors were able to find analytical expressions for SOP in which the fading of the legitimate and the eavesdropper channels follow a combination of Rayleigh, Weibull and Hoyt (Nakagami-q) fading channels. Those different combinations represent different real-life scenarios that can arise when the legitimate receiver and the eavesdropper receiver are spatially apart from each other and thus, the fading models that are used to represent the channels vary resulting in the different combinations that the authors address, the secrecy performance metric derived by the authors are then verified by running Monte Carlo simulations.

2.2.4. PLS over more general fading channels

Different works in the literature started addressing PLS over more general fading channels which encompass various fading channel models. In [12], the authors focused their analysis on a classical wiretap model over Generalized Gamma (GG) also referred to as ($\alpha - \mu$) fading channels. GG distribution was first proposed by Stacy in [18] as a generalization of the gamma distribution, the GG fading channel can represent different fading channels as Gamma, Nakagami-m, exponential, Weibull, Rayleigh, Chi and Chi-squared [12, 18]. In [12] Lei et al., managed to derive closed form expressions for bounds on SOP and exact expressions for the PNSC, the Monte Carlo simulations verified the derived expression as well as the validity of the lower bound taken for the SOP.

Another work that addressed a general fading model is [19] in which the authors provide an in-depth analysis for PLS over a fading channel following Fox's H function which can represent most other fading channels as GG ($\alpha - \mu$), Fisher-Snedecor and

extended generalized-κ. The authors consider both the cases of colluding and non-colluding eavesdroppers, in the case of colluding eavesdroppers, maximum ratio combining (MRC) and selection combining (SC) are both studied. Simulation results of SOP, PNSC and ASC verified the resulting analysis of the expressions in the paper. The results show that MRC is a much more powerful technique for colluding Eavesdropper compared to SC, it is also clear that the secrecy performances have a noticeable degradation in performance when the number of colluding eavesdropper increases.

2.2.5. PLS over cascaded fading channels

Several works in the literature addressed cascaded channel models. The main motive behind a cascaded fading channel is being able to represent the cases where the message is not sent directly to the receiver but rather through a series of other nodes, this is most prominent in the cases of mobile-to-mobile, vehicle-to-vehicle (M2M/V2V) communication networks and multiple input multiple output (MIMO) system models which are used in 5G [4, 5]. The authors in [4, 5] analysed the PLS over cascaded $\kappa - \mu$ independent fading channels, the authors considered both the case in which eavesdropper are colluding and when the eavesdroppers are independent of each other. The results were then verified Monte-Carlo simulation and were shown to be highly matching the analysed results. Another study of a cascaded network is addressed in [20], in which the authors assume a cascaded Generalized Gamma ($\alpha - \mu$), the authors start by analysis of the PDF and CDF of the cascaded fading channels. System reliability was done by studying the SOP and PNSC, Results were then verified by Monte-Carlo simulations.

2.2.6. PLS improvement techniques

Several works in the literature researched into different techniques in order to improve secrecy performance of a network. In [21], a coding scheme is proposed in which the previous message transmitted is used as a code for the message after. Another approach to improving secrecy performance is jamming and artificial noise, [21] provide an overview of jamming strategies and the different jamming techniques that could be implemented to a system in order to improve the secrecy performance of the system at hand.

In [22] secrecy performance enhancement using artificial noise is studied over a Rician fading channel, the main idea behind this is artificial noise is broadcast in the null space of the legitimate receiver; therefore, not affecting the SNR at the legitimate receiver; however, degrading the SNR at the eavesdroppers and thus, the capacity of the legitimate channel stays the same and the capacity of the eavesdropper channel degrades, this increases the difference between the capacity of legitimate and eavesdropper receivers and thus, the secrecy capacity between the transmitter and the legitimate receiver increases.

A similar approach that utilizes the use of artificial noise to improve the secrecy performance of the wireless network for Rayleigh fading channels [23]. The authors then extended their work in [23] to consider the cases with several eavesdroppers and thus, more than two antennas were to be used in order to be able to degrade the eavesdropper channel. The authors also consider a scenario where the antennas that are responsible for transmitting the artificial noise is not at the transmitter but at helper amplifying relays, this could be useful when the transmit antenna does not have multiple antennas that can help in artificial noise generation or the number of transmitter that are responsible for artificial noise generation has to be improved in order to ensure secrecy against an increased number of colluding eavesdropper; however, this adds to the complexity of the system. The authors also study how the artificial noise can make communication secretly between the transmitter and the legitimate receiver possible at high average secrecy capacity even when the eavesdropper receiver is much closer to the transmitter compared to the legitimate receiver.

In [24] the authors look at different approaches for improving the secrecy performance than the use artificial noise, more specifically, the use of different diversity techniques such as MIMO, multiuser diversity and cooperative diversity. A case study is provided where cooperative relaying is used to help in the transmission of the signals and the secrecy performance improvement that it can bring about.

Another approach that is based on degrading the eavesdropper channel is presented by [25], where the authors consider the secrecy performance of a D2D unmanned aerial vehicles network. The authors present a spectrum sharing strategy to make sure that the

interference in the network is utilised such that it acts as a noise source for the eavesdropper and thus degrading the eavesdropper channel.

Chapter 3. Methodology

In this chapter, we provide the analysis that we have performed for the two channels that are under study. In order to start the physical layer security analysis for the channels under study we start by deriving expressions for their probability distribution functions in order to be able to work with the metrics equations given in Section 2.1.

3.1. Composite Generalized Gamma-Lognormal Fading Channels

The first model that we are going to discuss is a wireless network where the SNRs at the legitimate and eavesdropper receivers follow a composite generalized gamma log normal fading channel. This model is important as it takes into consideration both large scale fading (shadowing) as well as small scale fading. Moreover, the small-scale fading that is used in the model is a generalized gamma distribution which adds flexibility to the use cases of such analysis as it can be used to represent various composite channel models.

3.1.1. Derivation of the PDF

In this section we aim to derive the PDF of the legitimate and the eavesdropper channel SNRs which are assumed to follow a GG-lognormal composite fading distribution. Due to the fact that such a PDF is not readily available for us to use from the literature, it had to be derived. The idea that we have a GG fading superimposed on log normal shadowing is represented by making the assumption used that one of the parameters of the GG distribution follows the lognormal distribution. This dependency is then eliminated as shown in the steps below.

$$f(x_k) = \int_0^\infty f(x_k|\overline{x}_k) f(\overline{x}_k) \mathrm{d}\overline{x}_k \,, \tag{6}$$

where $f(\mathrm{x}_k|\overline{\mathrm{x}}_k)$ is the conditional generalized gamma distribution given by [12] as the following expression

$$f(x_k|\overline{x}_k) = \frac{\alpha_k c_k^{c_k} x_k^{\frac{\alpha_k c_k}{2}-1}}{2\overline{x}_k^{\frac{\alpha_k c_k}{2}} \Gamma(c_k)} \exp\left(-c_k \left(\frac{x_k}{\overline{x}_k}\right)^{\frac{\alpha_k}{2}}\right), k \in \{d, e\}, \tag{7}$$

where $\alpha_k, (k \in \{d, e\})$ is the fading parameter of the channels, $c_k, (k \in \{d, e\})$ is the normalized variance of the channels envelopes and $\Gamma(z)$ is the well-known Gamma

function given by $\int_0^\infty t^{z-1}\,\mathrm{e}^{-t}\,\mathrm{d}t$ [26, Eq. (8.352)]. In (6), the PDF $f(\overline{x}_k)$ follows the lognormal distribution and is given by [16]

$$f(\overline{x}_k) = \frac{1}{\sqrt{2\pi}\sigma_{\overline{x}_k}\overline{x}_k} exp\left(-\frac{\left(ln\,\overline{x}_k - \mu_{\overline{x}_k}\right)^2}{2\sigma_{\overline{x}_k}^2}\right). \tag{8}$$

Therefore, the PDF of the SNR $f(x_k)$ can be expressed as

$$\begin{aligned} & f(x_k) \\ &= \int_0^\infty \frac{\alpha_k c_k^{c_k} x_k^{\frac{\alpha_k c_k}{2}-1}}{2\overline{x}_k^{\frac{\alpha_k c_k}{2}}\Gamma(c_k)} \exp\left(-c_k\left(\frac{x_k}{\overline{x}_k}\right)^{\frac{\alpha_k}{2}}\right) \frac{1}{\sqrt{2\pi}\sigma_{\overline{x}_k}\overline{x}_k} \exp\left(-\frac{\left(\ln\overline{x}_k - \mu_{\overline{x}_k}\right)^2}{2\sigma_{\overline{x}_k}^2}\right) \mathrm{d}\overline{x}_k \\ &= \frac{\alpha_k c_k^{c_k} x_k^{\frac{\alpha_k c_k}{2}-1}}{2\Gamma(c_k)\sqrt{2\pi}\sigma_{\overline{x}_k}} \int_0^\infty \frac{1}{\overline{x}_k^{\frac{\alpha_k c_k}{2}}} \exp\left(-c_k\left(\frac{x_k}{\overline{x}_k}\right)^{\frac{\alpha_k}{2}}\right) \frac{1}{\overline{x}_k} \exp\left(-\frac{\left(\ln\overline{x}_k - \mu_{\overline{x}_k}\right)^2}{2\sigma_{\overline{x}_k}^2}\right) \mathrm{d}\overline{x}_k \\ &= \frac{\alpha_k c_k^{c_k} x_k^{\frac{\alpha_k c_k}{2}-1}}{2\Gamma(c_k)\sqrt{2\pi}\sigma_{\overline{x}_k}} \int_0^\infty \frac{1}{\overline{x}_k^{\frac{\alpha_k c_k}{2}+1}} \exp\left(-c_k\left(\frac{x_k}{\overline{x}_k}\right)^{\frac{\alpha_k}{2}} - \frac{\left(\ln\overline{x}_\mathrm{k} - \mu_{\overline{x}_k}\right)^2}{2\sigma_{\overline{x}_k}^2}\right) \mathrm{d}\overline{x}_k. \end{aligned} \tag{9}$$

Due to the complex nature of the integral in (9), Gauss-Hermite (GH) approximation [27, Table (25.10)] can be used. Generally, the GH approximation can be used to approximate integrals in the following way:

$$\int_{-\infty}^{\infty} \exp(-x^2)\, f(x)\mathrm{d}x \approx \sum_{i=1}^{N} w_i\, f(x_i), \tag{10}$$

where N is the degree of the Hermite polynomial used, $\{x_i\}$, $i = 1,2,\ldots,N$ are the roots of the Hermite polynomial $H_N(x)$ and w_i are the weights found using [27, Eq. (25.4.46)]

$$w_i = \frac{2^{N-1}N!\sqrt{\pi}}{N^2[H_{N-1}(x_i)]^2}. \tag{11}$$

In order to be able to evaluate the integral in (9), a change of variable $z = \ln\overline{x}_k / \sqrt{2\sigma_{x_k}}$ is proposed. This results in an integral in a similar form to (10), which then evaluates to the expression shown below for the joint PDF of the SNRs of the legitimate and eavesdropper channels.

$$f(x_k) = \frac{\alpha_k c_k^{c_k} x_k^{\frac{\alpha_k c_k}{2}-1}}{2\Gamma(c_k)\sqrt{\pi}} \exp\left(-\frac{\mu_{\overline{x}_k}^2}{2\sigma_{\overline{x}_k}^2}\right) \sum_{p=1}^{N} w_p \overline{x}_{k_p}^{\frac{\mu_{\overline{x}_k}}{\sigma_{\overline{x}_k}^2} - \frac{\alpha_k c_k}{2}} \exp\left(-\frac{c_k x_k^{\alpha_k/2}}{\overline{x}_{k_p}^{\alpha_k/2}}\right). \quad (12)$$

3.1.2. Derivation of the CDF

The cumulative distribution function (CDF) of the SNR can then be directly evaluated as

$$F(x_k) = \int_0^{x_k} f(x_k)\mathrm{d}x_k$$

$$= \frac{\alpha_k c_k^{c_k}}{2\Gamma(c_k)\sqrt{\pi}} \exp\left(-\frac{\mu_{x_k}^2}{2\sigma_{\overline{x}_k}^2}\right) \sum_{p=1}^{N} w_p \overline{x}_{k_p}^{\frac{\mu_{\overline{x}_k}}{\sigma_{\overline{x}_k}^2} - \frac{\alpha_k c_k}{2}} \int_0^{x_k} x_k^{\frac{\alpha_k c_k}{2}-1} \exp\left(-\frac{c_k x_k^{\alpha_k/2}}{\overline{x}_{k_p}^{\alpha_k/2}}\right) \mathrm{d}x_k. \quad (13)$$

This last integral can be evaluated using [26, Eq. (3.381-8)] to yield

$$F(x_k) = \int_0^{x_k} f(x_k)\mathrm{d}x_k$$

$$= \frac{1}{\Gamma(c_k)\sqrt{\pi}} \exp\left(-\frac{\mu_{\overline{x}_k}^2}{2\sigma_{\overline{x}_k}^2}\right) \sum_{p=1}^{N} w_p \overline{x}_{k_p}^{\mu_{\overline{x}_k}/\sigma_{\overline{x}_k}^2} \gamma\left(c_k, \frac{c_k x_k^{\alpha_k/2}}{\overline{x}_{k_p}^{\alpha_k/2}}\right), \quad (14)$$

where $\gamma(a, x)$ is the lower incomplete gamma function given by $\int_0^x t^{a-1} e^{-t}\mathrm{d}t$ [26, Eq. (8.350)]. We are now ready to start deriving expressions for the metrics of interest, namely, ASC, PNSC and SOP.

3.1.3. Average secrecy capacity analysis

The general definition of ASC is given by (3) and due to the sign restriction on secrecy capacity and the independence of the main and the eavesdropper channels, this expression can be re-written as

$$\overline{C}_s = \int_0^{\infty} \int_0^{x_d} \ln(1 + x_d)\, f_{x_d}(x_d) f_{x_e}(x_e)\ \mathrm{d}x_e\, \mathrm{d}x_d$$

$$- \int_0^{\infty} \int_{x_e}^{\infty} \ln(1 + x_e)\, f_{x_d}(x_d) f_{x_e}(x_e)\ \mathrm{d}x_d\, \mathrm{d}x_e$$

$$= \int_0^{\infty} \ln(1 + x_d)\, f_{x_d}(x_d) F_{x_e}(x_d)\ \mathrm{d}x_d - \int_0^{\infty} \ln(1 + x_e)\, f_{x_e}(x_e) \left(1 - F_{x_d}(x_e)\right) \mathrm{d}x_e$$

$$= \int_0^\infty \ln(1+x_d)\, f_{x_d}(x_d) F_{x_e}(x_d)\, \mathrm{d}x_d + \int_0^\infty \ln(1+x_e)\, f_{x_e}(x_e) F_{x_d}(x_e)\, \mathrm{d}x_e$$

$$- \int_0^\infty \ln(1+x_e)\, f_{x_e}(x_e)\, \mathrm{d}x_e$$

$$= I_1 + I_2 - I_3. \tag{15}$$

We will now start deriving results for each of the three integrals I_1, I_2 and I_3. Starting with I_1, it can be evaluated as shown in (16) below.

$$I_1 = \int_0^\infty \ln(1+x_d)\, f_{x_d}(x_d) F_{x_e}(x_d)\, \mathrm{d}x_d$$

$$= \int_0^\infty \ln(1+x_d) \frac{\alpha_d c_d^{c_d} x_d^{\frac{\alpha_d c_d}{2}-1}}{2\Gamma(c_d)\sqrt{\pi}} \exp\left(-\frac{\mu_{\overline{x}_d}^2}{2\sigma_{\overline{x}_d}^2}\right) \sum_{p=1}^{N} w_p \overline{x}_{d_p}^{\frac{\mu_{\overline{x}_d}}{\sigma_{\overline{x}_d}^2}-\frac{\alpha_d c_d}{2}} \exp\left(-\frac{c_d x_d^{\alpha_d/2}}{\overline{x}_{d_p}^{\alpha_d/2}}\right)$$

$$\times \frac{1}{\Gamma(c_e)\sqrt{\pi}} \exp\left(-\frac{\mu_{\overline{x}_e}^2}{2\sigma_{\overline{x}_e}^2}\right) \sum_{q=1}^{N} w_q \overline{x}_{e_q}^{\mu_{\overline{x}_e}/\sigma_{\overline{x}_e}^2} \gamma\left(c_e, \frac{c_e x_d^{\alpha_e/2}}{\overline{x}_{e_q}^{\alpha_e/2}}\right) \mathrm{d}x_d$$

$$= \frac{\alpha_d c_d^{c_d}}{2\Gamma(c_d)\Gamma(c_e)\pi} \exp\left(-\frac{\mu_{\overline{x}_d}^2}{2\sigma_{\overline{x}_d}^2} - \frac{\mu_{\overline{x}_e}^2}{2\sigma_{\overline{x}_e}^2}\right) \sum_{p=1}^{N}\sum_{q=1}^{N} w_p w_q \overline{x}_{d_p}^{\frac{\mu_{\overline{x}_d}}{\sigma_{\overline{x}_d}^2}-\frac{\alpha_d c_d}{2}} \overline{x}_{e_q}^{\mu_{\overline{x}_e}/\sigma_{\overline{x}_e}^2}$$

$$\times \int_0^\infty \ln(1+x_d)\, x_d^{\frac{\alpha_d c_d}{2}-1} \exp\left(-\frac{c_d x_d^{\alpha_d/2}}{\overline{x}_{d_p}^{\alpha_d/2}}\right) \gamma\left(c_e, \frac{c_e x_d^{\alpha_e/2}}{\overline{x}_{e_q}^{\alpha_e/2}}\right) \mathrm{d}x_d. \tag{16}$$

Evaluating the integral in (16) in closed form is a very challenging task, in order to overcome this problem, a high SNR scenario is assumed and hence, we use the approximation $\ln(1+x_d) \approx \ln(x_d)$. Furthermore, assuming that c_e can only take integer values, the lower incomplete gamma function can be represented by the following series representation $\gamma(n,x) = (n-1)!\left[1 - e^{-x}\sum_{m=0}^{n-1}\frac{x^m}{m!}\right]$ [26, Eq. (8.352)]. Therefore, (16) can now be expressed as in (17) as shown below.

$$I_1 = \frac{\alpha_d c_d^{c_d} (c_e-1)!}{2\Gamma(c_d)\Gamma(c_e)\pi} \exp\left(-\frac{\mu_{\overline{x}_d}^2}{2\sigma_{\overline{x}_d}^2} - \frac{\mu_{\overline{x}_e}^2}{2\sigma_{\overline{x}_e}^2}\right)$$

$$\times \sum_{p=1}^{N}\sum_{q=1}^{N} w_p w_q \overline{x}_{d_p}^{\frac{\mu_{\overline{x}_d}}{\sigma_{\overline{x}_d}^2}-\frac{\alpha_d c_d}{2}} \overline{x}_{e_q}^{\mu_{\overline{x}_e}/\sigma_{\overline{x}_e}^2} \int_0^\infty \ln(x_d)\, x_d^{\frac{\alpha_d c_d}{2}-1} \exp\left(-\frac{c_d x_d^{\alpha_d/2}}{\overline{x}_{d_p}^{\alpha_d/2}}\right)$$

$$\times\left[1-\exp\left(-\frac{c_e x_d^{\alpha_e/2}}{\overline{x}_{e_q}^{\alpha_e/2}}\right)\sum_{m=0}^{c_e-1}\frac{\left(\frac{c_e x_d^{\alpha_e/2}}{\overline{x}_{e_q}^{\alpha_e/2}}\right)^m}{m!}\right]\mathrm{d}x_d, \tag{17}$$

Finally, using the change of variable $u = x_d^{\alpha_d/2}$, the integral in (17) can be put on the same form in [26, Eq. (4.352)] and therefore, I_1 evaluates to the final result in (18) as shown below.

$$I_1 = \frac{2c_d^{c_d}(c_e-1)!}{\alpha_d\Gamma(c_d)\Gamma(c_e)\pi}\exp\left(-\frac{\mu_{\overline{x}_d}^2}{2\sigma_{\overline{x}_d}^2}-\frac{\mu_{\overline{x}_e}^2}{2\sigma_{\overline{x}_e}^2}\right)\sum_{p=1}^{N}\sum_{q=1}^{N}w_p w_q\,\overline{x}_{d_p}^{\frac{\mu_{\overline{x}_d}}{\sigma_{\overline{x}_d}^2}-\frac{\alpha_d c_d}{2}}\overline{x}_{e_q}^{\mu_{\overline{x}_e}/\sigma_{\overline{x}_e}^2}$$

$$\times\left[\frac{\Gamma(c_d)}{c_d^{c_d}}\overline{x}_{d_p}^{\frac{\alpha_d c_d}{2}}\left(\psi(c_d)-\ln\left\{\left(\frac{c_d}{\overline{x}_{d_p}^{\alpha_d/2}}\right\}\right)\right)-\right.$$

$$\left.\sum_{m=0}^{c_e-1}\frac{c_e^m\Gamma(c_d+m)}{m!\left(\overline{x}_{e_q}^{m\alpha_e/2}\right)}\left(\frac{1}{\frac{c_d}{\overline{x}_{d_p}^{\alpha_d/2}}+\frac{c_e}{\overline{x}_{e_q}^{\alpha_e/2}}}\right)^{c_d+m}\left(\psi(c_d+m)-\ln\left(\frac{c_d}{\overline{x}_{d_p}^{\alpha_d/2}}+\frac{c_e}{\overline{x}_{e_q}^{\alpha_e/2}}\right)\right)\right], \tag{18}$$

where $\psi(x)$ is the digamma function defined as $\psi(x) = \frac{\mathrm{d}}{\mathrm{d}x}\ln\Gamma(x)$ [26, Eq. (8.360)]. In a similar manner to I_1, I_2 can be evaluated as shown in (19) below.

$$I_2 = \frac{2c_e^{c_e}(c_d-1)!}{\alpha_e\Gamma(c_d)\Gamma(c_e)\pi}\exp\left(-\frac{\mu_{\overline{x}_d}^2}{2\sigma_{\overline{x}_d}^2}-\frac{\mu_{\overline{x}_e}^2}{2\sigma_{\overline{x}_e}^2}\right)\sum_{p=1}^{N}\sum_{q=1}^{N}w_p w_q\,\overline{x}_{e_p}^{\frac{\mu_{\overline{x}_e}}{\sigma_{\overline{x}_e}^2}-\frac{\alpha_e c_e}{2}}\overline{x}_{d_q}^{\mu_{\overline{x}_d}/\sigma_{\overline{x}_d}^2}$$

$$\times\left[\frac{\Gamma(c_e)}{c_e^{c_e}}\overline{x}_{e_p}^{\frac{\alpha_e c_e}{2}}\left(\psi(c_e)-\ln\left(\frac{c_e}{\overline{x}_{e_p}^{\alpha_e/2}}\right)\right)-\sum_{m=0}^{c_d-1}\frac{c_d^m\Gamma(c_d+m)}{m!\overline{x}_{d_q}^{m\alpha_d/2}}\left(\frac{1}{\frac{c_d}{\overline{x}_{d_q}^{\alpha_d/2}}+\frac{c_e}{\overline{x}_{e_d}^{\alpha_d/2}}}\right)^{c_e+m}\left(\psi(c_e+\right.\right.$$

$$\left.\left.m)-\ln\left(\frac{c_d}{\overline{x}_{d_q}^{\alpha_d/2}}+\frac{c_e}{\overline{x}_{e_p}^{\alpha_e/2}}\right)\right)\right]. \tag{19}$$

Moving on to I_3, following a similar approximation and change of variable as for I_1, it can be evaluated as follows

$$I_3 = \frac{2}{\alpha_e\sqrt{\pi}} \exp\left(-\frac{\mu_{\overline{x}_e}^2}{2\sigma_{\overline{x}_e}^2}\right) \sum_{p=1}^{N} w_p \overline{x}_{e_p}^{\frac{\mu_{\overline{x}_e}}{\sigma_{\overline{x}_e}^2}} \left[\psi(c_e) - \ln\left(\frac{c_e}{\overline{x}_{e_p}^{\alpha_e/2}}\right)\right]. \tag{20}$$

Therefore, the final expression for the average secrecy capacity can be expressed by using equations (15) and (18-20).

3.1.4. Probability of non-zero secrecy capacity

The general definition of PNSC is given by (4) and due to the independence of the main and the eavesdropper channels, this expression can be re-written in (21) as shown below.

$$\mathrm{P}(C_s > 0) = \int_0^{\infty}\int_0^{x_d} f_{x_d}(x_d) f_{x_e}(x_e)\, \mathrm{d}x_e\, \mathrm{d}x_d = \int_0^{\infty} f_{x_d}(x_d) F_{x_e}(x_d)\, \mathrm{d}x_d$$

$$= \int_0^{\infty} \frac{\alpha_d c_d^{c_d} x_d^{\frac{\alpha_d c_d}{2}-1}}{2\Gamma(c_d)\sqrt{\pi}} \exp\left(-\frac{\mu_{\overline{x}_d}^2}{2\sigma_{\overline{x}_d}^2}\right) \sum_{p=1}^{N} w_p \overline{x}_{d_p}^{\frac{\mu_{\overline{x}_d}}{\sigma_{\overline{x}_d}^2}-\frac{\alpha_d c_d}{2}} \exp\left(-\frac{c_d x_d^{\alpha_d/2}}{\overline{x}_{d_p}^{\alpha_d/2}}\right)$$

$$\times \frac{1}{\Gamma(c_e)\sqrt{\pi}} \exp\left(-\frac{\mu_{\overline{x}_e}^2}{2\sigma_{\overline{x}_e}^2}\right) \sum_{q=1}^{N} w_q \overline{x}_{e_q}^{\mu_{\overline{x}_e}/\sigma_{\overline{x}_e}^2} \gamma\left(c_e, \frac{c_e x_d^{\alpha_e/2}}{\overline{x}_{e_q}^{\alpha_e/2}}\right) \mathrm{d}x_d$$

$$= \frac{\alpha_d c_d^{c_d}}{2\Gamma(c_d)\Gamma(c_e)\pi} exp\left(-\frac{\mu_{\overline{x}_d}^2}{2\sigma_{\overline{x}_d}^2} - \frac{\mu_{\overline{x}_e}^2}{2\sigma_{\overline{x}_e}^2}\right) \sum_{p=1}^{N}\sum_{q=1}^{N} w_p w_q \overline{x}_{d_p}^{\frac{\mu_{\overline{x}_d}}{\sigma_{\overline{x}_d}^2}-\frac{\alpha_d c_d}{2}} \overline{x}_{e_q}^{\mu_{\overline{x}_e}/\sigma_{\overline{x}_e}^2}$$

$$\times \int_0^{\infty} x_d^{\frac{\alpha_d c_d}{2}-1} \exp\left(-\frac{c_d x_d^{\alpha_d/2}}{\overline{x}_{d_p}^{\alpha_d/2}}\right) \gamma\left(c_e, \frac{c_e x_d^{\alpha_e/2}}{\overline{x}_{e_q}^{\alpha_e/2}}\right) \mathrm{d}x_d. \tag{21}$$

which following the multiple steps in the equation lead to the final expression shown. After a change of variable of $u = x_d^{\alpha_d/2}$, the integral in (21) can be evaluated using [26, Eq. (6.455)] giving the closed form expression for PNSC in (22)

$$\mathrm{P}(C_s > 0) = \frac{c_d^{c_d} c_e^{c_e} \Gamma(c_d + c_e)}{c_e \Gamma(c_d)\Gamma(c_e)\pi} \exp\left(-\frac{\mu_{\overline{x}_d}^2}{2\sigma_{\overline{x}_d}^2} - \frac{\mu_{\overline{x}_e}^2}{2\sigma_{\overline{x}_e}^2}\right)$$

$$\times \sum_{p=1}^{N}\sum_{q=1}^{N} w_p w_q \overline{x}_{d_p}^{\mu_{\overline{x}_d}/\sigma_{\overline{x}_d}^2} \overline{x}_{e_q}^{\mu_{\overline{x}_e}/\sigma_{\overline{x}_e}^2} \frac{\overline{x}_{d_p}^{\frac{\alpha_d c_d}{2}} \overline{x}_{e_q}^{\frac{\alpha_e c_e}{2}}}{\left(c_e \overline{x}_{d_p}^{\alpha_d/2} + c_d \overline{x}_{e_q}^{\alpha_e/2}\right)^{c_e + c_e}}$$

$$ {}_2F_1\left(1, c_d + c_e; c_e + 1; \frac{c_e\, \overline{x}_{d_p}^{\alpha_d/2}}{c_e \overline{x}_{d_p}^{\alpha_d/2} + c_d \overline{x}_{e_q}^{\alpha_e/2}}\right), \tag{22} $$

where ${}_2F_1(\alpha, \beta; \gamma; z)$ is the hypergeometric function defined in [26, Eq. (9.111)].

3.1.5. Secrecy outage probability

The general definition of SOP is given by (5). However, due to the complexity this form would bring in the integral, we propose a lower bound as follows [12]

$$ \mathrm{P}_{out}(R_{th}) \le \mathrm{P}_{out}^{L}(R_{th}) = \mathrm{P}(x_d < \mathrm{e}^{R_{th}} \times x_e), \tag{23} $$

which can be evaluated as follows

$$ \begin{aligned} \mathrm{P}_{out}^{L}(R_{th}) &= \int_0^{\infty} \int_0^{\mathrm{e}^{R_{th}} x_e} f_{x_d}(x_d) f_{x_e}(x_e)\, \mathrm{d}x_e\, \mathrm{d}x_d = \int_0^{\infty} F_{x_d}(\mathrm{e}^{R_{th}} x_e) f_{x_e}(x_e)\, \mathrm{d}x_e \\ &= \frac{\alpha_e c_e^{c_e}}{2\pi \Gamma(c_d)\Gamma(c_e)} \exp\left(-\frac{\mu_{\overline{x}_d}^2}{2\sigma_{\overline{x}_d}^2} - \frac{\mu_{\overline{x}_e}^2}{2\sigma_{\overline{x}_e}^2}\right) \sum_{p=1}^{N} \sum_{q=1}^{N} w_p w_q \overline{x}_{d_q}^{\mu_{\overline{x}_d}/\sigma_{\overline{x}_d}^2} \overline{x}_{e_p}^{\frac{\mu_{\overline{x}_e}}{\sigma_{\overline{x}_e}^2} - \frac{\alpha_e c_e}{2}} \\ &\quad \times \int_0^{\infty} x_e^{\frac{\alpha_e c_e}{2} - 1} \exp\left(-\frac{c_e x_e^{\alpha_e/2}}{\overline{x}_{e_p}^{\alpha_e/2}}\right) \gamma\left(c_d, \frac{c_d (\mathrm{e}^{R_{th}} x_e)^{\alpha_d/2}}{\overline{x}_{d_q}^{\alpha_d/2}}\right) \mathrm{d}x_e. \end{aligned} \tag{24} $$

This last integral can be evaluated in a similar way to (21) yielding the expression in (25).

$$ \begin{aligned} \mathrm{P}_{out}^{L}(R_{th}) &= \frac{c_d^{c_d} c_e^{c_e} \Gamma(c_d + c_e)}{\pi \Gamma(c_d)\Gamma(c_e) c_d} \exp\left(\frac{R_{th}\alpha_d c_d}{2} - \frac{\mu_{\overline{x}_d}^2}{2\sigma_{\overline{x}_d}^2} - \frac{\mu_{\overline{x}_e}^2}{2\sigma_{\overline{x}_e}^2}\right) \\ &\quad \times \sum_{p=1}^{N} \sum_{q=1}^{N} w_p\, w_q \overline{x}_{e_p}^{\frac{\mu_{\overline{x}_e}}{\sigma_{\overline{x}_e}^2} - \frac{\alpha_e c_e}{2}} \overline{x}_{d_q}^{\frac{\mu_{\overline{x}_d}}{\sigma_{\overline{x}_d}^2} - \frac{\alpha_d c_d}{2}} \left(\frac{c_d e^{\frac{R_{th}\alpha_d}{2}}}{\overline{x}_{d_q}^{\alpha_d/2}} + \frac{c_e}{\overline{x}_{e_p}^{\alpha_e/2}}\right)^{-c_d - c_e} \\ &\quad {}_2F_1\left(1, c_d + c_e; c_d + 1; \frac{c_d \exp\left(\frac{R_{th}\alpha_d}{2}\right) \overline{x}_{e_p}^{\alpha_e/2}}{c_d \exp\left(\frac{R_{th}\alpha_d}{2}\right) \overline{x}_{e_p}^{\alpha_e/2} + c_e \overline{x}_{d_q}^{\alpha_d/2}}\right) \end{aligned} \tag{25} $$

3.2. Correlated Generalized Gamma Fading Channels

As mentioned earlier, the second case that we are going to study physical layer security is a case where the legitimate and eavesdropper channels are assumed to follow a

correlated generalized gamma fading distribution that can be used to represent various fading channels as discussed in Section 2.2. Due to the unavailability of such a PDF in the literature, we start by deriving the PDF of the said channel and then find an expression for the SNR and then move to the physical layer security analysis by finding the expressions for metrics discussed earlier.

3.2.1. Derivation of the PDF

In order to derive an expression for the PDF of the correlated generalized gamma distribution, we start by the expression for the correlated Nakagami-m expression, which is given by equation (26) shown below [28].

$$f_{Y_1,Y_2}(y_1,y_2) = 4(1-\rho)^{m_2}\sum_{k=0}^{\infty}\frac{(m_1)_k\rho^k}{k!}\left(\frac{m_1}{\Omega_1(1-\rho)}\right)^{m_1+k}\left(\frac{m_2}{\Omega_2(1-\rho)}\right)^{m_2+k}$$

$$\times\frac{y_1^{2(m_1+k)-1}}{\Gamma(m_1+k)}\frac{y_2^{2(m_2+k)-1}}{\Gamma(m_2+k)}\exp\left\{-\frac{1}{(1-\rho)}\left(\frac{m_1y_1^2}{\Omega_1}+\frac{m_2y_2^2}{\Omega_2}\right)\right\}$$

$$\times\,{}_1F_1\left(m_e-m_1,m_2+k;\frac{\rho m_2y_2^2}{\Omega_2(1-p)}\right);y_1\geq 0,y_2\geq 0, \qquad (26)$$

In this equation, $m_2 \geq m_1 \geq 1/2$ are the Nakagami fading parameters, ${}_1F_1$ is the confluent hypergeometric function [26], $\Omega_i = \mathrm{E}[Y_i^2]$, $i \in \{1,2\}$, $\rho = \mathrm{cov}(Y_1^2, Y_2^2)/\sqrt{\mathrm{var}(Y_1^2)\mathrm{var}(Y_2^2)}$ is the correlation coefficient between Y_1^2 and Y_2^2 and $(a)_n = \Gamma(a+n)/\Gamma(a)$ is the Pochhammer symbol as defined by [26].

To model the correlated generalized gamma random variables, the parameter $v_i, i \in \{1,2\}$ is introduced and the following transformation is used [28]:

$$R_i = Y_i^{1/v_i},\ v_i > 0,\ i = 1,2. \qquad (27)$$

Following the transformations of random variables, an expression for the PDF of correlated generalized gamma distribution can be derived as shown in (28) below [28].

$$f_{R_1,R_2}(r_1,r_2) = 4v_1v_2(1-\rho)^{m_2}\sum_{k=0}^{\infty}\frac{(m_1)_k\rho^k}{k!}\left(\frac{m_1}{\Omega_1(1-\rho)}\right)^{m_1+k}\left(\frac{m_2}{\Omega_2(1-\rho)}\right)^{m_2+k}$$

$$\times\frac{r_1^{2v_1(m_1+k)-1}}{\Gamma(m_1+k)}\frac{r_2^{2v_2(m_2+k)-1}}{\Gamma(m_2+k)}\exp\left\{-\frac{1}{(1-\rho)}\left(\frac{m_1r_1^{2v_1}}{\Omega_1}+\frac{m_2r_2^{2v_2}}{\Omega_2}\right)\right\}$$

$$\times {}_1F_1\left(m_2 - m_1, m_2 + k; \frac{\rho m_2 r_2^{2v_2}}{\Omega_2(1-p)}\right); r_1 \geq 0, r_2 \geq 0, \quad (28)$$

The authors in [28] then derive an expression for the joint CDF of the SNR, which was given as shown in (29) below where $\beta_i = \frac{\Gamma(m_i + 1/v_i)}{\Gamma(m_i)}$, $\overline{X}_i = \beta_i(\Omega)^{1/v_i}$ is the average SNR.

$$F_{X_1,X_2}(x_1, x_2) = (1-\rho)^{m_2} \sum_{k=0}^{\infty} \frac{(m_1)_k \rho^k}{k!\,\Gamma(m_1+k)\Gamma(m_2+k)} \gamma\left(m_1 + k, \frac{\left(x_1\beta_1/\overline{X}_1\right)^{v_1}}{(1-\rho)}\right)$$

$$\times \sum_{i=0}^{\infty} \frac{(m_2 - m_1)_i \rho^i}{(m_2+k)_i\, i!} \gamma\left(m_2 + k + i, \frac{\left(x_2\beta_2/\overline{X}_2\right)^{v_2}}{(1-\rho)}\right); x_1 \geq 0, x_2 \geq 0, \quad (29)$$

Taking the derivative of the expression in (29), we can get an expression for the joint PDF of the SNRs as shown in (30). We are now ready to start deriving expressions for the metrics of interest.

$$f_{X_1,X_2}(x_1, x_2) = v_1 v_2 (1-\rho)^{m_2} \sum_{k=0}^{\infty} \frac{(m_1)_k \rho^k \beta_1^{v_1(m_1+k)} x_1^{v_1(m_1+k)-1}}{k!\,\Gamma(m_1+k)\Gamma(m_2+k)\left((1-\rho)\overline{x}_1^{v_1}\right)^{m_1+k}}$$

$$\exp\left(-\frac{(x_1\beta_1)^{v_1}}{(1-\rho)\overline{x}_1^{v_1}}\right) \sum_{i=0}^{\infty} \frac{(m_2 - m_1)_i \rho^i \beta_2^{v_2(m_2+k+i)} x_2^{v_2(m_2+k+i)-1}}{(m_2+k)_i\, i!\left((1-\rho)\overline{x}_2^{v_2}\right)^{m_2+k+i}} \exp\left(-\frac{(x_2\beta_2)^{v_2}}{(1-\rho)\overline{x}_2^{v_2}}\right);$$

$$x_1 \geq 0, x_2 \geq 0, \quad (30)$$

3.2.2. Probability of non-zero secrecy capacity

The general definition of PNSC is given by (4), which can be re-written as

$$\mathrm{P}(C_s > 0) = 1 - \int_0^{\infty} \int_0^{x_e} f_{X_d,X_e}(x_d, x_e)\, \mathrm{d}x_d\, \mathrm{d}x_e. \quad (31)$$

Therefore, PNSC can be expressed as shown in (32) below.

$$\mathrm{P}(C_s > 0) = 1 - \int_0^{\infty} v_d\, v_e (1-\rho)^{m_e}$$

$$\sum_{k=0}^{\infty} \sum_{i=0}^{\infty} \frac{(m_d)_k \rho^k \beta_d^{v_d(m_d+k)} (m_e - m_d)_i \rho^i \beta_e^{v_e(m_e+k+i)} x_e^{v_e(m_e+k+i)-1}}{k!\,\Gamma(m_d+k)\Gamma(m_d+k)\left((1-\rho)\overline{x}_d^{v_d}\right)^{m_d+k} (m_e+k)_i\, i!\left((1-\rho)\overline{x}_e^{v_e}\right)^{m_e+k+i}}$$

$$\times \exp\left(-\frac{(x_e\beta_e)^{v_e}}{(1-\rho)\overline{x}_e^{v_e}}\right)\int_0^{x_e} x_d^{v_d(m_d+k)-1}\ \exp\left(-\frac{(x_d\beta_d)^{v_d}}{(1-\rho)\overline{x}_d^{v_d}}\right)\mathrm{d}x_d\,\mathrm{d}x_e \qquad (32)$$

The inner integral in (32) can be evaluated using [26, Eq. (3.381-8)] and with rearrangement, PNSC can be given by the expression in (33)

$$\mathrm{P}(C_s>0)$$
$$= 1-(1-\rho)^{m_e v_e}\sum_{k=0}^{\infty}\sum_{i=0}^{\infty}\frac{(m_d)_k\rho^k(m_e-m_d)_i\rho^i\beta_e^{v_e(m_e+k+i)}}{k!\,\Gamma(m_d+k)\Gamma(m_e+k)(m_e+k)_i i!\left((1-\rho)\overline{x}_e^{v_e}\right)^{m_e+k+i}}$$

$$\int_0^{\infty} x_e^{v_e(m_e+k+i)-1}\exp\left(-\frac{(x_e\beta_e)^{v_e}}{(1-\rho)\overline{x}_e^{v_e}}\right)\gamma\left(m_d+k,\frac{(x_d\beta_d)^{v_d}}{(1-\rho)\overline{x}_d^{v_d}}\right)\mathrm{d}x_e \qquad (33)$$

After a change of variable of $z=x_e^v$ and the assumption that $v=v_d=v_e$, which is a valid assumption since the correlated channels would be in close proximity geographically indicating similar channel parameters, the integral in (33) can be evaluated using [26, Eq. (6.455-2)] giving the closed form expression for PNSC in (34) in which ${}_2F_1(\alpha,\beta;\gamma;z)$ is the hypergeometric function defined in [26, Eq. (9.111)].

$$\mathrm{P}(C_s>0) = 1-(1-\rho)^{m_e}\sum_{k=0}^{\infty}\sum_{i=0}^{\infty}\frac{(m_d)_k\rho^{k+i}(m_e-m_d)_i\beta_d^{v(m_d+k)}\beta_e^{v(m_e+k+i)}}{\Gamma(m_d+k)\Gamma(m_e+k)k!\,(m_e+k)_i i!\,(m_d+k)}$$

$$\times\frac{\Gamma(m_d+m_e+2k+i)\overline{x}_d^{v(m_e+k+i)}\overline{x}_e^{v(m_d+k)}}{((\overline{x}_d\beta_e)^v+(\overline{x}_e\beta_d)^v)^{m_d+m_e+2k+i}}$$

$$\times\,{}_2F_1\left(1,m_d+m_e+2k+i;m_d+k+1;\frac{(\beta_d\overline{x}_e)^v}{(\beta_d\overline{x}_e)^v+(\beta_e\overline{x}_d)^v}\right) \qquad (34)$$

3.2.3. Secrecy outage probability

The general definition of SOP is given by (5). However, due to the complexity this form would bring in the integral, we propose a lower bound as follows [12]:

$$\mathrm{P}_{out}(R_{th}) \geq \mathrm{P}_{out}^{L}(R_{th}) = \mathrm{P}(x_d < e^{R_{th}}x_e), \qquad (35)$$

which can be evaluated as follows

$$\mathrm{P}_{out}^{L}(R_{th}) = \int_0^{\infty}\int_0^{\mathrm{e}^{R_{th}}x_2} f_{X_1,X_2}(x_1,x_2)\ \mathrm{d}x_2\,\mathrm{d}x_1. \qquad (36)$$

This last integral can be evaluated in a similar way to (34) yielding the expression in (37) as shown below

$$\mathrm{P}_{out}^{L}(R_{th}) = (1-\rho)^{m_e} \sum_{k=0}^{\infty}\sum_{i=0}^{\infty} \frac{(m_d)_k \rho^{k+i} (m_e - m_d)_i (\beta_d e^{R_{th}})^{v(m_d+k)} \beta_e^{v(m_e+k+i)}}{\Gamma(m_d+k)\Gamma(m_e+k) k!\,(m_e+k)_i i!\,(m_d+k)}$$

$$\times \frac{\Gamma(m_d+m_e+2k+i)\overline{x}_d^{v(m_e+k+i)}\overline{x}_e^{v(m_d+k)}}{((\overline{x}_d\beta_e \mathrm{e}^{R_{th}})^v + (\overline{x}_e\beta_d)^v)^{m_d+m_e+2k+i}}$$

$$\times {}_2F_1\left(1, m_d+m_e+2k+i; m_d+k+1; \frac{(\beta_d\overline{x}_e \mathrm{e}^{R_{th}})^v}{(\beta_d\overline{x}_e \mathrm{e}^{R_{th}})^v + (\beta_e\overline{x}_d)^v}\right) \tag{37}$$

3.2.4. Average Secrecy Capacity

The general definition of ASC is given by (3) and due to the sign restriction on secrecy capacity, this expression can be re-written as

$$\overline{C}_s = \int_0^{\infty}\int_0^{x_1} \ln(1+x_1)\, f_{X_1,X_2}(x_1,x_2)\ \mathrm{d}x_2\,\mathrm{d}x_1$$

$$-\int_0^{\infty}\int_{x_2}^{\infty} \ln(1+x_2)\, f_{X_1,X_2}(x_1,x_2)\ \mathrm{d}x_1\,\mathrm{d}x_2$$

$$= I_1 - I_2. \tag{38}$$

Each of the integrals I_1 and I_2 are now going to be evaluated independently. Starting with I_1, it can be evaluated as shown in (39) as shown below.

$$I_1 = \int_0^{\infty}\int_0^{x_d} \ln(1+x_d)\, f_{X_d,X_e}(x_d,x_e)\ \mathrm{d}x_e\,\mathrm{d}x_d$$

$$= v_d v_e (1-\rho)^{m_e} \int_0^{\infty} \ln(x_d) \sum_{k=0}^{\infty} \frac{(m_d)_k \rho^k \beta_d^{v_d(m_d+k)} x_d^{v_d(m_d+k)-1}}{k!\,\Gamma(m_d+k)\Gamma(m_e+k)\left((1-\rho)\overline{x}_d^{v_d}\right)^{m_d+k}}$$

$$\times \exp\left(-\frac{(x_d\beta_d)^{v_d}}{(1-\rho)\overline{x}_d^{v_d}}\right) \sum_{i=0}^{\infty} \frac{(m_e-m_d)_i \rho^i \beta_e^{v_e(m_e+k+i)}}{(m_e+k)_i i!\left((1-\rho)\overline{x}_2^{v_e}\right)^{m_e+k+i}}$$

$$\times \int_0^{x_1} x_e^{v_e(m_e+k+i)-1} \exp\left(-\frac{(x_e\beta_2)^{v_e}}{(1-\rho)\overline{x}_2^{v_e}}\right) \mathrm{d}x_e\,\mathrm{d}x_d \tag{39}$$

Evaluating the integral in (39) in closed form is a very challenging task, in order to overcome this problem, a high SNR scenario is assumed and hence, we use the approximation $\ln(1+\gamma_d) \approx \ln(\gamma_d)$. The inner integral in (39) can be evaluated using [26, Eq. (3.381-8)] giving the result in (40) as shown below

$$I_1 = v_d(1-\rho)^{m_e} \sum_{k=0}^{\infty} \frac{(m_d)_k \rho^k \beta_d^{v_d(m_d+k)}}{k!\,\Gamma(m_d+k)\Gamma(m_e+k)\left((1-\rho)\overline{x}_d^{v_d}\right)^{m_d+k}} \sum_{i=0}^{\infty} \frac{(m_e-m_d)_i \rho^i}{(m_e+k)_i i!}$$

$$\times \int_0^{\infty} \ln(x_d)\, x_d^{v_d(m_d+k)-1} \exp\left(-\frac{(x_d\beta_d)^{v_d}}{(1-\rho)\overline{x}_d^{v_d}}\right) \gamma\left(m_e+k+i, \frac{(x_e\beta_e)^{v_e}}{(1-\rho)\overline{x}_e^{v_e}}\right) \mathrm{d}x_d \quad (40)$$

the lower incomplete gamma function can be represented by the following series representation $\gamma(n,x) = (n-1)!\left[1 - e^{-x}\sum_{m=0}^{n-1}\frac{x^m}{m!}\right]$ [26, Eq. (8.352-4)]. In order to be able to evaluate this integral it is assumed that $v_d = v_e$, which can be justified since the correlated channels are in close proximity and such a parameter can be assumed to be equal and thus, the integral in (40) can be put in the same form in [26, Eq. (4.352-1)] after a change of variables of $z = x_d^v$ and therefore, I_1 evaluates to the final result in (41) as shown below

$$I_1 = \frac{(1-\rho)^{m_e}}{v} \sum_{k=0}^{\infty} \frac{(m_d)_k \rho^k \beta_d^{v(m_d+k)}}{k!\,\Gamma(m_d+k)\Gamma(m_e+k)} \sum_{i=0}^{\infty} \frac{(m_e-m_d)_i \rho^i (m_e+k+i-1)!}{(m_e+k)_i i!} \times$$

$$\left[\frac{\Gamma(m_d+k)}{\beta_d^{v(m_d+k)}}\left\{\Psi(m_d+k) - \ln\left(\frac{\beta_d^v}{(1-\rho)\overline{x}_d^v}\right)\right\} - \left(\frac{\overline{x}_e^v}{(\beta_d\overline{x}_e)^v + (\beta_e\overline{x}_d)^v}\right)^{(m_d+k)}\right.$$
$$\left. \times \sum_{j=0}^{(m_e+k+i-1)} \frac{\Gamma(m_d+k+j)}{j!}\left(\frac{(\beta_e\overline{x}_d)^v}{(\beta_d\overline{x}_e)^v + (\beta_e\overline{x}_d)^v}\right)^j \times \left\{\Psi(m_d+k+j) - \ln\left(\frac{(\beta_d\overline{x}_e)^v + (\beta_e\overline{x}_d)^v}{(1-\rho)(\overline{x}_d\overline{x}_e)^v}\right)\right\}\right] \quad (41)$$

where $\psi(x)$ is the digamma function defined as $\psi(x) = \frac{\mathrm{d}}{\mathrm{d}x}\ln\Gamma(x)$ [26, Eq. (8.360)]. In a similar manner to I_1, I_2 can be evaluated as shown in (42).

$$I_2 = \frac{(1-\rho)^{m_e}}{v} \sum_{k=0}^{\infty} \frac{(m_1)_k \rho^k}{k!\,\Gamma(m_e+k)} \sum_{i=0}^{\infty} \frac{(m_e-m_d)_i \rho^i (\beta_e\overline{x}_d)^{v(m_e+k+i)}}{(m_e+k)_i i!\,((\beta_d\overline{x}_e)^v + (\beta_e\overline{x}_d)^v)^{(m_e+k+i)}}$$

$$\times \sum_{j=0}^{(m_d+k-1)} \left[\Psi(m_e+k+i+j) - \ln\left(\frac{(\beta_d\overline{x}_e)^v + (\beta_e\overline{x}_d)^v}{(1-\rho)(\overline{x}_d\overline{x}_e)^v}\right)\right]$$

$$\times \frac{(\beta_d\overline{x}_e)^{vj}\Gamma(m_e+k+i+j)}{j!\,((\beta_d\overline{x}_e)^v + (\beta_e\overline{x}_d)^v)^j} \tag{42}$$

3.3. PLS Improvement

The improvement technique that we are going to implement to enhance the secrecy performance for the fading channels considered is a technique that is based on making use of an array of antennas at the transmitter in order to add dimensionality to our channel space. The key idea here is that in the case that the transmitter has more antennas than the eavesdropper receiver, we can utilise the added dimensionality in order to transmit artificial noise signals from the transmitter in the null space of the legitimate channel. This ensures that the channels between the receiver antennas and the eavesdropper antennas are degraded while the legitimate channel is unaffected. This technique is viable as it only requires information about the legitimate channel as the artificial noise is sent in the null space of the main channel which is a reasonable consideration as the transmitter and the legitimate receiver can communicate information regarding the legitimate channel to correctly approximate it. It is also important to note that it is possible for the eavesdropper to have access to the channel information of the legitimate channel, but this does not affect the secrecy performance enhancement that the artificial noise bring about. However, a limitation to this method is having more transmitter antennas than receiver antennas at the eavesdropper, otherwise, the eavesdropper might be able to perform noise cancellation techniques and negate the effect of the artificial noise.

Since the it is required to work with an array of antennas in order to improve the secrecy performance using artificial noise, the equations in (1) can be re-written in matrix/vector form as given by [23] as

$$y_d = \boldsymbol{h_d^H s} + n_d, \tag{43a}$$

$$y_e = \boldsymbol{h_e^H s} + n_e, \tag{43b}$$

The null space $\boldsymbol{B}$ of $\boldsymbol{h_d^H}$ can then be found where $\boldsymbol{h_d^H B} = \mathbf{0}$. The transmitted signal $\boldsymbol{s}$ can then be defined as $\boldsymbol{s}$ = **p**u + **w**. where u is the information bearing message and $\boldsymbol{p}$ =

$\boldsymbol{h_d}/||\boldsymbol{h_d}||$ and **w** = $\boldsymbol{B}$ **P** lies in the null space where **P** is the vector of the powers of the transmitter antennas thus the equations in (43) can be re-written as

$$y_d = \boldsymbol{h_d^H p}u + n_d, \tag{44a}$$

$$y_e = \boldsymbol{h_e^H p}u + \boldsymbol{h_e^H w} + n_e. \tag{44b}$$

It is clear from the equations in (44) that the signal component $\boldsymbol{h_d^H}$**p**u and $\boldsymbol{h_e^H}$**p**u in the received signals at the transmitter and the receiver, respectively. Those are similar to that in the equations in (43). The noise component in the signal received at the legitimate receiver is still the same. However, the noise component of the received signal at the eavesdropper receiver has considerably increased from n_e to $\boldsymbol{h_e^H}\mathbf{w} + n_e$. This significantly degrades the eavesdropper channel while the legitimate channel remains unaffected.

While using artificial noise surely improves the secrecy performance of the wireless network, it is important to note that using artificial noise does not come free of any costs as this transmission requires power; however, in order to properly investigate the effect of implementing an artificial noise technique it is reasonable to fix the total power used in a single transmission. That is in the case of not using the artificial noise technique, all the allocated power for the transmission is used in transmission of the signal information and in the case of using artificial noise, the total allocated power transmission should be divided between transmitting the signal message and generating the artificial noise. Since between those two cases the power used in the transmission of the messages is higher in the first scenario, it results in the legitimate channel to have a higher capacity; however, while an increased signal power does indeed increase the capacity of the legitimate channel, it does as well increase the SNR of the signal received at the eavesdropper receiver and thus, the eavesdropper channel capacity is improved as well; therefore, the overall result of having higher power allocated for the messages transmission is negligible as it improves both the legitimate and eavesdropper channels which is clear from the definition of instantaneous secrecy capacity as per equation (2). In the other scenario, the artificial noise technique results in the degradation of the eavesdropper channel and thus decreasing its capacity and while it is true that allocating power for the artificial noise instead of message transmission indicate that the SNR at the legitimate receiver is degraded and thus the legitimate

channel capacity is reduced; however, reduced signal transmission power indicate that the SNR at the eavesdropper receiver is degraded as well and thus the eavesdropper channel capacity is also reduced and thus, this does not affect the secrecy capacity while the artificial noise degrades only the eavesdropper channel and thus improving the secrecy capacity of the network.

Chapter 4. Monte Carlo Simulation

In this chapter, we are going to discuss the performed Monte Carlo simulations that were used to support our analysis for the physical layer security over both proposed channels and the improvement technique implemented. Monte Carlo simulations where repeated sampling is used to present results based on random variables [29]. MATLAB software was used for the generation of the random numbers used to verify our analysis in our simulations. We also verify the improvement algorithm suggested in the previous section and compare the improvement in ASC without any improvement techniques implemented.

4.1. PLS Over Composite Generalized Gamma-Lognormal Fading Channels

In order to verify our analysis, we generated 100,000 samples that follow the distribution that we are studying in order to have statistically reliable results. In order to generate the samples following the desired distribution we use MATLAB; however, due to the unavailability of a predefined function for the generation of random variables a composite generalized gamma-lognormal distribution. We turn to the inverse CDF method in order to generate the samples following the generalized gamma distribution [30] in order to generate the composite random variables, we start by using the predefined MATLAB function to generate lognormal variables which are then used as means for generating the generalized gamma variables as mentioned earlier. A similar method of generating a composite random variable was introduced by [17] where a parameter of one distribution follows the lognormal distribution. This process for generating the SNR samples is shown in Figure 4-1 below.

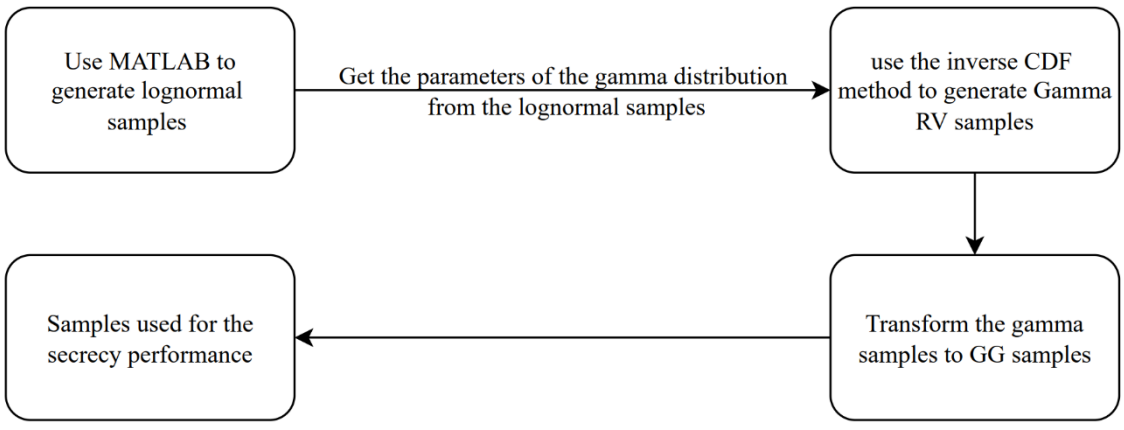

Figure 4-1: Generation of composite GG lognormal samples.

Before using those generated samples of the random variable to verify our analysis we started by having to verify that the samples generated match with the expression of the PDF that we have derived. This is done by plotting the histogram of the generated samples with narrow bar width and comparing the normalized count of the samples within a certain interval with the corresponding evaluation of the PDF at the mid-point of the interval. In order to ease the visualization of such a step, the marginal results are compared instead of plotting a 2D histogram (3D plot). The normalization of the samples count is done according to the equation below.

$$v_i = \frac{c_i}{N.w_i}, \tag{44}$$

where v_i is the height of the bin, c_i is the count of the samples that fall within the specified interval, N is the total number of samples generated and w_i is the width of the decided interval. We also made sure that the PDF and the histogram normalized as per (43) both satisfy PDF properties. The instantaneous secrecy capacity was then found for all the generated samples and then averaged out in order to find the average secrecy capacity. The instantaneous secrecy capacity that was found earlier is then used to find the probability of non-zero secrecy capacity by binary classifying the secrecy capacity for each instance by whether the instantaneous secrecy capacity is zero or not. Finally, secrecy outage probability is found in a similar way to PNSC; however, the instantaneous secrecy capacity is compared to a predetermined secrecy capacity value as opposed to zero. The parameters that are used in our simulation are as shown in table 4-1 below.

Table 4-1: Simulation Parameters for composite GG Lognormal channels.

Parameter	**Value**	**Parameter**	**Value**
α_d	1	α_e	1
c_d	3	c_e	3
$\sigma_{\overline{\gamma}_d}$	1	$\sigma_{\overline{\gamma}_e}$	1
N	40		

The parameters for the main channel and the eavesdropper channel were chosen to be similar in order to have identical channels. The main reason behind doing that is adding an extra layer of verification to our results as the PNSC is equal to 0.5 when both the legitimate and eavesdropper channels are identical as it will be shown in the next section.

4.2. PLS Over Correlated Generalized Fading Channels

A problem similar to the one faced earlier in generating samples following the composite generalized gamma log normal distribution and that is MATLAB does not have an inbuilt function for generation of samples following a correlated generalized distribution. Therefore, we start from the built-in function in MATLAB that can generate samples following correlated normal distribution and with following appropriate transformations we can transform the samples following a correlated normal distribution to samples following correlated exponential distribution [31] which could then be transformed to samples following correlated gamma distribution [31]. The samples following a correlated gamma distribution can then be transformed to samples following a correlated Nakagami-m distribution [32] and then the final transformation can be made to the samples for them to follow a correlated generalized gamma distribution [31]. This process of generating the samples following the generalized gamma and the corresponding correlated SNRs of the channels is shown in Figure 4-2 shown below.

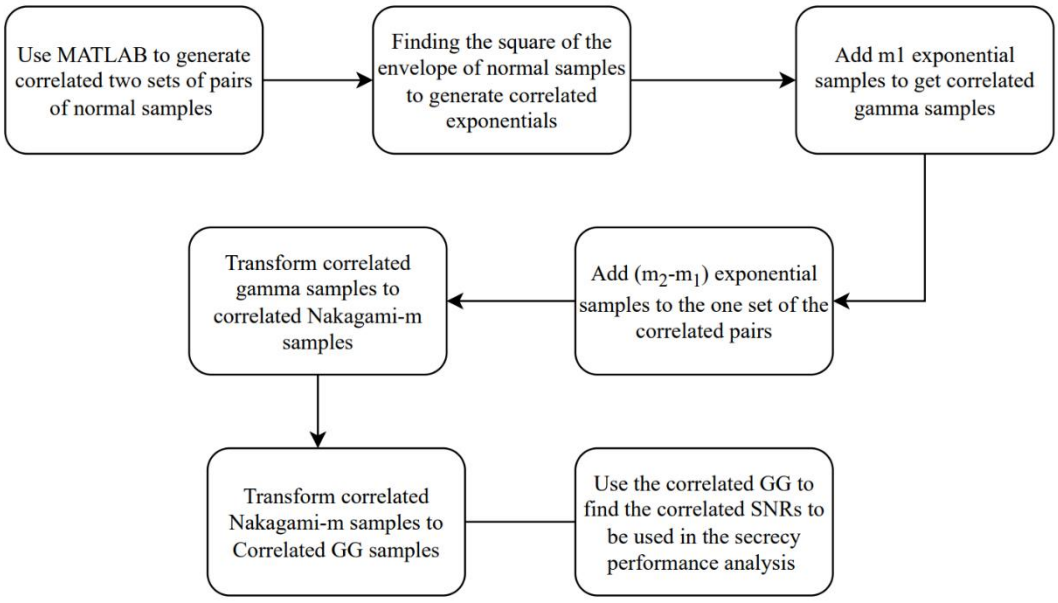

Figure 4-2: Generation of correlated GG samples.

The samples in the final steps are also cross checked with the PDF of the generalized gamma distribution that we derived earlier. This is done mentioned in the earlier section before proceeding further with the simulation to verify our analysis in similar approach

to the previous section. The parameters that are used in our simulation are as shown in table 4-2 below.

Table 4-2: Simulation Parameters for correlated GG channels.

Parameter	Value	Parameter	Value
m_d	4	m_e	4
v_d	2	v_e	2
ρ	0.8		

The values are chosen that we can verify that the values of both the derived expression and the simulation for PNSC it be equal to 0.5 when the average SNRs of the channels are equal as that is the case in identical channels.

4.3. PLS Improvement

As discussed in Section 3.3, we need to study the trade-off that arises when deciding on the power allocation schemes between the antenna transmitting the message and the antennas transmitting the artificial noise. In our simulation we are going to consider a correlated generalized gamma fading channel and that the transmitter has only two antennas, one for the signal transmission and one for artificial noise generation and as mentioned earlier in Section 3.3, for the transmitter to be able to generate noise in the null space of the main channel while forcing the eavesdropper to be unable to cancel that noise, the eavesdropper receiver has to have less antennas than the transmitter and thus in our scenario we are going to assume a single antenna of the eavesdropper receiver. Since the channel coefficients are random in nature. We are going to look to maximize the average secrecy capacity. This is done by running a brute force algorithm that runs through different feasible allocations in our sample space and for each feasible solution, the secrecy capacity is calculated for 100,000 different samples finding an average, in order eliminate the randomness of the fading channel. This process is repeated for various selected feasible solutions over the sample space of feasible solutions and the feasible solution giving the highest average secrecy capacity is recorded for the total power for which the sample space is generated. We then repeat this process for different total transmit power in order to study the effect of the increasing the total transmit power in improving the average secrecy capacity. The simulation can be demonstrated as shown in Figure 4-3 shown below. We then compare

the results between the results when the artificial noise has been used and in the case where no improvement technique is utilised.

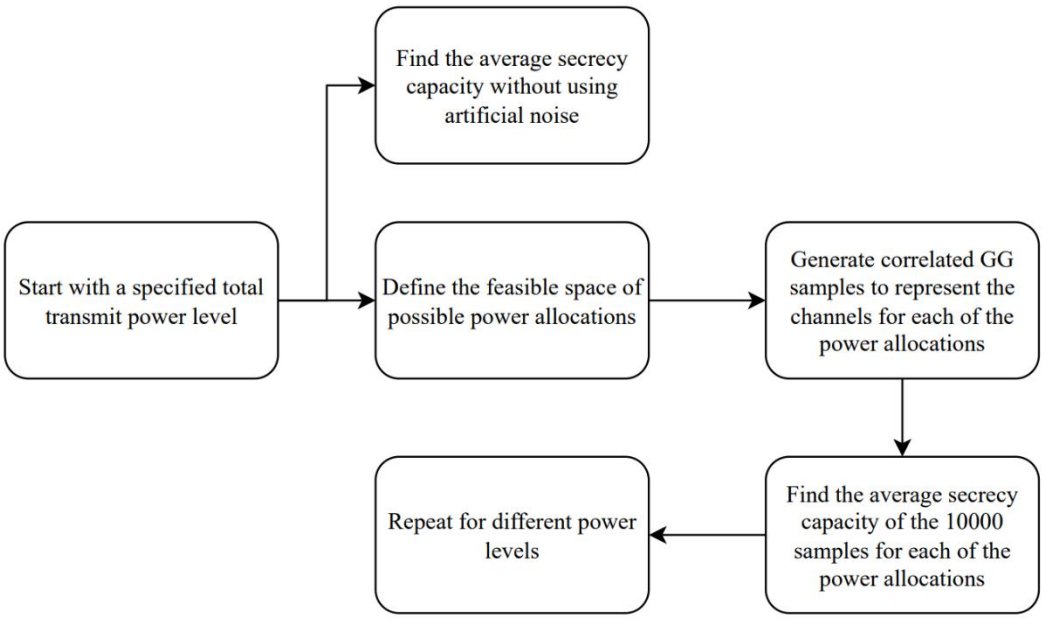

Figure 4-3: Studying the effect of using AN to improve ASC.

Chapter 5. Results and Analysis

In this chapter, we demonstrate with the simulation results that the secrecy performance analysis for both channel models and the derived expressions for all the metrics studied present accurate results since they highly match with the simulations and thus the expressions can be used directly to evaluate the secrecy performance metrics of any channel that fall under the generalized channels that were studied. We also verify the improvement in the secrecy performance that is due to using artificial noise.

5.1. PLS Over Composite Generalized Gamma-Lognormal Fading Channels

We start by verifying the probability density function of the proposed distribution that is going to represent the signal to noise ratio of both the legitimate and eavesdropper channels which is a composite generalized gamma lognormal distribution. This is important as the rest of the results are based on the derived expression in (12). The procedure is detailed in Section 4.1. It is clear from Figure 5-1 that our derived expression for the PDF matches closely with the normalized histogram and thus, we it can be used to derive the secrecy performance metrics.

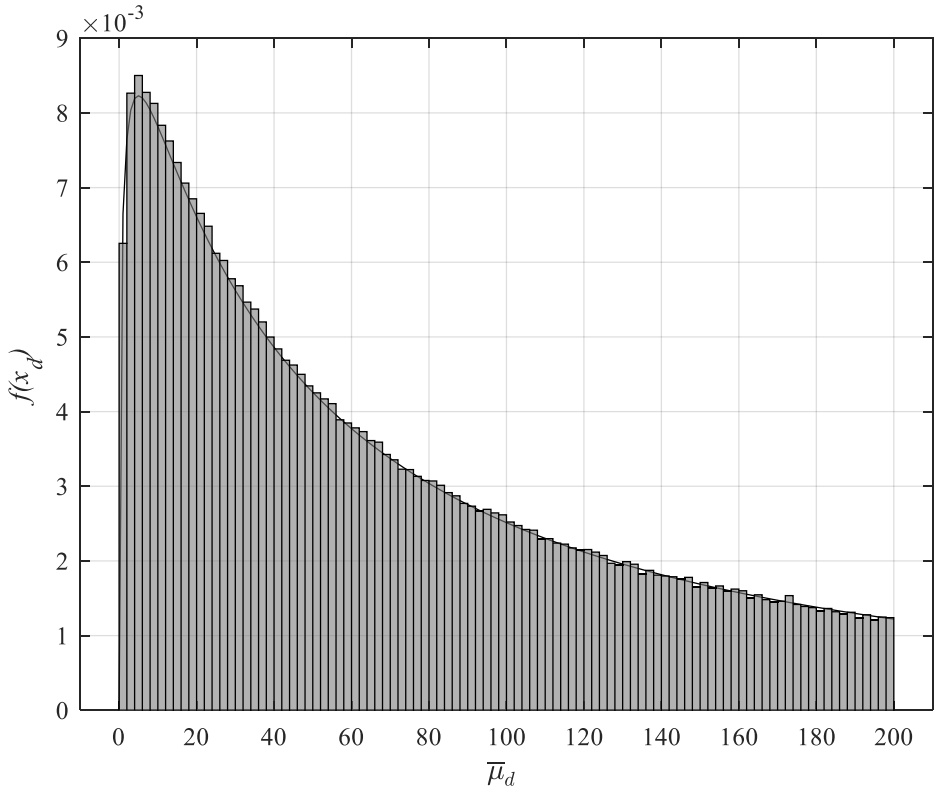

Figure 5-1: PDF verification of the composite distribution.

We then proceed with verifying the derived expressions for the metrics under study. The parameters values used in the simulations were set the values in Table 4-1 as a representative example. We start by verifying the results for the average secrecy capacity. Monte Carlo simulations were used to find the average secrecy capacity which were then compared to the value of the average secrecy capacity presented by the expressions in (15, 18-20). In Figure 5-2, the lines represent the average secrecy capacity found using the derived expressions while the circles are used to represent the results from Monte Carlo simulations. The figure shows how the average secrecy capacity changes with $\overline{\mu}_d$ for different $\overline{\mu}_e$ it is clear that the analysis and simulation results highly match. As expected, the figure shows that for the same realization of the legitimate channel, the better the eavesdropper channel, the lower ASC becomes due to the improvement in the eavesdropper channel.

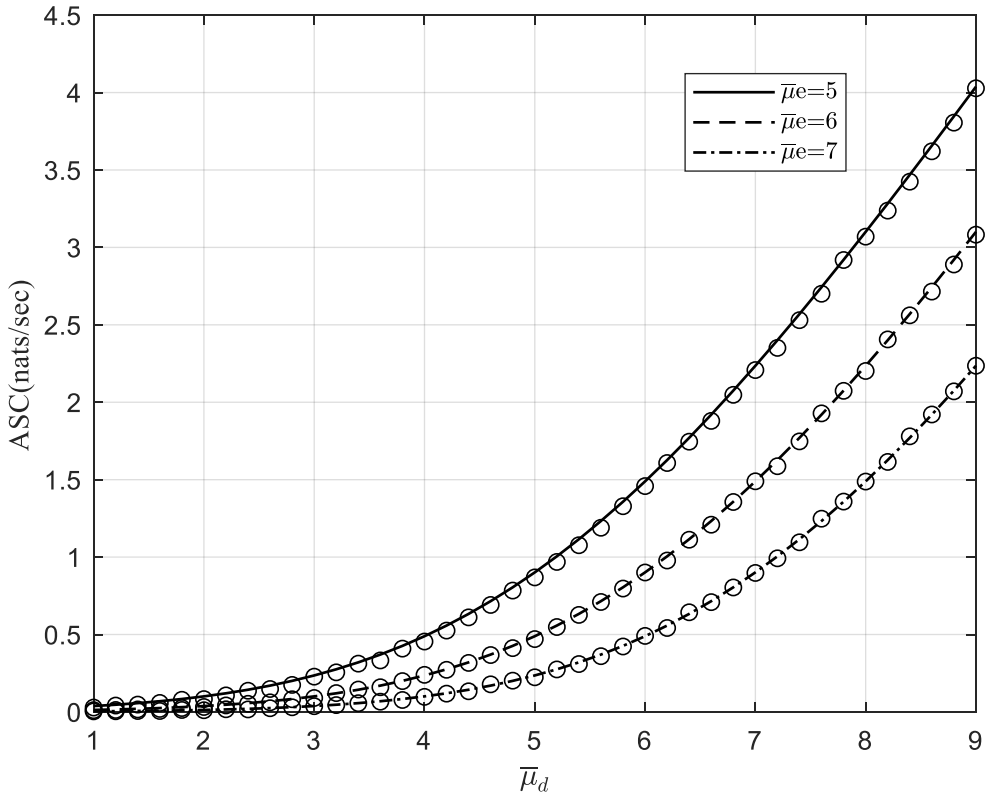

Figure 5-2: ASC vs. $\overline{\mu}_d$ for different $\overline{\mu}_e$.

We then move to verifying the expression for the probability of non-zero secrecy capacity. Figure 5-3 depicts how PNSC changes with $\overline{\mu}_d$ for different $\overline{\mu}_e$, the figure shows that the analysis depicted by the lines is matching perfectly with the simulation depicted by the circles, it also shows that the PNSC is higher at the same value of $\overline{\mu}_d$

for a lower value of $\overline{\mu}_e$ as expected. It is also clear for high $\overline{\mu}_d$ compared with $\overline{\mu}_e$, PNSC approaches 1 which is due to the fact that the legitimate channel has significantly better channel than the eavesdropper channel and thus the main channel is almost guaranteed to have higher SNR than the eavesdropper channel and thus have a secrecy capacity more than 0. Another point also to note which verify our results is that the PNSC is equal to 0.5 when $\overline{\mu}_d$ and $\overline{\mu}_e$ values are equal as this indicates that the legitimate and eavesdropper channels are identical and thus, there is equal chances that either the SNR of both channels is higher than the other and thus, there is equal chances that the channel can have a non-zero secrecy capacity or that we cannot communicate securely over the channel (PNSC=0).

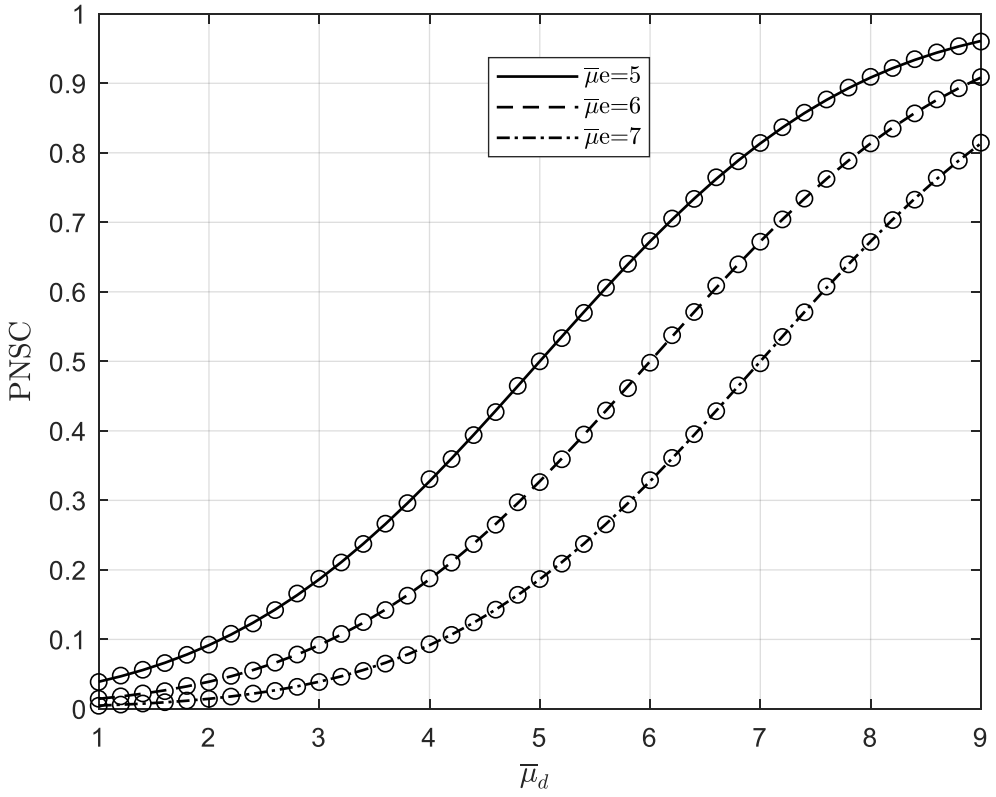

Figure 5-3: PNSC vs. $\overline{\mu}_d$ for different $\overline{\mu}_e$.

Finally, Monte Carlo simulation were run to SOP simulation was done for $R_{th} = 0.5$ over a range of values $\overline{\mu}_d$ for different $\overline{\mu}_e$, Figure 5-4 shows the accuracy of the lower bound used in the analysis as compared with the simulation. It is clear that the higher $\overline{\mu}_e$ is for the same $\overline{\mu}_d$ the higher the secrecy outage probability. This is due to the fact that for the same legitimate channel, a better eavesdropper channel would mean a higher chance of the secrecy capacity to be below the specified threshold. As expected, for low

values of $\overline{\mu}_d$, the SOP is almost 1, this is because the eavesdropper channel is considerably better than the main channel so the probability that the channel capacity of the main channel is higher than the eavesdropper capacity by a value of $R_{th} = 0.5$ is very low and thus, the SOP is almost 1.

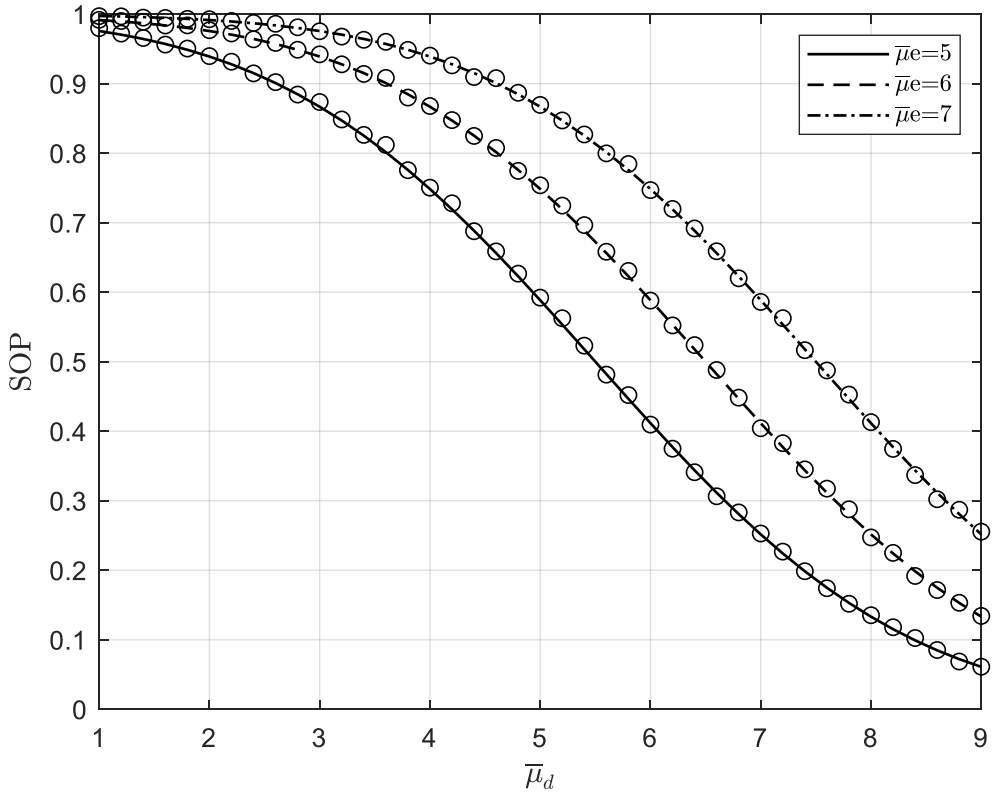

Figure 5-4: $SOP(R_{th})$ vs. $\overline{\mu}_d$ for different $\overline{\mu}_e$ for $R_{th} = 0.5$.

This verifies the accuracy of our secrecy performance analysis for this channel model, and we move on to presenting our results for the correlated generalized gamma channel model.

5.2. PLS Over Correlated Generalized Gamma Fading Channels

Monte Carlo simulation described in Section 4.2 is used in order to verify our analysis for our numerical analysis presented in the previous sections. The parameters values used in the simulations were set as in Table 4-2 as an example. Figure 5-5 depicts how PNSC changes with $\overline{x}_d$ for different values of $\overline{x}_e$, the figure shows a perfect match between the simulation and our analysis, which is expected as no approximations were used in the analysis of PNSC. The figure also illustrates that at higher values of $\overline{x}_e$ for the same value of $\overline{x}_d$, the PNSC is lower as expected from the definition of secrecy

capacity. It is also clear from the figure that at higher values of $\overline{x}_d$, PNSC approaches 1 as expected as the capacity of the legitimate channel is very likely to have a higher value compared to the capacity of the eavesdropper channel as the legitimate channel SNR is much higher than that of the eavesdropper channel. It is also clear that when $\overline{x}_d$ is equal to $\overline{x}_e$, the PNSC is equal to 0.5 which lines up with our expectations as both channels are identical and thus, there is equal chance for either to be better than the other indicating that we have equal probability of instantaneous secrecy capacity to be equal to zero or to have a non-zero value and thus PNSC is equal to 0.5 in that case.

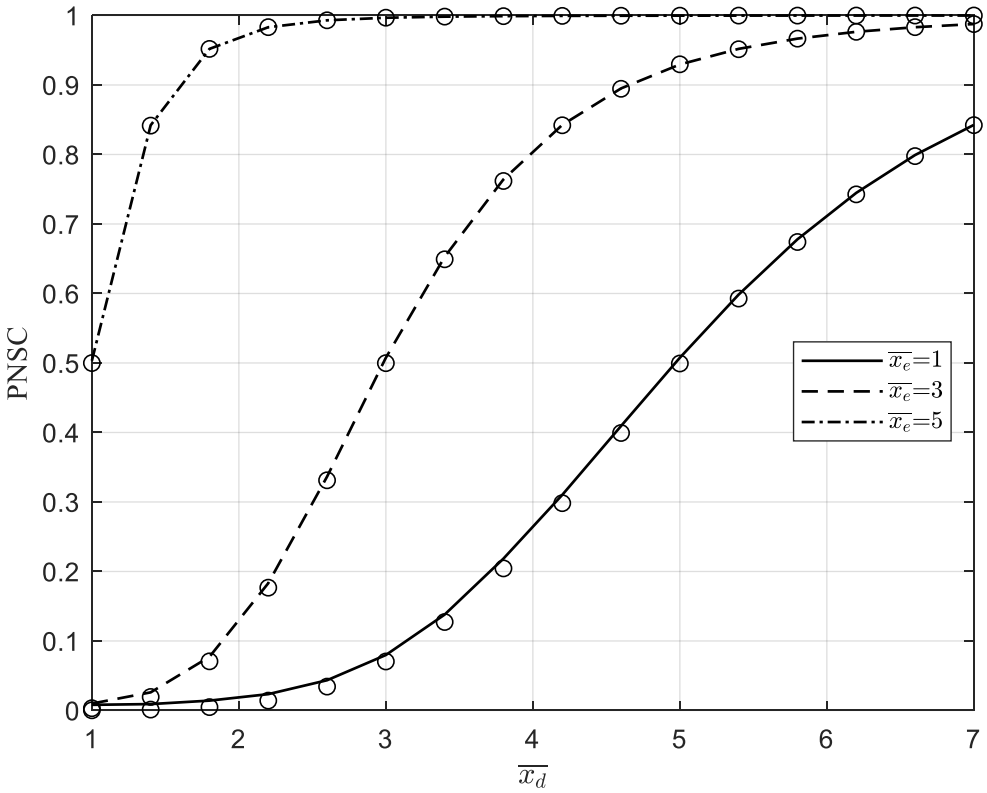

Figure 5-5: PNSC vs. $\overline{x}_d$ for different $\overline{x}_e$.

The second metric that we verify with our simulation is the SOP simulation was assuming a threshold of $R_{th} = 0.2$ over a range of values for $\overline{x}_d$ for different $\overline{x}_e$ values and the results are shown in Figure 5-6. The figure shows how the lower bound used in the analysis performs as compared with the simulation results. The lower bound is within 10% accurate at lower average values of the SNRs' of then channels when compared to the simulation. The performance of the SOP lower bound compared to the simulation gets relatively more accurate at higher SNRs. It is also clear from the figure that at high values of SNRs for the legitimate channel, the secrecy outage probability is

almost 0 which matches with our expectation as the legitimate channel is much better than the eavesdropper channel and thus, there is a very high chance that the SNR of the legitimate channel is high enough for the capacity of the legitimate channel to be higher than the capacity of the eavesdropper channel by the value of R_{th}. It is clear that unlike the PNSC, when the SNRs of the legitimate and eavesdropper channels are equal, the secrecy outage probability is higher than 0.5, this is expected as for the calculation of the secrecy outage probability, it is not enough for the legitimate channel capacity to be higher than the eavesdropper channel capacity (Instantaneous secrecy capacity > 0) for the transmission to be a success as we are considering our success transmission when the instantaneous secrecy capacity is more than the predetermined value.

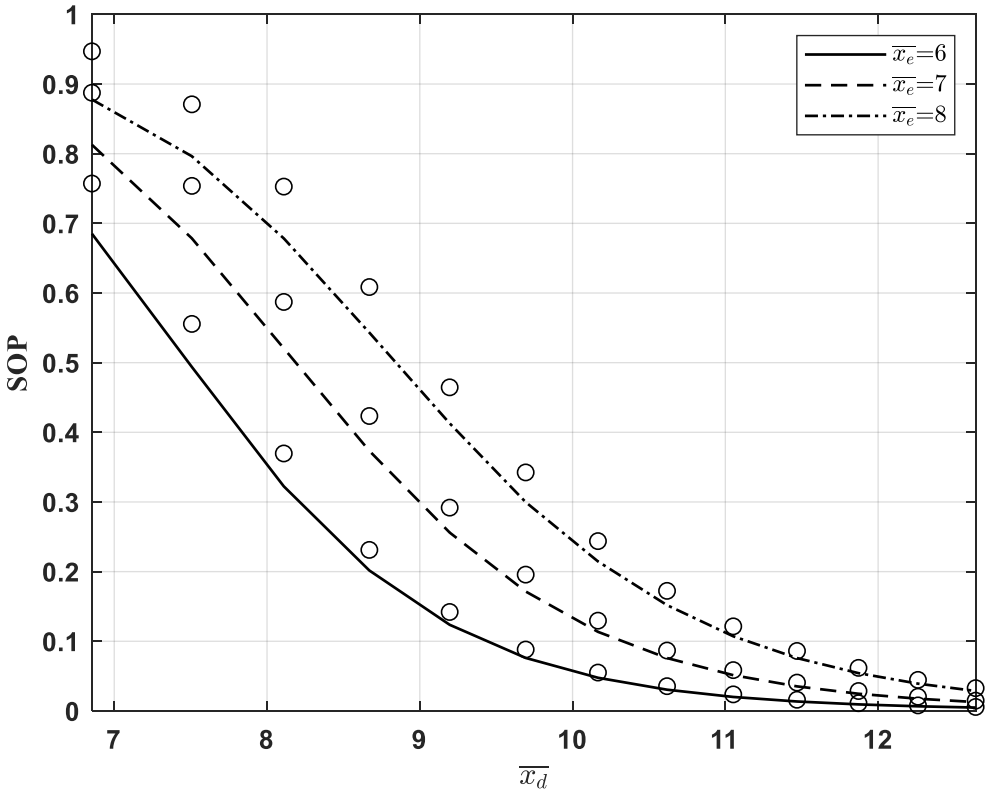

Figure 5-6: SOP vs. $\overline{\mathrm{x}}_d$ for different $\overline{\mathrm{x}}_e$.

Finally, Figure 5-7 shows the accuracy of the high SNR approximation used in the analysis of average secrecy capacity as the analysis highly matches the simulation results. It is also clear that, as expected, for the same realization of the legitimate channel average SNR and the better the eavesdropper channel average SNR, the lower the ASC becomes due to the improvement in the eavesdropper channel and this

decreases the instantaneous secrecy capacity for every transmission under these conditions and thus, decreasing the average secrecy capacity for this case.

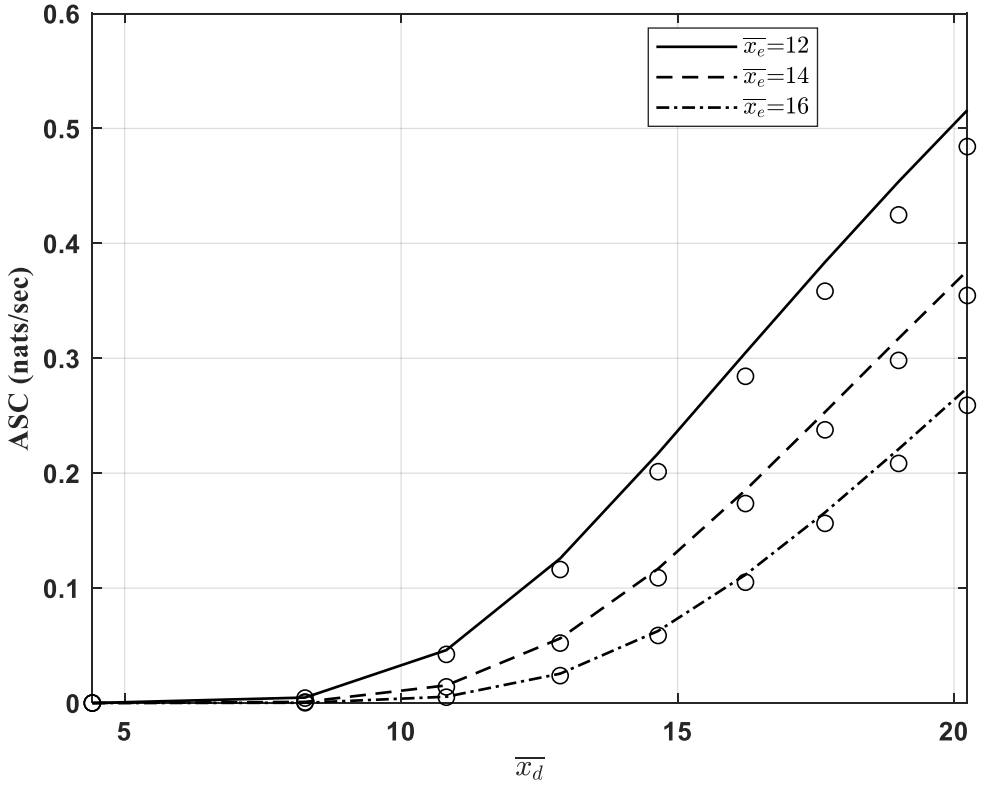

Figure 5-7: ASC vs. $\overline{x}_d$ for different $\overline{x}_e$.

5.3. PLS Improvement Based on Artificial Noise

Monte Carlo simulations were used to find the effect of using artificial noise on the average secrecy capacity for transmission of Figure 5-8 shows how significantly the artificial noise algorithm can help in improving the average secrecy capacity of the legitimate channel. It is clear from the figure that increasing the transmit power for a network where artificial noise is not implemented has little to no effect on the average secrecy capacity which is as expected as mentioned in Section 3.3. This is due to the fact that an increase in signal power without utilising any of the added power resource for artificial noise improves both the legitimate and eavesdropper channels capacities by the same factor and this results in a small to no change in the instantaneous secrecy capacity as it is defined as the difference between the legitimate and eavesdropper channels and thus, the average secrecy capacity of the network almost stays unchanged. However, with the case of allocating some power from the total transmission power for transmitting artificial noise in the null space of the main channel, we are able to degrade

the eavesdropper channel by decreasing the SNR and thus degrading the eavesdropper channel capacity without affecting the legitimate channel capacity and thus, improving the instantaneous capacity and thus, the average secrecy capacity.

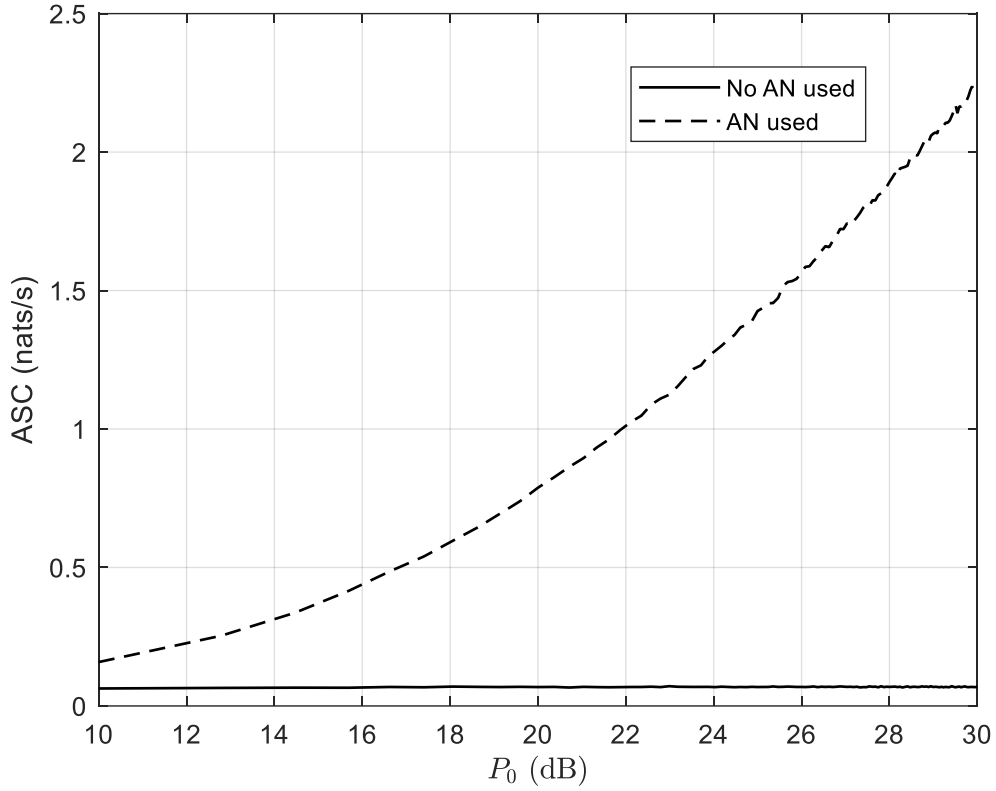

Figure 5-8: Effect of implementing AN on ASC.

Table 5-1 below shows the optimal power allocation between the two antennas at different power constraint levels

Table 5-1: Optimal power allocations.

Total Power	**Signal Antenna**	**AN Antenna**	**ASC**
10	3.0000	7.0000	0.1584
100	17.6667	82.3333	0.7881
190	28.1429	161.8571	1.1097
280	28.4510	251.5490	1.3393
370	45.6552	324.3448	1.5307
460	50.5385	409.4615	1.6566
550	70.7183	479.2817	1.7995
640	76.7895	563.2105	1.9069
730	98.9268	631.0732	1.9868
820	96.3488	723.6512	2.0958
910	91.0000	819.0000	2.1645
1000	127.3158	872.6842	2.2320
1090	120.9000	969.1000	2.2903

The table below shows the different power allocations that were tested by our brute force algorithm for a total power of 100 and the resulting ASC. The table shows that with the different power allocations between the signal transmitting antenna and the antenna transmitting the artificial noise, the average secrecy capacity could improve by more than a factor of 6 when the optimal power allocation between the signal transmitting and artificial noise antennas as compared to choosing a random power allocation case or using all the power available for transmission for the transmission of the message. It can also be noted from Table 5-2 that equal power allocation can provide significant improvement as well. The equal power allocation between the signal transmitting antenna and the artificial noise transmitting antenna provides almost 5 times improvement compared to not using artificial noise. Even though this is not the optimal power allocation, it could be a quick allocation scheme that can provide significant improvement in the secrecy performance of the network.

Table 5-2: Feasible solution space and corresponding ASC.

Signal Antenna	**AN Antenna**	**ASC**
1.0000	99.0000	0.4380
4.3333	95.6667	0.7000
7.6667	92.3333	0.7621
11.0000	89.0000	0.7825
14.3333	85.6667	0.7736
17.6667	82.3333	0.7836
21.0000	79.0000	0.7720
24.3333	75.6667	0.7584
27.6667	72.3333	0.7417
31.0000	69.0000	0.7222
34.3333	65.6667	0.7120
37.6667	62.3333	0.6949
41.0000	59.0000	0.6810
44.3333	55.6667	0.6510
47.6667	52.3333	0.6337
51.0000	49.0000	0.6071
54.3333	45.6667	0.5883
57.6667	42.3333	0.5698
61.0000	39.0000	0.5340
64.3333	35.6667	0.5065
67.6667	32.3333	0.4764
71.0000	29.0000	0.4478
74.3333	25.6667	0.4090
77.6667	22.3333	0.3828
81.0000	19.0000	0.3480

84.3333	15.6667	0.3087
87.6667	12.3333	0.2671
91.0000	9.0000	0.2187
94.3333	5.6667	0.1693
97.6667	2.3333	0.1213

Chapter 6. Conclusion and Future Work

In this thesis, we considered the problem of eavesdropping which is a form of passive attacks that a wireless network can be a target of. This is a greater risk than ever due to the improvements in computational power. This leads us to looking for a stricter notion of security and thus, we address the physical layer which from an information theoretic point of view can guarantee full secrecy from the eavesdropper when the transmitter sends data at a certain rate. We managed to perform physical layer security analysis for two different fading channels which were chosen such that they can help in secrecy performance analysis for various real-life scenarios. We started by analysing a wireless network where the signals at the legitimate and eavesdropper receivers follow an independent composite generalized gamma lognormal distribution. To be able to start with our analysis we derived an expression for the PDF and verified it by comparing the marginal PDFs using Monte Carlo simulations where the generated samples are used to plot marginal 1D histograms. In our analysis we were able to derive expressions for ASC, PNSC and SOP. Using Monte Carlo simulations, we managed to verify our analysis for the derived expressions. The second channel that we analysed is a correlated generalized gamma distribution. We were able to derive expressions for the joint PDF of the SNRs of the messages at the legitimate and eavesdropper receivers. The derived expression for the SNR was verified using a Monte Carlo simulation. Monte Carlo simulations were also used to verify the analysis that we have done that resulted in expressions for ASC, PNSC and SOP for correlated generalized gamma fading channels. The final part of our work revolved around degrading the eavesdropper channel by using artificial noise that is transmitted in the null space of the legitimate channel through utilizing an antenna array at the transmitter. A brute force method was applied in order to decide on the power allocation between the antenna transmitting the message and the antenna responsible for the transmission of the artificial noise. The artificial noise was verified to significantly improve the ASC performance for a correlated generalized gamma fading channel.

As a future work, we can consider different algorithms that can help in deciding the power allocation between the transmitter antennas since we resorted to brute force method as we only considered two transmit antennas and thus, in a case where the transmitter has more than two antennas, the feasible space for the different power

allocations drastically increase as the only limitation that we have is the sum of the allocated power to be within a threshold value. The different approaches can look into power allocation optimization techniques while considering the randomness. Another approach is looking for methods that can minimize our search within the feasible space and thus, even if a search is required it would be much more computationally efficient than a brute search.

References

[1] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE wireless Communications*, vol. 18, no. 2, pp. 66–74, 2011.

[2] L. Kong, Y. Ai, L. Lei, G. Kaddoum, S. Chatzinotas, and B. Ottersten, "An overview of generic tools for information-theoretic secrecy performance analysis over wiretap fading channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, pp. 1–21, 2021.

[3] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[4] D. Tashman and W. Hamouda, "Cascaded $\kappa - \mu$ fading channels with colluding and non-colluding eavesdroppers: Physical-layer security analysis," *Future Internet*, vol. 13, no. 8, p. 205, 2021.

[5] D. H. Tashman and W. Hamouda, "Cascaded $\kappa - \mu$ fading channels with colluding eavesdroppers: Physical-layer security analysis," in 2020 *International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*. IEEE, 2021, pp. 1–6.

[6] X. Sun, J. Wang, W. Xu, and C. Zhao, "Performance of secure communications over correlated fading channels," *IEEE Signal Processing Letters*, vol. 19, no. 8, pp. 479–482, 2012.

[7] G. Pan, C. Tang, X. Zhang, T. Li, Y. Weng, and Y. Chen, "Physical-layer security over non-small-scale fading channels," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1326–1339, 2015.

[8] J. Barros and M. R. Rodrigues, "Secrecy capacity of wireless channels," in 2006 *IEEE international symposium on information theory*. IEEE, 2006, pp. 356–360.

[9] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[10] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[11] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE transactions on information theory*, vol. 24, no. 3, pp. 339–348, 1978.

[12] H. Lei, C. Gao, Y. Guo, and G. Pan, "On physical layer security over generalized gamma fading channels," *IEEE Communications Letters*, vol. 19, no. 7, pp. 1257–1260, 2015.

[13] B. Sklar, "Rayleigh fading channels in mobile digital communication systems: Part I: Characterization," *IEEE Commun. Mag.*, vol. 35, pp. 90–100, Jul. 1997.

[14] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high SNR," *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 1975–1983, 2011.

[15] A. J. Coulson, A. G. Williamson, and R. G. Vaughan, "A statistical basis for lognormal shadowing effects in multipath fading channels," *IEEE Transactions on communications*, vol. 46, no. 4, pp. 494–502, 1998.

[16] R. Singh and M. Rawat, "Performance analysis of physical layer security over Weibull/lognormal composite fading channel with MRC reception," *AEU-International Journal of Electronics and Communications*, vol. 110, no. 152849, pp. 1-13, 2019.

[17] F. Jameel, M. A. A. Haider, A. A. Butt et al., "Physical layer security under Rayleigh/Weibull and Hoyt/Weibull fading," in *2017 13th International Conference on Emerging Technologies (ICET)*. IEEE, 2017, pp. 1–5.

[18] E. W. Stacy, "A generalization of the gamma distribution," *The Annals of mathematical statistics*, pp. 1187–1192, 1962.

[19] L. Kong, G. Kaddoum, and H. Chergui, "On physical layer security over Fox's H-function wiretap fading channels," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 6608–6621, 2019.

[20] L. Kong, G. Kaddoum, and D. B. Da Costa, "Cascaded $\alpha - \mu$ fading channels: Reliability and security analysis," *IEEE Access*, vol. 6, pp. 41 978–41 992, 2018.

[21] S. M. Shah and V. Sharma, "Enhancing secrecy rates in a wiretap channel," *Digital Communications and Networks*, vol. 6, no. 1, pp. 129–135, 2020.

[22] M. Ahmed and L. Bai, "Secrecy capacity of artificial noise aided secure communication in MIMO Rician channels," *IEEE Access*, vol. 6, pp. 7921–7929, 2018.

[23] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE transactions on wireless communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[24] Y. Zou, J. Zhu, X. Wang, and V. C. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42–48, 2015.

[25] B. Yang, T. Taleb, Z. Wu, and L. Ma, "Spectrum sharing for secrecy performance enhancement in D2D-enabled UAV networks," *IEEE Network*, vol. 34, no. 6, pp. 156–163, 2020.

[26] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*. Academic press, 2014.

[27] M. Abramowitz and I. Stegun, *Handbook of mathematical functions* 9th ed. New York: National Bureau of Standards, 1970, pp. 890-925.

[28] V. A. Aalo and T. Piboongungon, "On the multivariate generalized gamma distribution with exponential correlation," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Nov. 2005, pp. 1229–1233.

[29] S. Raychaudhuri, “Introduction to Monte Carlo simulation,” in 2008 *Winter simulation conference*. IEEE, 2008, pp. 91–100.

[30] W. T. Shaw, “Sampling student’s T distribution-use of the inverse cumulative distribution function,” *Journal of Computational Finance*, vol. 9, no. 4, p. 37, 2006.

[31] M. Reig, L. Rubio Arjona, and N. Cardona Marcet, “Bivariate Nakagami-m distribution with arbitrary fading parameters,” *Electronics Letters*, vol. 38, no. 25, pp. 1715–1717, 2002.

[32] G. K. Karagiannidis, D. A. Zogas, and S. A. Kotsopoulos, “On the multivariate Nakagami-m distribution with exponential correlation,” *IEEE Transactions on Communications*, vol. 51, no. 8, pp. 1240–1244, 2003.

Vita

Youssef Mohamed Eldokmak was born in 1998, in Giza, Egypt, where he received his primary education. He received his secondary education in Abu Dhabi, UAE. He received his B.Sc. degree in Electrical Engineering from the American University of Sharjah in 2020.

In September 2020, he joined the Electrical Engineering master's program in the American University of Sharjah as a graduate research and teaching assistant. During his master's study, he co-authored 2 papers which were presented in international conferences. His research interests are in wireless communications, digital communications and optimization of communication systems.