Physical-Layer Security in Cognitive Radio Networks

Deemah Hail Tashman

A Thesis

in

the Department

of

Electrical and Computer Engineering

Presented in Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy (Electrical and Computer Engineering) at

Concordia University

Montréal, Québec, Canada

April 2022

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: **Deemah Hail Tashman**

Entitled: **Physical-Layer Security in Cognitive Radio Networks**

and submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy (Electrical and Computer Engineering)

complies with the regulations of this University and meets the accepted standards with respect to originality and quality. Signed by the final examining committee:

_____ Chair
Dr. Ahmed Soliman

_____ External Examiner
Dr. Cheng Li

_____ Thesis Supervisor
Dr. Walaa Hamouda

_____ Examiner
Dr. Amr Youssef

_____ Examiner
Dr. Yousef Shayan

_____ Examiner
Dr. Dongyu Qiu

Approved by _____
Dr. Wei-Ping Zhu, Graduate Program Director

4/22/2022 _____
Dr. Mourad Debbabi, Dean
Gina Cody School of Engineering and Computer Science

Abstract

Physical-Layer Security in Cognitive Radio Networks

Deemah Hail Tashman, Ph.D.

Concordia University, 2022

The fifth-generation (5G) communications and beyond are expected to serve a huge number of devices and services. However, due to the fixed spectrum allocation policies, the need for cognitive radio networks (CRNs) has increased accordingly. CRNs have been proposed as a promising approach to address the problem of under-utilization and scarcity of the spectrum. In CRNs, secondary users (SUs) access the licensed spectrum of the primary users (PUs) using underlay, overlay, or interweave paradigms. SUs can access the spectrum band simultaneously with the PUs in underlay access mode provided that the SUs' transmission power does not cause interference to the PUs' communication. In this case, SUs should keep monitoring the interference level that the PU receiver can tolerate and adjust the transmission power accordingly. However, varying the transmission power may lead to some threats to the privacy of the information transfer of CRNs. Therefore, securing data transmission in an underlay CRN is a challenge that should be addressed. Physical-layer security (PLS) has recently emerged as a reliable method to protect the confidentiality of the SUs' transmission against attacks, especially for the underlay model with no need for sharing security keys. Indeed, PLS has the advantage of safeguarding the data transmission without the necessity of adding enormous additional resources, specifically when there are massively connected devices.

Apart from the energy consumed by the various functions carried out by SUs, enhancing security consumes additional energy. Therefore, energy harvesting (EH) is adopted in our work to achieve both; energy efficiency and spectral efficiency. EH is a significant breakthrough for green communication, allowing the network nodes to reap energy from multiple sources to lengthen battery

life. The energy from various sources, such as solar, wind, vibration, and radio frequency (RF) signals, can be obtained through the process of EH. This accumulated energy can be stored to be used for various processes, such as improving the users' privacy and prolonging the energy-constrained devices' battery life.

In this thesis, for the purpose of realistic modelling of signal transmission, we explicitly assume scenarios involving moving vehicles or nodes in networks that are densely surrounded by obstacles. Hence, we begin our investigations by studying the link performance under the impact of cascaded $\kappa-\mu$ fading channels. Moreover, using the approach of PLS, we address the privacy of several three-node wiretap system models, in which there are two legitimate devices communicating under the threat of eavesdroppers. We begin by a three-node wiretap system model operating over cascaded $\kappa-\mu$ fading channels and under worst-case assumptions. Moreover, assuming cascaded $\kappa-\mu$ distributions for all the links, we investigate the impact of these cascade levels, as well as the impact of multiple antennas employed at the eavesdropper on security. Additionally, the PLS is examined for two distinct eavesdropping scenarios: colluding and non-colluding eavesdroppers. Throughout the thesis, PLS is mainly evaluated through the secrecy outage probability (SOP), the probability of non-zero secrecy capacity (P_r^{nzc}), and the intercept probability (P_{int}).

Considering an underlay CRN operating over cascaded Rayleigh fading channel, with the presence of an eavesdropper, we explore the PLS for SUs in the network. This study is then extended to investigate the PLS of SUs in an underlay single-input-multiple-output (SIMO) CRN over cascaded κ-μ general fading channels with the presence of a multi-antenna eavesdropper. The impact of the constraint over the transmission power of the SU transmitter due to the underlay access mode is investigated. In addition, the effects of multiple antennas and cascade levels over security are well-explored.

In the second part of our thesis, we propose an underlay CRN, in which an SU transmitter communicates with an SU destination over cascaded κ-μ channels. The confidentiality of the shared information between SUs is threatened by an eavesdropper. Our major objective is to achieve a secured network, while at the same time improving the energy and spectrum efficiencies with practical modeling for signals' propagation. Hence, we presume that the SU destination harvests energy from the SU transmitter. The harvested energy is used to produce jamming signals to be transmitted

to mislead the eavesdropper. In this scenario, a comparison is made between an energy-harvesting eavesdropper and a non-energy harvesting one. Additionally, we present another scenario in which cooperative jamming is utilized as one of the means to boost security. In this system model, the users are assumed to communicate over cascaded Rayleigh channels. Moreover, two scenarios for the tapping capabilities of the eavesdroppers are presented; colluding and non-colluding eavesdroppers. This study is then extended for the case of non-colluding eavesdroppers, operating over cascaded κ-μ channels.

Finally, we investigate the reliability of the SUs and PUs while accessing the licensed bands using the overlay mode, while enhancing the energy efficiency via EH techniques. Hence, we assume that multiple SUs are randomly distributed, in which one of the SUs is selected to harvest energy from the PUs' messages. Then, utilizing the gathered energy, this SU combines its own messages with the amplified PUs messages and forwards them to the destinations. Furthermore, we develop two optimization problems with the potential of maximizing the secondary users' rate and the sum rate of both networks.

Acknowledgments

First and foremost, I am grateful to God Almighty for without his blessings, this achievement would not be possible. I would love also to express my deep and sincere gratitude to my research supervisor, Professor Walaa Hamouda for giving me the opportunity to be one of his students and for providing invaluable guidance throughout this research. His encouragement, vision, and motivation have deeply inspired me. His knowledge and unwavering support have been important in motivating me to achieve my objectives and successfully complete this degree. It was an incredible joy and honor to work and learn under his direction, and I am appreciative of everything he has given me.

I would also like to thank my committee members, Professor Dr. Y.R. Shayan, Professor Dr. A. Youssef, and Professor Dr. D. Qiu for serving as my committee members. I appreciate your constructive remarks and recommendations throughout this research.

I am sincerely thankful to Concordia Graduate Student Support Program (GSSP) and the Department of Electrical and Computer Engineering at Concordia University for their financial support for funding my Ph.D. studies.

I am tremendously appreciative of my parents' love, prayers, and sacrifices in educating and preparing me for the future. I appreciate your faith in me and my abilities. You have motivated and encouraged me during all the steps of my life and without this, I would not have grown into the person I am today. I would also like to express my gratitude to my brothers and sisters and their lovely families. Your concern and support were vital in assisting me in achieving my objective.

I would like to express my gratefulness and appreciation to have been blessed with wonderful friends who showered me with endless support during my journey. Special thanks goes to my friends A. Ismail and N. Abdel Khalek.

To my beloved parents, Hayel and Sawsan Tashman,

My brothers, Jawad and Fakher,

My sisters, Marina, Hazar, and Areen, and their families .

Contents

List of Figures

List of Tables

List of Acronyms

5G Fifth Generation.

ABEP Average Bit Error Probability.

ACC Average Channel Capacity.

AF Amplify and Forward.

AS Antenna Selection.

ASC Average Secrecy Capacity.

ASEP Average Symbol Error Probability.

ASR Average Secrecy Rate.

AWGN Additive-White Gaussian Noise.

BPSK Binary-Phase-Shift-Keying.

CDF Cumulative Distribution Function.

COP Connection Outage Probability.

CRNs Cognitive Radio Networks.

CSI Channel-State Information.

CVN Cognitive Vehicular Network.

EC Ergodic Capacity.

EH Energy Harvesting.

GSC Generalized Selection Combining.

HPPP Homogeneous Poisson Point Process.

IVC Intervehicular Communication.

LOS Line-Of-Sight.

M2M Mobile-to-Mobile Communication.

MIMO Multiple-Input-Multiple-Output.

MRC Maximal-Ratio Combining.

NOMA Non-Orthogonal Multiple Access.

OP Outage Probability.

PDF Probability Density Function.

PLS Physical-Layer Security.

PS Power Splitting.

PU Primary User.

PUEA Primary User Emulation Attack.

RF Radio Frequency.

RFID Radio-Frequency Identification.

SIMO Single-Input-Multiple-Output.

SISO Single-Input-Single-Output.

SNR Signal-to-Noise Ratio.

SOP Secrecy Outage Probability.

SPSC Strictly of Positive Secrecy Capacity.

SU Secondary User.

SWIPT Simultaneous Wireless Information and Power Transfer.

TAS Transmit Antenna Selection.

TS Time Switching.

V2V Vehicle-to-Vehicle Communication.

WPCN Wireless Powered Communication Network.

WPT Wireless Power Transfer.

List of Symbols

η	Energy harvesting conversion efficiency coefficient
$\exp(.)$	Exponential function
$\Gamma(.)$	Gamma function
$\gamma(.,.)$	Upper incomplete gamma function
κ & μ	Main channel fading parameters
κ_e & μ_e	Wiretap channel fading parameters
λ_e	Density of users
$\lim$	Limits
$\ln$	Natural logarithm
$\log_2$	Logarithm with base 2
$G_{p\ q}^{m\ n}\left(\begin{smallmatrix} a_r \\ b_s \end{smallmatrix} \middle\vert z\right)$	Univariate Meijer G-function
ρ	Time switching factor
θ	Power splitting factor
C_s	Secrecy capacity
dB	Decibel
E	Expectation operator

$erfc(.)$ Complementary error function

I_{th} Interference threshold

n Main channel cascade level

n_e Wiretap channel cascade level

P_r^{nzc} Probability of non-zero secrecy capacity

P_{int} Intercept probability

PL Path loss exponent

$Res(f(x), s)$ The residue of function $f(x)$ at pole $x = p$

SOP Secrecy outage probability

Chapter 1

Introduction

1.1 Cognitive Radio Networks and Physical-Layer Security

The tremendous growth of the projected number of connections and services expected in 5G and beyond elevates the challenge of the frequency spectrum scarcity. Cognitive radio networks (CRNs) have been recognized to be a reputable approach to deal with certain concerns. In the context of CRNs, two types of users exist; primary users (PUs) and secondary users (SUs). Given the paradigm used for transmission by SUs, i.e., underlay, overlay, or interweave, the physical layer of the CRN may be threatened by attacks. For instance, when SUs adopt an underlay paradigm for communication, a continuous adaptation of the transmit power should occur to keep the interference caused to the primary network below a certain threshold. This poses a threat to SUs' secrecy due to the variations in the conditions of the channel [1]. Moreover, the broadcast nature of CRNs causes a threat on tapping the shared information.

Among the communication security techniques, physical-layer security (PLS) has emerged as a reliable method for improving security. This method improves the secrecy without relying on the encryption or decryption of messages. Moreover, Wyner proposed the three-node wiretap model, in which two channels should be addressed while examining a system's PLS; the main channel and the wiretap channel [2]. The main channel is the one between the transmitter (Tx) and the legitimate receiver (Rx), while the wiretap channel exists between Tx and the untrusted user, such as an eavesdropper. Given these definitions, PLS protects the transmissions by improving the main

channel's conditions or degrading the wiretap channel's conditions. Motivated by the reliability of PLS in securing networks, users in CRNs can apply PLS to secure the exchanged messages. On the other hand, protecting CRNs necessitates certain energy-consuming procedures. This adds another layer of complexity for the users of CRNs.

Energy harvesting (EH) is a significant breakthrough for green communication, allowing the network nodes to reap energy from multiple sources to lengthen battery life. The energy from various sources, such as solar, wind, vibration, and radio frequency (RF) signals, can be obtained through the process of EH. The process of EH converts the AC signals to DC signals (electricity) to power the devices. This accumulated energy can be stored to be used for various processes. Energy harvesting provides us with many promising advantages, such as self-sustainable capability, reduction of carbon emission, truly wireless nodes without requiring battery replacement, and easy and fast deployment in any toxic, hostile or inaccessible environment. EH was identified as a viable approach to the energy-constrained devices dilemma. One of the consequences of the information and the energy content of radio frequency (RF) signals is the simultaneous wireless information and power transfer (SWIPT) technology [3]. Furthermore, to enable the SWIPT technique effectively, on the receiving side, the receiver is designed to conduct either power splitting (PS) or time switching (TS) protocol to extract the energy from the received RF signal. In PS, the receiver partitions the energy of the RF signal into segments depending on a splitting factor; one portion of the power is used for energy harvesting, while the remaining is used for information processing [3]. However, the entire power is utilized in TS protocol and the time is split into two or more slots, one of which is spent on EH and the rest of its time is used to process the data, i.e., information decoding (ID) process. EH approach can be utilized to improve the PLS for CRN users, which has been an intriguing area of study. Given this, it is more accurate and practical to assume these users moving or surrounded by obstacles when investigating PLS for CRNs, which cannot be achieved assuming classical fading channels [4].

Cascaded fading channels have developed as an accurate method for modeling signals' propagation, especially when devices are moving or when a significant number of obstacles exist between the transmitter and receiver [5], such as cognitive vehicular networks. Cascaded channels assume that the received signal is generated by the multiplication of a large number of rays reflected from

the objects [6]. Moreover, cascaded channels are recognized to be effective in modeling various systems, such as multi-hop relaying systems and mobile-to-mobile/vehicle-to-vehicle (M2M/V2V) communication systems, to name a few [7].

1.2 Motivation

The primary objectives of this thesis are to:

- Investigate the challenges inherent in the implementation of cognitive radio networks (CRNs);
- Develop novel methodology and strategies for addressing physical-layer security (PLS) challenges associated with CRN-based vehicles (cognitive vehicular networks (CVNs)) while preserving energy-efficient devices;
- Establish analytical and simulation frameworks for the proposed methodologies.

While designing CRNs, it is critical to secure users' transmissions as CRNs are vulnerable to a variety of threats, particularly at the physical layer [8]. This is due to several reasons; *first*, attacks in CRN may occur during the three stages of the cognition process, namely spectrum sensing, spectrum analysis, and spectrum decision. Malicious users may attempt to attack the network during one or more of the three transitions. *Second*, SUs should distinguish legitimate PUs from malicious PUs. For instance, a malicious selfish SU attempts to mimic the PUs' transmissions' characteristics when the band is vacant to prohibit the other SUs from using the band. As a result, the secondary network misses the opportunity to use an availability in the spectrum, which can lead to throughput degradation. *Third*, SUs should pay attention to the accuracy of the sensed data as the attacks sometimes occur from legitimate SUs. In this case, a malicious user attempts to inject false sensed data into the fusion center (centralized sensing) to prevent it from correctly deciding the status of the bands. Moreover, threats on CRNs can be initiated from outside the network. In this case, users within the coverage range of transmission are able to overhear confidential information due to the broadcasting nature of the transmission. Furthermore, attackers may intend to send harmful signals (jamming) towards the SU or PU receiver to disturb their communication. Moreover, since SUs and PUs both reside on the same network, they need to be protected from different types of threats.

All the aforementioned reasons emphasize the importance of securing the physical layer of CRNs and physical-layer security (PLS) approach is suggested for similar concerns. However, protecting the SUs' networks against attacks involves following certain approaches that consume energy, such as cooperative jamming in addition to the energy-consuming operations that SUs already conduct. As a result, when securing the SUs' networks, the energy consumption issue should be taken into consideration.

Energy harvesting (EH) is a promising approach to prolong the lifetime of energy-constrained devices. Utilizing EH while attempting to secure the physical layer of CRNs is a challenge that should be tackled due to its role in saving energy. For instance, the energy can be harvested by the SU's transmitter from the PU transmission for the sake of improving the security of the SUs network for the underlay mode. For overlay CRN, the SUs may harvest energy that can be used to improve the PUs' network reliability and security. Moreover, energy can be harvested by the SU's receiver from the SU's transmitter or any other source to prolong its battery life. In addition, EH can be used to enhance network security by generating jamming signals to mislead the eavesdroppers. Improving PLS through EH in CRNs would result in a more secured network while achieving high spectrum and energy efficiencies. However, prior research with similar scenarios has assumed the nodes operate over classical channels. These channels neglect the fact that the nodes may be moving or surrounded by objects, resulting in a signals propagation modeling that is inaccurate.

Cascaded fading channels have been lately recognized to model signals' propagation sufficiently close to realistic scenarios. The notion of cascaded fading channels implies that the received signal at the destination is composed of a large number of signals reflected from obstacles blocking the path between a transmitter and a receiver, especially when these devices are moving or reside in rich scattering areas [5, 9]. Cognitive vehicular networks and mobile-to-mobile (M2M) communication have been lately an interesting issue to consider [10] and conventional fading channel models may not be appropriate for signals' propagation modeling in these networks. This is because using these models, it is assumed that the signal travels from the transmitter to the receiver without passing through multiple obstacles in the path. Due to the importance of the applications of cascaded channel models and their role in impacting the security of communications, it is necessary to utilize these models when studying and improving the PLS for CRNs. Particularly, while the nodes are moving

or in rich scattering areas.

1.3 Thesis Contribution

Motivated by open issues mentioned in the previous section. The contributions of this thesis are summarized as follows:

- We began our investigations by studying the link performance under the effect of cascaded $\kappa-\mu$ fading channels by performing the statistical analyses for this distribution. Moreover, using the approach of PLS, we studied the secrecy of several three-node wiretap system models, in which two legitimate devices are communicating under the threat of eavesdroppers. The first case was a three-node wiretap system model operating over cascaded $\kappa-\mu$ fading channel and under worst-case assumptions. Moreover, assuming cascaded $\kappa-\mu$ distributions for the main channel and the wiretap channel, we investigated the impact of these cascade levels, in addition to the impact of multiple antennas employed at the eavesdropper. Additionally, the PLS is explored and compared for two different scenarios for the manner the eavesdroppers tap the conveyed messages, which are colluding and non-colluding eavesdroppers.

- Considering an underlay CRN operating over cascaded Rayleigh fading channels with the presence of an eavesdropper, the PLS for the SUs was explored. This study is then extended to investigate the PLS of SUs in an underlay SIMO CRN over cascaded κ-μ general fading channels with the presence of a multi-antenna eavesdropper. The entire system model can be regarded as a SIMO underlay cognitive vehicular network operating over cascaded κ-μ fading channels. Both of the receivers, i.e., the SU receiver and the eavesdropper, utilize the maximal-ratio combining (MRC) technique. The impact of the constraint on the transmission power of the SU transmitter due to the underlay access mode was investigated. Additionally, the effect of the number of antennas at the receivers, the cascade level, and the fading channel parameters are assessed.

- To enhance user security in CRNs while also increasing energy efficiency, we presented an underlay CRN in which an SU transmitter communicates with an SU destination via a cascaded

κ-μ channel in the presence of a PU receiver. An eavesdropper threatens the confidentiality of information communicated between SUs. We consider that the SU destination harvests energy from the SU transmitter to generate jamming signals designed to deceive the eavesdropper. In this scenario, an energy-harvesting eavesdropper is compared to a non-energy-harvesting eavesdropper. This scenario is then updated to include an external cooperative jammer that harvests energy to provide additional security. The links are supposed to be subjected to a cascaded Rayleigh model. Two scenarios for the eavesdroppers' tapping capabilities are provided and compared in this system model: colluding and non-colluding eavesdroppers. These analyses are then extended to include non-cooperative and randomly distributed eavesdroppers functioning over cascaded κ-μ channels.

- Finally, we analyzed the reliability of SUs and PUs accessing licensed bands via the overlay mode, while maximizing energy efficiency through the EH approach. We suppose that several SUs are dispersed randomly and that one of the SUs is selected based on the Euclidean distance. By utilizing the time switching protocol, the selected SU gathers energy from the PUs' messages. Then, using the accumulated energy, this SU combines its own signals with those of the amplified PUs' and forwards them to their destinations. The reliability of SUs and PUs networks is evaluated in terms of outage probability. Additionally, we designed two optimization problems that maximize the time switching and power allocation variables. These problems' principal objective is to maximize the rate of users' links.

1.4 Thesis Organization

The rest of the thesis is organized as follows:

In Chapter 2, a background regarding the main topics of this thesis is given. An overview of cognitive radio networks (CRNs), as well as the primary challenges that users of similar networks experience are provided. Then, certain attacks on the physical layer of CRNs are surveyed with possible countermeasures that have been considered in the literature to combat them. We then direct our attention to the security challenge, presenting the physical-layer security (PLS) approach for resolving it. An overview of PLS along with a list of the important security metrics that will

be evaluated in this thesis are presented. We review the primary benefits of energy harvesting (EH) systems, the various types of EH transmitters and receivers, and energy harvesting management schemes. Finally, an overview of cascaded fading channels and their applications are included. By the end of Chapter 2, a literature review related to the research area is given.

In Chapter 3, we show the statistical analysis of cascaded κ-μ fading channels. Then, we assess the security of three different system models operating over these cascaded channels with multiple eavesdroppers via PLS. In the first scenario, worst-case assumptions ate assumed. In the second system model, it is assumed that both links follow the cascade model. In addition, in the third system model, two scenarios are explored and compared; colluding and non-colluding eavesdroppers. We show clearly the impact of cascade level on security besides other system parameters. Additionally, in this chapter, a general SIMO CRN is given over cascaded κ-μ channels and with receivers configured with multiple antennas. Then, we present a special case of the previous general system model for an underlay CRN operating over cascaded Rayleigh channel and we use the PLS approach to investigate the security level of the exchanged messages. Each scenario concludes with the presentation of analytical and simulation results, as well as an explicit discussion of these results.

In Chapter 4, for three underlying CRNs scenarios, energy harvesting is proposed to improve security and energy efficiency. In the first scenario, under the impact of the cascaded κ-μ model, the legitimate receiver is presumed to harvest energy to be utilized to broadcast jamming signals to improve security. In the second scenario, it is presumed that energy is being harvested by an external collaborating jammer and then used to ensure security. To demonstrate which scenario poses the greatest threat to the confidentiality of the shared information, we present two possible scenarios for how eavesdroppers can overhear and capture the messages over cascaded Rayleigh model. Finally, this case is extended to include multiple eavesdroppers operating over cascaded κ-μ model. Following the conclusion of each system model, the results and related discussions are provided.

In Chapter 5, we propose an overlay CRN with multiple randomly distributed SUs. One of these SUs is selected based on the k^{th} closest user to the primary user. Using the time switching mechanism, this selected SU gathers energy and uses it to amplify and convey the messages. Two

optimization problems with the potential to maximize the users' link rate are addressed in this chapter. The results and their discussions are also provided in the chapter.

Finally, in Chapter 6, we present our thesis's conclusions, along with a few suggestions for further future investigations.

Chapter 2

Background and Literature Review

2.1 Introduction

This chapter provides a brief background to the thesis's primary subjects, as well as a review of recent literature in the field of study. An overview of cognitive radio networks (CRNs) is provided. Additionally, the major issues facing CRNs are discussed, with an emphasis on the security challenge, with specific reference to physical layer potential threats. Additionally, a description of physical-layer security (PLS) is included. Furthermore, we present a review of energy harvesting techniques, their benefits, transmission and reception schemes, and energy harvesting management systems. Finally, we define cascaded fading channels and discuss their applications.

2.2 Cognitive Radio Networks (CRNs)

Cognitive radio networks (CRNs) have been proposed as a promising approach to tackle the problem of scarcity and the misuse of the allocated radio spectrum. This is because the radio spectrum is regulated by a fixed policy for spectrum assignment by the federal communications commission (FCC). As the number of devices and connections increases with 5G communications and beyond, the need for CRNs is on the rise [11]. In the context of CRNs, there are two types of users, namely secondary users (also called cognitive users) and primary users (called licensed

users). There are three different access modes under CR; overlay, underlay, and interweave. Secondary users (SUs) operating under the overlay model cooperate with the primary users (PUs) in return for certain advantages. For example, SUs can relay the PUs' transmissions in order to have the opportunity to use the licensed band. In underlay CR networks, the SUs access the radio spectrum concurrently with the PUs provided that the SUs' transmit power does not impair the PU's transmission. In this case, SUs must adapt their transmitting power in order not to exceed the interference level that the PU receiver can tolerate. Finally, SUs in an interweave CR network are permitted to utilize the PUs' bands only if they are vacant. In this case, SUs start sensing the licensed bands in order to find available spectrum holes by gathering radio environment variables. Moreover, SUs collect information about the characteristics of these bands. There are several techniques for spectrum sensing that SUs can utilize, such as energy detection, wave-form based sensing, cyclostationarity-based sensing, and matched filter-based sensing.

The cognitive radio cycle consists of three main transitions; spectrum sensing, spectrum analysis, and spectrum decision. Spectrum sensing is an important stage since the following stages are dependent on the accuracy and reliability of the sensing information. The SUs should keep monitoring the environment to be aware of the sudden reappearance of the PU. Spectrum analysis is the step where the SU starts analyzing the gathered information during the spectrum sensing. Through this step, a characterization of the spectrum bands is performed in order to match the appropriate available bands to the requirements of the users. The main bands' characteristics estimated at this transition are the signal-to-noise ratio (SNR), error rate, path loss, holding time, and interference. Finally, spectrum decision is executed to decide on which of the bands the SU will use according to the band's characteristics and the user's requirements. After deciding which band to use, the SU decides its transmission parameters, such as the type of modulation and data rate.

Spectrum sensing is performed over the band of frequencies by measuring the energy content of the band to find a transmission opportunity in a particular time or in a particular area. However, there are other dimensions that may be exploited for transmission opportunities. These main dimensions are [12]:

- Frequency: For a given period of time, the frequency dimension is monitored. This is because not all frequency bands are used at the same time. Hence, there may be a transmission

opportunity in the frequency domain to be used.

- Time: Since a band of frequencies will not be used all the time, observing a specific band of frequencies over the time may bring a transmission opportunity over this band in time.

- Geographical space: CR users can measure the path loss of the received PU's signal at their receivers. This is to use the path loss measurements to decide whether there is a transmission on the monitored geographical space or not at a specific band and time. This is because there may be a chance that the area will not be occupied by PUs for the whole fixed time and band. Moreover, SUs can use the same band at the same time with the PUs while making a physical separation between them and the PUs.

- Code: If the SU has information about the code used by the PU, SU can transmit over the same time and band, but using an orthogonal code to the code used by the PU. In addition, PU may use one of the spread spectrum (SS) techniques, where the PU spreads the signal's energy over the band. In similar cases, if the SU has the knowledge about the spreading code used by the PU, the SU can transmit over the same band without interfering with the PU. However, it is not straightforward to know the codes used by the PU.

- Angle: SU needs to know the location or the direction of the PU's antenna's beam. Given this knowledge, SU can transmit in other directions to avoid interfering with the PU. In addition, with the advances in the beamforming technology, many users can use the same band at the same time and on the same geographical area, without interfering with each other.

2.2.1 Challenges

Cognitive radio technology faces different challenges that are worth to be mentioned. The main challenges include the following:

- **Hardware Requirements**

  Sensing may be performed using two different architectures; single radio and dual radio. In single radio, only one RF chain performs sensing and communication but not at the same time. A small period of the dedicated time is reserved for sensing, while the rest of the period is

reserved for communication. Single radio architecture has simple implementation complexity, but it has low spectrum efficiency. This is because the transmission cannot be performed during the whole period of time. Moreover, sensing is not guaranteed to be always accurate. This is because sensing is not performed during transmission. On the other hand, in dual radio, two RF chains are used, one is used for sensing and one is used for communication. Dual radio has more implementation complexity than single radio with a higher implementation cost. However, dual radio is more spectrum efficient and makes the process of sensing more accurate. This is because sensing is performed all the time. Hence, SU should consider these challenges with both architectures [13].

- **Hidden Primary User Problem**

  In some scenarios, during spectrum sensing, the PU may be behind an obstacle (shadowing) (see Figure 2.1) [13]. In other scenarios, the received primary signals may pass through a fading channel. These factors cause large fluctuations in the power of the received primary signals at the SU's receiver. Moreover, these fluctuations can vary over time due to changing distances between PU's transmitter and SU's receiver. In similar conditions, SU will not be able to sense the PU's signal transmission. In this case, SU will assume that the band is available and starts the transmission in the range of the PU's transmission. This issue could be handled using cooperative sensing.

- **Detecting Spread Spectrum Primary Users**

  Primary users may use spread spectrum (SS) techniques, such as frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS). In the case of using FHSS, the PU keeps hopping between different operational frequencies over narrow bands. This is performed according to a sequence known between the transmitter and the receiver. The problem may be avoided if the pattern of the PU's hopping is known at the SU, and a perfect synchronization and timing for the PU's signal are achieved. In DSSS, PU spreads the signal's energy over a single band without changing the band of operation [13]. Hence, using SS techniques produces new challenges for the SU to consider to detect a PU.

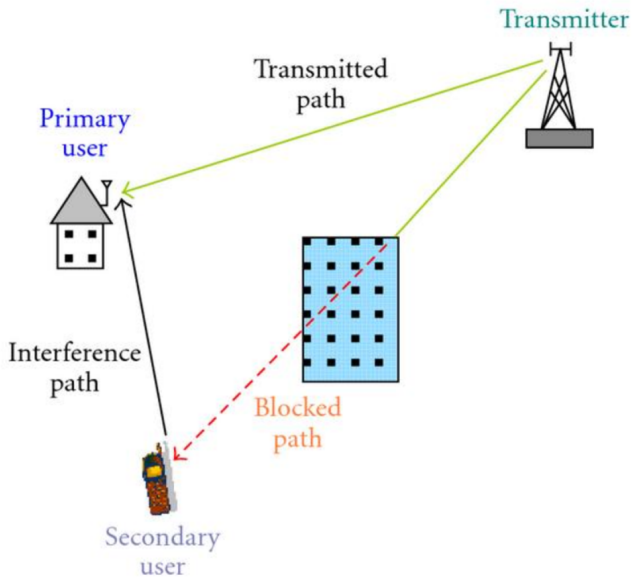

Figure 2.1: Hidden primary user problem.

- **Sensing Duration and Frequency**

  Sensing duration and sensing frequency are two important design parameters that have to be chosen carefully. Sensing duration is the period of time that the SU spends to detect a PU. SU should keep sensing the band even during transmission. This is because if a PU attempts to reuse the band, SU should vacate as quickly as possible (spectrum mobility). This produces a new challenge associated with the CRN because PU has the higher priority to use the band. However, if the SU does not have the ability to sense during transmission (single radio), there has to be a trade-off between the sensing duration and the reliability of sensing. As the sensing duration increases, the accuracy of sensing increases. However, the duration of transmission will be reduced, which decreases the transmission efficiency of the SUs. Sensing duration can affect both the SU and PU. Therefore, it has to be chosen carefully to make the communication of the SU reliable, while avoiding interference to the PU's. Sensing frequency reflects how often the SU should sense the bands. Sensing frequency has to be chosen based on the status of the bands occupied by PUs. If the status changes slowly, sensing frequency requirements may be relaxed. Moreover, interference tolerance over the PU's channels is an important

factor to be considered by SUs. If the SU is sensing a band that is reserved for public safety issues, sensing frequency has to be high, it should happen as frequently as possible.

- **Decision Fusion in Cooperative Sensing**

  Decision fusion is the process that has to be performed after the spectrum sensing process. In cooperative sensing, decision fusion is the process of combining the sensing information from the SUs to a central unit (centralized sensing). Decision fusion defines the way each user combine the information form the neighboring users (distributed sensing). CR users share their sensing information using soft or hard decisions. In soft decision, SUs send the sensing information of the observed band to a central unit. On the other hand, in hard decision, each SU determines the availability of a band and sends the result about the status of the band to a central unit. Spectrum sensing using soft decision is usually more accurate than hard decision because there may be a hidden terminal problem facing one or more of the secondary users. Hence, making a final decision from their behalf could lead to producing interference to the PU. This poses a new challenge to be considered for the CRN. On the other hand, sensing using hard decision requires less information to be exchanged among users [14]. Using hard decision for spectrum sensing, the process of combining the sensing information from users can be performed using logic operations, such as AND, OR, or M-out-of-N. In "AND" combining method, sensing results from all users should be H1 (the band is occupied by PU) for the SU to decide that it is really occupied by a PU (H1). In "OR" method, SU decides on H1 if any of the received decisions plus his own decision of the sensed band are H1. For "M-out-of-N" method, SU decides on H1 if the received number of decisions of H1 is equal to or larger than a pre-specified number M.

- **Security**

  Different types of attacks against CRNs may be performed either for selfish use or to produce harm to the CRNs. Passive attack is a major type of attacks, such as eavesdropping. Eaves-

droppers try to overhear the confidential information between SUs without causing harm. This makes it necessary for the CRN to consider some countermeasures against these threats. Specifically, the physical layer of the CRNs is susceptible to several attacks. In the following section, we mention some of the main attacks with certain countermeasures that have been considered in literature to combat them.

2.3 Cognitive Radio Networks and Physical-Layer Attacks

The main threats on the physical layer of CRNs are depicted in Figure 2.2. In the next subsections, we mention briefly these attacks.

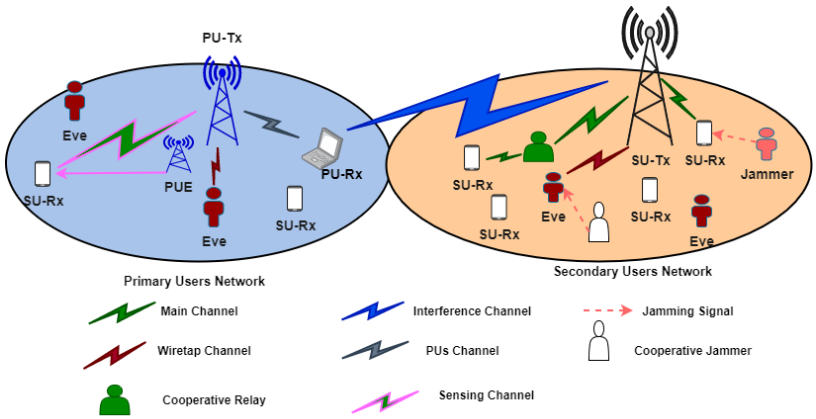

Figure 2.2: Physical-layer security implementation in cognitive radio network with different types of attacks.

2.3.1 Primary User Emulation Attack

Primary user emulation attack (PUEA) occurs when an SU emulates a PU, which is called a primary user emulator (PUE). This attack occurs in the spectrum sensing stage and is performed by sending a signal that has the same characteristics as the PU's signal over the licensed band when the PUs are absent. In this case, the attacker attempts to mimic the PUs characteristics. Hence, the opportunity of using the band will be missed. One of the methods used to defend against PUEA is through the transmitter verification scheme [15]. In this scheme, a PU signal is verified through checking the location of the transmitter through the received signal characteristics, such as its energy

level. Furthermore, there is a different method used to combat the PUEA, which is based on the power of transmission of the SUs in the network. The SUs send their observations regarding the licensed bands to a fusion center, which would keep track of the power levels of these SUs in order to detect a malicious user. A malicious user is recognized when an unordinary power level is observed. Then, the fusion center would notify the other SUs.

2.3.2 Sensing Falsification

In sensing falsification attack, the attackers attempt to make a change in the sensing information by injecting different and false sensing results either to the neighboring secondary users (distributed sensing) or to a fusion center (centralized sensing). This is to change the decisions about the available bands in order to disturb the SUs' transmissions, which leads to an increase in the probability of false alarm. In fact, users injecting these false data are usually a small fraction of the total number of nodes. To defend against this threat for the case of centralized sensing, a majority vote at the fusion center regarding the final decision about the bands' status can be considered. On the other hand, in the case of non-centralized cooperative sensing, every SU can come up with a final decision on the bands' status by using its own decision along with the surrounding SUs' decisions and applying the majority rule [16].

2.3.3 Jamming

Once the SU determines which of the bands to use, the transmission begins. In this stage, the CRN may be exposed to jamming. A jammer is a node which emits an interfering signal (very high power signal transmitted on the same band) to disrupt the communication between the SUs. The jammer may send jamming signals over a single or multiple bands. In order to combat this threat, an SU receiver needs to recognize the jamming attack by measuring the received signal strength, which in this case should presumably be high. Once the SU receiver detects the attack, one of the spread spectrum techniques can be utilized, such as frequency hopping. In this case, when the SU distinguishes a jamming threat, an immediate switch to other unjammed bands takes place.

2.3.4 Eavesdropping

During an SU's broadcast transmission, users within the coverage area of the SU's transmitter will be able to overhear or eavesdrop the confidential information. Eavesdroppers are classified into two types; passive and active. In the former, the eavesdropper attempts to overhear the confidential information silently. In this case, eavesdroppers do not send any harmful signals. Instead, they attempt to intercept the confidential information between SUs or PUs. Thus, it is hard for the transmitter to recognize the channel state information (CSI) of the link between the transmitter and the eavesdropper. However, in the latter, a legitimate user of the network who is not trusted is considered an active eavesdropper. Indeed, considering passive eavesdropping in the network is more common and practical than active eavesdropping.

2.4 Physical-Layer Security (PLS)

2.4.1 Notion of Physical-Layer Security (PLS)

Up until now, the methods used to enhance the secrecy of networks have been heavily dependent on the cryptography approach implemented in the upper layers of the network. However, security methods based on encryption approaches have several drawbacks, especially for 5G communications [17]. For instance, the added software and hardware complexity of these approaches to the network since high processing power is needed. In addition, the heterogeneous networks used in 5G make the process of exchanging the secret keys very difficult. This is because encryption is usually done with powerful algorithms that presume that the receiver of the eavesdropper is computationally constrained. Nevertheless, recent improvements have been made in devices' computing power to break encryption codes. Hence, certain measures are necessary to improve the security of communication systems. Therefore, physical-layer security (PLS) has become a very interesting approach to investigate and improve the safety of the sharing of confidential information between legitimate ends in 5G. As PLS does not depend on encryption and decryption techniques, there is no need for the exchange of security keys. PLS was first addressed by Shannon and further explored later by Wyner and it clearly shows that security of the data is guaranteed if the channel between legitimate

users has better conditions than the channel exists between the transmitter and the attackers [2], [18].

2.4.2 Wiretap Channel

The three-node wiretap communication system is depicted in Figure 2.3. In order to study the PLS of a system, we should consider two different channels; the main channel and the wiretap channel. The main channel is the one between the transmitter (Tx) and the legitimate receiver (Rx), while the wiretap channel exists between Tx and the eavesdropper (Eve).

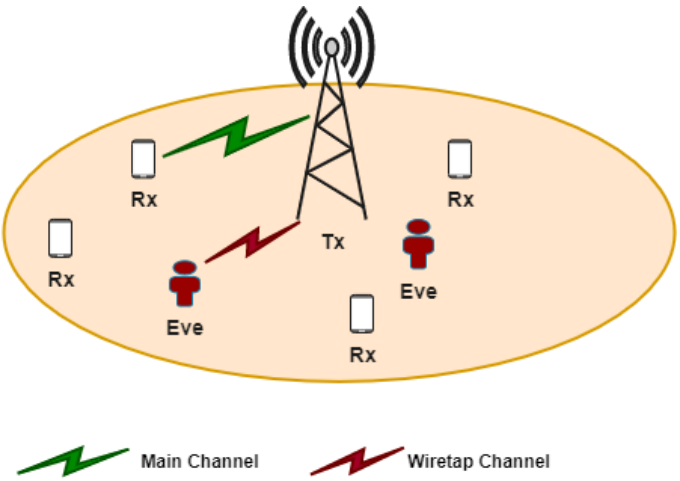

Figure 2.3: Three-node wiretap channel.

2.4.3 Physical-Layer Security Metrics

In this section, the main secrecy metrics used in this thesis are defined.

- **Secrecy Outage Probability**

  Eavesdroppers seeking to overhear the confidential information silently (passive eavesdroppers) make it difficult to recognize the channel-state information (CSI) of the wiretap channel. Hence, CSI is usually not available at the transmitter and thereby it transmits on a constant rate (C_{th}). A leakage of the confidential information through the wiretap link is possible and the most effective way to assess the level of secrecy of the system model is through the secrecy outage probability (SOP). SOP is defined as the probability that the secrecy capacity

falls below a given threshold (C_{th}) as

$$SOP \quad = \quad P_r\left(C_s < C_{th}\right), \tag{2.1}$$

where C_s is the secrecy capacity and C_{th} is the threshold secrecy rate. For the system model considered in Figure 2.3, the secrecy capacity is defined as [19]

$$C_s = \begin{cases} C_M - C_E, & \text{if } \gamma_M > \gamma_E \\ 0, & \text{if } \gamma_M \leq \gamma_E \end{cases}, \tag{2.2}$$

where C_M is the capacity of the main channel and C_E is the capacity of the wiretap channel. γ_M and γ_E are the received SNRs at the legitimate and the eavesdropper receivers for the three-node wiretap model, respectively.

- **Probability of Non-Zero Secrecy Capacity**

  The probability of non-zero secrecy capacity (P_r^{nzc}) is defined as the probability that the secrecy capacity is positive. In other words, it is the probability that the capacity of the main channel is larger than the capacity of the wiretap channel. This event occurs when the conditions of the main channel are better than those for the wiretap channel in terms of the received SNRs,

$$P_r^{nzc} = P_r\left(C_s > 0\right) = P_r\left(\gamma_M > \gamma_E\right) \cdot \tag{2.3}$$

2.5 Physical-Layer Security in Cognitive Radio Networks

Given the paradigm used for transmission by SUs, i.e., underlay, overlay, or interweave, the physical layer of the CRN may be threatened by attacks. For example, when SUs adopt an underlay paradigm for communication, a continuous adaptation of the transmit power should occur to keep

the interference caused to the primary network below a certain threshold. Since the capacities of the main and the wiretap channels can both be affected by this variation, the conditions of these channels are also impacted. This indicates that the received SNRs obtained at both ends are influenced and thus the confidentiality of the transmission will be impacted as well. For example, given that the wiretap channel's conditions are constant while the average received SNR at the legitimate receiver is the one that varies, lowering the transmit power due to the underlay mode would degrade the PLS for the users. Moreover, the cooperation between the SUs and PUs networks is carried out when the overlay mode is employed. In the case where a secondary malicious node exists, the PU transmission could be jeopardized, as the SU network could be untrusted to assist the PU with its transmissions. Hence, PLS is suggested to be applied by users in CRNs to safeguard their transmissions.

Apart from other non-cognitive networks, it is found more complex to apply PLS to CRNs. This is due to several reasons; *first*, attacks and threats over one network, i.e., SUs' or PUs' network, can impact the communication of both networks. *Second*, indoor or outdoor network attacks can occur. Hence, an additional challenge is posed on the SU node to be able to differentiate between legitimate users and malicious nodes. *Third*, attacks could occur during the three states of the cognition cycle. For instance, the sensing process could be an open platform for attacks. When assuming cooperative sensing, an appearance of a single malicious user can corrupt the sensed data and damage the communication for the other SUs. This will also negatively impact the quality of the PUs' communication. *Finally*, comparing the attacks for CRNs with non-cognitive networks, there are specific types that are unique to CRNs and thus requiring different countermeasures and procedures to combat them, such as the ones mentioned in section 2.3. This results in an additional complexity compared to non-cognitive networks. Nevertheless, protecting the SUs' networks from attacks requires employing energy-intensive techniques such as cooperative jamming in addition to the energy-consuming operations that SUs already perform. As a result, when protecting the SUs' networks, consideration should be given to energy consumption. Energy harvesting (EH) is one step towards green communication and is useful in addressing the issue of energy consumption, particularly for energy-constrained devices. The following section will provide an overview of EH.

2.6 Energy Harvesting (EH)

Energy harvesting (EH) is a key advancement in green communication that enables network nodes to gather energy to extend the battery life. Through the process of EH, energy can be extracted from a variety of sources, including solar, wind, vibration, and radio frequency (RF) waves. EH converts alternating current (AC) to direct current (DC) in order to power devices. This stored energy can be used for a variety of purposes, such as improving the energy efficiency and the security level of the confidential information for CRN's users. In this section, the main advantages of EH are listed along with the two main categories of RF-EH sources. Additionally, the EH transmit and receiving schemes are included. The receiver architecture and the main power management schemes in EH are also presented.

2.6.1 Energy Harvesting Advantages

Energy harvesting provides us with many promising advantages, including:

- Self-sustainable capability.
- Reduction of carbon emission.
- Truly wireless nodes without requiring battery replacement.
- Easy and fast deployment in any toxic, hostile or inaccessible environments.

2.6.2 Types of Radio Frequency (RF)-EH Sources

Radio frequency (RF)-EH has attracted attention as no additional expenses are required since the signal carrying the information also carries power. The sources of RF-EH can be classified into two main categories; dedicated sources and ambient sources:

- Dedicated energy transmitters, such as powercast. These sources are intended to enable the end-devices to harvest energy and charge their batteries. Only power is transmitted here to guarantee that the network's lifetime is adequate to achieve the necessary quality of service (QoS).

- Ambient RF sources refer to the sources that are not intended to charge the end devices but using certain methods, energy can be derived from these signals. Examples for the ambient sources include TV broadcasting, radio broadcasting, and mobile base stations.

  Since the ambient sources can be impacted by location, weather, and time, dedicated RF sources are more reliable. That is, these dedicated sources are presented under the request of nodes in the network to prolong the lifetime of nodes and ensure that QoS is achieved.

2.6.3 Energy Harvesting Transmit Schemes

On the transmitting side, there are three main types of EH-transmitters as shown in Figure 2.4 and explained below:

- Wireless power transfer (WPT): in WPT, a transmission power station designed to transfer power for charging devices is available. An example of WPT can be found in [20], in which there is an access point (AP) in a clustered wireless sensor networks (WSN) with the potential of emitting power for all the nodes in the network (sensors and cluster heads) to be used as a supply of EH. This harvested energy is stored and used for the purpose of sensing, processing the sensed data, and for communication.

- Simultaneous wireless information and power transfer (SWIPT): SWIPT is regarded as a viable energy scarcity solution as it is based on the premise that energy and information compose the RF signal. In this case, two nodes exchanging information can also harvest energy from the received RF signal. The key benefit of this type is that opposed to the WPT, no added infrastructure or expenses are required. To be able to successfully benefit from this scheme of transmitters, the receiver should be designed with an energy harvester circuit to carry out either time switching (TS), power splitting (PS), or antenna selection (AS) which will be presented in this thesis.

- Wireless powered communication network (WPCN): Two time slots are necessary for the entire procedure of WPCN. In the first slot, a power signal is transmitted by the transmitter, which is used as a supply of energy at the receiver. The receiver harvests the energy and stores it in its storage device to be used for its own transmissions in the uplink in the next time slot.

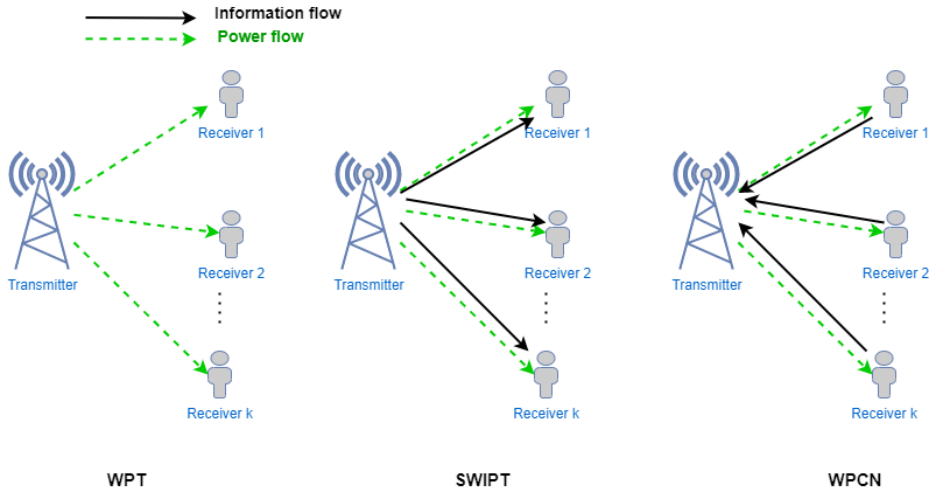

Figure 2.4: EH transmit schemes

2.6.4 Energy Harvesting Receivers

On the receiving side, two types of energy harvesting receivers exist. These receivers are categorized as:

- Ideal receivers: in ideal receivers, the receiver is considered to be able to use the same circuit to extract the energy from the received RF signal . Additionally, the receiver is expected to be able to concurrently execute EH and information decoding (ID). Nevertheless, due to the constraints in the hardware architecture of the receiver, this is not practical. However, it is treated in some previous studies as an upper limit for the system performance [21].

- Co-located receivers: the receiver should be adapted to satisfy the SWIPT specifications to allow the receiver to profit from this transmission scheme. This can be accomplished when a receiver utilizes one of the following schemes: power splitting (PS), time switching (TS), or antenna selection (AS).

  Figure 2.5 shows the three schemes of co-located RF-EH receivers. For the PS protocol, the receiver divides the power of the received signal into two parts based on a power splitting factor (θ). A portion of the power will be used for EH and it will be stored in one of the device's storage units, such as a battery or a capacitor. The remaining of the power is spent on ID. In TS, the entire power is utilized and the time is split into two or more slots, one of which

is spent on EH and the rest of its time is used to process the data, i.e., ID. The switching is based on a time switching factor (ρ). Finally, a collection of antennas is mounted in the AS scheme, a few of which are used for EH, and the others are used for ID.

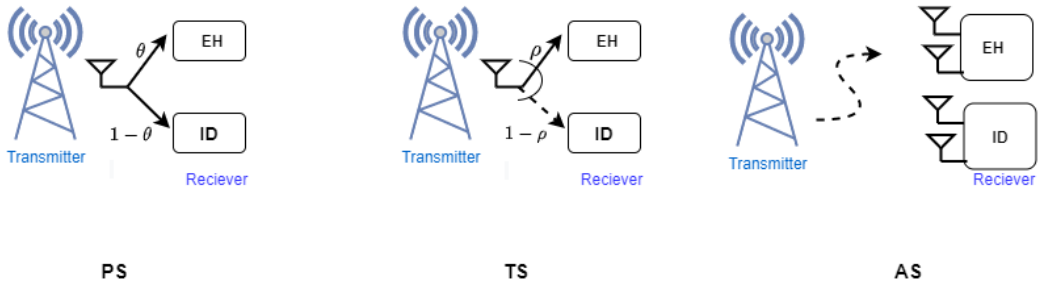

Figure 2.5: EH receiver schemes

2.6.5 SWIPT-EH Receiver Architecture

On the receiving side, the structure of the receiver should be designed as shown in Figure 2.6 to be compatible with the SWIPT scheme. For TS and PS, the receiver has one receiving antenna that is connected to two independent circuits. One of the circuits is used for EH and the other one for ID. The main components of the EH circuit are:

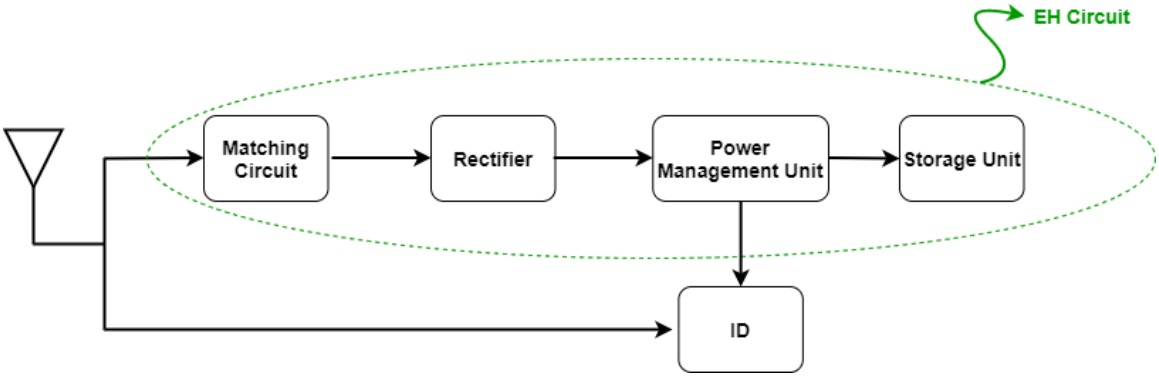

Figure 2.6: EH receiver structure

- The receiving antenna: the antenna is designed to work on a single or multiple bands of frequencies. This corresponds to the fact that the EH receiver is able to harvest energy from a single or multiple bands of frequencies. It is noteworthy that with increasing the antenna gain, the efficiency of the receiver improves.

- The matching circuit: it is a resonator circuit aimed to boost the power transmitted to the rectifier circuit and to reduce the lost power. When the impedance matching occurs between the loads and the antenna output in the circuit, the maximum power can be reached.

- Rectifier: the rectifier circuit's main component is the diode which has the function of converting the RF signal, i.e., AC signal into DC signal. The lower the built-in voltage in the diode, the higher the circuit's efficiency. The other component of the rectifier is the capacitor, which ensures that the power drawn to the load is delivered smoothly.

- Power management unit: this is an essential unit as it handles several functions in the receiver. For instance, this unit determines whether the accumulated energy must be stored or utilized for the node's processing immediately. Moreover, the power management unit shall determine the amount of power that the various sections of the receiver consumes. That is to guarantee a long lifetime while retaining the appropriate QoS required level.

2.6.6 Energy Harvesting Management Schemes

In EH networks, there are three types of power management schemes:

- Harvest-use (HU): for the HU scheme, the harvested energy is not stored and it will be immediately consumed by the node. This scheme is principally limited by ensuring that the amount of energy that is extracted is greater than the energy consumed.

- Harvest-store-use (HSU): in this scheme, the harvested energy is initially stored in one of the storage devices, such as a rechargeable battery or a capacitor. Then, the node will use the accumulated energy for various tasks over the next period. The major concern with this scheme is that the charging phase creates a loss of energy. This amount differs based on the type of the storage device.

- Harvest-use-store (HUS): in HUS, temporary preservation of the accumulated energy in a storage unit occurs to be used immediately by the node. Then, the excess of the energy will be stored in another storage device to be consumed later. The key limitation of this form is that for the procedure to be performed successfully two storage devices are involved.

2.7 Cascaded Fading Channels

For practical modeling of signals propagation and an accurate evaluation of communication security between moving nodes in CRNs, cascaded channels should be utilized. Classical fading channels, such as Rician, Rayleigh, and Nakagami-m fading channels do not consider the scattering in the area between the transmitter and the receiver, which has a considerable effect on the system performance and security. Consequently, cascaded fading channels have recently been considered an accurate modeling form of these channels. [22], [23]. Cascaded fading channels are also referred to as multiplicative channels since the received signal is generated by the multiplication of a large number of rays reflected from the scatters. These signals are considered to be independent but not necessarily identically distributed [23].

2.7.1 Applications of Cascaded Fading Channels

Cascaded fading channels are used to model the propagation of RF signals in different types of communication systems, such as, mobile-to-mobile/vehicle-to-vehicle (M2M/V2V) transmission channels [22], [24, 25, 26], radio-frequency identification (RFID) pinhole channels [27], [28], multi-hop relaying systems [26], [18], [29], and multiple-input-multiple-output (MIMO) keyhole communication systems [23], [30]. In multi-hop relaying systems, the entire system can be modeled using cascaded fading channels model, where the signal from the transmitter to the receiver is transmitted from one relay to another, which works as a non-regenerative node. In addition, for the propagation in the presence of keyholes, the signal from the transmitter to the receiver moves through small keyholes among obstacles, where each keyhole acts as a new source to the next one [30]. For instance, some research has shown that cascaded Rayleigh fading channels are suitable for modeling the intervehicular communication (IVC) channels [28]. Double Rayleigh fading channels have been used to model the keyhole channel model for MIMO communication systems [30], [31], [32], M2M communication systems, and vehicular communications [24], [33], [34]. Furthermore, N$*$Nakagami-m fading channels were utilized to model the links for V2V communications [24], [34].

2.8 Fading Channels

General fading distributions, such as $\alpha - \mu$, $\eta - \mu$, and $\kappa - \mu$ fading distributions are necessary for more accurate channel modeling [35]. General fading channels have been verified via field measurement campaigns to better fit the experimental data compared to other known distributions, such as Rician and Nakagami-m [35]. κ-μ general fading model is used to present the small-scale variation of the signal under the line-of-sight (LOS) condition (there is a LOS component). The $\kappa - \mu$ distribution models the signal as it is composed of clusters of multi-path waves. κ-μ fading channel is known for its flexibility as it includes some of the well-known classical channels as special cases by adjusting the values of the parameters κ and μ, such as Rician ($\mu = 1$ and κ = LOS component in the Rician channel), Rayleigh ($\kappa = 0, \mu = 1$), Nakagami-m ($\kappa = 0, \mu = m$), and the one-sided Gaussian ($\kappa = 0, \mu = 0.5$) distributions [35].

2.9 Literature Review

In this section, we present several previous investigations regarding the considered research. In [36], the PDF and CDF of the multiplication of a large number of Nakagami-m random variables are derived along with the link performance metrics, such as the outage probability (OP) and the average bit error probability (ABEP). The PDF and CDF of cascaded generalised-K fading channels were derived in [30]. The average symbol error probability (ASEP) and the ergodic capacity (EC) were derived as well. Cascaded Rayleigh fading channels were analyzed in [37]. Cascaded Rician fading channels along with the performance metrics including the ABEP, the OP, and the average channel capacity (ACC) were presented in [6]. One of the general fading models, which is the $\alpha - \mu$ fading channel has been considered in the cascaded fading channel, where the PDF and the CDF of the cascaded $\alpha - \mu$ fading channel envelope were derived [38]. Moreover, in [39], the PDF, CDF, and the statistics of the signal-to-noise-ratio (SNR) at the input of the receiver were derived for cascaded $\alpha - \mu$ channels. In [40], the PDF and the CDF of cascaded Fisher-Snedecor $\mathcal{F}$ fading channels were derived. Moreover, link performance was studied in terms of the channel quality estimation index, the OP, and the ABEP.

Recently, attention has been drawn to the work on physical-layer security (PLS) for communication systems. Some works have focused on a single-input-single-output (SISO) systems to study secrecy using the classical fading channels. For instance, in [41], for a network consisting of a transmitter, a receiver, and a single eavesdropper, the probability of a strictly positive secrecy capacity (SPSC) was studied over the Rician fading channels. The same analyses were carried out for the Weibull fading channel in [42]. SOP and SPSC were derived in [43] for a three-node wiretap system model operating over Generalized Gamma fading channels. SPSC was derived in [44] for a three node-wiretap system operating over log-normal fading channels. Secrecy over SISO systems assuming general fading distributions was studied as well. In [45], the α-μ general fading channels are used for a three-node wiretap system, where active eavesdropping exists. Average secrecy capacity (ASC) is evaluated to test the secrecy of the system. Moreover, the performance evaluation of the system's secrecy over $\alpha - \mu$ fading channel in [46] and over α-κ-μ and α-η-μ generalized fading channels in [47] was investigated in terms of SOP. Single-input-multiple-output (SIMO) system models were also of great interest to study the PLS for classical and general fading channels. For example, in [48] secrecy was studied for a SIMO system operating over the general κ-μ fading channel in terms of SOP and SPSC. For the same general κ-μ fading channel, secrecy was studied in [49] and also in [50] for correlated κ-μ shadowed fading channels in terms of the SOP and the SPSC. PLS was also studied for MIMO systems using different diversity techniques. In [51], secrecy has been studied for a three-node MIMO wiretap system over α-μ fading channels, where the transmitter employs transmit antenna selection (TAS) technique. A single antenna is selected to send the information to a multi-antenna receiver in the presence of a passive multi-antenna eavesdropper. Both of the receivers (the legitimate receiver and the eavesdropper) employ maximal-ratio combining (MRC) technique to enhance the receiver SNR. Hence, a worst-case scenario is assumed in this work. The secrecy was studied in terms of the SOP and SPSC. For the same fading channel, in [52] stochastic geometry was used to study the secrecy for a MIMO system, where both the legitimate receivers and eavesdroppers are distributed with two independent homogeneous Poisson point processes. In this work, the eavesdroppers are assumed to be non-colluding. The secrecy is evaluated in terms of the connection outage probability (COP), the probability of non-zero secrecy capacity (P_r^{nzc}), and EC based on two scenarios; the k^{th} nearest and the k^{th} best legitimate receiver.

In [53], SOP was studied for a MIMO system that used TAS/MRC techniques over the general fading distribution, which is the η-μ fading channel with and without co-channel interference. TAS and generalized selection combining (GSC) for a MIMO three-node system were used in [54] to study the system secrecy over Nakagami-m fading channels. Secrecy was studied in terms of the SOP and average secrecy rate (ASR) for two scenarios; the first one corresponds to that the legitimate receiver is located near the transmitter and the second one considers that the legitimate receiver and the eavesdropper are located near the transmitter.

Studying PLS over cascaded fading channels is also an area of interest. PLS was studied for a system model consisting of a transmitter, a receiver, and one eavesdropper in terms of the SOP and SPSC over double Rayleigh fading channel in [55] and over double Nakagami-m fading channel in [18]. Similar analyses were performed in [33] over cascaded $\alpha - \mu$ fading channel and in [26] and [56] over cascaded Nakagami-m fading channel. In [56], the secrecy performance was studied for two scenarios of one eavesdropper and two eavesdroppers. Secrecy was studied over cascaded Fisher-Snedecor $\mathcal{F}$ fading channels using stochastic geometry in [57] in the presence of randomly distributed eavesdroppers. Intercept probability is evaluated in this model, where two different cases are considered, which are the k^{th} nearest and k^{th} best eavesdropper. PLS for a three-node wiretap system model over cascaded κ-μ fading channels was explored in [7] assuming worst-case scenarios. In this work, cascaded channels were presumed at the main channel only, with multiple colluding eavesdroppers. PLS was investigated in terms of SOP and P_r^{nzc}. Similar analysis were carried out in [58], in which both channels are assumed to follow cascaded κ-μ model. A comparison between the impact of colluding and non-colluding eavesdroppers on security has been presented in [59] over cascaded κ-μ channels, in which the non-colluding ones are assumed to be randomly distributed in the area.

Considerable research has been conducted to analyze and improve the privacy of underlay CRNs. In [60], PLS has been studied for an underlay CRN over Rayleigh fading channels in terms of the SOP and the probability of non-zero secrecy capacity (P_r^{nzc}) with a multi-antenna legitimate receiver. Results reveal that the secrecy can be improved as the number of antennas increases. PLS analyses have been performed in [61] for a single-input-multiple-output (SIMO) underlay CRN in

terms of SOP. Moreover, PLS has been studied for a multiple-input-multiple-output (MIMO) underlay CRN in [62] over Nakagami-m fading channels and in [63] over Rayleigh fading channels in terms of the SOP and with the existence of multi-antenna eavesdropper. Moreover, in [64], PLS has been studied for an underlay CRN, where the SU transmitter is equipped with multiple antennas and the SU receiver and the eavesdroppers are equipped with a single antenna over Rayleigh fading channels. Outdated channel state information (CSI) was considered in [64] and in the presence of multiple primary users. In [65], secrecy was studied in terms of the intercept probability with the existence of multiple PUs over Rayleigh fading channels. PLS for CRNs over cascaded fading channels was first introduced in [66] over cascaded Rayleigh fading channels in terms of SOP, P_r^{nzc}, and INT. Finally, PLS was investigated for a SIMO underlay CRN over cascaded κ-μ fading channels in [67] in terms of the SOP and P_r^{nzc}.

CRNs-based energy harvesting (EH) has recently gained a significant interest due to its role in enhancing the PLS of CRNs' users while saving energy. For instance, in [68], PLS for an underlay CRN based-simultaneous wireless information and power transfer (SWIPT) system was studied over Rayleigh channels, in which several power splitting (PS)-EH receivers acting as eavesdroppers are presumed in the network. In [69], PLS for a CRN consisting of a pair of SUs, a pair of PUs, an eavesdropper, and an external EH jammer was investigated over Nakagami-m channels. The jammer uses the harvested energy to send artificial noise to mislead the eavesdropper. In addition, in [70], in exchange for the access to the licensed band for their own transmissions, SUs collaborate with PUs by employing EH and providing data transfer protection for PUs. The operation in [70] is divided into several time slots and the Rayleigh fading model is presumed at all channels. Additionally, in [71], PLS for an underlay CRN under the threat of eavesdropping over Rayleigh fading channel was explored. A full-duplex (FD) SU destination assisting the system's secrecy by emitting artificial noise was assumed. Recent research has focused on improving the energy efficiency of the underlying CRN through the utilization of EH. However, few studies have been conducted on employing EH for overlay CRN. For instance, in [72], a cooperation between a pair of SUs and PUs is conducted, in which the assistant SU harvests energy using PS protocol from the PUs' messages. The outage probability and the energy efficiency for both networks have been evaluated. Moreover, in [73], a TS energy harvesting process is performed by SUs, in which the SU that assists

the PUs decodes and forwards the PUs messages in exchange for utilizing the licensed band. The outage probability and system throughput have been assessed in this work. Additionally, in [74], an overlay CRN was studied, in which the SU forwards the PUs messages in exchange for utilizing the bands, whereas the PU harvests energy from the received SUs' messages to improve its battery energy level. The PS factor has been optimized with the objective of improving the SUs' and PUs' communication reliability. Furthermore, PLS was studied for an underlay CRN with a destination assisting the SUs security by harvesting energy to emit jamming signals towards the eavesdropper in [75] over cascaded κ-μ model. PLS was explored in [76] for an underlay CRN over κ-μ channels with non-colluding and randomly distributed eavesdroppers, in which a cooperating jammer exists to harvest energy and mislead the eavesdropper.

Chapter 3

Physical-Layer Security over Cascaded Fading Channels

3.1 Introduction

Recently, attention has been drawn to the work on physical-layer security (PLS) for communication systems. In [41], for a network consisting of a transmitter, a receiver, and a single eavesdropper, the probability of a strictly positive secrecy capacity was studied over the Rician fading channel. Same analyses were carried out for the Weibull fading channel in [42]. Secrecy over mixed α-μ and κ-μ fading channels was analyzed in [77] in terms of the average secrecy capacity. Moreover, the performance evaluation of the system's secrecy over $\alpha - \mu$ fading channel in [46], and over α-κ-μ and α-η-μ genealized fading channels in [47] was investigated. The secrecy performance of a system that employs single-input multiple-output (SIMO) was investigated in [78] over generalized-K fading channel, in [49] over $\kappa - \mu$ fading channel, and in [79] over η-μ fading channels. In addition, the secrecy of a SIMO system operating over correlated κ-μ shadowed fading channels was analyzed in [50] in terms of the secrecy outage probability (SOP) and the probability of strictly positive secrecy capacity. Same analyses were performed for a multiple-input multiple-output (MIMO) system model that employs transmit antenna selection (TAS) and maximal-ratio combining (MRC) schemes over α-μ fading channels in [51] and in [80] using TAS scheme. The effect of fading and co-channel interference over secrecy was studied in [81]. Furthermore, PLS was explored for a

system model consisting of a transmitter, a receiver, and one eavesdropper in terms of the SOP and the probability of positive secrecy capacity over double Rayleigh fading channel in [55] and over double Nakagami-m fading channel in [18]. Similar analyses were performed in [33] over cascaded $\alpha-\mu$ fading channel and in [26] and [56] over cascaded Nakagami-m fading channel. In [56], the secrecy performance was studied for two scenarios of one eavesdropper and two eavesdroppers.

In this chapter, cascaded κ-μ fading channels are selected for studying PLS of different system models. Hence, we begin our analyses by deriving the probability density function (PDF) and the cumulative distribution function (CDF) of cascaded κ-μ fading channels. Then, we study the performance of a point-to-point link using three evaluation metrics, which are the outage probability (OP), average symbol error probability (ASEP), and average channel capacity (ACC). In addition, we study the PLS of a three-node wiretap system model over the derived cascaded channels under three different scenarios.

3.2 κ-μ Fading Channels

κ-μ fading channel is one of the general fading channels which represent the fading in an environment in a more practical and general way. κ-μ distribution suits the LOS applications and it is defined by two physical parameters, which are κ and μ. $\kappa > 0$ is defined as the ratio between the total power of the dominant components and the power of the scattered waves, while $\mu > 0$ represents the number of the multi-path clusters. μ can be mathematically given by $\mu = \frac{E\left[R^2\right](1+2\kappa)}{V[R^2](1+\kappa)^2}$, with $E[\cdot]$ representing the expectation operator and $V[\cdot]$ representing the variance. R represents the envelope of the fading signal. The PDF of a single κ-μ random variable (X) is given by [35]

$$f_X(x) = \frac{2\mu\left(1+\kappa\right)^{\frac{\mu+1}{2}}}{\kappa^{\frac{\mu-1}{2}}\exp\left(\kappa\mu\right)} x^{\mu}\exp\left[-\mu\left(1+\kappa\right)x^2\right] I_{\mu-1}\left[2\mu\left(\sqrt{\kappa\left(1+\kappa\right)}\right)x\right], \quad (3.1)$$

where $I_{\nu}(z)$ is the modified Bessel function of the first kind with order ν [82, eq. 8.445].

3.3 Cascaded κ-μ Fading Channels

For the case of cascaded κ-μ fading channels, the received signal at the receiver is generated by the multiplication of a number of κ-μ random variables, which represent the virtual rays that are reflected from the scatters in the path between the transmitter and receiver. These random variables are assumed to be independent but not necessarily identically distributed. The overall channel can be used to model different types of communication systems, such as keyhole channel for MIMO systems and mutihop relaying systems.

3.3.1 The PDF and CDF of Cascaded κ-μ Fading channels

The channel is considered to be cascaded (multiplicative) as discussed above. Hence, the distribution of the received signal follows the cascaded κ-μ distribution (see Figure 3.1). The PDF of the cascaded $\kappa - \mu$ random variables can be found through intuition, where we can find a general formula for the PDF of the multiplication of "n" $\kappa - \mu$ random variables.

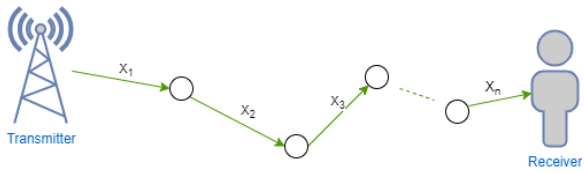

Figure 3.1: Cascaded fading channel system model.

Let the multiplication of X_i independent κ-μ random variables with the parameters κ_i and μ_i $(i \in \{1, 2, \cdots, n\})$ given by

$$Y_n = \prod_{i=1}^{n} X_i. \tag{3.2}$$

Let $Y_2 = X_1 X_2$ be the multiplication of two random variables with the PDF of X_1 and X_2 following the κ-μ distribution defined in (3.1). Using the transformation of random variables, the PDF of Y_2 is given by

$$f_{Y_2}(y) = \int_{-\infty}^{\infty} \frac{1}{|t|} f_{X_1}\left(\frac{y}{t}\right) f_{X_2}(t) dt. \tag{3.3}$$

Substituting the PDF of X_1 and X_2 from (3.1) yields

$$f_{Y_2}(y) = c_1 y^{\mu_1} \int_0^\infty t^{-1-\mu_1+\mu_2} \exp\left(\frac{-\mu_1(1+\kappa_1)y^2}{t^2}\right) \times \exp\left(-\mu_2(1+\kappa_2)t^2\right) I_{\mu_2-1}\left[2\mu_2\sqrt{\kappa_2(1+\kappa_2)}t\right] I_{\mu_1-1}\left[2\mu_1\sqrt{\kappa_1(1+\kappa_1)}\frac{y}{t}\right] dt, \tag{3.4}$$

where $c_1 = \frac{2\mu_1(1+\kappa_1)^{\frac{\mu_1+1}{2}} 2\mu_2(1+\kappa_2)^{\frac{\mu_2+1}{2}}}{\kappa_1^{\frac{\mu_1-1}{2}}\exp(\mu_1\kappa_1)\kappa_2^{\frac{\mu_2-1}{2}}\exp(\mu_2\kappa_2)}$. Using [82, eq. 8.445] and with some mathematical manipulations, (3.4) can be expressed by

$$f_{Y_2}(y) = \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty} \frac{c_1 c_2}{2}\left[\mu_2(1+\kappa_2)\right]^{\mu_1-\mu_2+l_1-l_2} y^{2\mu_1+2l_1-1} \times G_{2\,0}^{0\,2}\left(\begin{matrix}\mu_1-\mu_2+l_1-l_2+1,1\\ -\end{matrix}\middle|\frac{1}{\prod_{i=1}^{2}\mu_i(1+\kappa_i)y^2}\right), \tag{3.5}$$

where $G_{p\ q}^{m\ n}\left(\begin{matrix}a_r\\ b_s\end{matrix}\middle|z\right)$ is the Meijer G-function defined in [82, eq. 9-301] and

$$c_2 = \frac{\left[2\mu_1\sqrt{\kappa_1(1+\kappa_1)}\right]^{2l_1+\mu_1-1}\left[2\mu_2\sqrt{\kappa_2(1+\kappa_2)}\right]^{2l_2+\mu_2-1}}{\Gamma(l_1+\mu_1)(l_1)!\,2^{2l_1+\mu_1-1}\Gamma(l_2+\mu_2)(l_2)!\,2^{2l_2+\mu_2-1}}.$$

It is straightforward to prove that the PDF of the cascaded $\kappa-\mu$ channel is given by

$$f_{Y_n}(y) = \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty} c_x y^{2\mu_1+2l_1-1} G_{n\ 0}^{0\ n}\left(\begin{matrix}\beta\\ -\end{matrix}\middle|\frac{1}{y^2\prod_{i=1}^{n}\mu_i(1+\kappa_i)}\right), \tag{3.6}$$

where $\beta = \mu_1-\mu_2+l_1-l_2+1,\cdots,\mu_1-\mu_n+l_1-l_n+1,1$ and

$$c_x = 2\prod_{i=1}^{n}\left[\frac{\left[\mu_i(1+\kappa_i)\right]^{\mu_1-\mu_i+l_1-l_i}\mu_i(1+\kappa_i)^{\frac{\mu_i+1}{2}}\left[2\mu_i\sqrt{\kappa_i(1+\kappa_i)}\right]^{2l_i+\mu_i-1}}{\kappa_i^{\frac{\mu_i-1}{2}}\exp(\kappa_i\mu_i)\Gamma(l_i+\mu_i)(l_i)!\,2^{2l_i+\mu_i-1}}\right].$$

When the cascade level $n=1$ and $\kappa=K$ (LOS component in Rician fading channel) and $\mu=1$, the PDF in (3.6) reduces to

$$f_{Y_1}(y) = \sum_{l_1=0}^{\infty} c_x' y^{2l_1+1} G_{0\ 1}^{1\ 0}\left(\begin{matrix}-\\ 0\end{matrix}\middle|y^2(1+K)\right), \tag{3.7}$$

where $c'_x = \frac{2(1+K)\left[2\sqrt{K(1+K)}\right]^{2l_1}}{\exp(K)(l_1!)^2 2^{2l_1}}$. Using [83, eq. (8.4.3.1)] and [82, eq. 8.447.1], (3.7) reduces to the PDF of the Rician random variable [84, eq. 2.3-62]. Moreover, setting $K = 0$ reduces to the PDF of the Rayleigh random variable [84, eq. 2.3-43]. Certain expressions for the PDF of fading channels such as Nakagami-m can be extracted from (3.6) by modifying the values for κ and μ. The CDF of the multiplication of "n" κ-μ random variables can be derived from the PDF in (3.6) as

$$F_{Y_n}(y) = \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty} c_x \int_0^y x^{2\mu_1+2l_1-1} G_{n\ 0}^{0\ n}\left(\begin{matrix}\beta\\ -\end{matrix}\middle|\frac{1}{x^2\prod_{i=1}^{n}\mu_i(1+\kappa_i)}\right)dx\,. \tag{3.8}$$

Using [82, eq. (9.31-2)] and [85, eq. (26)], (3.8) becomes

$$F_{Y_n}(y) = \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty} \frac{c_x}{2} y^{2(\mu_1+l_1)} G_{1\ n+1}^{n\ 1}\left(\begin{matrix}1-\mu_1-l_1\\ \eta'\end{matrix}\middle|y^2\prod_{i=1}^{n}\mu_i(1+\kappa_i)\right), \tag{3.9}$$

where $\eta' = -\mu_1+\mu_2-l_1+l_2,\cdots,-\mu_1+\mu_n-l_1+l_n,0,-\mu_1-l_1$.

3.4 Signal-to-Noise-Ratio Statistics

Assume we have a digital communication system operating over the cascaded κ-μ fading channel. The received SNR statistics will be derived in this section. Then, the outage probability, the average symbol error probability, and the average channel capacity are derived. The SNR at the input of the receiving node is denoted by the variable γ. The average received SNR $(\bar{\gamma})$ is given by

$$\bar{\gamma} = E\left[Y_n^2\right]\frac{P}{N_\circ}, \tag{3.10}$$

where Y_n is the vector representing the multiplication of "n" κ-μ random variables in (3.2), P is the transmit power and $N_\circ$ is the power spectral density of the additive-white-Gaussian-noise (AWGN). Using (3.2), (3.10) can be written as

$$\bar{\gamma} = \frac{P}{N_\circ}\prod_{i=1}^{n} E\left[X_i^2\right]. \tag{3.11}$$

The PDF of the SNR at the receiving node can be expressed as [86, eq. (2.3)]

$$f_{\gamma}(\gamma) = \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\frac{c_x}{2}\gamma^{\mu_1+l_1-1}\left(\frac{\prod_{i=1}^{n}E\left[X_i^2\right]}{\bar{\gamma}}\right)^{\mu_1+l_1} \times G_{n\ 0}^{0\ n}\left(\begin{matrix}\beta\\ -\end{matrix}\middle|\frac{\bar{\gamma}}{\gamma\prod_{i=1}^{n}E\left[X_i^2\right]\mu_i\left(1+\kappa_i\right)}\right). \tag{3.12}$$

The CDF of the SNR can be found from (3.12) Using [82, eq. (9.31-2)] and [85, eq. (26)] as

$$F_{\gamma}(\gamma) = \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\frac{c_x}{2}\left(\gamma\frac{\prod_{i=1}^{n}E\left[X_i^2\right]}{\bar{\gamma}}\right)^{(\mu_1+l_1)} \times G_{1\ n+1}^{n\ 1}\left(\begin{matrix}1-\mu_1-l_1\\ \eta'\end{matrix}\middle|\frac{\gamma\prod_{i=1}^{n}E\left[X_i^2\right]\mu_i\left(1+\kappa_i\right)}{\bar{\gamma}}\right). \tag{3.13}$$

3.5 Link Performance over Cascaded κ-μ Fading Channels

In this section, the system performance is studied over the cascaded $\kappa-\mu$ fading channel and in the presence of the AWGN.

3.5.1 Outage Probability

-Exact outage probability: Outage probability (P_o) is the probability that the SNR (γ) falls below a given threshold (γ_{th}) and can be found as

$$P_o = P_r\left(\gamma \leq \gamma_{th}\right) = F_{\gamma}\left(\gamma_{th}\right). \tag{3.14}$$

Substituting (3.13) into (3.14) yields

$$P_o = \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\frac{c_x}{2}\left(\gamma_{th}\frac{\prod_{i=1}^{n}E\left[X_i^2\right]}{\bar{\gamma}}\right)^{(\mu_1+l_1)} \times G_{1\ n+1}^{n\ 1}\left(\begin{matrix}1-\mu_1-l_1\\ \eta'\end{matrix}\middle|\frac{\gamma_{th}\prod_{i=1}^{n}E\left[X_i^2\right]\mu_i\left(1+\kappa_i\right)}{\bar{\gamma}}\right). \tag{3.15}$$

-Asymptotic outage probability: The asymptotic outage probability is calculated when $\frac{\gamma_{th}}{\bar{\gamma}} \to \infty$. Using [87, eq. (2.2.1)] and [87, eq. (3.11.3)], (3.15) can be rewritten as

$$P_o = \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\frac{c_x}{2\left(\mu_i(1+\kappa_i)\right)^{\mu_1+l_1}} H_{\,1\;\,n+1}^{\,n\;\,1}\left(\begin{matrix}\phi_1\\ \phi_2\end{matrix}\middle|\frac{\gamma_{th}\prod_{i=1}^{n}E\left[X_i^2\right]\mu_i\left(1+\kappa_i\right)}{\bar{\gamma}}\right), \tag{3.16}$$

where $H_{\,p\;\,q}^{\,m\;\,n}\left(\begin{smallmatrix}a\\ b\end{smallmatrix}|\cdot\right)$ is the Fox H-function defined in [87, eq. 3.11.1], $\phi_1 = \{1,1\}$, and $\phi_2 = \{\mu_2+l_2,1\},\cdots,\{\mu_n+l_n,1\},\{\mu_1+l_1,1\},\{0,1\}$. Using [88, eq. (2.1)], (3.16) can be expressed as

$$P_o = \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\frac{c_x}{2(2\pi i)\left(\mu_i(1+\kappa_i)\right)^{\mu_1+l_1}}\int_C \frac{\Gamma[-s]\prod_{i=1}^{n}\Gamma[\mu_i+l_i+s]}{\Gamma[1-s]\left(\frac{\gamma_{th}\prod_{i=1}^{n}E\left[X_i^2\right]\mu_i(1+\kappa_i)}{\bar{\gamma}}\right)^{s}}ds\cdot \tag{3.17}$$

Using the residue method defined in [89], (3.17) can be approximated as

$$\begin{aligned} P_o &\approx \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\frac{c_x}{2\left(\mu_i(1+\kappa_i)\right)^{\mu_1+l_1}} Res\left[\frac{\Gamma[-s]\prod_{i=1}^{n}\Gamma[\mu_i+l_i+s]}{\Gamma[1-s]\left(\frac{\gamma_{th}\prod_{i=1}^{n}E\left[X_i^2\right]\mu_i(1+\kappa_i)}{\bar{\gamma}}\right)^{s}},0\right] \\ &\approx \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\frac{c_x}{2\left(\mu_i(1+\kappa_i)\right)^{\mu_1+l_1}}\prod_{i=1}^{n}\Gamma[\mu_i+l_i]. \end{aligned} \tag{3.18}$$

Note that the expression in (3.18) is independent of the average received SNR $(\bar{\gamma})$ since the required threshold is very high. That is the system is in outage and cannot satisfy its requirement, which means that the communication cannot be reliable regardless of the average transmitted power value. This case represents the worst-case scenario of the system performance.

3.5.2 Average Symbol Error Probability

The average symbol error probability (ASEP) is evaluated by averaging the conditional symbol error probability over the PDF of the SNR (γ) as

$$\bar{P}_e = \int_0^{\infty} P_e(\gamma) f_\gamma(\gamma) d\gamma \cdot \tag{3.19}$$

The modulation scheme assumed here is Binary-Phase-Shift-Keying (BPSK). However, any type of modulation may be used. For BPSK, the conditional symbol error probability $P_e(\gamma)$ is given by

$$P_e(\gamma) = \frac{1}{2} erfc(\sqrt{\gamma}), \tag{3.20}$$

where $erfc(\cdot)$ is the complementary error function, which can be represented through the Meijer G-function as [83, eq. (8.4.14.2)]

$$erfc(\sqrt{z}) = \frac{1}{\sqrt{\pi}} G_{1\ 2}^{2\ 0}\left(\begin{matrix}1\\ 0,\frac{1}{2}\end{matrix}\middle| z\right) \cdot \tag{3.21}$$

Using [82, eq. (9.31-2)], (3.21), and [83, eq. (2.24.1.1)], (3.19) can be expressed as

$$\begin{aligned} \bar{P}_e &= \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty} \frac{c_x}{4\sqrt{\pi}} \left(\frac{\prod_{i=1}^{n} E\left[X_i^2\right]}{\bar{\gamma}}\right)^{\mu_1+l_1} \\ &\times G_{2\ n+1}^{n\ 2}\left(\begin{matrix}c_p\\ \beta', -\mu_1-l_1\end{matrix}\middle| \frac{\prod_{i=1}^{n} E\left[X_i^2\right]\mu_i(1+\kappa_i)}{\bar{\gamma}}\right), \end{aligned} \tag{3.22}$$

where $c_p = 1-\mu_1-l_1, 0.5-\mu_1-l_1$ and $\beta' = -\mu_1+\mu_2-l_1+l_2, \cdots, -\mu_1+\mu_n-l_1+l_n, 0$.

3.5.3 Average Channel Capacity

The average channel capacity (ACC) represents an important metric for the system performance, which measures the maximum transmission rate of the communication system. Let $B.W$ denotes the channel bandwidth and ACC represents the channel capacity over an AWGN channel, which is

given by

$$ACC = B.W \log_2 \left(1 + \frac{E_s}{N_\circ}\right) \cdot \tag{3.23}$$

Using the cascaded $\kappa - \mu$ fading channel, we may evaluate the average channel capacity (normalized by the bandwidth $B.W$) as

$$\overline{ACC} = \int_0^\infty \log_2 (1+\gamma)\, f_\gamma(\gamma)\, d\gamma \cdot \tag{3.24}$$

Using [85, eq. (11)], [82, eq. (9.31-2)] and [83, eq. (2.24.1.1)] and after some mathematical manipulation yields

$$\overline{ACC} = \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty} \frac{c_x}{2\log(2)} \left(\frac{\prod_{i=1}^n E\left[X_i^2\right]}{\bar{\gamma}}\right)^{\mu_1+l_1} G_{2\ n+2}^{\,n+2\ 1}\left(\begin{matrix}\zeta' \\ \zeta"\end{matrix}\middle| \frac{\prod_{i=1}^n E\left[X_i^2\right]\mu_i(1+\kappa_i)}{\bar{\gamma}}\right), \tag{3.25}$$

where $\zeta' = -\mu_1 - l_1, 1 - \mu_1 - l_1$ and $\zeta" = \beta', -\mu_1 - l_1, -\mu_1 - l_1$.

3.6 Numerical Results

Figure 3.2 shows the effect of the cascade level "n" on the shape form of the PDF and CDF of cascaded κ-μ channel. Moreover, Figure 3.2 (a) shows two of the special cases of the cascaded κ-μ fading channels. The first is the Rician fading channel in which the fading parameter $\kappa = K$ (LOS component for the Rician channel) and $\mu = 1$. Two different values of κ are considered; $\kappa = 1$ and $\kappa = 10$. Comparing these two curves with the ones in [84, Figure 2.3–5], one can notice that they are in a perfect match. Moreover, it includes another special case, namely the Nakagami-m fading channel $(n = 1, \kappa = 0, \mu = 2)$ agreeing with the results in [84, Figure 2.3-6] for the Nakagami-m fading parameter $m = 2$. That is the κ-μ fading channel is a general distribution modeling many practical and well-known channels.

Figures 3.3 and 3.4 show how the outage probability, average channel capacity, and average symbol error probability are influenced by the cascade degree n, respectively. For Figure 3.4, for

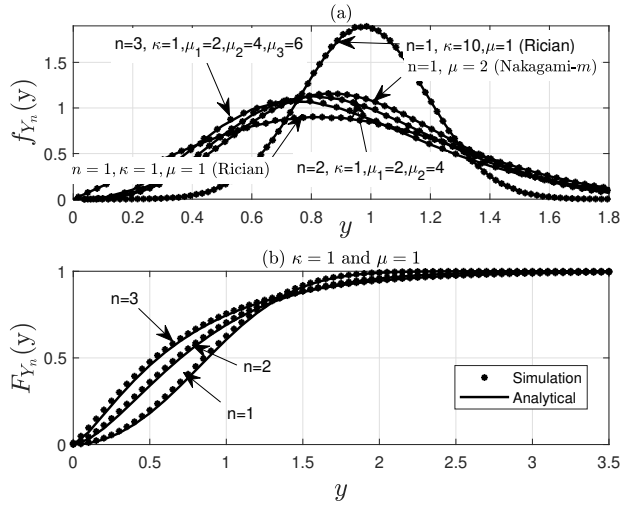

Figure 3.2: (a) The PDF and (b) CDF of the cascaded κ-μ fading channels.

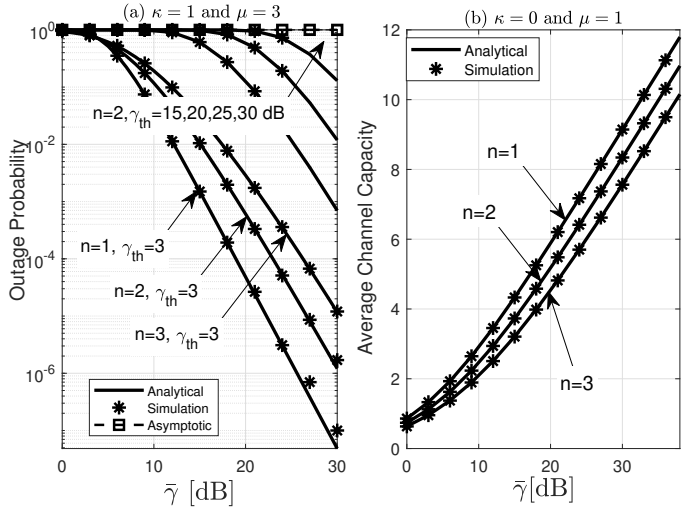

Figure 3.3: (a) The outage probability (P_o) and (b) the average channel capacity (ACC) of cascaded κ-μ fading channels.

identically distributed RV_s: $\kappa = 2$ and $\mu = 2$. For non-identically distributed RV_s: for $n = 2$: $\kappa_1 = \kappa_2 = 2, \mu_1 = 1, \mu_2 = 2$, and for $n = 3$: $\kappa_1 = \kappa_2 = \kappa_3 = 2, \mu_1 = 1, \mu_2 = 2, \mu_3 = 3$. It can be observed that as the cascade level (number of keyholes) increases, the system performance becomes worse as the number of scatters between the transmitter and receiver increases, making it less likely to successfully transmit the information. In addition, it is noticed that the communication can still be efficient as the average received SNR $(\bar{\gamma})$ is increased. Moreover, Figure 3.3 (a) shows the impact of increasing the threshold SNR (γ_{th}) for double κ-μ fading channel $(n = 2)$ over

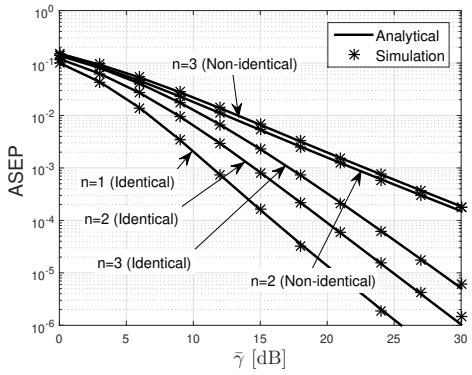

Figure 3.4: The average symbol error probability (ASEP) of the cascaded κ-μ fading channel for different cascade levels "n" for BPSK modulation.

the outage probability of the system. Figure 3.3 (a) includes the case of the asymptotic outage probability given in (3.18) showing that the outage probability is independent of the average received SNR $(\bar{\gamma})$ since the required SNR value (γ_{th}) is very high. That is, reliable communications cannot be achieved regardless of the level of the quality of the channel in terms of the received SNR, which represents a worst-case system performance scenario.

3.7 PLS Model and Performance Considering Worst-Case Scenarios

In this section, we study the secrecy of a system consisting of a single antenna transmitter (Alice), a single antenna receiver (Bob), and multiple colluding eavesdroppers (see Figure 3.5). Eavesdroppers may either be colluding or non-colluding. Non-colluding eavesdroppers intercept the information individually. However, colluding eavesdroppers jointly process the gathered intercepted information by sending it to a centralized processor. Hence, multiple colluding eavesdroppers can be considered as a multi-antenna eavesdropper (Eve) [90], [91], where MRC is employed. Having a single antenna at Bob while Eve is equipped with multiple antennas (L_e) is a logical hypothesis to evaluate the system in its worst cases. To further analyze the worst case scenario, we consider poor environment with many obstacles and objects for the main channel. That is, the received signal at Bob is generated by the product of a large number of rays reflected from the scatters in this environment. Hence, the main channel is more practical to be modeled as a cascaded $\kappa - \mu$ fading channel reflecting severe fading conditions. On the other hand, the wiretap channel is presumed to

have better conditions with less scatters where it is more likely to follow a single $\kappa - \mu$ fading. The secrecy performance is studied in terms of the secrecy outage probability (SOP) and the probability of non-zero secrecy capacity P_r^{nzc}. In addition, all the derived analytical results are in a perfect match with Monte-Carlo simulations, which emphasizes that the considered system model and the obtained analyses are reliable to be used in characterizing the keyhole channel and the multi-hop relaying systems.

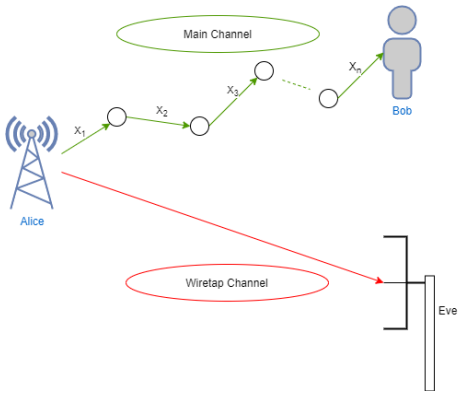

Figure 3.5: The system model.

The received signal at Bob is given by

$$y_b = \sqrt{P} Y_n x + z_b, \tag{3.26}$$

where P is the transmit power. Y_n is the channel coefficient between Alice and Bob, which follows the cascaded $\kappa - \mu$ fading channel given by (3.2) with the PDF in (3.6). x is the message transmitted to Bob and z_b is the AWGN at the receiver with zero mean and variance N_0. The intercepted message at Eve is given by

$$y_{e,i} = \sqrt{P} Y_{e,i} x + z_{e,i}, \tag{3.27}$$

where $Y_{e,i}$ is the channel coefficient between Alice and the i^{th} antenna of Eve. $z_{e,i}$ is the AWGN at the i^{th} antenna of Eve with zero mean and variance N_0. The SNR at Bob is given by $\gamma = |Y_n|^2 \frac{P}{N_0}$ with $\bar{\gamma}$ being the average received SNR at Bob. The SNR at Eve is given by $\gamma_e = \sum_{i=1}^{L_e} \gamma_{e,i}$, where

$\gamma_{e,i} = |Y_{e,i}|^2 \frac{P}{N_0}$. The PDF and the CDF of γ_e are given by [49]

$$f_{\gamma_e}(\gamma) = \beta_e \gamma^{\frac{L_e\mu_e-1}{2}} \exp\left(-\frac{\mu_e(1+\kappa_e)\gamma}{\bar{\gamma_e}}\right) I_{L_e\mu_e-1}\left(2\mu_e\sqrt{\frac{L_e\kappa_e(1+\kappa_e)\gamma}{\bar{\gamma_e}}}\right), \tag{3.28}$$

$$F_{\gamma_e} = 1 - Q_{L_e\mu_e}\left(\sqrt{2L_e\mu_e\kappa_e}, \sqrt{\frac{2\mu_e(1+\kappa_e)\gamma}{\bar{\gamma_e}}}\right), \tag{3.29}$$

where $\beta_e = \frac{L_e\mu_e(1+\kappa_e)^{\frac{L_e\mu_e+1}{2}}}{\exp(L_e\mu_e\kappa_e)(L_e\bar{\gamma_e})^{\frac{L_e\mu_e+1}{2}}\kappa_e^{\frac{L_e\mu_e-1}{2}}}$, $\bar{\gamma_e}$ is the average received SNR at Eve, and $Q_m(\cdot)$ is the generalized Marcum Q-function of the m^{th} order.

3.7.1 Secrecy Outage Probability

The secrecy outage probability is an important security metric for passive eavesdropping as Alice is not aware of the channel state information (CSI) of Eve. SOP is defined as the probability that the secrecy capacity falls below a given threshold (C_{th}) as

$$SOP = P_r(C_s < C_{th}) = \int_0^\infty f_{\gamma_e}(\gamma_e) F_\gamma\left(2^{C_{th}}(1+\gamma_e) - 1\right) d\gamma_e, \tag{3.30}$$

where C_s is the secrecy capacity and C_{th} is the threshold secrecy rate. The secrecy capacity is defined in (2.2). The expression for the SOP in (3.30) is hard to be solved because of the complexity of the argument of the CDF $\left(2^{C_{th}}(1+\gamma_e) - 1\right)$. Hence, instead of calculating the SOP, we evaluate the lower bound of the SOP given by [49]

$$SOP_{LB} = \int_0^\infty f_{\gamma_e}(\gamma_e) F_\gamma\left(2^{C_{th}}\gamma_e\right) d\gamma_e. \tag{3.31}$$

Substituting (3.28) and (3.13) into (3.31) and using [82, eq. 8.445] and [82, eq. (7.813-1)] yields

$$\begin{aligned} SOP_{LB} &= \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\sum_{A=0}^{\infty}\frac{c_x}{2}\beta_e 2^{C_{th}(\mu_1+l_1)}\left(\frac{\mu_e\left(1+\kappa_e\right)}{\bar{\gamma}_e}\right)^{-L_e\mu_e-\mu_1-l_1-A} \\ &\times \frac{\left(\mu_e\sqrt{\frac{L_e\kappa_e(1+\kappa_e)}{\bar{\gamma}_e}}\right)^{2A-1+L_e\mu_e}}{A!\,\Gamma\left(A+L_e\mu_e\right)} G_{\,2\;\,n+1}^{\,n\;\,2}\left(\begin{matrix}\epsilon\\ \eta'\end{matrix}\middle|\frac{D}{\mu_e\left(1+\kappa_e\right)\bar{\gamma}}\right) \\ &\times \left(\frac{\prod_{i=1}^{n}E\left[X_i^2\right]}{\bar{\gamma}}\right)^{(\mu_1+l_1)}, \end{aligned} \tag{3.32}$$

where $\epsilon = -L_e\mu_e - \mu_1 - l_1 - A + 1, 1 - \mu_1 - l_1$ and $D = 2^{C_{th}}\bar{\gamma}_e\prod_{i=1}^{n}E\left[X_i^2\right]\mu_i\left(1+\kappa_i\right)$.

-Asymptotic secrecy outage probability: Asymptotic SOP_{LB} can be calculated when $\bar{\gamma}_e \to \infty$. Using [87, eq. (2.2.1)] and [87, eq. (3.11.3)], (3.32) can be rewritten as

$$SOP_{LB} = \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\sum_{A=0}^{\infty}c_a H_{\,2\;\,n+1}^{\,n\;\,2}\left(\begin{matrix}\epsilon_d\\ \eta_d\end{matrix}\middle|\frac{D'}{\mu_e\left(1+\kappa_e\right)\bar{\gamma}}\right), \tag{3.33}$$

where $H_{\,p\;\,q}^{\,m\;\,n}\left(\begin{smallmatrix}a\\ b\end{smallmatrix}\middle|\cdot\right)$ is the H-function defined in [87, eq. 3.11.1], $D' = 2^{C_{th}}\bar{\gamma}_e\prod_{i=1}^{n}E\left[X_i^2\right]$ $\mu_i\left(1+\kappa_i\right), \epsilon_d = \left\{-L_e\mu_e - A + 1, 1\right\}, \left\{1,1\right\}, \eta_d = \left\{\mu_2+l_2, 1\right\}, \cdots, \left\{\mu_n+l_n, 1\right\}, \left\{\mu_1+l_1, 1\right\},$ $\left\{0,1\right\}$, and

$$c_a = \frac{\left(\mu_e\left(1+\kappa_e\right)\right)^{-L_e\mu_e-A} c_x\left(\mu_e\sqrt{L_e\kappa_e\left(1+\kappa_e\right)}\right)^{2A-1+L_e\mu_e} L_e\mu_e\left(1+\kappa_e\right)^{\frac{L_e\mu_e+1}{2}}}{2A!\,\Gamma\left(A+L_e\mu_e\right)\exp\left(L_e\mu_e\kappa_e\right)\left(L_e\right)^{\frac{L_e\mu_e+1}{2}}\kappa_e^{\frac{L_e\mu_e-1}{2}}}.$$

Using the integral representation of the H-function, (3.33) can be expressed as

$$\begin{aligned} SOP_{LB} &= \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\sum_{A=0}^{\infty}\frac{c_a}{2\pi i}\int_C \frac{\Gamma[s]\Gamma[L_e\mu_e+A+s]\prod_{i=1}^{n}\Gamma[\mu_i+l_i-s]}{\Gamma[1+s]} \\ &\times \left(\frac{2^{C_{th}}\bar{\gamma}_e\prod_{i=1}^{n}E\left[X_i^2\right]\mu_i\left(1+\kappa_i\right)}{\mu_e\left(1+\kappa_e\right)\bar{\gamma}}\right)^{s} ds. \end{aligned} \tag{3.34}$$

As $\bar{\gamma_e} \to \infty$, the last term in (3.34) $\to \infty$. The asymptotic SOP can be calculated using the residue method defined in [89] as

$$\begin{aligned} SOP_{LB} &\approx \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\sum_{A=0}^{\infty}\frac{c_a}{2\pi i}\text{Res}\left\{g(s),0\right\} \\ &\approx \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\sum_{A=0}^{\infty}c_a\Gamma[L_e\mu_e+A]\prod_{i=0}^{n}\Gamma[\mu_i+l_i], \end{aligned} \tag{3.35}$$

where $g(s)$ is given by

$$g(s) = \frac{\Gamma[s]\Gamma[L_e\mu_e+A+s]\prod_{i=1}^{n}\Gamma[\mu_i+l_i-s]}{\Gamma[1+s]}\left(\frac{2^{C_{th}}\bar{\gamma_e}\prod_{i=1}^{n}E\left[X_i^2\right]\mu_i\left(1+\kappa_i\right)}{\mu_e\left(1+\kappa_e\right)\bar{\gamma}}\right)^{s}. \tag{3.36}$$

Note that the expression in (3.35) is independent of $\bar{\gamma}$. Therefore, the diversity order is zero, which means that there are no independent links (paths) between Alice and Bob. Hence, the slope of the SOP curve at high values of the SNR $\bar{\gamma}$ is zero. In terms of PLS, this means that the information will be intercepted by the eavesdropper and the secrecy of the confidential information cannot be achieved.

3.7.2 Probability of Non-Zero Secrecy Capacity

Probability of non-zero secrecy capacity appears when the secrecy capacity C_s defined in (2.2) is positive. The probability of non-zero secrecy capacity can be expressed by

$$P_r^{nzc} = P_r\left(C_s>0\right) = P_r\left(\gamma>\gamma_e\right) = F_{\frac{\gamma_e}{\gamma}}\left(1\right)\cdot \tag{3.37}$$

To obtain the probability of non-zero secrecy capacity, one needs to find the PDF and then the CDF of the ratio $\frac{\gamma_e}{\gamma}$. With some mathematical manipulations, (3.12) can be rewritten as

$$f_{\gamma}\left(\gamma\right) = \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\frac{c_x\prod_{i=1}^{n}E\left[X_i^2\right]}{2\bar{\gamma}\left(\prod_{i=1}^{n}\mu_i\left(1+\kappa_i\right)\right)^{\mu_1+l_1-1}}H_{0\ n}^{n\ 0}\left(\begin{matrix}-\\ h'\end{matrix}\middle|\frac{\gamma\prod_{i=1}^{n}E\left[X_i^2\right]\mu_i\left(1+\kappa_i\right)}{\bar{\gamma}}\right), \tag{3.38}$$

where $h' = \{\mu_2 + l_2 - 1, 1\}, \cdots, \{\mu_n + l_n - 1, 1\}, \{\mu_1 + l_1 - 1, 1\}$. Similarly, (3.28) can be rewritten as

$$f_{\gamma_e}(\gamma) = \sum_{B=0}^{\infty} \frac{\beta_e}{B!\,\Gamma(B+\mu_e L_e)} \left(\frac{\bar{\gamma_e}}{\mu_e(1+\kappa_e)}\right)^{B+L_e\mu_e-1} \left(\mu_e \sqrt{\frac{L_e\kappa_e(1+\kappa_e)}{\bar{\gamma_e}}}\right)^{2B+L_e\mu_e-1} \times H_{0\,1}^{1\,0}\left(\begin{matrix} - \\ \{B+L_e\mu_e-1,1\} \end{matrix} \middle| \frac{\gamma\mu_e(1+\kappa_e)}{\bar{\gamma_e}}\right). \tag{3.39}$$

Using (3.38) and (3.39), $f_{\frac{\gamma_e}{\gamma}}(\gamma)$ can be expressed as

$$f_{\frac{\gamma_e}{\gamma}}(y) = \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\sum_{B=0}^{\infty} \frac{c_x\chi_e \prod_{i=1}^{n} E\left[X_i^2\right]}{\left(\prod_{i=1}^{n}\mu_i(1+\kappa_i)\right)^{\mu_1+l_1-1} 2\bar{\gamma}\left(\frac{\prod_{i=1}^{n} E\left[X_i^2\right]\mu_i(1+\kappa_i)}{\bar{\gamma}}\right)^2} \times H_{n\,1}^{1\,n}\left(\begin{matrix} \varphi' \\ \varphi'' \end{matrix} \middle| \frac{\bar{\gamma}\mu_e(1+\kappa_e)}{\bar{\gamma_e}\prod_{i=1}^{n} E\left[X_i^2\right]\mu_i(1+\kappa_i)} y\right), \tag{3.40}$$

where $\varphi' = \{-\mu_2 - l_2, 1\}, \cdots, \{-\mu_n - l_n, 1\}, \{-\mu_1 - l_1, 1\}$, $\varphi'' = \{B + L_e\mu_e - 1, 1\}$, and $\chi_e = \frac{\beta_e}{B!\Gamma(B+\mu_e L_e)}\left(\mu_e\sqrt{\frac{L_e\kappa_e(1+\kappa_e)}{\bar{\gamma_e}}}\right)^{2B+L_e\mu_e-1}\left(\frac{\bar{\gamma_e}}{\mu_e(1+\kappa_e)}\right)^{B+L_e\mu_e-1}$. Using (3.40) and [88], P_r^{nzc} can be expressed as

$$P_r^{nzc} = 1 - \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\sum_{B=0}^{\infty} \frac{c_x\prod_{i=1}^{n} E\left[X_i^2\right]}{2\bar{\gamma}\left(\prod_{i=1}^{n}\mu_i(1+\kappa_i)\right)^{\mu_1+l_1-1}} \times \frac{\chi e}{\left(\frac{\mu_e(1+\kappa_e)\prod_{i=1}^{n} E\left[X_i^2\right]\mu_i(1+\kappa_i)}{\bar{\gamma_e}\bar{\gamma}}\right)} H_{n+1\,2}^{2\,n}\left(\begin{matrix} \phi' \\ \phi'' \end{matrix} \middle| \frac{\bar{\gamma}\mu_e(1+\kappa_e)}{\bar{\gamma_e}\prod_{i=1}^{n} E\left[X_i^2\right]\mu_i(1+\kappa_i)}\right), \tag{3.41}$$

where $\phi' = \{-\mu_2 - l_2 + 1, 1\}, \cdots, \{-\mu_n - l_n + 1, 1\}, \{-\mu_1 - l_1 + 1, 1\}, \{1, 1\}$ and $\phi'' = \{0, 1\}, \{B + L_e\mu_e, 1\}$.

3.8 Numerical Results

In this section, both simulations and analytical results are presented. All figures show a perfect match of the simulation results with the analytical ones. The analytical curves are obtained by truncating the infinite series expansion over the index l to the first 17 terms ($l = 17$).

Figure 3.6 represents the lower bound of the secrecy outage probability (SOP_{LB}) against the average received SNR at Bob ($\bar{\gamma}$) for two antennas at Eve ($L_e = 2$). For the main channel: $\kappa = 2, \mu = 2$ and for the wiretap channel: $\kappa_e = 2, \mu_e = 1$. One can observe that increasing the average received SNR at Bob ($\bar{\gamma}$) improves the secrecy capacity and reduces the secrecy outage probability. Furthermore, increasing the number of scatters, which is represented by the cascade level (n) in the channel between Alice and Bob leads to worse channel conditions as more severe fading exists when the number of keyholes increases. This will make the channel less reliable which reduces the secrecy level of the confidential information. Moreover, Figure 3.6 shows how the secrecy outage probability behaves as the average received SNR at Eve ($\bar{\gamma_e}$) is increased. The asymptotic lower bound of the secrecy outage probability (SOP_{LB}) can be observed when the average received SNR at the Eve ($\bar{\gamma_e}$) is improved (high value), where the zero diversity order is clear. This means that even enhancing the quality of the main channel in terms of the average received SNR at Bob will not improve the secrecy and the confidential information will be intercepted by Eve. Such a scenario can occur when the Eve is very close to the transmitter Alice, where the wiretap channel conditions are very good in terms of the received SNR.

Figure 3.7 (a) shows the effect of the number of antennas at Eve over the probability of non-zero secrecy capacity (P_r^{nzc}). For the main channel: $\kappa = 1, \mu = 2$ and for the wiretap channel for the case of $n = 2$: $\kappa_e = 1, \mu_e = 2$. For a selected value of the average received SNR at Bob ($\bar{\gamma}$) for double κ-μ fading channel ($n = 2$), increasing the number of antennas at Eve brings a higher chance for Eve to overhear the information. In addition, it would be more likely to combat the effect of this passive eavesdropping and for the positive secrecy capacity to be achieved as the average received SNR at Bob ($\bar{\gamma}$) increases due to an improvement in the channel conditions. Furthermore, the effect of the wiretap channel parameter (κ_e) over the probability of non-zero secrecy capacity (P_r^{nzc}) is studied in Figure 3.7 (a) for a single fading channel ($n = 1$) with Eve being equipped with a single antenna ($L_e = 1$). We can note from these results that as the condition of the wiretap channel gets better (κ_e increases), the secrecy of the main channel becomes poorer. Moreover, the results in Figure 3.7 (a) show that the gap between the probability of non-zero secrecy capacity at low average received SNR at Bob ($\bar{\gamma}$) is higher than the gap when the average received SNR is increased. In other words, the effect of increasing the number of antennas at Eve is reduced as the average

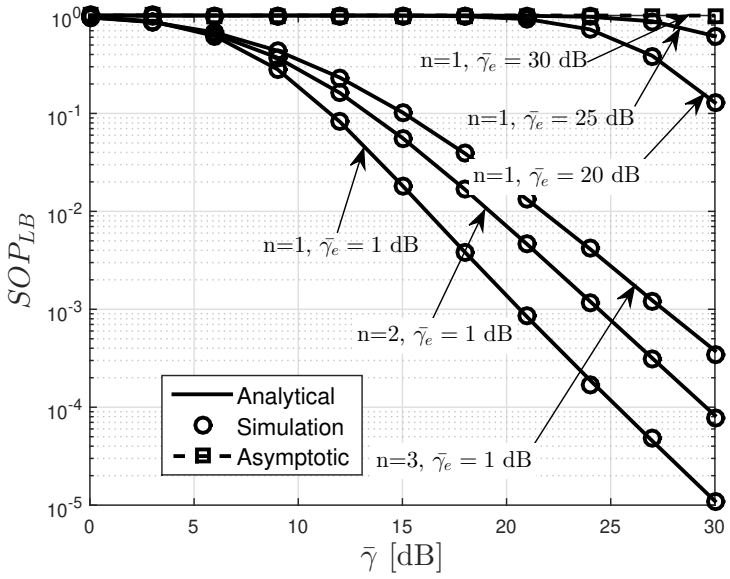

Figure 3.6: The secrecy outage probability (SOP_{LB}) for two antennas at Eve $(L_e = 2)$ for different cascade levels "n". $C_{th} = 1$

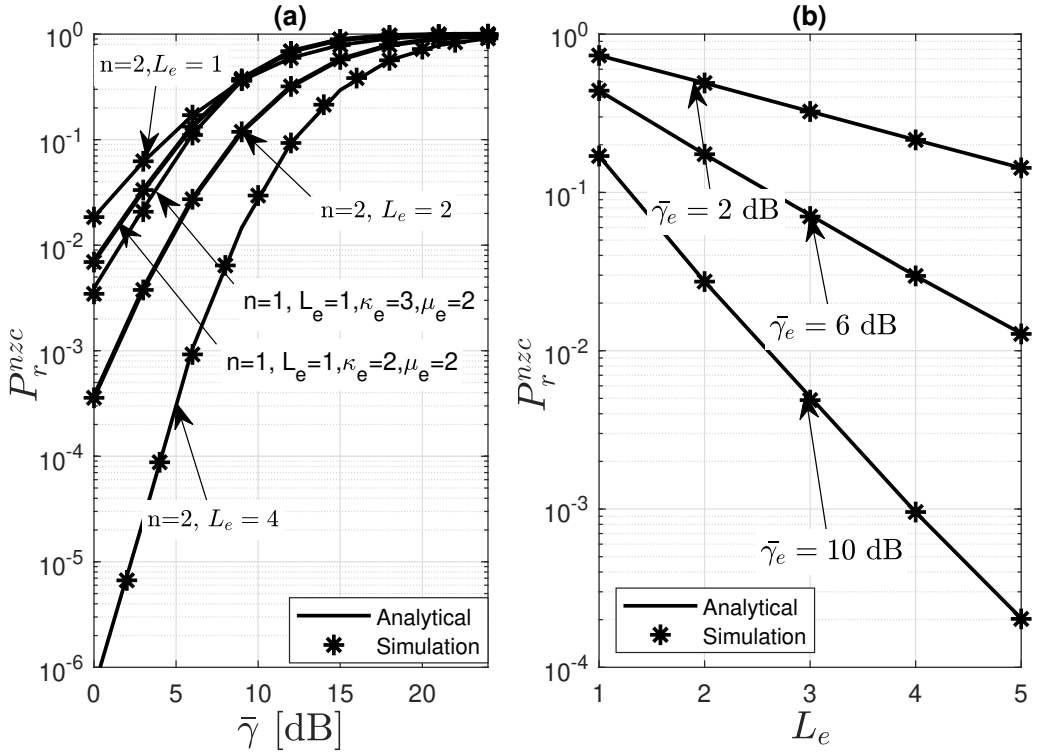

Figure 3.7: The probability of non-zero secrecy capacity (P_r^{nzc}). For (a), $\bar{\gamma}_e = 10$ dB. For (b), $n = 2$ and $\bar{\gamma} = 6$ dB.

received SNR at Bob becomes higher. Figure 3.7 (b) shows the probability of non-zero secrecy capacity as a function of the number of antennas at Eve (L_e). For the main channel: $\kappa = 1, \mu = 2$ and for the wiretap channel $\kappa_e = 1, \mu_e = 2$. One can conclude that as the average received SNR at Eve $(\bar{\gamma}_e)$ increases or as the number of antennas increases, the secrecy is degraded. This is because higher values of $\bar{\gamma}_e$ or L_e implies better conditions in the wiretap link, which increases the chance for Eve to be able to decode the intercepted information successfully. One can note the effect of the number of antennas at Eve on the probability of non-zero secrecy capacity, where signal combining (MRC) at Eve becomes more efficient as the number of antennas gets larger. Such a problem can be solved by enhancing the average received SNR at Bob $(\bar{\gamma})$, which can be seen clearly in Figure 3.7 (a).

3.9 Physical-Layer Security with Cascaded κ-μ Fading Channels at the Main and the Wiretap Links with Multiple Colluding Eavesdroppers

In this section, PLS is investigated for the system model shown in Figure 3.8. The main and the wiretap channels are assumed to follow the cascaded κ-μ fading distribution. The transmitter Alice and Bob are equipped with a single antenna, while the eavesdropper (Eve) is equipped with multi-antennas and the receiver employs MRC technique to enhance the received SNRs. The received

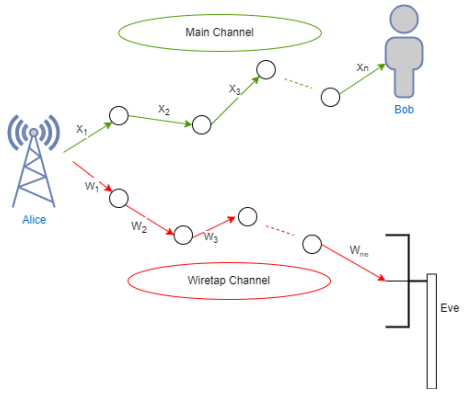

Figure 3.8: The system model/ Colluding Eavesdroppers.

signal at the legitimate receiver (Bob) was given in (3.26). The PDF and the CDF for the channel

coefficient variable (Y_n) for the main channel were derived in (3.6) and (3.9), respectively. The intercepted message at Eve is given by

$$y_{E,k} = \sqrt{P} Z_{E,k} x + w_{E,k}, \tag{3.42}$$

where $w_{E,k}$ is the AWGN at the k^{th} antenna of Eve with zero mean and variance N_0. $Z_{E,k}$ is the channel gain for the wiretap link, which is the one between Alice and the k^{th} antenna of Eve for $k = 1, 2, \cdots, L_e$. L_e is the number of antennas at Eve. $Z_{E,k}$ is defined by $Z_{E,k} = \prod_{j=1}^{n_e} W_j^{(k)}$. $W_j^{(k)}$ is a set of independent κ-μ RVs with the parameters $\kappa_{ej}^{(k)}$ and $\mu_{ej}^{(k)}$ $(j \in \{1, 2, \cdots, n_e\})$ for the k^{th} link. Hence, $Z_{E,k}$ follows the cascaded $\kappa - \mu$ fading distribution with the following PDF

$$\begin{aligned} f_{Z_{E,k}}(z_e) &= \sum_{r_1^{(k)}=0}^{\infty} \sum_{r_2^{(k)}=0}^{\infty} \cdots \sum_{r_{n_e}^{(k)}=0}^{\infty} a_2^{(k)} z_e^{2\mu_{e1}^{(k)} + 2r_1^{(k)} - 1} \\ &\times G_{n_e^{(k)}}^{0\ n_e^{(k)}} \left(\begin{matrix} \beta_e^{(k)} \\ - \end{matrix} \middle| \frac{1}{z_e^2 \prod_{j=1}^{n_e^{(k)}} \mu_{ej}^{(k)} \left(1 + \kappa_{ej}^{(k)}\right)} \right), \end{aligned} \tag{3.43}$$

where $\beta_e^{(k)} = \mu_{e1}^{(k)} - \mu_{e2}^{(k)} + r_1^{(k)} - r_2^{(k)} + 1, \cdots, \mu_{e1}^{(k)} - \mu_{en_e}^{(k)} + r_1^{(k)} - r_{n_e}^{(k)} + 1, 1$ and

$$\begin{aligned} a_2^{(k)} = 2 \prod_{j=1}^{n_e^{(k)}} & \left[\frac{\left[\mu_{ej}^{(k)} \left(1 + \kappa_{ej}^{(k)}\right)\right]^{\mu_{e1}^{(k)} - \mu_{ej}^{(k)} + r_1^{(k)} - r_j^{(k)}} \mu_{ej}^{(k)} \left[2\mu_{ej}^{(k)} \sqrt{\kappa_{ej}^{(k)} \left(1 + \kappa_{ej}^{(k)}\right)}\right]^{2r_j^{(k)} + \mu_{ej}^{(k)} - 1}}{{\kappa_{ej}^{(k)}}^{\frac{\mu_{ej}^{(k)} - 1}{2}} \exp\left(\kappa_{ej}^{(k)} \mu_{ej}^{(k)}\right) \Gamma\left(r_j^{(k)} + \mu_{ej}^{(k)}\right) (r_j^{(k)})! \, 2^{2r_j^{(k)} + \mu_{ej}^{(k)} - 1}} \right] \\ \times \prod_{j=1}^{n_e^{(k)}} & \left[\left(1 + \kappa_{ej}^{(k)}\right)^{\frac{\mu_{ej}^{(k)} + 1}{2}} \right]. \end{aligned}$$

The CDF of the RV $Z_{E,k}$ is given by

$$\begin{aligned} F_{Z_{E,k}}(z_e) &= \sum_{r_1^{(k)}=0}^{\infty} \sum_{r_2^{(k)}=0}^{\infty} \cdots \sum_{r_{n_e}^{(k)}=0}^{\infty} \frac{a_2^{(k)}}{2} z_e^{2\left(\mu_{e1}^{(k)} + r_1^{(k)}\right)} \\ &\times G_{1\ n_e^{(k)}+1}^{n_e^{(k)}\ 1} \left(\begin{matrix} 1 - \mu_{e1}^{(k)} - r_1^{(k)} \\ s^{(k)} \end{matrix} \middle| z_e^2 \prod_{j=1}^{n_e^{(k)}} \mu_{ej}^{(k)} \left(1 + \kappa_{ej}^{(k)}\right) \right), \end{aligned} \tag{3.44}$$

where $s^{(k)} = -\mu_{e1}^{(k)} + \mu_{e2}^{(k)} - r_1^{(k)} + r_2^{(k)}, \cdots, -\mu_{e1}^{(k)} + \mu_{en_e}^{(k)} - r_1^{(k)} + r_{n_e}^{(k)}, 0, -\mu_{e1} - r_1^{(k)}$. The PDF and the CDF of the received SNR at Bob were derived in (3.12) and (3.13), respectively. The eavesdropper (Eve) employs MRC over the received signals. Hence, the received SNR at Eve is given by $\gamma_E = \sum_{i=1}^{K} \gamma_{E,i} = \sum_{i=1}^{K} |Z_{E,i}|^2 \frac{P}{N_0}$. Using [92] and (3.43), the PDF of γ_E is given by

$$f_{\gamma_E}(\gamma_e) = \sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty} \frac{c_{x,e}}{2}\left(\frac{\prod_{j=1}^{n_e} E\left[X_j^2\right]}{\bar{\gamma_E} L_e}\right)^{\mu_{e1}L_e+r_1} \gamma_e^{\mu_{e1}L_e+r_1-1} \times G_{n_e\ 0}^{0\ n_e}\left(\begin{matrix}\beta_e' \\ -\end{matrix}\middle| \frac{\bar{\gamma_E} L_e}{\gamma_e \prod_{j=1}^{n_e} E\left[X_j^2\right] \mu_{ej} L_{ej} (1+\kappa_{ej})}\right), \tag{3.45}$$

where $\bar{\gamma_E}$ is the average received SNR at Eve, $\beta_e' = \mu_{e1}L_e - \mu_{e2}L_e + r_1 - r_2 + 1, \cdots, \mu_{e1}L_e - \mu_{en_e}L_e + r_1 - r_{ne} + 1, 1$, and

$$c_{x,e} = 2\prod_{j=1}^{n_e}\left[\frac{\left[2\mu_{ej}L_{ej}\sqrt{\kappa_{ej}(1+\kappa_{ej})}\right]^{2r_j+\mu_{ej}L_{ej}-1}\left[\mu_{ej}L_{ej}(1+\kappa_{ej})\right]^{\mu_{e1}L_e-\mu_{ej}L_{ej}+r_1-r_j}}{(r_j)!\, 2^{2r_j+\mu_{ej}L_{ej}-1}\kappa_{ej}^{\frac{\mu_{ej}L_{ej}-1}{2}}\exp(\kappa_{ej}\mu_{ej}L_{ej})}\right] \times \prod_{j=1}^{n_e}\left[\frac{\mu_{ej}L_{ej}(1+\kappa_{ej})^{\frac{\mu_{ej}L_{ej}+1}{2}}}{\Gamma(r_j+\mu_{ej}L_{ej})}\right].$$

To prove the accuracy of (3.45), the PDF is plotted along with Monte-Carlo simulation in Figure 3.9. Using (3.45) and [85, eq. (26)], the CDF of γ_E can be given by

$$F_{\gamma_E}(\gamma_e) = \sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty} \frac{c_{x,e}}{2}\left(\gamma_e\frac{\prod_{j=1}^{n_e} E\left[X_j^2\right]}{\bar{\gamma_E} L_e}\right)^{\mu_{e1}L_e+r_1} G_{1\ n_e+1}^{n_e\ 1}\left(\begin{matrix}\epsilon' \\ \eta_e'\end{matrix}\middle| \frac{A\gamma_e}{\bar{\gamma_E} L_e}\right), \tag{3.46}$$

where $\epsilon' = 1 - \mu_{e1}L_e - r_1$, $\eta_e' = -\mu_{e1}L_e + \mu_{e2}L_e - r_1 + r_2, \cdots, -\mu_{e1}L_e + \mu_{e'n_e}L_e - r_1 + r_{n_e}, 0, -\mu_{e1}L_e - r_1$, and $A = \prod_{j=1}^{n_e} E\left[X_j^2\right] \mu_{ej}L_{ej}(1+\kappa_{ej})$.

3.9.1 Secrecy Outage Probability

Here, the secrecy outage probability for this system model is studied. Using the definition of the lower bound of the secrecy outage probability in (3.31), one can obtain the SOP_{LB}. Using (3.13)

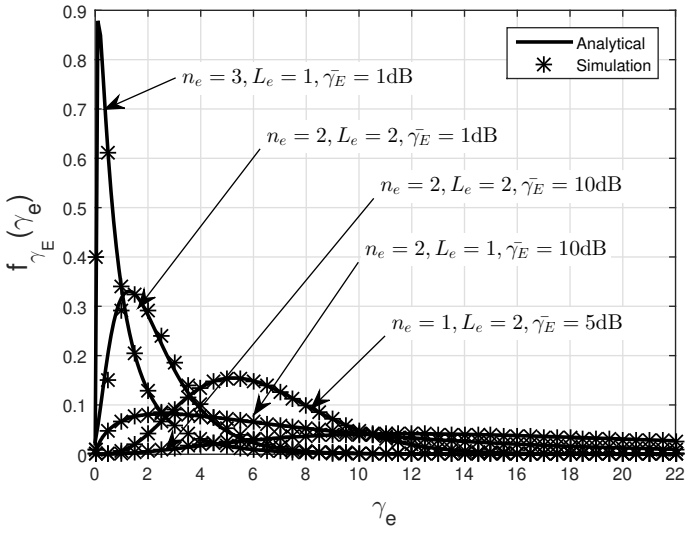

Figure 3.9: The PDF of the received SNR at the eavesdropper (γ_E) for multiple values of cascade level of the wiretap channel (n_e) and multiple number of antennas at Eve (L_e). $\kappa_e = 1$ and $\mu_e = 2$.

and (3.45) and with the help of [93, eq. (2.3.31)] and [82, eq. (7.813-1)] yields

$$SOP_{LB} = \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{ne}=0}^{\infty} c_a G_{\,n_e+1\;\;n+1}^{\;n\;\;n_e+1}\left(\begin{matrix}\xi\\ \eta'\end{matrix}\middle| U\right), \tag{3.47}$$

where $\xi = 1-\mu_1-l_1, 1-\mu_1-l_1-\mu_{e2}L_e-r_2, \cdots, 1-\mu_1-l_1-\mu_{ene}L_e-r_{n_e}, 1-\mu_{e1}L_e-r_1-\mu_1-l_1, U = \frac{2^{C_{th}}\bar{\gamma_E}L_e\prod_{i=1}^{n}E[X_i^2]\mu_i(1+\kappa_i)}{\bar{\gamma}\prod_{j=1}^{n_e}E[X_j^2]\mu_{ej}L_{ej}(1+\kappa_{ej})}$, and

$$c_a = \frac{c_x c_{x,e}}{4}2^{C_{th}(\mu_1+l_1)}\left(\frac{\prod_{i=1}^{n}E\left[X_i^2\right]}{\bar{\gamma}}\right)^{\mu_1+l_1}\left(\frac{\prod_{j=1}^{n_e}E[X_j^2]\mu_{ej}L_e\left(1+\kappa_{ej}\right)}{\bar{\gamma_E}L_e}\right)^{-\mu_{e1}L_e-r_1-\mu_1-l_1}$$
$$\times\left(\frac{\prod_{j=1}^{n_e}E[X_j^2]}{\bar{\gamma_E}L_e}\right)^{\mu_{e1}L_e+r_1}.$$

-Asymptotic Secrecy Outage Probability as $\bar{\gamma_E}\to\infty$: The asymptotic SOP_{LB} is evaluated when $\bar{\gamma_E}\to\infty$. Performing the same steps utilized to find equation (3.35), one can obtain the asymptotic SOP_{LB} as

$$SOP_{LB} \approx \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{ne}=0}^{\infty} c_a c_b\prod_{i=1}^{n}\Gamma[\mu_i+v_i]\prod_{j=1}^{n_e}\Gamma[\mu_{ej}L_e+r_j] \tag{3.48}$$

where $c_b = \left(\frac{\bar{\gamma} \prod_{j=1}^{n_e} E[X_j^2] \mu_{ej} L_{ej} (1+\kappa_{ej})}{2^{C_{th}} L_e \prod_{i=1}^{n} E[X_i^2] \mu_i (1+\kappa_i)} \right)^{\mu_1 + l_1}$. One can notice from (3.48) that the diversity order is zero, which means that the secrecy cannot be achieved at all when the wiretap channel's conditions are highly improved ($\bar{\gamma_E} \to \infty$) and Eve will be able to overhear the confidential information.

-Asymptotic Secrecy Outage Probability as $\bar{\gamma} \to \infty$***:*** We assess the impact of having very reliable conditions on the main link in terms of the average received SNR over the security. That is, the asymptotic SOP_{LB} as $\bar{\gamma} \to \infty$ is evaluated. The secrecy outage probability in (3.32) can be rewritten as

$$SOP_{LB} = \sum_{l_1=0}^{\infty} \sum_{l_2=0}^{\infty} \cdots \sum_{l_n=0}^{\infty} \sum_{r_1=0}^{\infty} \sum_{r_2=0}^{\infty} \cdots \sum_{r_{n_e}=0}^{\infty} \frac{c_a c_d^{-\mu_1 - l_1}}{2\pi i} \times \int_C \frac{\prod_{j=1}^{n} \Gamma[\mu_j + l_j - s] \Gamma[s] \prod_{j=1}^{n_e} \Gamma[\mu_{ej} K_j + r_j + s] \Gamma[s]}{\Gamma[1+s]} M^s ds, \tag{3.49}$$

where $c_d = \frac{2^{C_{th}} \bar{\gamma_E} K \prod_{i=1}^{n} E[X_i^2] \mu_i (1+\kappa_i)}{\prod_{j=1}^{n_e} \mu_{ej} K_j (1+\kappa_{ej})}$ and $M = \frac{c_d}{\bar{\gamma}}$. Similar to the previous section, using the residue method [89], the asymptotic secrecy outage probability can be finally given by

$$SOP_{LB} \approx \sum_{l_1=0}^{\infty} \sum_{l_2=0}^{\infty} \cdots \sum_{l_n=0}^{\infty} \sum_{r_1=0}^{\infty} \sum_{r_2=0}^{\infty} \cdots \sum_{r_{n_e}=0}^{\infty} c_a c_d^{-\mu_1 - l_1} \prod_{j=1, j \neq I}^{n} \Gamma[\mu_j + l_j - \mu_I - l_I] \times \prod_{j=1}^{n_e} \Gamma[\mu_{ej} K_j + r_j + \mu_I + l_I] M^{\mu_I + l_I}, \tag{3.50}$$

where $\mu_I + l_I = \min(\mu_j + l_j)$, for $j = 1, 2, \cdots, n$, which represents the minimum pole at which the residue method is evaluated.

3.9.2 Probability of Non-Zero Secrecy Capacity

Using the definition of the probability of non-zero secrecy capacity in (3.37), P_r^{nzc} for this system model can be mathematically defined as

$$P_r^{nzc} = P_r(C_s > 0) = P_r(\gamma > \gamma_E) = F_{\frac{\gamma_E}{\gamma}}(1) \cdot \tag{3.51}$$

To find the probability of non-zero secrecy capacity, some mathematical manipulations are performed over equation (3.45) as

$$f_{\gamma_E}(\gamma_e) = \sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{ne}=0}^{\infty}\frac{c_{x,e}\prod_{j=1}^{n_e}E[X_j^2]}{2\bar{\gamma_E}L_e\left(\prod_{j=1}^{n_e}\mu_{ej}L_{ej}(1+\kappa_{ej})\right)^{\mu_{e1}L_e+r_1-1}} \times H_{0\ n_e}^{n_e\ 0}\left(\bar{P}\left|\frac{\gamma_e\prod_{j=1}^{n_e}E[X_j^2]\mu_{ej}L_{ej}(1+\kappa_{ej})}{\bar{\gamma_E}L_e}\right.\right), \tag{3.52}$$

where $P = \{\mu_{e2}L_e + r_2 - 1, 1\}, \cdots, \{\mu_{e_{ne}}L_e + r_{n_e} - 1, 1\}, \{\mu_{e1}L_e + r_1 - 1, 1\}$. Using (3.38) and (3.52), $f_{\frac{\gamma_E}{\gamma}}(\gamma)$ can be expressed as

$$f_{\frac{\gamma_E}{\gamma}}(y) = \sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{ne}=0}^{\infty}\sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\frac{c_{x,e}c_x\prod_{j=1}^{n_e}E[X_j^2]}{2\bar{\gamma_E}L_e\left(\prod_{j=1}^{n_e}\mu_{ej}L_{ej}(1+\kappa_{ej})\right)^{\mu_{e1}L_e+r_1-1}} \times H_{n\ n_e}^{n_e\ n}\left(P\left|\frac{\bar{\gamma}\prod_{j=1}^{n_e}E[X_j^2]\mu_{ej}L_{ej}(1+\kappa_{ej})}{\bar{\gamma_E}L_e\prod_{i=1}^{n}E\left[X_i^2\right]\mu_i(1+\kappa_i)}y\right.\right) \times \frac{\bar{\gamma}}{2\prod_{i=1}^{n}E[X_i^2]\left(\prod_{i=1}^{n}\mu_i(1+\kappa_i)\right)^{\mu_1+l_1+1}}, \tag{3.53}$$

where $\delta' = \{-\mu_2 - l_2, 1\}, \cdots, \{-\mu_n - l_n, 1\}, \{-\mu_1 - l_1, 1\}$. Using (3.53) and [88], P_r^{nzc} can be found as

$$P_r^{nzc} = 1 - \sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{ne}=0}^{\infty}\sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\frac{c_{x,e}c_x\prod_{j=1}^{n_e}E[X_j^2]}{4\prod_{i=1}^{n}E[X_i^2]\left(\prod_{j=1}^{n_e}\mu_{ej}L_{ej}(1+\kappa_{ej})\right)^{\mu_{e1}L_e+r_1}} \times \frac{1}{\left(\prod_{i=1}^{n}\mu_i(1+\kappa_i)\right)^{\mu_1+l_1}}H_{n+1\ n_e+1}^{n_e+1\ n}\left(\begin{matrix}\psi\\ \psi'\end{matrix}\left|\frac{\bar{\gamma}\prod_{j=1}^{n_e}E[X_j^2]\mu_{ej}L_{ej}(1+\kappa_{ej})}{\bar{\gamma_E}L_e\prod_{i=1}^{n}E\left[X_i^2\right]\mu_i(1+\kappa_i)}\right.\right), \tag{3.54}$$

where $\psi = \{-\mu_2 - l_2 + 1, 1\}, \cdots, \{-\mu_n - l_n + 1, 1\}, \{-\mu_1 - l_1 + 1, 1\}, \{1, 1\}$ and $\psi' = \{0, 1\}, \{\mu_{e2}L_e + r_2, 1\}, \cdots, \{\mu_{e_{ne}}L_e + r_{n_e}, 1\}, \{\mu_{e1}L_e + r_1, 1\}$.

-Asymptotic Probability of Non-Zero Secrecy Capacity as $\bar{\gamma_E} \to \infty$: The asymptotic P_r^{nzc} is evaluated when $\bar{\gamma_E} \to \infty$ to notice the effect of improving the wiretap channel's conditions over the secrecy. Following the same procedure utilized to find the asymptotic secrecy outage probability,

the asymptotic probability of non-zero secrecy capacity can be expressed as

$$P_r^{nzc} \approx 1 - \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty} c_{x,e}c_x c_c \prod_{i=1}^{n}\Gamma[\mu_i + v_i]\prod_{j=1}^{n_e}\Gamma[\mu_{ej}L_e + r_j], \tag{3.55}$$

where $c_c = \frac{\prod_{j=1}^{n_e} E[X_j^2]}{4\prod_{i=1}^{n} E[X_i^2]\left(\prod_{j=1}^{n_e}\mu_{ej}L_{e_j}(1+\kappa_{ej})\right)^{\mu_{e1}L_e+r_1}\left(\prod_{i=1}^{n}\mu_i(1+\kappa_i)\right)^{\mu_1+l_1}}$. Equation (3.55) proves that no secrecy can be achieved when the average received SNR at Eve is very high and the wiretap channel's conditions are extremely good in terms of the average received SNR. This is possible if the eavesdropper is very close to the transmitter, which makes the eavesdropper strongly capable of successfully decoding the intercepted information.

3.9.3 Intercept Probability

The intercept probability (P_{int}) estimates the probability that the eavesdropper is able to intercept the information. This occurs when the wiretap channel conditions are more reliable than the main channel conditions. Mathematically, P_{int} is expressed as

$$P_{int} = P_r\left(C_s < 0\right) = P_r\left(\gamma < \gamma_E\right) = 1 - P_r^{nzc}. \tag{3.56}$$

Substituting (3.54) and (3.55) into (3.56) yields the exact and asymptotic intercept probability, respectively. It is worth mentioning that while the probability of non-zero secrecy capacity highlights the reliability level of the main channel, the intercept probability measures the intercept capabilities of the eavesdropper instead. This aids in comprehending the security implications of both channels.

3.10 Numerical Results

In this section, analytical results are presented along with simulations. The analytical curves are plotted by truncating the infinite series expansion indices (l and r) to the first 20 terms.

Figure 3.10 shows the secrecy outage probability versus the average received SNR at Bob $(\bar{\gamma})$. In this figure, setting the fading channel parameters for the main and the wiretap channels to $\kappa = 0$ and $\mu = 1$ results in the Rayleigh fading as a special case of the κ-μ fading model. The impact

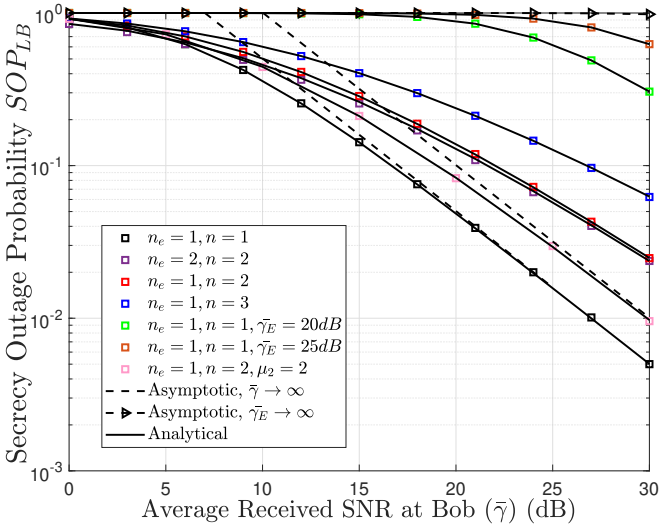

Figure 3.10: The lower bound of the secrecy outage probability (OP_{sec}^{L}) versus the average received SNR at Bob $(\bar{\gamma})$. For the main channel: $\kappa = 0, \mu = 1$ and for the wiretap channel: $\kappa_e = 0, \mu_e = 1$ (Rayleigh). $C_{th} = 1$, $L_e = 2$, and $\bar{\gamma_E} = 1$ dB.

of the cascade levels (number of keyholes) for the main channel (n) and for the wiretap channel (n_e) is provided in this figure. Indeed, privacy worsens as the cascade level grows in the main channel or reduces in the wiretap channel. The fact is that a greater n signifies a larger number of scatters and obstacles in the main channel, resulting in a more severe fading. Additionally, it is noted that the probability of an outage in the security of the transmitted messages is higher as the eavesdropper channel's circumstances improve by increasing the average received SNR $(\bar{\gamma_E})$. Moreover, the figure includes the asymptotic secrecy outage probability derived in (3.48) as $\bar{\gamma_E}$ becomes very high. At the highest value of $\bar{\gamma_E}$, a zero slope appears and a value of one for the secrecy outage probability is provided. This demonstrates that for these parameters, the secrecy is completely compromised and the information will be certainly intercepted by E irrespective of the value of $\bar{\gamma}$. Finally, the results show that the information may be delivered more securely regardless of the cascade levels as the main channel conditions improve in terms of $\bar{\gamma}$. Finally, the asymptotic secrecy outage probability derived in (3.50) as $\bar{\gamma} \to \infty$ is included and it is clear that it matches the results as $\bar{\gamma}$ takes high values.

Figure 3.11 depicts the effect of varying the number of antennas at the eavesdropper (L_e) over the security. It can be seen that increasing the number of antennas improves the eavesdropper's

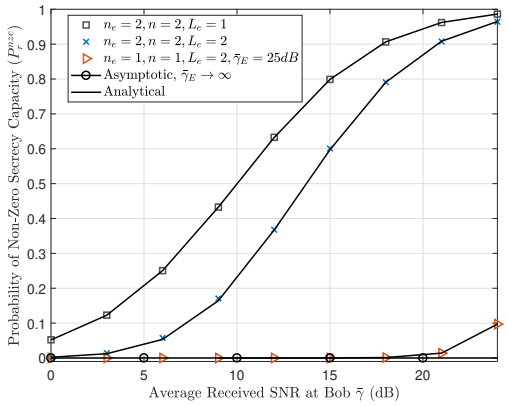

Figure 3.11: The probability of non-zero secrecy capacity (P_r^{nzc}) versus the average received SNR at Bob $(\bar{\gamma})$. For the main channel: $\kappa = 1, \mu = 2$ and for the wiretap channel: $\kappa_e = 1, \mu_e = 2$. $\bar{\gamma_E} = 10$ dB.

reception capabilities and aids in effectively decoding the tapped messages owing to the use of the MRC method. Hence, the shared information's privacy is compromised. Additionally, the figure illustrates that improving the wiretap channel conditions in terms of the average received SNR at the eavesdropper $(\bar{\gamma_E})$ will eventually result in an extremely low probability of non-zero secrecy capacity. This indicates the P_r^{nzc} asymptotic case derived in (3.55). However, the privacy of shared information may be enhanced by raising the value of $\bar{\gamma}$, which can be achieved by having fewer scatters (n) obstructing the main channel path.

To take the path loss effect over the secrecy into considerations, in Figure 3.13, we consider the Rayleigh fading as a special case of the κ-μ distribution for $n = 2$ and $n_e = 1$. As shown in the two-dimensional (2D) graph in Figure 3.12, assume that the transmitter Alice (A) is the reference location. That is, Alice is located at $(0, 0)$ and the other receivers $(B$ and $E)$ have different distances from Alice, with B stands for the legitimate receiver Bob and E stands for the eavesdropper. Assume $d_{XY}^{-PL} = \frac{1}{2\lambda_J}$, with PL is the path loss exponent, $X \in \{A, p_1, p_2, \cdots\}$, $Y \in \{B, E, p_1, p_2, \cdots\}$, and $J \in \{B, E\}$. $\lambda_J = \frac{1}{2\sigma_J^2}$ is the Rayleigh fading parameter and σ_J is the scale parameter of the distribution. d_{XY} represents the distance from node X to node Y in meters (m). p_i (for $i = 1, 2, \cdots, n-1$) are the locations of the obstacles in the main channel. This is to notice the effect of the cascade level between A and B. It is concluded from Figure 3.13 that regardless of the number of antennas at the eavesdropper and the effectiveness of the MRC

technique, as the eavesdropper moves further away from the transmitter Alice, i.e., d_{AE} becomes larger, the privacy of the transferred information improves. This can be interpreted by the fact that as d_{AE} rises, the wiretap channel's conditions worsen and the received SNR at the eavesdropper deteriorates accordingly. This graph demonstrates the importance of considering the impact of distances between nodes on privacy.

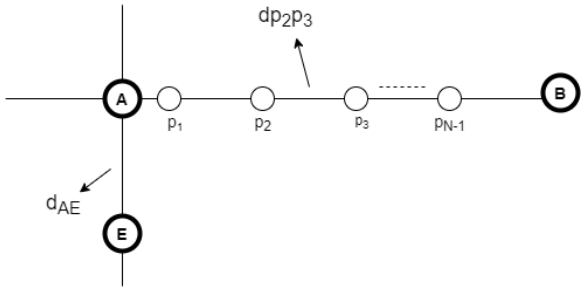

Figure 3.12: The 2D graph.

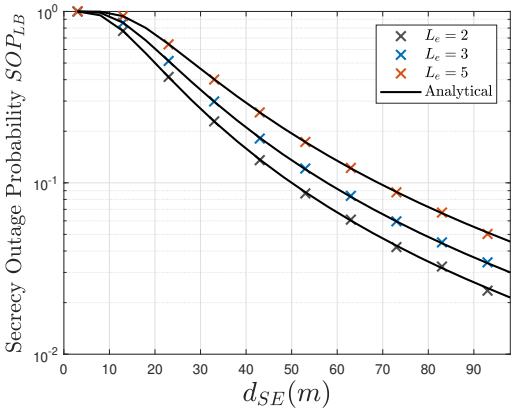

Figure 3.13: The lower bound of the secrecy outage probability (SOP_{LB}) versus the distance between Alice and the eavesdropper for different number of antennas L_e. For the main channel: $\kappa = 0, \mu = 1$ and for the wiretap channel: $\kappa_e = 0, \mu_e = 1$. $\bar{\gamma_E} = 1$ dB, $\bar{\gamma} = 10$ dB, $C_{th} = 1$, $n = 2$, $n_e = 1$, $PL = 3$, $d_{Ap_1} = 5m$, and $d_{p_1B} = 5m$.

3.11 PLS with Cascaded κ-μ Fading Channels at the Main and the Wiretap Links with Multiple Non-Colluding Eavesdroppers

This section considers the third scenario, in which the eavesdroppers are expected to process the intercepted information independently without the messages being jointly processed. In this context,

the eavesdroppers' locations are assumed to be random according to a homogeneous Poisson point process (HPPP) with a density of λ_e, as shown in Fig. 3.14. We assume that the eavesdroppers are distributed in an unbounded Euclidean space of dimension U. The eavesdroppers' information regarding the positions related to Alice can be obtained by assuming that the eavesdroppers are users in the network but they are untrusted and do not have the authorization to access the channel [94], [95]. Our analyses are based on selecting the k^{th} closest eavesdropper to the transmitter Alice, once the distances between Alice and the eavesdroppers have been ordered in an ascending matter [57].

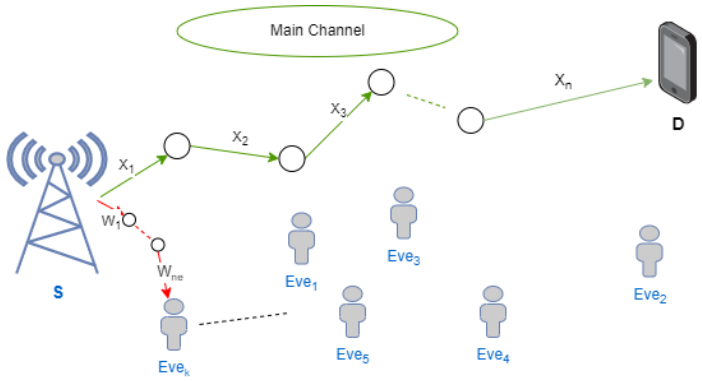

Figure 3.14: The system model/ Non-Colluding Eavesdroppers.

3.11.1 Probability of Non-Zero Secrecy Capacity

To explore the physical-layer security for the three-node wiretap system model under the threat of non-colluding eavesdroppers, the probability of non-zero secrecy capacity and the intercept probability are utilized. From (3.37), the probability of non-zero secrecy capacity is expressed as

$$P_r^{nzc} = 1 - \int_0^{\infty} F_{\gamma}(y) f_Y(y) dy, \tag{3.57}$$

where $Y = \frac{\gamma_E}{d^{PL}}$, with d is the distance between the transmitter (Alice) and the k^{th} closest eavesdropper and PL is the path loss exponent. The PDF of the path loss d^{PL} is distributed as [96]

$$f_{d^{PL}}(x) \quad = \quad \exp\left(-A_e x^{\delta}\right) \frac{\delta A_e^k x^{\delta k - 1}}{\Gamma(k)}, \tag{3.58}$$

where $A_e = \pi\lambda_e$, $\delta = \frac{U}{PL}$, and $\Gamma(\cdot)$ is the gamma function. First, one needs to obtain the PDF of Y as

$$f_Y(y) = \int_0^\infty y_b f_{\gamma_E}(y y_b) f_{d^{PL}}(y_b) dy_b. \tag{3.59}$$

Substituting (3.45) and (3.58) and with the help of [83, Eq. (2.24.3.1)] yields

$$f_Y(y) = \sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty} C_1 y^{-1-\delta k} G_{\delta n_e}^{1\ \delta n_e}_{1} \left(\begin{matrix} F \\ F' \end{matrix} \middle| \frac{A_e \delta^{\delta n_e} (\bar{\gamma_E} L_e)^{\delta}}{y^{\delta}\left(\prod_{j=1}^{n_e} E\left[X_j^2\right] \mu_{ej} L_{e_j} (1+\kappa_{ej})\right)^{\delta}} \right), \tag{3.60}$$

where

$$C_1 = \left(\frac{\prod_{j=1}^{n_e} E\left[X_j^2\right]}{\bar{\gamma_E} L_e}\right)^{\mu_{e1}L_e + r_1} \frac{c_{x,e} A_e^k \delta^{n_e(\delta k + \mu_{e1}L_e + r_1) + \rho_{th}^*}}{2\Gamma(k)(2\pi)^{\frac{(\delta-1)n_e}{2}}} \times \left(\frac{\prod_{j=1}^{n_e} E\left[X_j^2\right] \mu_{ej} L_{e_j} (1+\kappa_{ej})}{\bar{\gamma_E} L_e}\right)^{-\delta k - \mu_{e1}L_e - r_1},$$

$F = \frac{1-\delta k-\mu_{e2}L_e-r_2}{\delta}, \cdots, \frac{1-\delta k-\mu_{ene}L_e-r_{ne}}{\delta}, \frac{1-\delta k-\mu_{e1}L_e-r_1}{\delta}$, $F' = 0$, and $\rho_{th}^* = \sum_{j=1}^{n_e} 1 - \beta_e' + 1 - \frac{n_e}{2}$. Using (3.60), (3.13), and [83, Eq. (2.24.3.1)], the probability of non-zero secrecy capacity given in (3.57) is solved as

$$P_r^{nzc} = 1 - \sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{ne}=0}^{\infty}\sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty} C_2 G_{\delta n+1+\delta\ \delta n_e+\delta}^{\delta n_e+\delta\ \delta n+1} \left(\begin{matrix} \zeta \\ \zeta' \end{matrix} \middle| \phi \right), \tag{3.61}$$

where

$$C_2 = \frac{C_1 a_1}{2} \left(\frac{\prod_{i=1}^{n} E\left[X_i^2\right]}{\bar{\gamma}}\right)^{\mu_1+v_1} \frac{\delta^{n(\mu_1+v_1-\delta k)-1+q}}{(2\pi)^{\frac{(\delta-1)n}{2}}} \left(\frac{\prod_{i=1}^{n} E\left[X_i^2\right] \mu_i (1+\kappa_i)}{\bar{\gamma}}\right)^{\delta k-\mu_1-l_1},$$

$q = \sum_{j=1}^{n+1} \rho + \mu_1 + v_1 - \frac{n}{2}$, $\zeta = 1, \frac{1+\delta k-\mu_2-l_2}{\delta}, \cdots, \frac{1+\delta k-\mu_n-l_n}{\delta}, \frac{1+\delta k-\mu_1-l_1}{\delta}, \frac{1+\delta k}{\delta}$, $\zeta' =$

$1-F$, k, and $\phi = \dfrac{\frac{\left(\prod_{j=1}^{n_e} E\left[X_j^2\right]\mu_{ej}L_{e_j}\left(1+\kappa_{ej}\right)\right)^{\delta}}{A_e\delta^{\delta n_e}\left(\bar{\gamma_E}L_e\right)^{\delta}}}{\left(\frac{\prod_{i=1}^{n} E\left[X_i^2\right]\mu_i(1+\kappa_i)}{\bar{\gamma}}\right)^{\delta}}$.

-Asymptotic probability of non-zero secrecy capacity as $\bar{\gamma_E} \to \infty$**:** Here, the security is evaluated as the wiretap channel's conditions are extremely strong. Particularly, we evaluate the probability of non-zero secrecy capacity as $\bar{\gamma_E} \to \infty$. Hence, (3.61) is rewritten as

$$\begin{aligned} P_r^{nzc} &= 1 - \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty}\frac{C_2 c_f^k}{2\pi j} \\ &\times \int_C \frac{\prod_{j=1}^{\delta n_e}\Gamma\left[-k+\frac{\delta k+\mu_{ej}L_{e_j}+r_j}{\delta}-s\right]\Gamma[-s]\prod_{j=1}^{\delta n}\Gamma\left[1+k+\frac{-1-\delta k+\mu_j+r_j}{\delta}+s\right]}{\Gamma\left[\frac{1}{\delta}+s\right]} \\ &\times \Gamma[k+s]T^s ds, \end{aligned} \tag{3.62}$$

where $c_f = \dfrac{\frac{\left(\prod_{j=1}^{n_e} E\left[X_j^2\right]\mu_{ej}L_{e_j}\left(1+\kappa_{ej}\right)\right)^{\delta}}{A_e\delta^{\delta n_e}\left(\bar{\gamma_E}L_e\right)^{\delta}}}{\left(\prod_{i=1}^{n} E\left[X_i^2\right]\mu_i(1+\kappa_i)\right)^{\delta}}$ and $T = \frac{c_f}{\bar{\gamma_E}^{\delta}}$. Using the residue method [89], the probability of non-zero secrecy capacity can be finally approximated as

$$\begin{aligned} P_r^{nzc} &\approx 1 - \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty} C_2 c_f^k \prod_{j=1}^{n}\Gamma\left[1-\frac{1}{\delta}+\frac{\mu_j+l_j}{\delta}\right] \\ &\times \prod_{j=1}^{\delta n_e}\Gamma\left[\frac{\mu_{ej}L_{e_j}+r_j}{\delta}\right]\frac{\Gamma[k]}{\Gamma[1/\delta]}. \end{aligned} \tag{3.63}$$

It is worth mentioning that according to (3.63), the security is independent of the average received SNR at the eavesdropper $(\bar{\gamma_E})$. This indicates that the probability of achieving a positive secrecy capacity under such conditions is extremely low. This represents the scenario where the wiretap channel is very reliable and the eavesdropper has a very strong reception level as opposed to the legitimate receiver reception quality.

3.11.2 Intercept Probability

Intercept probability is evaluated with the help of (3.61) as

$$P_{int} = 1 - P_r^{nzc}. \tag{3.64}$$

Moreover, the asymptotic P_{int} can be directly attained from (3.63) as $\bar{\gamma_E} \to \infty$.

3.12 Numerical Results

In this section, the results along with Monte-Carlo simulations are given. The analytical curves are plotted by truncating the infinite series summations (l and r) to the first twenty terms.

Figure 3.15 illustrates the intercept probability (P_{int}) versus the density of eavesdroppers (λ_e) for two different values of k, in which k represents the selection of the closest eavesdropper. For example, $k = 1$ denotes choosing the first nearest eavesdropper to the transmitter, and thus the wiretap channel will be the one between Alice and this selected eavesdropper. We assume a 2D area ($U = 2$) and we generate 10^5 realizations of the positions of the eavesdroppers in a square area of 100 m^2. The figure shows that the probability of the information interception grows as the density of eavesdroppers increases. This is owing to the fact that the probability of a more harmful eavesdropper is rising as the λ_e grows. That is, as λ_e rises, there is a greater probability of having a closer eavesdropper to Alice. Additionally, the privacy of the shared information is under a higher risk when selecting the first closest eavesdropper ($k = 1$) as opposed to selecting the second closest one ($k = 2$). The reason is that the first closest eavesdropper is more probable to have better channel conditions compared to the other farther eavesdroppers. This figure proves the significance of considering random locations for the eavesdroppers, rather than being fixed at specific locations and distances from the transmitter.

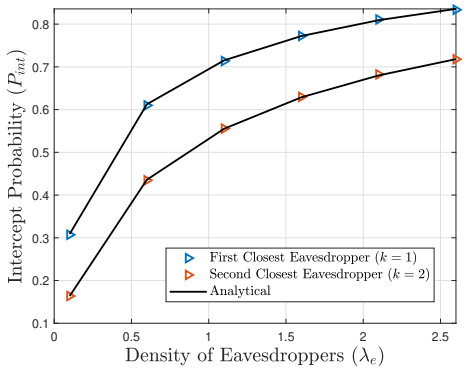

Figure 3.15: The intercept probability (P_{int}) versus the density of the eavesdropper for different values of k. For the main channel: $\kappa = 1, \mu = 1$ and for the wiretap channel: $\kappa_e = 1, \mu_e = 1$. $\bar{\gamma_E} = 1$ dB, $\bar{\gamma} = 5$ dB, $n = 2$, $n_e = 2$, $PL = 2$, $L_e = 1$.

Figure 3.16 presents a comparison between colluding and non-colluding eavesdroppers with a density of $\lambda_e = 0.1$. In the case of non-colluding eavesdroppers, the security declines as the number of antennas rise. Moreover, comparing the case of non-colluding eavesdroppers for $L_e = 2$ with the colluding eavesdroppers case, it is noted that although the number of non-colluding eavesdroppers is greater, the interception and decoding ability of the colluding eavesdroppers is stronger. Hence, the privacy of information is more vulnerable when colluding eavesdroppers exist in the network. This leads to the realization that further countermeasures should be adopted at the main channel in the presence of colluding eavesdroppers.

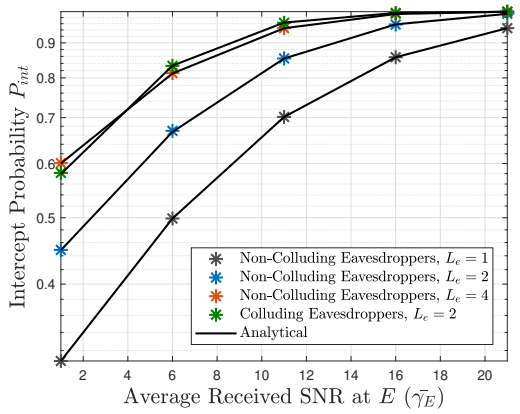

Figure 3.16: The intercept probability (P_{int}) versus the average received SNR at the eavesdropper. For the main channel: $\kappa = 1, \mu = 1$ and for the wiretap channel: $\kappa_e = 1, \mu_e = 1$. $\bar{\gamma} = 5$ dB, $n = 2$, $n_e = 1$, $PL = 2$, $\lambda_e = 0.1$, and $k = 1$.

As a final investigation, Figure 3.17 demonstrates the probability of non-zero secrecy capacity for different values of the average received SNR at the eavesdropper $(\bar{\gamma_E})$ for the non-colluding eavesdroppers case. The results clearly demonstrate how the system's privacy behaves as the eavesdroppers' channel quality improves. Particularly, fixing the legitimate receiver received SNR, the privacy of the shared information is severely compromised as $\bar{\gamma_E}$ takes high values. After a certain limit, the P_r^{nzc} approaches its asymptotic degree, i.e., lowest value. That is, the curve reaches a value of zero as $\bar{\gamma_E} \to \infty$. Indeed, this is in agreement with the asymptotic results obtained in (3.63).

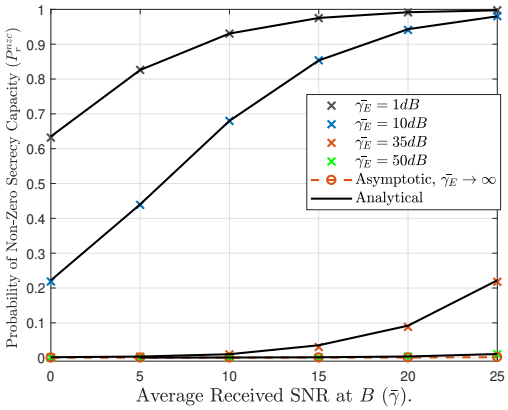

Figure 3.17: The probability of non-zero secrecy capacity (P_r^{nzc}) for different values of the average received SNR at the eavesdropper $(\bar{\gamma_E})$. For the main channel: $\kappa = 2, \mu = 2$ and for the wiretap channel: $\kappa_e = 0, \mu_e = 1$. $n = 2$, $n_e = 1$, $L_e = 1$, $PL = 2$, $\lambda_e = 0.1$, and $k = 1$.

3.13 PLS on MRC for SIMO CRNs

Due to the fixed spectrum allocation policies, the need for CRNs have increased accordingly [11], [97]. CRNs have been proposed as a promising approach to address the problem of under-utilization and scarcity of the spectrum [98]. In CRNs, SUs access the licensed spectrum of the PUs using underlay, overlay, or interweave paradigms [99]. SUs can access the spectrum band simultaneously with the PUs in underlay access mode provided that the SUs' transmission power does not cause an interference to the PUs' communication [100]. In this case, SUs should keep monitoring the interference level that the PU receiver can tolerate and adjusting the transmission power accordingly. However, varying the transmission power may lead to some threats to the privacy of the information transfer of CRNs. Therefore, PLS has recently emerged as a reliable method to protect the confidentiality of the SUs' transmission against attacks [101], [102], especially for the underlay model [99]. In addition, vehicular communication has been established to provide reliable communication for vehicle-to-vehicle (V2V) and for vehicle-to-infrastructure (V2I) systems. However, the demands for vehicle communication are growing exponentially and the band allocated for vehicular communication may not satisfy the demands of vehicular users. Hence, cognitive vehicular networks (CVNs) have been developed in order to provide a reliable approach to tackle these challenges [103]. In CVNs, all devices are moving and presumably reside in scattered areas [10], [104].

Prior studies have assumed that the channels in CVNs are modeled as classical fading channels, such as the Rayleigh fading model. However, experimental studies indicate that the cascaded channels are more appropriate than other non-cascaded channels for modelling these types of networks [10].

In the following two sections, we explore the PLS for an underlay CRN with the presence of eavesdroppers. In the first system model, we assume a SIMO CRN over cascaded κ-μ fading channels. However, in the following section, we take a special case of this scenario, where we assume a single-input-single-output (SISO) operating over cascaded Rayleigh fading channels. We also prove the accuracy of our general system model by generating the second scenario by alternating certain system parameters.

3.13.1 System Model and PLS Analysis

Consider a SIMO CVN represented by Fig. 3.18, in which there is a stationary PU receiver (P_R) and moving SUs. A similar CVN system model can represent a PU destination which is a roadside infrastructure and SUs represent moving vehicles [103], [10]. The SU transmitter (S) is communicating with a SU receiver (D) over the main channel, which follows a cascaded κ-μ fading model. An eavesdropper (E) is attempting to intercept the confidential information transmitted by S through the wiretap channel. In addition, the SUs are attempting to access the licensed band occupied by PUsrs through the underlay mode. The transmitter S should avoid degrading the quality of the PUs' communication by respecting the interference threshold that the PU receiver (P_R) can tolerate. The PU transmitter is assumed to be located far away from the SUs network and the eavesdropper and its impact over the SUs' communication is ignored [68]. To investigate the system in its worst-case conditions, the main channel is assumed to follow a cascaded κ-μ fading model with the cascade level n, while the wiretap channel follows a single κ-μ fading distribution and the channel between S and P_R follows a Rayleigh fading model [7]. Furthermore, both D and E receivers employ L and L_e antennas, respectively and they both implement the MRC technique.

The received message at the k^{th} antenna of SU destination (D) is given by

$$y_D^{(k)} = \sqrt{P_s} h_{SD}^{(k)} x_s + n_D^{(k)}, \tag{3.65}$$

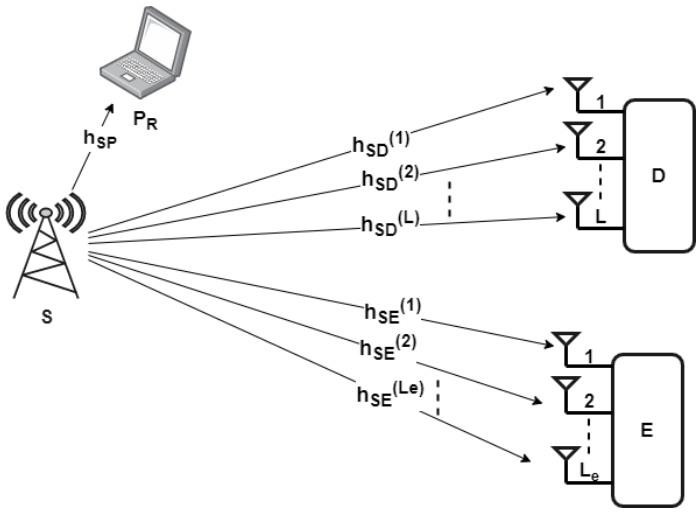

Figure 3.18: The system model.

where P_s is the transmit power at S, $h_{SD}^{(k)}$ is the channel gain from the transmitter to the k^{th} antenna at D, x_s is the transmitted symbol, and $n_D^{(k)}$ is the additive-white-Gaussian-noise (AWGN) at the k^{th} antenna of D with zero mean and variance N_0. Moreover, the intercepted message at the w^{th} antenna of the eavesdropper E is given by

$$y_E^{(w)} = \sqrt{P_s} h_{SE}^{(w)} x_s + n_E^{(w)}, \tag{3.66}$$

where $h_{SE}^{(w)}$ is the channel gain from the transmitter to the w^{th} antenna at E and $n_E^{(w)}$ is the AWGN at the w^{th} antenna with zero mean and variance N_0. Considering the underlayed CRN, node S should ensure that the transmitting power (P_s) will not exceed an interference level (I_{th}) that the PU receiver P_R can tolerate as

$$P_s \leq \frac{I_{th}}{|h_{SP}|^2}, \tag{3.67}$$

where $|h_{SP}|^2$ is the channel power gain of S and P_R link. Using (3.65)-(3.67), the instantaneous received SNRs at D and E are expressed, respectively, as

$$\gamma_D = \frac{I_{th} \sum_{k=1}^{L} \left| h_{SD}^{(k)} \right|^2}{N_0 \left| h_{SP} \right|^2}, \tag{3.68}$$

$$\gamma_E = \frac{I_{th}\sum_{w=1}^{L_e}\left|h_{SE}^{(w)}\right|^2}{N_0\left|h_{SP}\right|^2}, \tag{3.69}$$

where L and L_e are the number of antennas at D and E, respectively. As mentioned earlier, the main channel follows the cascaded κ-μ fading model. Hence, let $h_{SD}^{(k)} = \prod_{j=1}^{n} z_j^{(k)}$, where z_j follows the κ-μ fading model [35] for $k = 1, 2, \cdots, L$. κ_j and μ_j (for $j = 1, 2, \cdots, n$) are the fading channel parameters for the random variable z_j, $h_{SD}^{(k)}$ is the channel gain from the transmitter to the k^{th} antenna generated by the multiplication of n of κ-μ random variables that are independent, but not necessarily identically distributed. Hence, the PDF of $h_{SD}^{(k)}$ follows the cascaded fading distribution as [7]

$$\begin{aligned} f_{h_{SD}}^{(k)}(x) &= \sum_{r_1^{(k)}=0}^{\infty}\sum_{r_2^{(k)}=0}^{\infty}\cdots\sum_{r_n^{(k)}=0}^{\infty} a_1^{(k)} x^{2\mu_1^{(k)}+2r_1^{(k)}-1} \\ &\quad\times G_{n^{(k)}\ 0}^{\ 0\ n^{(k)}}\left(\begin{matrix}\beta^{(k)}\\ -\end{matrix}\middle|\frac{1}{x^2\prod_{j=1}^{n^{(k)}}\mu_j^{(k)}\left(1+\kappa_j^{(k)}\right)}\right), \end{aligned} \tag{3.70}$$

where $G_{p\ q}^{\ m\ n}\left(\begin{smallmatrix}a_r\\ b_s\end{smallmatrix}\middle|z\right)$ is the Meijer G-function defined in [82, Eq. 9-301], $\beta^{(k)} = \mu_1^{(k)} - \mu_2^{(k)} + r_1^{(k)} - r_2^{(k)} + 1, \cdots, \mu_1^{(k)} - \mu_n^{(k)} + r_1^{(k)} - r_n^{(k)} + 1, 1$

and

$$\begin{aligned} a_1^{(k)} = 2\prod_{j=1}^{n^{(k)}}&\left[\frac{\left[\mu_j^{(k)}\left(1+\kappa_j^{(k)}\right)\right]^{\mu_1^{(k)}-\mu_j^{(k)}+r_1^{(k)}-r_j^{(k)}}\left(2\mu_j^{(k)}\sqrt{\kappa_j^{(k)}\left(1+\kappa_j^{(k)}\right)}\right)^{2r_j^{(k)}+\mu_j^{(k)}-1}}{{\kappa_j^{(k)}}^{\frac{\mu_j^{(k)}-1}{2}}\exp\left(\kappa_j^{(k)}\mu_j^{(k)}\right)(r_j^{(k)})!\,2^{2r_j^{(k)}+\mu_j^{(k)}-1}}\right] \\ \times\prod_{j=1}^{n^{(k)}}&\left[\frac{\mu_j^{(k)}\left(1+\kappa_j^{(k)}\right)^{\frac{\mu_j^{(k)}+1}{2}}}{\Gamma\left(r_j^{(k)}+\mu_j^{(k)}\right)}\right], \end{aligned}$$

and $\Gamma(\cdot)$ is the gamma function defined in [82, Eq. 8.310.1]. The SU destination (D) employs MRC over the received signals. Hence, using (3.6) and [92], the PDF of $H_{SD} = \sum_{k=1}^{L}\left|h_{SD}^{(k)}\right|^2$ is given

by

$$f_{H_{SD}}(x) = \sum_{r_1=0}^{\infty} \sum_{r_2=0}^{\infty} \cdots \sum_{r_n=0}^{\infty} \frac{c_x}{2L^{\mu_1 L + r_1}} G_{n\ 0}^{0\ n} \left(\begin{matrix} \beta' \\ - \end{matrix} \middle| \frac{L}{x \prod_{j=1}^{n} \mu_j L_j \left(1+\kappa_j\right)} \right) x^{\mu_1 L + r_1 - 1}, \quad (3.71)$$

where $\beta' = \mu_1 L - \mu_2 L + r_1 - r_2 + 1, \cdots, \mu_1 L - \mu_n L + r_1 - r_n + 1, 1$ and

$$\begin{aligned} c_x =& 2 \prod_{j=1}^{n} \left[\frac{\left[2\mu_j L_j \sqrt{\kappa_j \left(1+\kappa_j\right)}\right]^{2r_j + \mu_j L_j - 1} \left[\mu_j L_j \left(1+\kappa_j\right)\right]^{\mu_1 L - \mu_j L_j + r_1 - r_j}}{(r_j)!\, 2^{2r_j + \mu_j L_j - 1} \kappa_j^{\frac{\mu_j L_j - 1}{2}} \exp\left(\kappa_j \mu_j L_j\right) \Gamma\left(r_j + \mu_j L_j\right)} \right] \\ & \times \prod_{j=1}^{n} \left[\mu_j L_j \left(1+\kappa_j\right)^{\frac{\mu_j L_j + 1}{2}} \right]. \end{aligned}$$

The PDF of H_{SD} is plotted along with Monte-Carlo simulations for different number of antennas (L) in Figure 3.19.

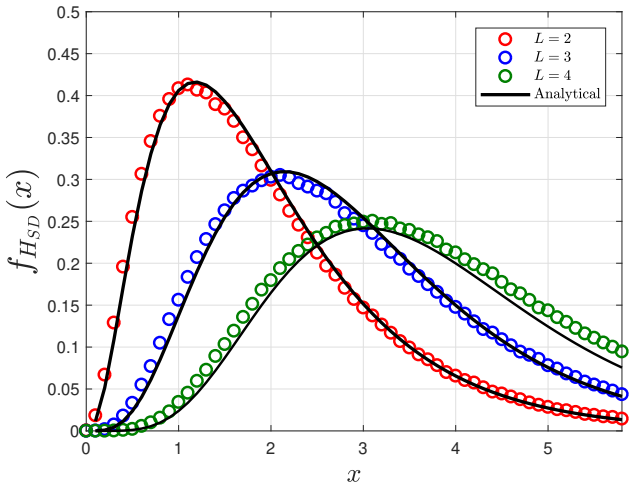

Figure 3.19: The PDF of H_{SD} for $n = 2$. $\kappa = 1$ and $\mu = 2$.

Considering the wiretap channel being a single κ-μ, the PDF of $H_{SE} = \sum_{w=1}^{L_e} \left| h_{SE}^{(w)} \right|^2$ is given by [35]

$$f_{H_{SE}}(x) = \sum_{A=0}^{\infty} \frac{c_1' \left(\mu_e L_e \sqrt{\kappa_e \left(1+\kappa_e\right)}\right)^{2A + \mu_e L_e - 1}}{2 L_e^{\mu_e L_e + A} A!\, \Gamma\left(A + \mu_e L_e\right)} x^{\mu_e L_e + A - 1} \exp\left(-\mu_e \left(1+\kappa_e\right) x\right), \quad (3.72)$$

where $c_1' = \frac{2\mu_e L_e (1+\kappa_e)^{\frac{\mu_e L_e + 1}{2}}}{\kappa_e^{\frac{\mu_e L_e - 1}{2}} \exp(\kappa_e \mu_e L_e)}$. Finally, the PDF of the channel power gain $|h_{SP}|^2$ with the

corresponding coefficient λ_p follows the Exponential distribution as

$$f_{|h_{SP}|^2}(y) \quad = \quad \lambda_p \exp\left(-\lambda_p y\right). \tag{3.73}$$

3.13.2 PLS Analysis

Here, PLS for an underlay SIMO CRN over cascaded κ-μ fading channels will be investigated. The analyses are presented in terms of the secrecy outage probability (SOP) and the probability of non-zero secrecy capacity (P_r^{nzc}).

3.13.3 Secrecy Outage Probability

Using the definition the secrecy outage probability (SOP) in (2.1), (3.67)-(3.69), and after mathematical manipulations, SOP is given by

$$\begin{aligned} SOP \quad &= \quad P_r\left(\log_2(1+\gamma_D) - \log_2(1+\gamma_E) \leqslant C_{th}\right) = P_r\left(\frac{1+\frac{I_{th}H_{SD}}{N_0|h_{SP}|^2}}{1+\frac{I_{th}H_{SE}}{N_0|h_{SP}|^2}} \leqslant 2^{C_{th}}\right) \\ &= P_r\left(\frac{\left(\epsilon-1\right)|h_{SP}|^2 + \epsilon\rho_{th}H_{SE}}{\rho_{th}H_{SD}} \geqslant 1\right), \end{aligned} \tag{3.74}$$

where $\rho_{th} = \frac{I_{th}}{N_0}$ and $\epsilon = 2^{C_{th}}$. Let $Y = \frac{(\epsilon-1)|h_{SP}|^2+\epsilon\rho_{th}H_{SE}}{\rho_{th}H_{SD}}$, $Y_a = \left(\epsilon-1\right)|h_{SP}|^2 + \epsilon\rho_{th}H_{SE}$ and $Y_b = \rho_{th}H_{SD}$. To find the secrecy outage probability, one needs to obtain the PDF of the random variable Y. Let $Y_a = M + N$, where $M = \left(\epsilon-1\right)|h_{SP}|^2$ and $N = \epsilon\rho_{th}H_{SE}$. The PDF of M is found using (3.73) as

$$f_M(x) \quad = \quad \frac{\lambda_p}{(\epsilon-1)} \exp\left(-\frac{\lambda_p x}{\epsilon-1}\right). \tag{3.75}$$

Using (3.72), the PDF of N is given by

$$f_N(x) = \sum_{A=0}^{\infty} \frac{c_1'\left(\mu_e L_e \sqrt{\frac{\kappa_e(1+\kappa_e)}{\epsilon\rho_{th}}}\right)^{2A+\mu_e L_e-1}}{2L_e^{\mu_e L_e+A} A!\,\Gamma\left(A+\mu_e L_e\right)\left(\epsilon\rho_{th}\right)^{\frac{\mu_e L_e+1}{2}}} x^{\mu_e L_e+A-1} \exp\left(-\mu_e\left(1+\kappa_e\right)\frac{x}{\epsilon\rho_{th}}\right) \tag{3.76}$$

Hence, the PDF of Y_a is given by

$$f_{Y_a}(y_a) = \int_0^{y_a} f_M(x) f_N(y_a - x) dx. \tag{3.77}$$

Substituting (3.75) and (3.76) into (3.77) and using [82, eq. (3.346.1)], the PDF of Y_a is given by

$$f_{Y_a}(y_a) = \sum_{A=0}^{\infty} C_a P^{-\mu_e L_e - A} \exp\left(\frac{-\lambda_p y_a}{\epsilon - 1}\right) \gamma\left(\mu_e L_e + A, P y_a\right), \tag{3.78}$$

where $C_a = \frac{\lambda_p c_1' \left(\mu_e L_e \sqrt{\frac{\kappa_e(1+\kappa_e)}{\epsilon \rho_{th}}}\right)^{2A+\mu_e L_e - 1}}{2(\epsilon-1) L_e^{\mu_e L_e + A} A! \Gamma(A+\mu_e L_e)(\epsilon \rho_{th})^{\frac{\mu_e L_e + 1}{2}}}$ and $P = \left(\frac{\mu_e(1+\kappa_e)}{\epsilon \rho_{th}} - \frac{\lambda_p}{\epsilon - 1}\right)$. The PDF of Y_b is found using (3.71) as

$$f_{Y_b}(y_b) = \sum_{r_1=0}^{\infty} \sum_{r_2=0}^{\infty} \cdots \sum_{r_n=0}^{\infty} \frac{c_x}{2\left(\rho_{th} L\right)^{\mu_1 L + r_1}} y_b^{\mu_1 L + r_1 - 1} G_{n\ 0}^{0\ n}\left(\begin{matrix} \beta' \\ - \end{matrix} \middle| \frac{\rho_{th} L}{y_b \prod_{j=1}^{n} \mu_j L_j \left(1 + \kappa_j\right)}\right) \tag{3.79}$$

Besides, the PDF of Y is found using the following integration

$$f_Y(y) = \int_0^{\infty} y_b f_{Y_a}(y y_b) f_{Y_b}(y_b) dy_b. \tag{3.80}$$

Substituting (3.78) and (3.79) into (3.80) yields

$$f_Y(y) = \sum_{r_1=0}^{\infty} \sum_{r_2=0}^{\infty} \cdots \sum_{r_n=0}^{\infty} \sum_{A=0}^{\infty} C_b \left[I_1 - \sum_{B=0}^{\mu_e L_e + A - 1} \frac{P^B y^B}{B!} I_2 \right], \tag{3.81}$$

where $C_b = C_a P^{-\mu_e L_e - A} \left(\mu_e + A - 1\right)! \frac{c_x}{2(\rho_{th} L)^{\mu_1 L + r_1}}$. I_1 is given by

$$I_1 = \int_0^{\infty} y_b^{\mu_1 L + r_1} \exp\left(-\frac{\lambda_p y y_b}{\epsilon - 1}\right) G_{0\ n}^{n\ 0}\left(\begin{matrix} - \\ 1 - \beta' \end{matrix} \middle| \frac{y_b \prod_{j=1}^{n} \mu_j L_j \left(1 + \kappa_j\right)}{\rho_{th} L}\right) dy_b. \tag{3.82}$$

Using [82, eq. (8.352.1)] and [82, eq. (7.813.1)], (3.82) is solved as

$$I_1 = \left(\frac{\lambda_p y}{\epsilon - 1}\right)^{-\mu_1 L - r_1 - 1} G_{1\ n}^{n\ 1}\left(\begin{matrix}-\mu_1 L - r_1 \\ 1-\beta'\end{matrix}\middle| \frac{(\epsilon-1)\prod_{j=1}^{n}\mu_j L_j\left(1+\kappa_j\right)}{\rho_{th} L \lambda_p y}\right). \tag{3.83}$$

Similarly, I_2 is solved as [82, eq. (7.813.1)]

$$I_2 = \left(\frac{\lambda_p y}{\epsilon - 1} + Py\right)^{-\mu_1 L - r_1 - B - 1} G_{1\ n}^{n\ 1}\left(\begin{matrix}-\mu_1 L - r_1 - B \\ 1-\beta'\end{matrix}\middle| \frac{\prod_{j=1}^{n}\mu_j L_j\left(1+\kappa_j\right)}{\rho_{th} L y\left(P + \frac{\lambda_p}{\epsilon-1}\right)}\right). \tag{3.84}$$

Given (3.74), the secrecy outage probability is represented as

$$\begin{aligned} SOP &= P_r\left(Y \geqslant 1\right) \\ &= \int_1^{\infty} f_Y(y) dy\cdot \end{aligned} \tag{3.85}$$

Using (3.81), (3.83), (3.84), and [85, eq. (26)] with some mathematical manipulations, (3.85) is expressed as

$$SOP = 1 - \sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_n=0}^{\infty}\sum_{A=0}^{\infty} C_b\left[S_1 - \sum_{B=0}^{\mu_e L_e + A - 1}\frac{P^B}{B!} S_2\right], \tag{3.86}$$

where

$$S_1 = \left(\frac{\lambda_p}{\epsilon - 1}\right)^{-\mu_1 L - r_1 - 1} G_{n+1\ 2}^{1\ n+1}\left(\begin{matrix}\beta', 1+\mu_1 L + r_1 \\ 1+\mu_1 L + r_1, \mu_1 L + r_1\end{matrix}\middle| \frac{\rho_{th} L \lambda_p}{(\epsilon-1) Q}\right), \tag{3.87}$$

and

$$S_2 = \left(\frac{\lambda_p}{\epsilon - 1} + P\right)^{-\mu_1 L - r_1 - B - 1} G_{n+1\ 2}^{1\ n+1}\left(\begin{matrix}\beta', 1+\mu_1 L + r_1 \\ 1+\mu_1 L + r_1 + B, \mu_1 L + r_1\end{matrix}\middle| \frac{\rho_{th} L\left(P + \frac{\lambda_p}{\epsilon-1}\right)}{Q}\right), \tag{3.88}$$

with $Q = \prod_{j=1}^{n}\mu_j L_j\left(1+\kappa_j\right)$.

In order to study the behaviour of the system as the constraint over the transmission power of S increases, we assess the secrecy outage probability when ρ_{th}, i.e., $\frac{I_{th}}{N_0}$ goes to infinity. Considering

this in (3.74), the asymptotic secrecy outage probability is expressed as

$$SOP^{ASMP} = P_r\left(H_{SD} \leq \epsilon H_{SE}\right) = \int_0^{\infty} F_{H_{SD}}(\epsilon x) f_{H_{SE}}(x) dx. \tag{3.89}$$

It is worth mentioning that (3.89) represents the lower bound of the secrecy outage probability [7]. To solve the integration in (3.89), the CDF of H_{SD} is found using (3.71) and [82, eq. (3.381.3)] as

$$\begin{aligned} F_{H_{SD}}(x) &= \sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_n=0}^{\infty} \frac{c_x}{2L^{\mu_1 L+r_1}} x^{\mu_1 L+r_1} \\ &\quad \times G_{1\ n+1}^{\ n\ \ 1}\left(\begin{matrix}1-\mu_1 L-r_1 \\ 1-\beta', -\mu_1 L-r_1\end{matrix}\middle| \frac{x\prod_{j=1}^{n}\mu_j L_j\left(1+\kappa_j\right)}{L}\right) \end{aligned} \tag{3.90}$$

Substituting (3.90) and (3.72) into (3.89) yields

$$\begin{aligned} SOP^{ASMP} &= \sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_n=0}^{\infty}\sum_{A=0}^{\infty} C_r \epsilon^{\mu_1 L+r_1}\left(\mu_e(1+\kappa_e)\right)^{-\mu_1 L-r_1-\mu_e L_e-A} \\ &= G_{2\ n+1}^{\ n\ \ 2}\left(\begin{matrix}\psi \\ 1-\beta', -\mu_1 L-r_1\end{matrix}\middle| \frac{\epsilon\prod_{j=1}^{n}\mu_j L_j\left(1+\kappa_j\right)}{L\mu_e(1+\kappa_e)}\right), \end{aligned} \tag{3.91}$$

where $\psi = -\mu_1 L - r_1 - \mu_e L_e - A + 1, 1 - \mu_1 L - r_1$ and $C_r = \frac{c_1' c_x\left(\mu_e L_e\sqrt{\kappa_e(1+\kappa_e)}\right)^{2A+\mu_e L_e-1}}{4L_e^{\mu_e L_e+A} L^{\mu_1 L+r_1} A!\Gamma(A+\mu_e L_e)}$. From (3.91), it can be concluded that the performance of the network is independent of ρ_{th} and thus independent of the underlay constraint defined in (3.67). This has a significant influence on the system design as the SU transmitter can transmit the confidential information with the maximum possible transmit power, given the PUs' quality of service (QoS) is maintained. In other words, the network is considered to be a non-cognitive network. Consequently, this tends to boost the security of exchanged information as the obtained SNR at the legitimate receiver is thereby improved. This effect is later illustrated by the numerical results.

3.13.4 Probability of Non-Zero Secrecy Capacity

The probability of non-zero secrecy capacity (P_r^{nzc}) is evaluated using (3.37) as

$$\begin{aligned} P_r^{nzc} &= P_r\left(C_s > 0\right) = 1 - P_r\left(\frac{1+\frac{\rho_{th}H_{SD}}{|h_{SP}|^2}}{1+\frac{\rho_{th}H_{SE}}{|h_{SP}|^2}} \leqslant 1\right) \\ &= 1 - P_r\left(H_{SD} \leqslant H_{SE}\right) = 1 - \int_0^\infty F_{H_{SD}}(x) f_{H_{SE}}(x) dx. \end{aligned} \tag{3.92}$$

Given (3.72) and (3.90), the probability of non-zero secrecy capacity is expressed as [82, eq. (7.813.1)]

$$\begin{aligned} P_r^{nzc} &= 1 - \sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_n=0}^{\infty}\sum_{A=0}^{\infty} C_r\left(\mu_e(1+\kappa_e)\right)^{-\mu_1 L - r_1 - \mu_e L_e - A} \\ &\quad \times G_{2\ n+1}^{n\ 2}\left(\begin{matrix}\psi \\ 1-\beta', -\mu_1 L - r_1\end{matrix}\middle| \frac{\prod_{j=1}^{n}\mu_j L_j\left(1+\kappa_j\right)}{L\mu_e(1+\kappa_e)}\right). \end{aligned} \tag{3.93}$$

3.14 Numerical Results

This section presents the theoretical results with Monte-Carlo simulations. The theoretical results are obtained by truncating the infinite series expansion to the first twenty terms $(r = 20, A = 20)$. The Meijer G-function can be easily computed using different software packages, such as Maple, Mathematica, and Matlab. Symbols in the figures represent the Monte-Carlo simulations.

Fig. 3.20 illustrates the secrecy outage probability (SOP) versus ρ_{th} for double κ-μ fading channels $(n = 2)$. The fading parameters for the main and the wiretap channels are $\kappa = 0$ and $\mu = 4$, which represents the Nakagami-m fading channel as a special case of this general fading model. One can notice that the secrecy is improved by the rise in the number of antennas at the SU destination (L). This is due to the employment of the MRC technique. The figure also compares the utilization of one antenna $(L = 1)$ with four antennas $(L = 4)$. The difference between the two curves indicates the important impact of utilizing multiple antennas at D over the security of the SUs' communication. Besides, it is shown that as ρ_{th} increases, the secrecy improves as the transmitter is capable of using the maximum transmit power.

Fig. 3.21 represents the impact of increasing the number of antennas at the eavesdropper (L_e)

over the secrecy outage probability for two cascade levels at the main channel ($n = 2$) and two antennas at D. It can be noted that increasing the number of antennas at the eavesdropper degrades the secrecy. That is, the eavesdropper is becoming more powerful for the interception of the confidential information as the number of antennas increases due to utilizing MRC technique over the received multiple copies of the intercepted signal. Furthermore, it is observed that all the curves tend to saturate for high values of ρ_{th}. This is because as ρ_{th} takes higher values, the limit over the transmit power of S is neglected and S can transmit with its maximum power. That is, the network becomes independent of the interference constraint. This effect was proven by (3.91).

Fig. 3.22 presents the secrecy outage probability as a function of the target secrecy rate (C_{th}) for different number of scatters in the main channel (n). It is observed that the system secrecy deteriorates as the target rate rises, which can be illustrated by (2.1). That is, there is a higher chance for a secrecy outage with an enhancement in the target rate. Furthermore, as the number of the scatters and obstacles in the main channel increases, i.e., cascade level n goes up, the higher the probability of a an outage in the secrecy of the information exchanged between the SUs as the level of fading severity is maximized. In addition, comparing the gap between the results for low C_{th} as L_e increases, one can conclude that the effect of the fading severity (n) on the security is reduced accordingly. This can be interpreted by the fact that when L_e increases, implying stronger eavesdropping, the impact of the wiretap channel over the secrecy is more critical than the impact of the conditions of the main channel. This proves that both the main and the wiretap channels impair the confidentiality of the shared information.

Fig. 3.23 depicts the Rayleigh fading model as one of the special cases of this general fading distribution. Moreover, the results include the effect of distances over the secrecy. Let $d_{JK}^{-PL} = \frac{1}{2\lambda_{JK}}$, where d_{JK} is the distance between node J and K. PL is the path loss exponent and λ_{JK} is the fading coefficient for the channel JK. $J \in \{S, O_1\}$ and $K \in \{O_1, D, P_R, E\}$, where O_1 represents the location of the obstacle in the main channel between S and D. The results prove that the secrecy of the SUs deteriorates as the distance between the source S and the eavesdropper E, i.e., d_{SE} becomes smaller. Indeed, this result will be more explored in the next section of this thesis, where we consider a special case system model of this general one.

Fig. 3.24 shows the secrecy outage probability as a function of the secrecy target rate (C_{th}).

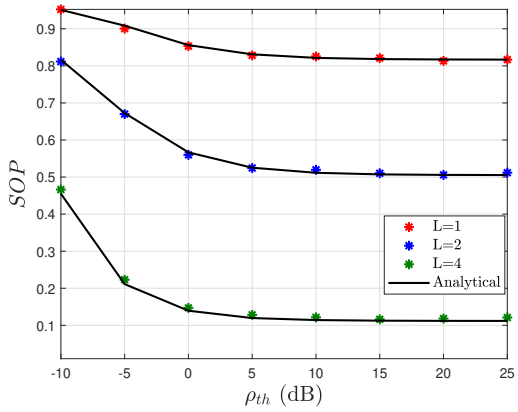

Figure 3.20: The secrecy outage probability versus $\rho_{th} = \frac{I_{th}}{N_0}$ for double κ-μ fading channel ($n = 2$). For the main channel: $\kappa = 0$ and $\mu = 4$. For the wiretap channel: $\kappa_e = 0$ and $\mu_e = 4$. $C_{th} = 1$ bit/sec/Hz, $L_e = 1$, and $\lambda_p = 5$.

The figure includes both the asymptotic secrecy outage probability (SOP^{ASMP}) and the exact SOP given in (3.86) for a high value of ρ_{th}. The SOP^{ASMP} represents the scenario when ρ_{th} goes to infinity, which matches the case of the exact result when substituting $\rho_{th} = 40$ dB in (3.86). This match demonstrates the accuracy of the derived SOP^{ASMP} and proves that the secrecy outage probability becomes independent of ρ_{th} as it takes high values. In this case, the CRN relaxes the restrictions on the transmitting power in an underlay CRN. Therefore, the results highlight the effect of the constraint (ρ_{th}) on the network design.

Fig. 3.25 represents the probability of non-zero secrecy capacity (P_r^{nzc}) versus the number of antennas at the eavesdropper (L_e) for a different number of scatters in the path (n). It is evident that as the cascade level increases, the secrecy deteriorates for a specific range of L_e. This is because more severe fading appears with the increment in the scatters at the main link. In addition, for the perceived parameters, the cascaded fading channel level may appear to have a different impact on the secrecy as the eavesdropper becomes empowered with more antennas (L_e), i.e., $L_e > L$. Moreover, it is clear that the probability of non-zero secrecy capacity is degrading when the eavesdropper becomes more powerful by deploying more antennas for reception. This is in agreement with the results in Fig. 3.22, which confirms that PLS is impacted by the conditions of both; the main and wiretap channels.

As a final investigation, Fig. 3.26 depicts the impact of the number of antennas at the SU receiver

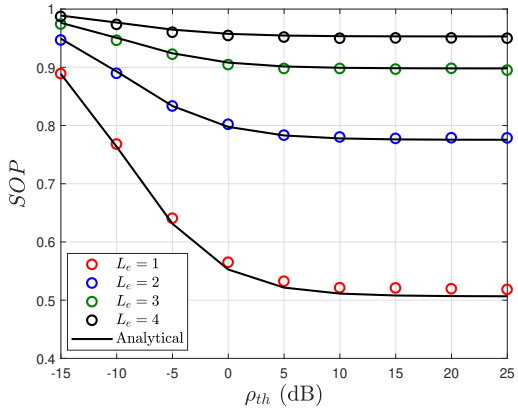

Figure 3.21: The secrecy outage probability versus $\rho_{th} = \frac{I_{th}}{N_0}$ for double κ-μ fading channel $(n = 2)$. For the main channel: $\kappa = 1$ and $\mu = 1$. For the wiretap channel: $\kappa_e = 1$ and $\mu_e = 1$. $C_{th} = 1$ bit/sec/Hz, $L = 2$, and $\lambda_p = 5$.

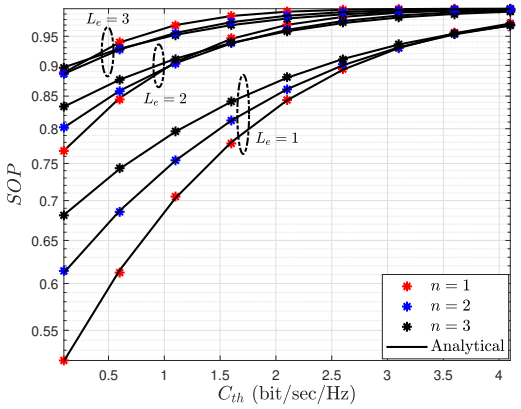

Figure 3.22: The secrecy outage probability versus the threshold secrecy rate (C_{th}) for different cascade level (n) and different number of antennas at the eavesdropper (L_e). For the main channel: $\kappa = 0$ and $\mu = 1$. For the wiretap channel: $\kappa_e = 0$ and $\mu_e = 1$. $L = 1$, $\lambda_p = 5$, and $\rho_{th} = 5$ dB.

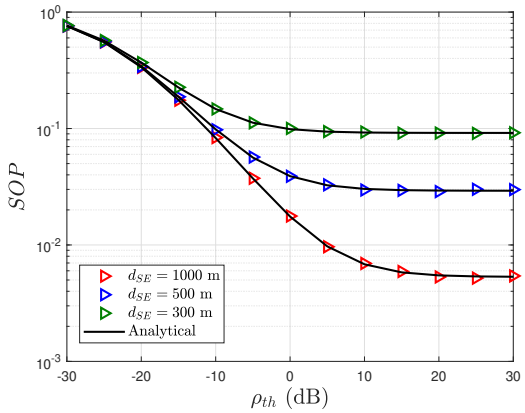

Figure 3.23: The secrecy outage probability versus $\rho_{th} = \frac{I_{th}}{N_0}$ for double cascade level $(n = 2)$ for Rayleigh fading channel as a special case. For the main channel: $\kappa = 0$ and $\mu = 1$. For the wiretap channel: $\kappa_e = 0$ and $\mu_e = 1$. $L = 1$, $L_e = 1$ and $C_{th} = 0.7$ bit/sec/Hz.

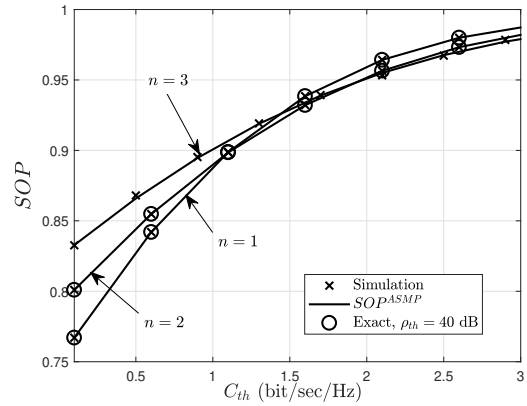

Figure 3.24: The secrecy outage probability versus the threshold secrecy rate (C_{th}) for different cascade level (n). For the main channel: $\kappa = 0$ and $\mu = 1$. For the wiretap channel: $\kappa_e = 0$ and $\mu_e = 1$. $L = 1$, $L_e = 2$, and $\lambda_p = 5$.

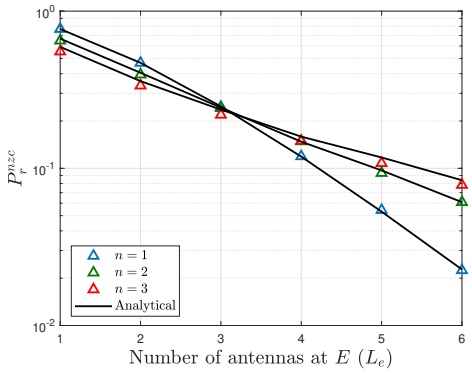

Figure 3.25: The probability of non-zero secrecy capacity versus the number of antennas at E (L_e) for different cascade level (n) and for $L = 2$. For the main channel: $\kappa = 1$ and $\mu = 1$. For the wiretap channel: $\kappa_e = 1$ and $\mu_e = 2$.

(L) and the eavesdropper (L_e) over the SUs' secrecy for double κ-μ fading channel $(n = 2)$. For $\kappa = 1, \kappa_e = 1, \mu_e = 2$, the results suggest that with the rise in the number of antennas at the legitimate receiver (L), the achieved confidentiality is improved. In other words, there is a higher chance for the main channel's capacity to be greater than the wiretap channel's capacity as the number of antennas at the legitimate receiver increases. The results show the impact of varying the value of the wiretap channel parameters for a double κ-μ channel and for a single antenna at the SU receiver $(L = 1)$ and $\kappa = 0, \mu_e = 1$. It is noteworthy that as the wiretap channel becomes reliable, i.e., κ_e increases, the confidentiality of the shared information at the main channel deteriorates. This depicts that the security is influenced by both; the main and the wiretap channels' conditions.

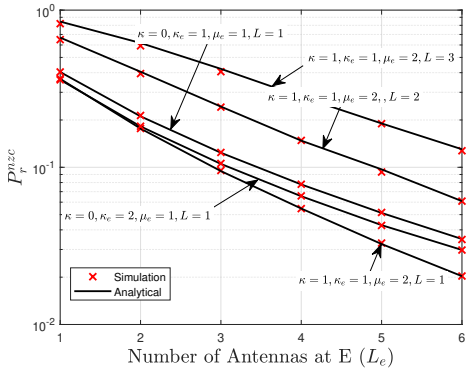

Figure 3.26: The probability of non-zero secrecy capacity versus the number of antennas at E (L_e) for cascade level $n = 2$ and $\mu = 1$.

3.15 PLS for CRNs over Cascaded Rayleigh Fading Channels

In this section, a special case of the previous SIMO system is considered. In our model, we consider a pair of SUs (S, D), a PU receiver (P_R), and an eavesdropper (E) as shown in Fig. 3.27. We assume that the SU pair, the PU receiver, and the eavesdropper are equipped with a single antenna. The channel h_{SD} follows cascaded Rayleigh fading model, whereas h_{SP} and h_{SE} both follow single Rayleigh fading model. Considering an underlay cognitive radio channel sharing model, the transmitting power at S should be limited by a threshold (I_{th}) that the PU receiver (P_R) can tolerate. The PU transmitter is assumed to be located far away from the SUs pair and does not affect the SUs communication.

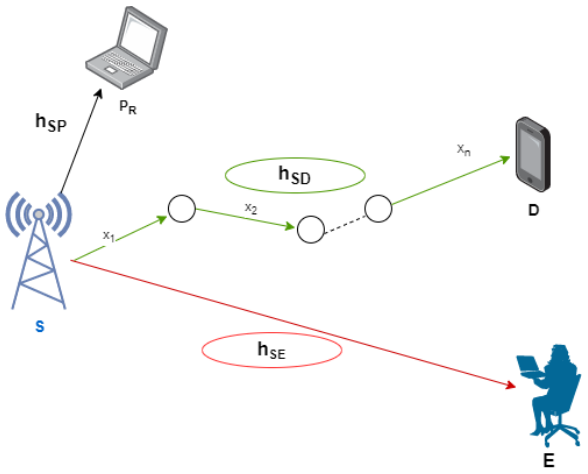

Figure 3.27: The system model.

Let $h_{SD} = \prod_i^n x_i$, where x_i follows the Rayleigh channel model. The probability density function (PDF) of h_{SD} was derived based-on a transformed Nakagami-m distribution in [105] as

$$f_{h_{SD}}(y) = \varpi y^{\frac{2m}{n}-1} \exp\left(-\frac{m}{\Omega\sigma^{\frac{2}{n}}} y^{\frac{2}{n}}\right), \tag{3.94}$$

where n is the cascade level, $\varpi = \frac{2\left(\frac{m}{\Omega}\right)^m}{n\Gamma(m)\sigma^{\frac{2m}{n}}}$, σ is the scale parameter of the distribution and $\sigma^2 = \prod_{i=1}^n \sigma_i^2$ for $i = 1, 2, \cdots, n$. The values of m and Ω are calculated based on the following

$$\begin{aligned} m &= 0.6102n + 0.4263, \\ \Omega &= 0.8808n^{-0.9661} + 1.12. \end{aligned} \tag{3.95}$$

The PDF of the channel power gain $|h_{SP}|^2$ with the corresponding coefficient λ_p and $|h_{SE}|^2$ with the corresponding coefficient λ_e can be expressed, respectively, as

$$f_{|h_{SP}|^2}(y) = \lambda_p \exp(-\lambda_p y), \tag{3.96}$$

$$f_{|h_{SE}|^2}(y) = \lambda_e \exp(-\lambda_e y). \tag{3.97}$$

The received message at the SU destination (D) is given by

$$y_D = \sqrt{P_s} h_{SD} x_s + n_D, \tag{3.98}$$

where P_s is the transmit power at S, x_s is the transmitted symbol, and n_D is the additive-white-Gaussian-noise (AWGN) at the receiver D with zero mean and variance N_0. Moreover, the intercepted message at the eavesdropper E is given by

$$y_E = \sqrt{P_s} h_{SE} x_s + n_E, \tag{3.99}$$

where n_E is the AWGN at E with zero mean and variance N_0. Using (3.98), (3.99), and (3.67) the instantaneous received SNRs at D and E can be expressed, respectively, as

$$\gamma_D = \frac{I_{th} |h_{SD}|^2}{N_0 |h_{SP}|^2}, \tag{3.100}$$

$$\gamma_E = \frac{I_{th} |h_{SE}|^2}{N_0 |h_{SP}|^2}. \tag{3.101}$$

3.16 PLS Analysis

In this section, PLS will be studied in terms of the secrecy outage probability (SOP), the probability of non-zero secrecy capacity (P_r^{nzc}), and the intercept probability (P_{int}).

3.16.1 Secrecy Outage Probability

Using (2.1), SOP for this system model is evaluated as

$$\begin{aligned} SOP &= P_r\left(\log_2(1+\gamma_D)-\log_2(1+\gamma_E)\leqslant C_{th}\right) \\ &= P_r\left(\frac{1+\frac{I_{th}|h_{SD}|^2}{N_0|h_{SP}|^2}}{1+\frac{I_{th}|h_{SE}|^2}{N_0|h_{SP}|^2}}\leqslant 2^{C_{th}}\right) P_r\left(\frac{(\eta-1)\left|h_{SP}\right|^2+\eta\rho_{th}\left|h_{SE}\right|^2}{\rho_{th}\left|h_{SD}\right|^2}\geqslant 1\right), \end{aligned} \tag{3.102}$$

where $\rho_{th}=\frac{I_{th}}{N_0}$ and $\epsilon=2^{C_{th}}$. Let $Y=\frac{(\epsilon-1)|h_{SP}|^2+\epsilon\rho_{th}|h_{SE}|^2}{\rho_{th}|h_{SD}|^2}$, $Y_a=(\epsilon-1)\left|h_{SP}\right|^2+\epsilon\rho_{th}\left|h_{SE}\right|^2$ and $Y_b=\rho_{th}\left|h_{SD}\right|^2$. To find the secrecy outage probability, one needs to find the PDF of the random variable Y. Let $Y_a=A+B$, where $A=(\epsilon-1)\left|h_{SP}\right|^2$ and $B=\epsilon\rho_{th}\left|h_{SE}\right|^2$. The PDF of A can be found using (3.96) as

$$f_A(x) = \frac{\lambda_p}{(\epsilon-1)}\exp\left(-\frac{\lambda_p x}{\epsilon-1}\right). \tag{3.103}$$

Using (3.97), the PDF of B can be given by

$$f_B(x) = \frac{\lambda_e}{\epsilon\rho_{th}}\exp\left(-\frac{\lambda_e x}{\epsilon\rho_{th}}\right). \tag{3.104}$$

Hence, the PDF of Y_a is given by

$$f_{Y_a}(y_a) = \int_0^{y_a} f_A(x)f_B(y_a-x)dx. \tag{3.105}$$

Substituting (3.103) and (3.104) into (3.105), the PDF of the random variable Y_a can be expressed as

$$f_{Y_a}(y_a)=a_1\left(\exp\left(-\frac{\lambda_p y_a}{\epsilon-1}\right)-\exp\left(-\frac{\lambda_e y_a}{\epsilon\rho_{th}}\right)\right), \tag{3.106}$$

where $a_1=\frac{\lambda_p\lambda_e}{\mu(\epsilon-1)(\epsilon\rho_{th})}$ and $\mu=\left(\frac{\lambda_e}{\epsilon\rho_{th}}-\frac{\lambda_p}{\epsilon-1}\right)$. The PDF of Y_b cab be found using (3.94) as

$$f_{Y_b}(y_b) = \frac{\varpi}{2\rho_{th}^{\frac{m}{n}}}y_b^{\frac{m}{n}-1}\exp\left(-\frac{m}{\rho_{th}^{\frac{1}{n}}\Omega\sigma^{\frac{2}{n}}}y_b^{\frac{1}{n}}\right). \tag{3.107}$$

Also, the PDF of Y can be found using the following

$$f_Y(y) \quad = \quad \int_0^{\infty} y_b f_{Y_a}(y y_b) f_{Y_b}(y_b) dy_b. \tag{3.108}$$

Using (3.106), (3.107), and [83, eq. (2.24.3.1)] and with some mathematical manipulations, (3.108) can be expressed as

$$\begin{aligned} f_Y(y) \quad = \quad & a_3 c_1 y^{\frac{-m}{n}-1} G_{1\ n}^{n\ 1}\left(\begin{matrix} \frac{-m}{n} \\ 0, \frac{1}{n}, \cdots, \frac{n-1}{n} \end{matrix} \middle| \frac{\left(\frac{m}{\Omega \sigma^{\frac{2}{n}}}\right)^n}{\rho_{th} n^n \frac{\lambda_p y}{\epsilon} - 1} \right) - a_3 c_2 y^{\frac{-m}{n}-1} \\ & \times G_{1\ n}^{n\ 1}\left(\begin{matrix} -\frac{m}{n} \\ 0, \frac{1}{n}, \cdots, \frac{n-1}{n} \end{matrix} \middle| \frac{\left(\frac{m}{\Omega \sigma^{\frac{2}{n}}}\right)^n}{\rho_{th} n^n y \left(\frac{\lambda_e}{\epsilon \rho_{th}}\right)} \right), \end{aligned} \tag{3.109}$$

where $a_3 = \frac{a_1 \varpi}{2 \rho_{th}^{\frac{m}{n}}}$, $c_1 = \frac{\sqrt{n}\left(\frac{\lambda_p}{\epsilon - 1}\right)^{\frac{-m}{n}-1}}{(2\pi)^{\frac{n-1}{2}}}$, and $c_2 = \frac{\sqrt{n}\left(\frac{\lambda_e}{\epsilon \rho_{th}}\right)^{-\frac{m}{n}-1}}{(2\pi)^{\frac{n-1}{2}}}$.
Given (3.102) and (3.109), the secrecy outage probability can be represented as

$$SOP \quad = \quad P_r\left(Y \geqslant 1\right) = \int_1^{\infty} f_Y(y) dy. \tag{3.110}$$

Substituting (3.109) into (3.110) and using [85, eq. (26)] with some mathematical manipulations, the SOP can be expressed as

$$SOP \quad = \quad 1 - \left[S_1 - S_2\right], \tag{3.111}$$

where

$$S_1 = a_3 c_1 G_{n+1\ \ 2}^{1\ \ n+1}\left(\begin{matrix} 1, \frac{n-1}{n}, \cdots, \frac{1}{n}, 1+\frac{m}{n} \\ 1+\frac{m}{n}, \frac{m}{n} \end{matrix} \middle| \frac{\rho_{th} n^n \frac{\lambda_p}{\epsilon - 1}}{\left(\frac{m}{\Omega \sigma^{\frac{2}{n}}}\right)^n} \right) \tag{3.112}$$

and

$$S_2 = a_3 c_2 G_{n+1\ \ 2}^{1\ \ n+1}\left(\begin{matrix} 1, \frac{n-1}{n}, \cdots, \frac{1}{n}, 1+\frac{m}{n} \\ 1+\frac{m}{n}, \frac{m}{n} \end{matrix} \middle| \frac{n^n \left(\frac{\lambda_e}{\epsilon}\right)}{\left(\frac{m}{\Omega \sigma^{\frac{2}{n}}}\right)^n} \right). \tag{3.113}$$

3.16.2 Probability of Non-Zero Secrecy Capacity

The probability of non-zero secrecy capacity (P_r^{nzc}) defined in (3.37) is given by

$$\begin{aligned} P_r^{nzc} &= P_r\left(C_s > 0\right) = 1 - P_r\left(\frac{1+\frac{\rho_{th}|h_{SD}|^2}{|h_{SP}|^2}}{1+\frac{\rho_{th}|h_{SE}|^2}{|h_{SP}|^2}} \leqslant 1\right) \\ &= 1 - P_r\left(|h_{SD}|^2 \leqslant |h_{SE}|^2\right) 1 - \int_0^\infty F_{|h_{SD}|^2}(x) f_{|h_{SE}|^2}(x) dx. \end{aligned} \tag{3.114}$$

In order to evaluate the probability of non-zero secrecy capacity, one needs to find the cumulative distribution function (CDF) of the channel power gain $|h_{SD}|^2$, which can be found using (3.94), [82, eq. (3.381.3)] and with some mathematical manipulations as

$$F_{|h_{SD}|^2}(x) = 1 - \frac{n\varpi\left(\frac{m}{\Omega\sigma^{\frac{2}{n}}}\right)^{-m}}{2}(m-1)!\exp\left(-\frac{m}{\Omega\sigma^{\frac{2}{n}}}x^{\frac{1}{n}}\right)\sum_{j=0}^{m-1}\frac{\left(\frac{m}{\Omega\sigma^{\frac{2}{n}}}\right)^{j}}{j!}x^{\frac{j}{n}}. \tag{3.115}$$

Using (3.115) and (3.97), (3.114) can be solved as [83, eq. (2.24.3.1)]

$$P_r^{nzc} = \sum_{j=0}^{m-1} q\lambda_e^{\frac{-j}{n}} G_{1\ n}^{n\ 1}\left(\begin{matrix} -\frac{j}{n} \\ 0, \frac{1}{n}, \cdots, \frac{n-1}{n} \end{matrix}\middle| \frac{\left(\frac{m}{\Omega\sigma^{\frac{2}{n}}}\right)^{n}}{n^n\lambda_e}\right), \tag{3.116}$$

where $q = \left(\frac{m}{\Omega\sigma^{\frac{2}{n}}}\right)^{-m+j}\frac{n\sqrt{n}\varpi(m-1)!}{2j!(2\pi)^{\frac{n-1}{2}}}$.

3.16.3 Intercept Probability

Intercept probability defined in is expressed as

$$\begin{aligned} P_{int} &= P_r\left(C_s < 0\right) = P_r\left(|h_{SD}|^2 < |h_{SE}|^2\right) \\ &= \int_0^\infty F_{|h_{SD}|^2}(x) f_{|h_{SE}|^2}(x) dx = 1 - P_r^{nzc}. \end{aligned} \tag{3.117}$$

3.17 Numerical Results

In this section, analytical results are presented with Monte-Carlo simulations. A perfect match can be noticed between the analytical and the simulation results. To take the path loss effect over the secrecy into consideration, we assume that the transmitter represents the reference location. That is S is located at $(0, 0)$ and the other nodes ($D, E,$ and P_R) are of different distances from S as shown in Fig. 3.28. Assume $d_{MN}^{-PL} = \frac{1}{2\lambda_J}$, where PL is the path loss exponent, $M \in \{S, d_1, d_2, d_3\}$, $N \in \{P_R, E, d_1, d_2, d_3, D\}$, and $J \in \{e, s, p\}$. $\lambda_s = \frac{1}{2\sigma^2}$ and d_{MN} represents the distance from node M to node N in meters (m). $d_1, d_2,$ and d_3 are the locations of the first, second, and third obstacle in the main channel, respectively. This is to notice the effect of the cascade level between S and D.

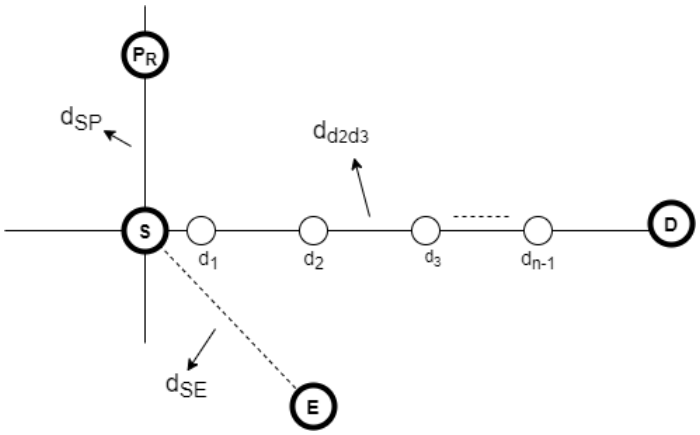

Figure 3.28: A representation of the distances between nodes.

Fig. 3.29 presents the secrecy outage probability versus the interference threshold ρ_{th} for different distances between the SU transmitter (S) and the eavesdropper (E), (d_{SE}). One can notice that as the eavesdropper becomes closer to the transmitter S (d_{SE} reduces), there is a higher probability that the wiretap channel's conditions improving, which implies better signal reception at the receiver. That is, the secrecy degrades as the capability of the eavesdropper to intercept the information improves. Moreover, as the interference threshold (ρ_{th}) increases, the secrecy improves as the transmitter can enhance the transmitting power. In addition, one can notice that regardless of the distance between S and E, all SOP curves saturate at high values of the threshold level (ρ_{th}). This is because as ρ_{th} increases to very high values, the system undergoes a non-cognitive state as

the limit over the transmit power is ignored and the transmitting power at S can take its maximum value. This can be noticed by setting the threshold ρ_{th} to ∞ in (3.102).

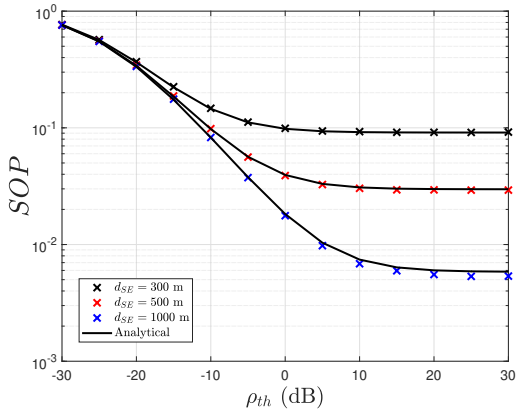

Figure 3.29: The secrecy outage probability (SOP) versus the interference level (ρ_{th}) for different distances between the transmitter S and the eavesdropper E, (d_{SE}). $d_{SP} = 500$ m, $d_{Sd_1} = 10$ m, $d_{d_1D} = 10$ m, $C_{th} = 0.7$ bit/sec/Hz, $PL = 3$, and $n = 2$.

Fig. 3.30 shows the secrecy outage probability as a function of the target secrecy rate (C_{th}) for different values of the interference threshold (ρ_{th}) and for a cascade level $n = 3$. One can notice that when the target secrecy rate increases, the overall achieved system secrecy becomes poorer. Furthermore, the results reveal that the gap between the SOP curves for different values of the interference threshold ρ_{th} for low values of C_{th} is lower than the gap for high values of C_{th}. That is, the effect of decreasing the interference level at the PU receiver (P_R) can be reduced for low values of the target secrecy rate.

Fig. 3.31 represents the effect of the cascade level n, i.e., the number of keyholes in the channel, over the probability of non-zero secrecy capacity (P_r^{nzc}). We assume that the distance from the transmitter S to the next object blocking the path to D (d_{Sd_1}) equals the distance between the node d_1 to d_2 $(d_{d_1d_2})$ and also the distance between node d_2 and the final destination D (d_{d_2D}). It can be noticed that as the distance between S and E increases, the system becomes more robust against this passive eavesdropping. This occurs because the received SNR reduces as the eavesdropper moves away from the transmitting node S, which results in a degradation in the strength of the signal received at the eavesdropper E as well as in the ability of E to intercept and decode the information correctly. Furthermore, as the cascade level n increases, the secrecy degrades since more severe

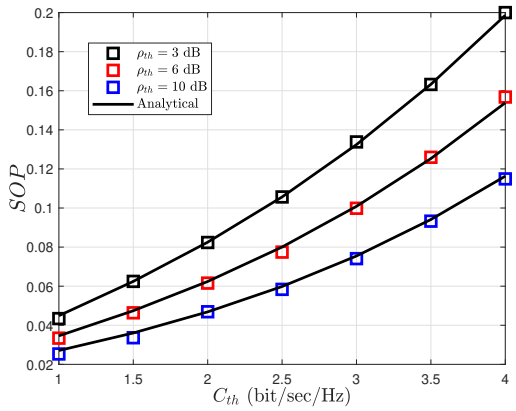

Figure 3.30: The secrecy outage probability (SOP) versus the target secrecy rate (C_{th}) for different values of the interference threshold ρ_{th}. $n = 3$, $d_{SP} = 500$ m, $d_{SE} = 1000$ m, $PL = 3$, $d_{Sd_1} = 5$ m, $d_{d_1 d_2} = 5$ m, and $d_{d_2 D} = 5$ m.

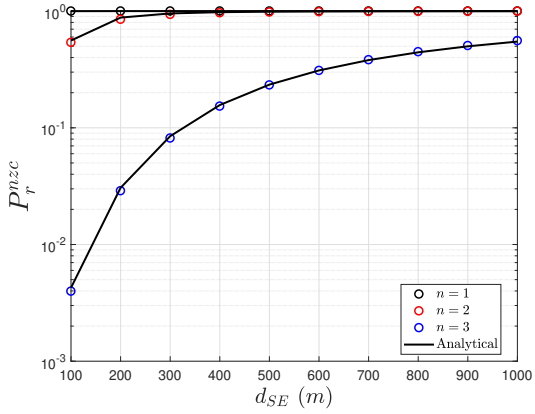

Figure 3.31: The probability of non-zero secrecy capacity (P_{rnzc}) versus the distance between S and E, (d_{SE}) for several values of cascade level (n). $PL = 3$, $d_{Sd_1} = 10$ m, $d_{d_1 d_2} = 10$ m, and $d_{d_2 D} = 10$ m.

fading conditions emerge as the level of the cascade (the number of keyholes) rises. Moreover, one can notice that the gap between the curves of the probability of non-zero secrecy capacity for a closer eavesdropper E is wider than the gap when d_{SE} gets larger. That is, the effect of the cascade level at the main channel can be reduced as d_{SE} increases.

Fig. 3.32 shows the effect of the cascade degree of the main channel over the intercept probability for a single $(n = 1)$ and a cascaded Rayleigh fading channels $(n = 4)$. It can be observed that for a single Rayleigh fading channel, when $d_{SE} \geq 300$ m, the communication secrecy is considered to be acceptable. However, if the eavesdropper is at distance $d_{SE} < 300$, the probability that the eavesdropper can intercept and decode the confidential information correctly increases. On the other hand, when the main channel becomes poorer for higher cascade levels as shown for $n = 4$, the secrecy is significantly affected.

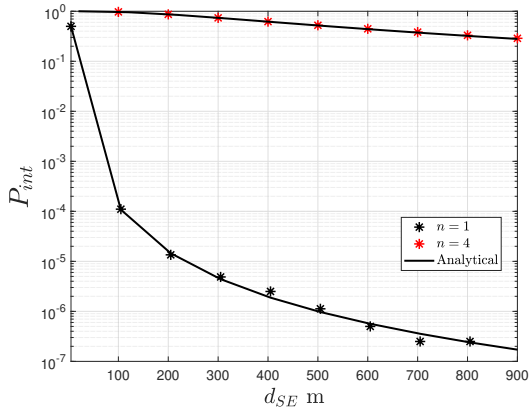

Figure 3.32: The intercept probability versus the distance between S and E, (d_{SE}) for single and cascaded Rayleigh fading channels. $PL = 3$, $d_{Sd_1} = 5$ m, $d_{d_1d_2} = 5$ m, $d_{d_2d_3} = 5$ m, and $d_{d_3D} = 5$ m.

3.18 Summery

This chapter establishes the PDF of cascaded κ-μ channels. Using these cascaded channels, the PLS was investigated for three wiretap system scenarios: the worst-case scenario, the regular scenario with colluding eavesdroppers, and the regular scenario with non-colluding eavesdroppers. We proved that the cascaded channel affects secrecy. The results indicate that increasing the cascade

level of the main channel and/or the number of eavesdropper's antennas compromises system secrecy. Additionally, the security of two cases involving CRN over cascaded channels was examined using PLS. The first scenario assumed the operation of a SIMO CRN over cascaded κ-μ channels, whereas the second assumed the operation of a SISO CRN over cascaded Rayleigh channels. We verified the generality of our first scenario by altering particular elements to generate the second scenario. Additionally, we demonstrated how privacy might be enhanced by adding extra antennas to the legitimate receiver. We highlighted how the constraint on transmit power can have a large impact on secrecy when SUs use the underlay model to access the channel.

Chapter 4

Secrecy Analysis for Energy Harvesting Enabled CRNs

4.1 Introduction

Apart from the additional functions performed by SUs which need energy, the energy consumption challenge associated with the collaboration among users in CRNs should be addressed. Therefore, energy harvesting (EH) has lately emerged as a viable method for addressing this issue, particularly for energy-constrained systems [3]. One of the effective energy harvesting techniques is simultaneous wireless information and power transfer (SWIPT). This technique is based on the notion that radio frequency (RF) signals are composed of both energy and information [106]. In this case, the receiver can harvest energy from the same received messages. However, to enable the SWIPT technique, the receiver must implement one of the following EH protocols: power splitting (PS), time switching (TS), or antenna selection (AS). Integrating EH with CRNs has the advantage of improving both spectral efficiency and energy efficiency.

In this chapter, PLS for underlay CRNs-based SWIPT over cascaded fading channels is investigated. Three different system models are considered and studied. The security is studied in terms of the probability of non-zero secrecy capacity and the intercept probability.

4.2 Secrecy Analysis for Energy Harvesting-Enabled CRNs in Cascaded Fading Channels with Destination Assistance

Consider an underlay CRN, in which an SU transmitter communicating with an SU destination with the presence of a PU receiver. The confidentiality of the shared information between SUs is threatened by an eavesdropper. We presume that the SU destination employs the power splitting (PS) technique to harvest energy from the SU transmitter. The harvested energy is used to produce jamming signals (artificial noise) to be transmitted to mislead the eavesdropper and degrade the reception's quality. Furthermore, the SU destination is empowered with the FD capability in order to receive the useful information and transmits jamming signals at the same time. The main channel is assumed to follow the cascaded κ-μ fading model, while the wiretap channel undergoes single κ-μ distribution to study the system in its worst-case conditions [66].

Assume an SU transmitter (S) communicating with an SU receiver (D) over a cascaded κ-μ fading channel with the attempt of an eavesdropper (E) for intercepting the SUs' information through the wiretap channel. The channel gain h_{SD} follows the cascaded κ-μ fading model, whereas h_{SE} and h_{DE} both follow a single κ-μ fading model. Supposing the SUs access the licensed band using underlay mode, a PU receiver (P_R) is residing in the transmission range of S. The channel between S and P_R is denoted by h_{SP} and follows a single Rayleigh fading model (see Fig. 4.1). All the devices are assumed to be equipped with a single antenna except for D. We assume that D is equipped with two isolated antennas; one for reception from S and one for transmitting jamming signals to confound E. We assume that P_R is located far away from D and the impact of jamming signals over P_R can be ignored. First, S transmits a "wake up" message to D. D will harvest energy from this message using the PS technique. The harvested energy will be stored in the battery of D to be used in the next symbol duration for jamming the eavesdropper [71]. In the next symbol duration, S sends the confidential information, which will be received by D and intercepted by E. Due to the FD capability of D, while receiving the signals using one of the antennas, jamming signals will be transmitted by exploiting the stored harvested energy in the previous symbol duration. Similar to [71], we assume that the battery of D charges and discharges at the same time.

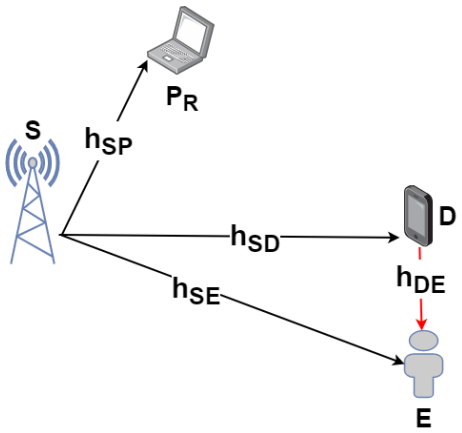

Figure 4.1: The system model.

The received message at the SU destination (D) is given as

$$y_D = \sqrt{(1-\theta)P_s}h_{SD}x_s + n_D, \tag{4.1}$$

where $0 < \theta < 1$ is the power splitting factor, in which θP_s is the portion used for energy harvesting. P_s is the transmission power of S, x_s is the transmitted symbol, and n_D is the AWGN at D with zero mean and variance N_0. Without loss of generality, in (4.1), we assume that the destination is capable of cancelling the self-interference generated due to the FD propriety [107] using one the techniques of self-interference cancellation (SIC) [108], [109]. In addition, the intercepted message at the eavesdropper is given by

$$y_E = \sqrt{(1-\tau)P_s}h_{SE}x_s + \sqrt{P_J}h_{DE}x_D + n_E, \tag{4.2}$$

where h_{DE} is the channel gain from D to E, P_J is the jamming power (artificial noise) sent by D, x_D is the jamming signal, and n_E is the AWGN at E with zero mean and variance N_0. In our work, we study two scenarios for the eavesdropper for comparison; one when E is harvesting energy from the intercepted RF signal from S $(\tau = \theta)$, while the other case is when E not harvesting energy $(\tau = 0)$.

In the context of underlay mode, S should ensure that the transmitting power (P_s) is maintained below an interference level (I_{th}) that is tolerable by the PU receiver (P_R) as $P_s \leqslant \frac{I_{th}}{|h_{SP}|^2}$. The

harvested energy at D during the previous symbol duration is given by

$$EH = \theta P_s \eta T \left| h_{SD}^{(P)} \right|^2, \tag{4.3}$$

where $0 < \eta < 1$ denotes the energy transfer efficiency coefficient, which depends on EH circuitry at D. T is the symbol duration. $h_{SD}^{(P)}$ is the channel gain between S and D in the previous symbol duration, which represents the link used for harvesting the energy [71]. Consequently, the transmission power at D is given by

$$P_J = \frac{EH}{T} = \theta P_s \eta \left| h_{SD}^{(P)} \right|^2. \tag{4.4}$$

Using (4.1), the instantaneous received SNR at D is given by

$$\gamma_D = \frac{(1-\theta) P_s \left| h_{SD} \right|^2}{N_0}. \tag{4.5}$$

Similarly, the received signal-to-interference-plus-noise ratio (SINR) at E is given by

$$\gamma_E = \frac{(1-\tau) P_s \left| h_{SE} \right|^2}{P_J \left| h_{DE} \right|^2 + N_0}. \tag{4.6}$$

We assume that the interference is dominant in the system [110]. Hence, the SINR at E is approximated as

$$\gamma_E \approx \frac{(1-\tau) P_s \left| h_{SE} \right|^2}{P_J \left| h_{DE} \right|^2}. \tag{4.7}$$

h_{SD} follows the cascaded κ-μ fading model with a cascade level n. Let $h_{SD} = \prod_{i=1}^{n} x_i$, where x_i follows the κ-μ fading model with the parameters κ_i and μ_i (for $i = 1, 2, \cdots, n$). The PDF of h_{SD} is given in (3.6). The PDF of $|h_{SE}|^2$ and $|h_{DE}|^2$ can be found from (3.1) and using transformation of random variables as

$$\begin{aligned} f_{|h_k|^2}(x) &= C_k x^{\frac{\mu_k - 1}{2}} \exp\left[-\mu_k \left(1 + \kappa_k\right) x\right] I_{\mu_k - 1}\left[2\mu_k \left(\sqrt{\kappa_k \left(1 + \kappa_k\right)}\right) x^{\frac{1}{2}}\right] \\ &\quad \text{for} \quad k \in \{SE, DE\}, \end{aligned} \tag{4.8}$$

where $C_k = \frac{\mu_k(1+\kappa_k)^{\frac{\mu_k+1}{2}}}{\kappa_k^{\frac{\mu_k-1}{2}}\exp(\kappa_k\mu_k)}$. Let $h_{SD}^{(P)} = \prod_{j=1}^{np} x_j$, where x_j follows the κ-μ fading model. κ_{jp} and μ_{jp} (for $j = 1, 2, \cdots, np$) are the fading channel parameters for the random variable x_j. The PDF of $h_{SD}^{(P)}$ follows the cascaded κ-μ fading channel with a cascade level np as

$$f_{h_{SD}^{(P)}}(y) = \sum_{l_{1p}=0}^{\infty}\sum_{l_{2p}=0}^{\infty}\cdots\sum_{l_{np}=0}^{\infty} C_{xp} y^{2\mu_{1p}+2l_{1p}-1} G_{np\ np}^{0\ np}\left(\begin{matrix}\beta_p \\ - \end{matrix}\middle| \frac{1}{y^2\prod_{j=1}^{np}\mu_{jp}(1+\kappa_{jp})}\right), \quad (4.9)$$

where $\beta_p = \mu_{1p} - \mu_{2p} + l_{1p} - l_{2p} + 1, \cdots, \mu_{1p} - \mu_{np} + l_{1p} - l_{np} + 1, 1$ and

$$\begin{aligned} C_{xp} =& 2\prod_{j=1}^{np}\left[\frac{[\mu_{jp}(1+\kappa_{jp})]^{\mu_{1p}-\mu_{ip}+l_{1p}-l_{jp}}\mu_{ip}}{\kappa_{jp}^{\frac{\mu_{jp}-1}{2}}\exp(\kappa_{jp}\mu_{jp})\Gamma(l_{jp}+\mu_{jp})}\right] \\ &\times\prod_{j=1}^{np}\left[\frac{(1+\kappa_{jp})^{\frac{\mu_{jp}+1}{2}}\left[2\mu_{jp}\sqrt{\kappa_{jp}(1+\kappa_{jp})}\right]^{2l_{jp}+\mu_{jp}-1}}{(l_{jp})!\,2^{2l_{jp}+\mu_{jp}-1}}\right]. \end{aligned}$$

4.2.1 PLS Analysis

In this section, we assess the secrecy in terms of probability of non-zero secrecy capacity (P_r^{nzc}) for two scenarios; scenario-I when both D and E are performing EH and scenario-II when only D is performing EH. Intercept probability P_{int} is also evaluated.

4.2.2 Probability of Non-Zero Secrecy Capacity: Scenario-I

The probability of achieving a better capacity at the main link compared to the wiretap channel's, i.e., the probability of non-zero secrecy capacity (P_r^{nzc}) is evaluated while E has a limited battery life and equipped with an energy harvester to prolong the battery lifetime ($\tau = \theta$) [111]. Given this, P_r^{nzc} is given by

$$P_r^{nzc} = P_r(C_s > 0) = 1 - P_r\left(g_{SD} \leqslant \frac{N_0 g_{SE} g_{SP}}{\theta\eta I_{th} g_{SD}^{(P)} g_{DE}}\right) = 1 - \int_0^{\infty} F_{g_{SD}}(y) f_Y(y) dy, \quad (4.10)$$

where $Y = \frac{N_0 g_{SE} g_{SP}}{\theta\eta I_{th} g_{SD}^{(P)} g_{DE}}$, and $g_m = |h_m|^2$, for $m = SD, SE, SP, SD^{(P)}$, and DE. Let $A = g_{SE} g_{SP}$ and $B = \frac{\theta\eta I_{th}}{N_0} g_{SD}^{(P)} g_{DE}$. To obtain the PDF of the variable Y, the PDFs of A and B

need to be obtained. The PDF of A is given by

$$f_A(y) = \int_{-\infty}^{\infty} \frac{1}{|t|} f_{g_{SE}}\left(\frac{y}{t}\right) f_{g_{SP}}(t)dt. \tag{4.11}$$

Using (4.8), $f_{g_{SP}}(y) = \lambda_p \exp(-\lambda_p y)$, [82, eq. 7.813.1], and [83, eq. (8.4.3.1)] yields

$$f_A(y) = \sum_{v=0}^{\infty} C_{N1} y^{\mu_{SE}+v-1} G_{2\ 0}^{0\ 2}\left(\begin{matrix}\mu_{SE}+v,1\\ -\end{matrix}\middle| \frac{1}{\mu_{SE}\lambda_p(1+\kappa_{SE})y}\right), \tag{4.12}$$

where $C_{N1} = \frac{\lambda_p^{\mu_{SE}+v-1} C_{SE} \lambda_p \left(\mu_{SE}\sqrt{\kappa_{SE}(1+\kappa_{SE})}\right)^{2v+\mu_{SE}-1}}{2\Gamma(v+\mu_{SE})v!}$. Let $B = \zeta B'$, where $\zeta = \frac{\theta\eta I_{th}}{N_0}$ and $B' = g_{SD}^{(P)} g_{DE}$. Using (4.11) and [82, eq. 7.813.1], the PDF of B' is given by

$$\begin{aligned} f_{B'}(y) &= \sum_{l_{1p}=0}^{\infty}\sum_{l_{2p}=0}^{\infty}\cdots\sum_{l_{np}=0}^{\infty}\sum_{\alpha_1=0}^{\infty} C_{t1} y^{\mu_{1p}+l_{1p}-1} \\ &\times G_{0\ np+1}^{np+1\ 0}\left(\begin{matrix}-\\ g\end{matrix}\middle| \mu_{DE}(1+\kappa_{DE})\prod_{j=1}^{np}\mu_{jp}(1+\kappa_{jp})y\right), \end{aligned} \tag{4.13}$$

where $g = 1-\beta_p, \mu_{DE} - \mu_{1p} - l_{1p} + \alpha_1$ and

$$C_{t1} = \frac{C_{DE}C_{xp}\left(\mu_{DE}\sqrt{\kappa_{DE}(1+\kappa_{DE})}\right)^{2\alpha_1+\mu_{DE}-1}\left(\mu_{DE}(1+\kappa_{DE})\right)^{-\mu_{DE}-\alpha_1+\mu_{1p}+l_{1p}}}{4\Gamma(\alpha_1+\mu_{DE})\alpha_1!}.$$

The PDF of Y is given by

$$f_Y(y) = \int_0^{\infty} y_b f_A(yy_b) f_B(y_b) dy_b. \tag{4.14}$$

Performing transformation of random variables and substituting (4.12) and (4.13) into (4.14) and using [83, eq. (2.24.1.1)] yields

$$\begin{aligned} f_Y(y) &= \sum_{l_{1p}=0}^{\infty}\sum_{l_{2p}=0}^{\infty}\cdots\sum_{l_{np}=0}^{\infty}\sum_{v=0}^{\infty}\sum_{\alpha_1=0}^{\infty} C_{t2} y^{-\mu_{1p}-l_{1p}-1} \\ &\times G_{2\ np+1}^{np+1\ 2}\left(\begin{matrix}-\mu_{1p}-l_{1p},1-\mu_{1p}-\mu_{SE}-v-l_{1p}\\ g\end{matrix}\middle| \frac{i_n}{y\zeta}\right), \end{aligned} \tag{4.15}$$

where $i_n = \frac{\mu_{DE}(1+\kappa_{DE})\prod_{j=1}^{np}\mu_{jp(1+\kappa_{jp})}}{\mu_{SE(1+\kappa_{SE})}\lambda_p}$ and $C_{t2} = \frac{C_{N1}C_{t1}(\mu_{SE}(1+\kappa_{SE})\lambda_p)^{-\mu_{1p}-l_{1p}-\mu_{SE}-v}}{\zeta^{\mu_{1p}+l_{1p}}\mu_{DE}(1+\kappa_{DE})^{\alpha_1+\mu_{DE}-\mu_{1p}-l_{1p}}}$.
Using (3.6), the CDF of g_{SD} is given by

$$F_{g_{SD}}(x) = \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\frac{c_x}{2}x^{\mu_1+l_1}G_{1\ n+1}^{n\ 1}\left(\begin{matrix}1-\mu_1-l_1\\ 1-\beta,-\mu_1-l_1\end{matrix}\middle| x\prod_{i=1}^{n}\mu_i\left(1+\kappa_i\right)\right). \tag{4.16}$$

Finally, using (4.15) and (4.16), P_r^{nzc} in (4.10) can be expressed as

$$\begin{aligned} P_r^{nzc} &= 1-\sum_{v=0}^{\infty}\sum_{\alpha_1=0}^{\infty}\sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}C_{tf}\sum_{l_{1p}=0}^{\infty}\sum_{l_{2p}=0}^{\infty}\cdots\sum_{l_{np}=0}^{\infty}\left(\prod_{i=1}^{n}\mu_i(1+\kappa_i)\right)^{-\mu_1-l_1+\mu_{1p}+l_{1p}} \\ &\times \quad G_{np+n+2\ 3}^{3\ \ np+n+1}\left(\begin{matrix}\psi\\ \psi'\end{matrix}\middle|\frac{\zeta}{i_n\prod_{i=1}^{n}\mu_i\left(1+\kappa_i\right)}\right), \end{aligned} \tag{4.17}$$

where $\psi = \beta_p, 1-\mu_{DE}+\mu_{1p}-\alpha_1+l_{1p}, -\mu_2-l_2+1+\mu_{1p}+l_{1p}, \cdots, -\mu_n-l_n+1+\mu_{1p}+l_{1p}, 1-\mu_1-l_1+\mu_{1p}+l_{1p}, 1+\mu_{1p}+l_{1p}$, $\psi' = \mu_{1p}+l_{1p}+1, \mu_{1p}+\mu_{SE}+v+l_{1p}, l_{1p}+\mu_{1p}$, and $C_{tf} = \frac{c_x C_{t2}(\mu_{SE}(1+\kappa_{SE})\lambda_p)^{-\mu_{1p}-l_{1p}-\mu_{SE}-v}}{2\zeta^{\mu_{1p}+l_{1p}}}$.

4.2.3 Probability of Non-Zero Secrecy Capacity: Scenario-II

Setting $\tau = 0$ in (4.7) implies that E is not performing EH, which is the case in which S is not aware of the EH capabilities of E. Using same steps to reach (4.17), P_r^{nzc} is given by

$$\begin{aligned} P_r^{nzc} &= 1-\sum_{v=0}^{\infty}\sum_{\alpha_1=0}^{\infty}\sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\chi\sum_{l_{1p}=0}^{\infty}\sum_{l_{2p}=0}^{\infty}\cdots\sum_{l_{np}=0}^{\infty}\left(\prod_{i=1}^{n}\mu_i(1+\kappa_i)\right)^{-\mu_1-l_1+\mu_{1p}+l_{1p}} \\ &\times \quad G_{np+n+2\ 3}^{3\ \ np+n+1}\left(\begin{matrix}\psi\\ \psi'\end{matrix}\middle|\frac{\zeta'}{i_n\prod_{i=1}^{n}\mu_i\left(1+\kappa_i\right)}\right), \end{aligned} \tag{4.18}$$

where $\psi = \beta_p, 1-\mu_{DE}+\mu_{1p}-\alpha_1+l_{1p}, -\mu_2-l_2+1+\mu_{1p}+l_{1p}, \cdots, -\mu_n-l_n+1+\mu_{1p}+l_{1p}, 1-\mu_1-l_1+\mu_{1p}+l_{1p}, 1+\mu_{1p}+l_{1p}$, $\psi' = \mu_{1p}+l_{1p}+1, \mu_{1p}+\mu_{SE}+v+l_{1p}, l_{1p}+\mu_{1p}$, $\chi = \frac{c_x C_{t2}(\mu_{SE}(1+\kappa_{SE})\lambda_p)^{-\mu_{1p}-l_{1p}-\mu_{SE}-v}}{2\zeta'^{\mu_{1p}+l_{1p}}}$, and $\zeta' = \frac{\theta(1-\theta)\eta I_{th}}{N_0}$.

4.2.4 Intercept Probability

The intercept probability (P_{int}) is defined as the probability that the eavesdropper is intercepting the confidential information, which is approached when the wiretap channel's capacity is higher than

the main channel's capacity [112] as

$$P_{int} \quad = \quad P_r\left(C_s < 0\right) = 1 - P_r^{nzc}. \tag{4.19}$$

Substituting (4.17) or (4.18), we evaluate the P_{int} for the two scenarios discussed above.

4.2.5 Reliability of the System

In this section, we evaluate the outage probability (OP) to assess the reliability of the system, which is defined as the probability that the main channel's capacity falls below a predetermined target rate R_s as

$$OP = P_r\left(C_D < R_s\right) = P_r\left(g_{SD} < J g_{SP}\right) = \int_0^{\infty} F_{g_{SD}}(z) f_Z(z), \tag{4.20}$$

where $J = \frac{(2^{R_s}-1)N_0}{(1-\theta)I_{th}}$ and $Z = J g_{SP}$. Using transformations of random variables, the PDF of Z is given by

$$f_Z(z) = \frac{\lambda_p}{J} \exp\left(-\frac{\lambda_p z}{J}\right). \tag{4.21}$$

Using (4.16), (4.21), and [82, eq. 7.813.1], (4.20) is solved as

$$OP = \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty} \frac{c_x}{2}\left(\frac{\lambda_p}{J}\right)^{-\mu_1-l_1} G_{2\ n+1}^{n\ 2}\left(\begin{matrix}-\mu_1-l_1, 1-\mu_1-l_1\\ 1-\beta, -\mu_1-l_1\end{matrix}\middle| \frac{J\prod_{i=1}^{n}\mu_i\left(1+\kappa_i\right)}{\lambda_p}\right). \tag{4.22}$$

4.3 Numerical Results

The numerical results and Monte-Carlo simulations are provided in this section. The results are obtained by truncating the infinite series expansion to the first 5 terms. The channel parameters are: $\kappa_k = 1, \mu_k = 1,$ for $k \in \{SE, DE, 1p\}$, $I_{th} = 5$ dB, and $\lambda_p = 5$.

Fig. 4.2 depicts the P_r^{nzc} versus the maximum interference tolerable at P_R (I_{th}) revealing the impact of the several number of scatters between S and D (n). It is noticeable that more obstacles distributed in the main channel, i.e., the cascade level n rise up, signify higher severe fading. This

will deteriorate the main channel's strength and hence weaken the secrecy of the SUs. In addition, as I_{th} becomes larger, more freedom is given to the SU transmitter to boost the transmission power. That is, increasing the transmission power will improve the main channel's conditions and thus achieving better secrecy.

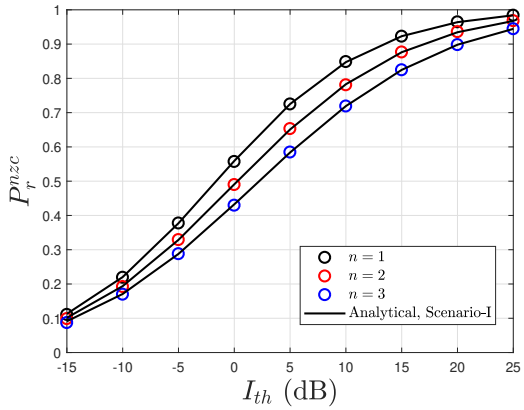

Figure 4.2: The probability of non-zero secrecy capacity versus the interference threshold (I_{th}) for multiple cascade level n. The main channel parameters are: $\kappa = 1$, $\mu = 1$. $\theta = 0.5$, $np = 1$ and $\eta = 0.8$.

Fig. 4.3 illustrates the P_r^{nzc} as a function of the power splitting factor (θ) for certain values of EH efficiency coefficient (η). The result represents the scenario when E is also harvesting energy from (S) with a PS factor (θ). This means that D and E have the same amount of energy left for information processing . Consequently, the impact of the transmission power at the main and wiretap channels is not comparable. However, E is still influenced by the jamming power flowing from D, which is a function of θ. Therefore, the greater the energy harvested, which is represented by the values of θ and η, the higher the chance for the SUs to share the confidential information securely. This highlights the effectiveness of jamming through EH for disrupting E and ensuring safer communication.

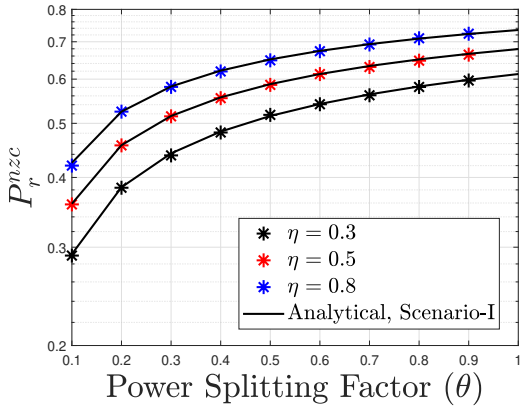

Figure 4.3: The probability of non-zero secrecy capacity versus the power splitting factor (θ). The main channel parameters are: $\kappa = 1$, $\mu = 1$. $n = 2$, and $np = 1$.

Fig. 4.4 shows the P_r^{nzc} against θ. The outcome is a concave function of θ. The result demonstrates the case where E is not presumed to harvest energy. In this case, for low values of the portion used for harvesting (θ), secrecy is guaranteed to be improving until $\theta = 0.5$. The optimal secrecy is reachable when $\theta \approx 0.5$. Beyond this value, the fraction used for information processing $(1 - \theta)$ at D declines. This weakens the main channel's capacity and renders a reduction in the privacy of the SUs' communication. For the same scenario, Fig. 4.5 shows the P_r^{nzc} versus θ and the EH conversion factor (η). According to the levels of the P_r^{nzc}, it is concluded that the optimum secrecy of data transmission is attainable when $\theta = 0.5$ and η is at its maximum $(\eta = 1)$.

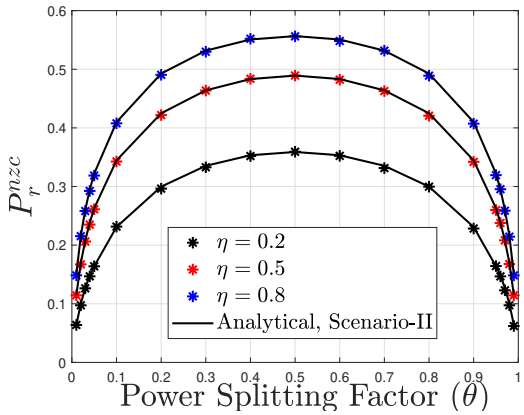

Figure 4.4: The probability of non-zero secrecy capacity versus the power splitting factor (θ). The main channel parameters are: $\kappa = 1$, $\mu = 1$. $n = 2$, and $np = 1$.

Fig. 4.6 presents a trade-off between system's reliability and security. As θ increases, implying

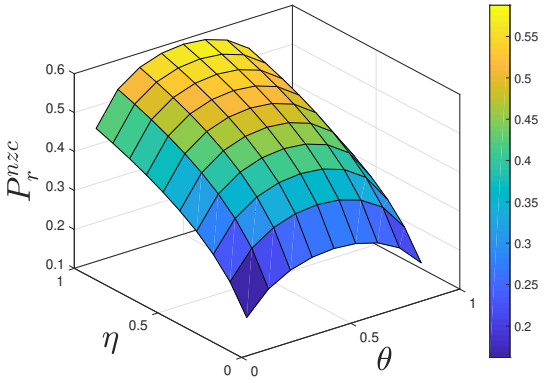

Figure 4.5: The probability of non-zero secrecy capacity versus θ and η. The main channel parameters are: $\kappa = 1$, $\mu = 1$. $n = 2$, and $np = 1$.

a higher share of the energy obtained for jamming, a smaller segment of energy left to process information. This lowers the capacity of the main channel, which deteriorates the data rate and thus raises the risk of an outage. Additionally, for the case of an energy harvesting E, the amount of energy remaining to process information at D and E is equivalent. However, E remains impaired by the jamming power, decreasing the capability of decoding and the risk of interception. Nevertheless, when E is not performing EH, the chance of E to intercept is at its highest when θ is very low or very high. This is due to the fact that at low θ, a small amount of jamming power is impacting E, while at high θ, a smaller fraction of energy used for information processing is recognized at D.

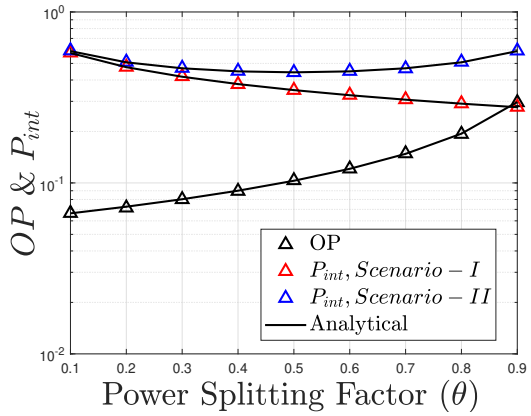

Figure 4.6: The outage probability and the intercept probability versus the power splitting factor (θ). The main channel parameters are: $\kappa = 1$, $\mu = 1$. $n = 2$, $I_{th} = 5$dB, $np = 1$, and $\eta = 0.8$.

4.4 Secrecy Analysis for EH-Enabled CRNs with Cooperative Jammer

In this section, we assume a CRN, in which a SU transmitter (S) communicates with a SU receiver (D) through the main channel (h_{SD}) in the presence of multiple non-colluding eavesdroppers. These eavesdroppers attempt to tap the confidential information shared between S and D. The eavesdroppers are assumed to be randomly distributed according to a homogeneous Poisson point process (HPPP) with density λ_e. We assume that the eavesdroppers are distributed in an unbounded Euclidean space of dimension U. The term $h_{S,Ei}$ represents the wiretap channel between S and the k^{th} eavesdropper (see Fig. 4.7). The channel h_{SD} follows a cascaded κ-μ fading model, whereas $h_{S,Ei}$ follows a single κ-μ fading channel[1]. All users are assumed to be equipped with a single antenna. In addition, the SUs are accessing the licensed band via the underlay access mode. Hence, S should ensure not to degrade the quality of service (QoS) of the PUs' communication by guaranteeing that the interference impacting the PU receiver (P_R) is tolerable. The interference channel between S and P_R follows a single Rayleigh model, which is a special case of the κ-μ model where $\kappa \to 0$ and $\mu = 1$ [67]. The system model under consideration is suitable to model the cognitive vehicular network (CVN) [5], [113], [10], [104]. This CVN model may represent a case where a PU destination is a roadside infrastructure and the SUs and eavesdroppers represent moving vehicles [103], [10].

Cooperative jamming is one of the means used to boost security, where a secondary user serves as a jammer (R_J) to disrupt the received signal at the eavesdropper. However, jamming consumes energy. Hence, assuming R_J gathers energy from S, the harvested energy can produce jamming signals to degrade the eavesdropper's decoding capability. First, the k^{th} nearest eavesdropper to the transmitter S will be selected from the group of eavesdroppers in the network. The eavesdroppers' information regarding the positions related to the source can be obtained by assuming that the eavesdroppers are users in the network but they are untrusted and do not have the authorization to access the channel [94], [95]. For example, pay-TV broadcast services where it is possible to

[1]Our analyses are based on a worst-case scenario assumption by assuming that the main link suffers from a poor environment with many obstacles and objects. Hence, the main channel is more practical to be modeled as a cascaded $\kappa - \mu$ fading channel reflecting severe fading conditions. However, the rest of the channels are assumed to have better conditions with fewer scatters where it is more likely to follow a single $\kappa - \mu$ distribution [7], [66].

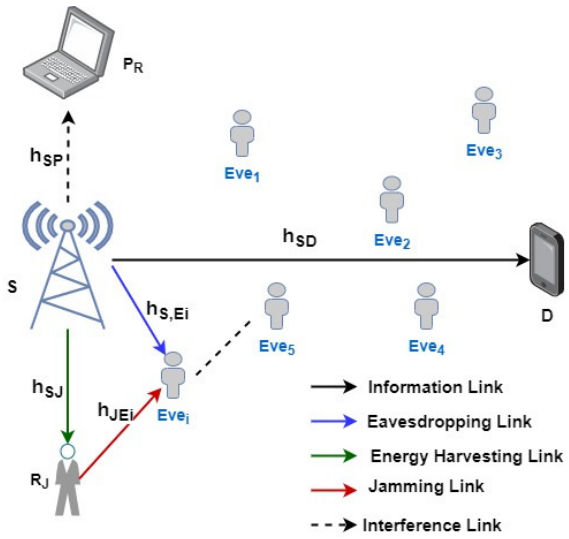

Figure 4.7: The system model.

assume that global channel state information of the eavesdroppers is available. Then, R_J harvests energy from the received RF signal from the transmitter S through the channel h_{SJ} using the power splitting (PS) technique [114, 69, 100]. In the PS technique, R_J splits the power of the received RF signal into; the energy harvesting part and the demodulation power part. The harvested energy will be stored in the battery and will be used to intervene with the signals received at the eavesdropper through channel h_{JEi}. In this section, we examine the scenario of secondary users cooperating to enhance security. That is, the remainder of the energy at R_J is required to charge the battery for subsequent transmissions. Particularly, R_J assists S in enhancing communication privacy while storing energy to compensate for the energy lost due to jamming. Moreover, it is worth mentioning that if R_J employs the remaining portion to transmit messages to D, the quality of the received messages at D will improve, hence enhancing the PLS. We assume that the channels h_{SJ} and h_{JEi} follow the κ-μ fading model. We also assume that the SU legitimate receiver D harvests energy with the power splitting technique to enhance its battery energy content.

The energy harvested at R_J is given by

$$EH = \frac{\theta \eta P_s T}{d_{SJ}^{PL}} \left| h_{SJ} \right|^2, \tag{4.23}$$

where P_s is the transmission power at S and $0 < \theta < 1$ is the power splitting factor at R_J, in which

θP_s is the portion used for energy harvesting and $(1-\theta)P_s$ is used for processing the information and recharging the battery of R_J. $0 < \eta < 1$ denotes the energy conversion efficiency coefficient. T is the energy harvesting duration, d_{SJ} is the distance between S and R_J, and PL is the path loss exponent. Using (4.23), the transmission power at R_J is given by

$$P_J = \frac{\theta\eta P_s \left|h_{SJ}\right|^2}{d_{SJ}^{PL}}. \tag{4.24}$$

Without loss of generality, we assume that the legitimate receiver (D) recognizes the pseudorandom sequence of the jamming signals transmitted by the friendly jammer and hence can be cancelled [69], [100]. At the SU destination, the received message is given by

$$y_D = \sqrt{\frac{(1-\phi)P_s}{d_{SD}^{PL}}} h_{SD} x_s + n_D, \tag{4.25}$$

where $0 < \phi < 1$ is the power splitting factor at D with $(1-\phi)P_s$ being the portion left for processing the information, d_{SD} is the distance between S and D, x_s is the transmitted symbol, and n_D is the AWGN at D with zero mean and variance N_0. The received message at the k^{th} eavesdropper (Eve_i) is given by

$$y_{Ei} = \sqrt{\frac{P_s}{d_i^{PL}}} h_{SEi} x_s + \sqrt{\frac{P_J}{d_{JEi}^{PL}}} h_{JEi} x_J + n_{Ei}, \tag{4.26}$$

where d_i is the distance between S and Eve_i, d_{JEi} is the distance between R_J and Eve_i, x_J is the jammer transmitted symbol, and n_{Ei} is the AWGN at Eve_i with zero mean and variance N_0. Using (4.25) and (4.26), the instantaneous received SNR at D and the received SINR at a random eavesdropper are given, respectively, by

$$\gamma_D = \frac{(1-\phi)P_s \left|h_{SD}\right|^2}{d_{SD}^{PL} N_0}, \tag{4.27}$$

$$\gamma_{Ei} = \frac{\frac{P_s \left|h_{S,Ei}\right|^2}{d_i^{PL}}}{\frac{P_J \left|h_{JEi}\right|^2}{d_{JEi}^{PL}} + N_0}. \tag{4.28}$$

We assume that the interference is dominant at the eavesdropper [110]. Hence, the SINR is approximated by

$$\gamma_{Ei} \approx \frac{\frac{P_s \left|h_{S,Ei}\right|^2}{d_i^{PL}}}{\frac{P_J |h_{JEi}|^2}{d_{JEi}^{PL}}}. \tag{4.29}$$

Assuming the underlay mode as aforementioned, the transmission power of S should be less than the interference threshold tolerable at P_R (I_{th}) . Given this, the jamming power in (4.24) is restricted to avoid degrading the PUs' communication [115]. As mentioned earlier, h_{SD} follows the cascaded κ-μ fading model. Hence, $h_{SD} = \prod_i^n x_i$, where x_i follows the κ-μ fading distribution with κ_i and μ_i (for $i = 1, 2, \cdots, n$) being the fading channel parameters. Hence, the PDF of h_{SD} is given as presented in (3.6) and the PDF of $|h_j|^2$ for $j \in \{(S, Ei), JEi, SJ\}$ can be found from (3.1) and using the transformation of random variables as

$$f_{|h_j|^2}(x) = c_j x^{\frac{\mu_j - 1}{2}} \exp\left[-\mu_j \left(1 + \kappa_j\right) x\right] I_{\mu_j - 1}\left[2\mu_j \left(\sqrt{\kappa_j \left(1 + \kappa_j\right)}\right) x^{\frac{1}{2}}\right], \tag{4.30}$$

where $c_j = \frac{\mu_j (1+\kappa_j)^{\frac{\mu_j+1}{2}}}{\kappa_j^{\frac{\mu_j-1}{2}} \exp(\kappa_j \mu_j)}$. Finally, the interference channel between S and PU receiver P_R (h_{SP}) follows the Rayleigh distribution. Hence, the PDF of $|h_{SP}|^2$ follows the Exponential distribution given in (3.73) with λ_P being the fading coefficient.

4.5 PLS Analysis

In this section, the probability of non-zero secrecy capacity and the intercept probability will be evaluated. In our analysis, the k^{th} nearest eavesdropper to the source S will be considered for intercepting the confidential information and for jamming. This is performed by measuring the Euclidean distance from S to each of the eavesdroppers and the distances will be in an ascending order.

4.5.1 Probability of Non-Zero Secrecy Capacity

Given the definition of the probability of non-zero secrecy capacity (P_r^{nzc}) in (3.37), (P_r^{nzc}) is expressed as

$$\begin{aligned} P_r^{nzc} &= P_r\left(C_s>0\right)=1-P_r\left(\frac{1+\frac{(1-\phi)P_s|h_{SD}|^2}{d_{SD}^{PL}N_0}}{1+\frac{\frac{P_s\left|h_{S,Ei}\right|^2}{d_i^{PL}}}{\frac{P_J|h_{JEi}|^2}{d_{JEi}^{PL}}}}\leqslant 1\right) \\ &= 1-P_r\left(|h_{SD}|^2\leqslant\frac{|h_{S,Ei}|^2|h_{SP}|^2/d_i^{PL}}{\left(\frac{\theta(1-\phi)\eta I_{th}}{N_0 d_{SD}^{PL}d_{JEi}^{PL}d_{SJ}^{PL}}\right)|h_{SJ}|^2|h_{JEi}|^2}\right)=1-I, \end{aligned} \tag{4.31}$$

where $I=\int_0^\infty F_{|h_{SD}|^2}(z)f_Z(z)dz$, $Z=\frac{|h_{SP}|^2\left|h_{S,Ei}\right|^2/d_i^{PL}}{q|h_{SJ}|^2|h_{JEi}|^2}$. Let $Z=\frac{Z_1}{qZ_2}$, where $Z_1=|h_{S,Ei}|^2/d_i^{PL}$, $Z_2=\frac{|h_{SJ}|^2|h_{JEi}|^2}{|h_{SP}|^2}$, and $q=\frac{\theta(1-\phi)\eta I_{th}}{d_{SD}^{PL}d_{JEi}^{PL}d_{SJ}^{PL}N_0}$. One needs to obtain the PDF of the variables Z_1 and Z_2 to find the PDF of Z. The CDF of $|h_{SD}|^2$ is found in (4.16). The PDF of the path loss d^{PL} is distributed as in (3.58). Furthermore, the PDF of Z_1 is found as

$$f_{Z_1}(z) = \int_0^\infty z_b f_{\left|h_{S,Ei}\right|^2}(zz_b)f_{d^{PL}}(z_b)dz_b. \tag{4.32}$$

Substituting (4.30) and (3.58) into (4.32) and using [83, Eq. (2.24.3.1)] with the help of some mathematical manipulations yields

$$f_{Z_1}(z)=\sum_{A=0}^{\infty}c_2 z^{-1-\delta k}G_{\,1\;\delta}^{\,\delta\;1}\left(\begin{matrix}\frac{1}{\frac{\delta-1+\mu_{SEi}+A+\delta k}{\delta}}\end{matrix}\middle|\frac{z^\delta\left(\mu_{SEi}\left(1+\kappa_{SEi}\right)\right)^\delta}{A_e\delta^\delta}\right), \tag{4.33}$$

where

$$c_2=\frac{c_1\delta A_e^k\left(\mu_{SEi}\sqrt{\kappa_{SEi}(1+\kappa_{SEi})}\right)^{\mu_{SEi}+2A-1}}{2\Gamma(k)A!\,\Gamma(\mu_e+A)(2\pi)^{\frac{\delta-1}{2}}}\delta^{\mu_{SEi}+A+\delta k-\frac{1}{2}}\left(\mu_{SEi}(1+\kappa_{SEi})\right)^{-\mu_{SEi}-A-\delta k}.$$

To obtain the PDF of the random variable Z_2, the PDF of $B=|h_{SJ}|^2|h_{JEi}|^2$ must be first obtained

as

$$f_B(y) = \int_{-\infty}^{\infty} \frac{1}{|t|} f_{|h_{SJ}|^2}\left(\frac{y}{t}\right) f_{|h_{JEi}|^2}(t)dt. \tag{4.34}$$

Substituting (4.30) into (4.34) and using [82, Eq. (7.813.1)] with some mathematical manipulations yields

$$\begin{aligned} f_B(y) &= \sum_{l_J=0}^{\infty}\sum_{l_{Ei}=0}^{\infty} y^{\mu_J+l_J-1} \frac{C_{SJ}C_{JEi}S_1\left(\mu_{JEi}(1+\kappa_{JEi})\right)^{\mu_{SJ}-\mu_{JEi}+l_J-l_{Ei}}}{4} \\ &\quad \times G_{0\,2}^{2\,0}\left(\begin{matrix} - \\ -\mu_{SJ}-l_J+\mu_{JEi}+l_{Ei},0 \end{matrix}\middle|\Upsilon y\right), \end{aligned} \tag{4.35}$$

where $\Upsilon = \mu_{SJ}(1+\kappa_{SJ})\mu_{JEi}(1+\kappa_{JEi})$ and

$$S_1 = \frac{\left(\mu_{SJ}\sqrt{\kappa_{SJ}(1+\kappa_{SJ})}\right)^{\mu_{SJ}+2l_J-1}\left(\mu_{JEi}\sqrt{\kappa_{JEi}(1+\kappa_{JEi})}\right)^{\mu_{JEi}+2l_{Ei}-1}}{(l_J)!\,\Gamma(\mu_{SJ}+l_J)(l_{Ei})!\,\Gamma(\mu_{JEi}+l_{Ei})}.$$

The PDF of Z_2 is then expressed as

$$f_{Z_2}(z) = \int_0^{\infty} z_b f_B(zz_b) f_{|h_{SP}|^2}(z_b)dz_b. \tag{4.36}$$

Using (3.73), (4.35), and [82, Eq. (7.813.1)], the PDF of Z_2 is given by

$$f_{Z_2}(y) = \sum_{l_J=0}^{\infty}\sum_{l_{Ei}=0}^{\infty} a_1 y^{\mu_J+l_J-1}\lambda_P^{-\mu_{SJ}-l_J-1} G_{1\,2}^{2\,1}\left(\begin{matrix} -\mu_{SJ}-l_J \\ -\mu_{SJ}-l_J+\mu_{JEi}+l_{Ei},0 \end{matrix}\middle|\frac{\Upsilon y}{\lambda_P}\right), \tag{4.37}$$

where $a_1 = \frac{\lambda_P C_{SJ}C_{JEi}S_1(\mu_{JEi}(1+\kappa_{JEi}))^{\mu_{SJ}-\mu_{JEi}+l_J-l_{Ei}}}{4}$. Using (4.33), (4.37), and [83, Eq. (2.24.1.1)] with the transformation of random variables, the PDF of Z is expressed as

$$f_Z(y) = \sum_{l_J=0}^{\infty}\sum_{l_{Ei}=0}^{\infty}\sum_{A=0}^{\infty} a_2' y^{-\delta k-1} G_{1+2\delta\;\;1+2\delta}^{2\delta\;\;\;\;2\delta}\left(\begin{matrix} 1,\frac{1+\delta k-\mu_{JEi}-l_{Ei}}{\delta},\frac{1-\mu_{SJ}-l_J+\delta k}{\delta} \\ \frac{\delta-1+\mu_{S,Ei}+A+\delta k}{\delta},\frac{1+\delta k}{\delta} \end{matrix}\middle|e_1 y^{\delta}\right), \tag{4.38}$$

where $L = 1/q$,

$$a_2' = \frac{a_1 c_2 \lambda_P^{-\mu_{SJ}-l_J-1} \delta^{\mu_{SJ}+l_J-\delta k-0.5}}{L^{-\delta k}\left(2\pi\right)^{1.5(\delta-1)}} \left(\frac{\Upsilon}{\lambda_P}\right)^{-\mu_{JEi}-l_J+\delta k},$$

and $e_1 = \frac{\left(\mu_{S,Ei}(1+\kappa_{S,Ei})\right)^{\delta}}{A_e L^{\delta}\left(\frac{\Upsilon}{\lambda_P}\right)^{\delta}}$. Finally, using (4.16), (4.38), and [83, Eq. (2.24.1.1)], P_r^{nzc} is given by

$$P_r^{nzc} = 1 - \sum_{l_1=0}^{\infty}\sum_{l_2=0}^{\infty}\cdots\sum_{l_n=0}^{\infty}\sum_{l_{Ei}=0}^{\infty}\sum_{l_J=0}^{\infty}\sum_{A=0}^{\infty} a_3' G_{1+3\delta+\delta n}^{\,3\delta\;\;1+2\delta+\delta n}{}_{3\delta} \left(\begin{matrix}\epsilon\\ \epsilon'\end{matrix}\middle| \frac{e_1\delta^{\delta n}}{\left(\prod_{i=1}^{n}\mu_i(1+\kappa_i)\right)^{\delta}}\right), \tag{4.39}$$

where $\epsilon = 1, \frac{1+\delta k-\mu_{JEi}-l_{Ei}}{\delta}, \frac{1+\delta k-\mu_{SJ}-l_J}{\delta}, \frac{1+\delta k-\mu_2-l_2}{\delta}\cdots, \frac{1+\delta k-\mu_n-l_n}{\delta}, \frac{1+\delta k-\mu_1-l_1}{\delta}, \frac{1+\delta k}{\delta}$, $\epsilon' = \frac{\delta-1+\mu_{S,Ei}+A+\delta k}{\delta}, \frac{1+\delta k}{\delta}, k$, and $a_3' = \frac{c_x a_2' \delta^{\mu_1 n+l_1 n-\delta k n+\sum_{i=1}^{n}\rho_i-0.5n-1}}{2(2\pi)^{0.5n(\delta-1)}}$ $\times\left(\prod_{i=1}^{n}\mu_i(1+\kappa_i)\right)^{-\mu_1-l_1+\delta k}$, with $\sum_{i=1}^{n}\rho_i = -\mu_1+\mu_2-l_1+l_2+\cdots-\mu_1+\mu_n-l_1+l_n$. Assessing the system security performance using (4.39) aids in testing all the system parameters and notice their impact over the level of privacy. Different from other security metrics, P_r^{nzc} demonstrates the reliability of the main channel compared to the wiretap channel.

4.5.2 Intercept Probability

The intercept probability (P_{int}) defined in (3.56) is expressed as

$$\begin{aligned} P_{int} &= P_r\left(C_s < 0\right) = P_r\left(C_D < C_{Ei}\right) \\ &= P_r\left(|h_{SD}|^2 \leqslant \frac{|h_{S,Ei}|^2 |h_{SP}|^2 / d_i^{PL}}{\left(\frac{\theta(1-\phi)\eta I_{th}}{N_0 d_{SD}^{PL} d_{JEi}^{PL} d_{SJ}^{PL}}\right)|h_{SJ}|^2 |h_{JEi}|^2}\right) = 1 - P_r^{nzc}. \end{aligned} \tag{4.40}$$

Substituting (4.39) into (4.40), the intercept probability of the system model under consideration can be reached. One may deduce from (4.40) that the intercept probability of an eavesdropper should be low in order to ensure safe messages transmission. One way to achieve this is through cooperative jamming-based energy harvesting. The numerical results section will demonstrate the impact of jamming and energy harvesting, as well as the effects of other system parameters.

4.6 Towards Improving the Security of the Main Channel

Determining the value of the power splitting factor aids the receiver, i.e., D, in estimating the quantity of energy to be harvested. Consequently, deciding on the value of the power splitting factor (ϕ) leads to determining the amount left for processing the information, i.e., $1-\phi$. In this context, the receiver can perform a trade-off between the reliability (security) of the system and the energy content in the receiver's storage devices.

In this section, the value of the PS factor (ϕ) that achieves a high secrecy is found. However, the value of the PS factor ϕ is determined by guaranteeing that the harvested energy at D is always greater than a minimum value (ζ) as

$$P_D \geq \zeta, \tag{4.41}$$

where P_D is the harvested power at D and is given by

$$P_D = \frac{\phi P_s \eta \left|h_{SD}\right|^2}{d_{SD}^{PL}}. \tag{4.42}$$

From (4.41) and (4.42), the optimal value of ϕ that would achieve the highest level of privacy without violating the power constraint in (4.41) is given by

$$\phi^* = \frac{\zeta d_{SD}^{PL}}{\eta P_s \left|h_{SD}\right|^2}. \tag{4.43}$$

In this scenario, the energy harvested at D cannot go below the minimum threshold ζ. This ensures that there is always enough energy available to charge the battery or accomplish other functions at the receiver end. Additionally, the effects of this adaptive PS factor on reaching the maximum privacy level, as well as a comparison of the security level reached by applying adaptive PS factor against fixed PS factors, will be addressed in the next section.

4.7 Numerical Results

In this section, we present our analytical results along with the Monte-carlo simulations. We assume a two-dimensional (2D) area $(U = 2)$ and a HPPP distribution of the eavesdroppers locations. We generate 10^5 realizations of the positions of the eavesdroppers in a square area of a side of 25 meters (m). The analytical results are obtained by truncating the infinite summations to the first seven terms $(l_i = 7, \text{ for } i = 1, 2, \cdots, n, l_{Ei} = 7, l_J = 7, \text{ and } A = 7)$ as the summations converge at these values. It is worth mentioning that the output saturates after the seventh term of the summation, and at this point the results match the simulations, demonstrating the precision of the obtained results. The transmitter S is located at the center of the designated area. To take the distance between the transmitter S and the PU receiver P_R, i.e., d_{SP} into account, we let $d_{SP}^{-PL} = \frac{1}{2\lambda_p}$. The parameters' values have been determined based on previous literature, such as [75], [116], [71] and are used here without loss of generality.

Fig. 4.8 shows the probability of non-zero secrecy capacity against the eavesdroppers' density (λ_e) for different values of k, where the value of k reflects the selected eavesdropper according to the Euclidean distance to the SU's transmitter (S). For instance, $k = 2$ indicates selecting the second closest eavesdropper to S. Clearly, the security of the SUs declines as the eavesdroppers' density grows irrespective of the value of k. This is interpreted by the fact that increasing λ_e elevates the probability of having a closer eavesdropper to S with improved interception capabilities. Additionally, the selection of the first nearest eavesdropper to the transmitter S, i.e., $k = 1$, has the most severe effect on SU's privacy as a result of the reliable channel conditions as opposed to larger values of k.

Fig. 4.9 depicts the probability of non-zero secrecy capacity versus the interference threshold tolerable at the PU receiver (P_R), i.e., I_{th} for different values of the power splitting factor at R_J (θ) and the energy harvesting conversion efficiency (η). Results reveal the improvement in the shared information's privacy with the increase of I_{th}. This is due to the fact that as I_{th} increases, the restriction over the transmission power of S becomes higher, resulting in higher transmission power and an improved obtained SNR at the legitimate receiver and the jammer. Furthermore, as the portion used for EH at R_J increases, indicating a higher portion of energy used for jamming the eavesdropper,

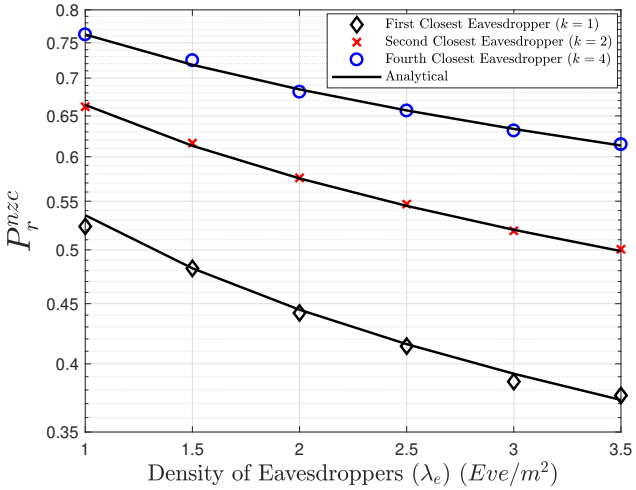

Figure 4.8: The probability of non-zero secrecy capacity versus the eavesdropper density (λ_e) for multiple values of k. The main channel parameters are: $\kappa = 1$, $\mu = 1$. The wiretap channel parameters are: $\kappa_e = 1$, $\mu_e = 1$. $PL = 2$, $\theta = 0.6$, $\eta = 0.8$, $\lambda_p = 5$, $\phi = 0.2$, $n = 2$, and $I_{th} = 5$ dB. $N_0 = 1$, $d_{SJ} = 1m$, $d_{JEi} = 5m$, $d_{SP} = 25m$, and $d_{SD} = 1m$.

the exchanged information can be shared more securely. Moreover, an energy harvesting conversion efficiency (η) is used to measure how effective energy harvesting is on degrading wiretap links. The privacy improves in accordance with the rise in η. This proves that cooperative jamming-based EH has a substantial influence in preventing eavesdroppers from successfully decoding intercepted information.

The impact of the cascade level (n) over the security of the shared information is explored in Fig. 4.10. It is evident that increasing the cascade level, which implies that the amount of obstacles along the path between S and D rises, results in poor privacy between legitimate users. On the other hand, regardless of the value of n, security is improved as the density of eavesdroppers (Eve/m^2) goes low. In addition, setting $\kappa \to 0$ and $\mu = 1$, represents the Rayleigh fading as a special case of this general fading model. For $n = 1$, our system model reduces to be operating over non-cascaded Rayleigh channels. This shows the generality of our assumptions and system model. Finally, as the channels fading severity reduces due to increasing the value of the fading parameter κ, the security improves. For these values of the fading parameters, it is clear that for the case of $\kappa \to 0$ and $n = 3$, the figure reveals a worst-case scenario.

Fig. 4.11 illustrates the probability of non-zero secrecy capacity versus the power splitting factor (θ) and the distance between the jammer R_J and the k^{th} eavesdropper (d_{JEi}). It is noteworthy that as the portion of energy dedicated for jamming the eavesdropper increases, the secrecy improves. This is because the jamming at the eavesdropper is greater as θ increases, worsening the state of the wiretap channel and weakening the ability of the eavesdropper to decode the information effectively. Furthermore, it is obvious that as the jammer gets closer to the eavesdropper, i.e., d_{JEi} becomes smaller, the jamming impact over the eavesdropper becomes higher. The optimum information privacy can be attained when θ is at its maximum value $(\theta = 1)$ and the jammer is very close to the eavesdropper $(d_{JEi} \leq 2m)$. This highlights the value of taking into account the distance impact over privacy. Finally, it can be concluded that depending on the distance to the eavesdropper, the jammer can adapt the amount of extracted energy. Specifically, the power of jamming signals received at the eavesdropper should be increased by R_J as the distance increases to ensure higher privacy. On the other hand, when d_{JEi} is small, the cooperating jammer R_J can adjust the transmission power by reducing the amount of harvested energy and increasing the amount for charging its battery, i.e., $(1-\theta)P_s$.

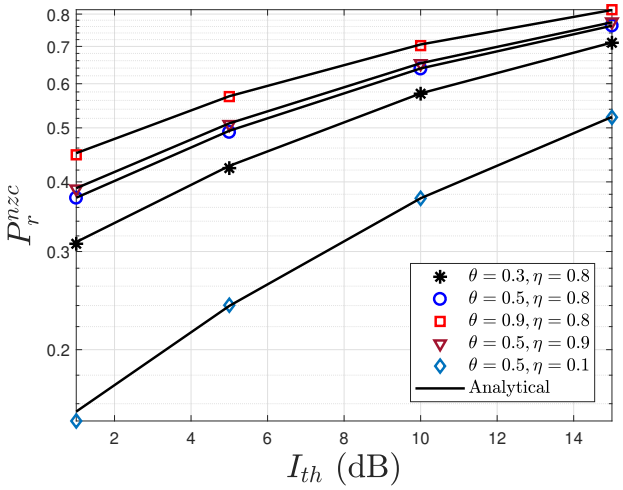

Figure 4.9: The probability of non-zero secrecy capacity versus I_{th} for multiple values of θ and η. The main channel parameters are: $\kappa = 1$, $\mu = 1$. The wiretap channel parameters are: $\kappa_e = 1$, $\mu_e = 1$. $PL = 2$, $k = 1$, $n = 2$, , $\phi = 0.3$, $\lambda_e = 1$, $N_0 = 1$, $d_{SJ} = 1m$, $d_{JEi} = 4m$, $d_{SP} = 20m$, and $d_{SD} = 1m$.

The intercept probability versus the density of the eavesdroppers is illustrated in Fig. 4.12 for

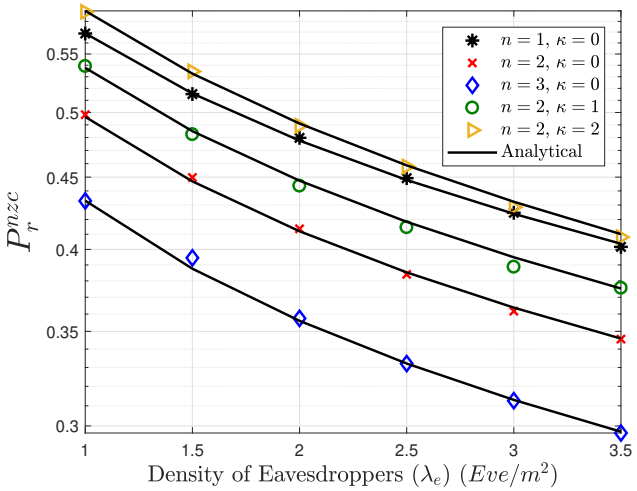

Figure 4.10: The probability of non-zero secrecy capacity versus the eavesdropper density (λ_e) for multiple values of n and κ. The main channel parameters are: $\mu = 1$. The wiretap channel parameters are: $\kappa_e = \kappa$, $\mu_e = 1$. $PL = 2$, $k = 1$, $\theta = 0.7$, $\eta = 0.8$, $\phi = 0.3$, $N_0 = 1$, $I_{th} = 5$ dB, $d_{SP} = 20m$, $d_{SJ} = 1m$, $d_{JEi} = 4m$, and $d_{SD} = 1m$.

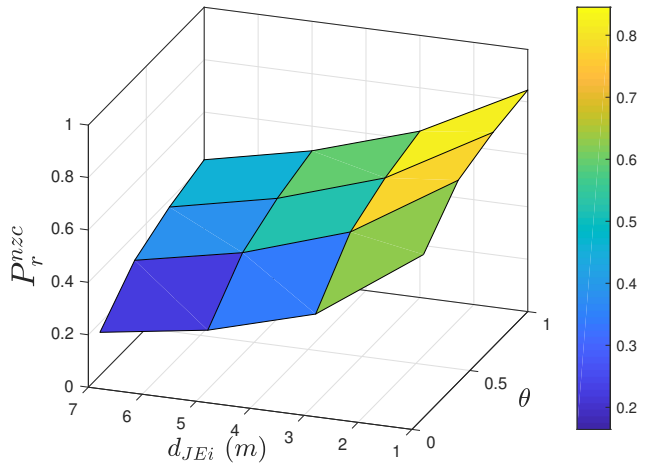

Figure 4.11: The probability of non-zero secrecy capacity versus the power splitting factor (θ) and the distance between R_J and the eavesdropper (d_{JEi}). The main channel parameters are: $\kappa = 1$, $\mu = 1$. The wiretap channel parameters are: $\kappa_e = 1$, $\mu_e = 1$. $PL = 2$, $k = 1$, $\lambda_e = 1$, $\eta = 0.8$, $N_0 = 1$, $n = 2$, $I_{th} = 5$ dB, $\phi = 0.4$, $d_{SJ} = 1m$, $d_{SP} = 20m$, and $d_{SD} = 1m$.

different values of d_{JEi}. Results demonstrate that the risk of intercepting the information grows with the density of the eavesdroppers. This can be interpreted by the fact that more eavesdroppers in the area result in a higher chance of having one with stronger signals' reception and decoding capabilities. In addition, it can be noticed that as the jammer moves farther away from the eavesdropper,

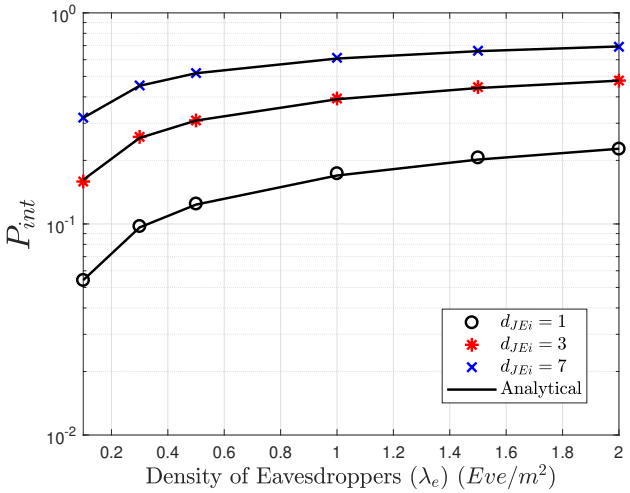

Figure 4.12: The intercept probability versus the density of eavesdroppers (λ_e) for different values of d_{JEi}. The main channel parameters are: $\kappa = 1$, $\mu = 1$. The wiretap channel parameters are: $\kappa_e = 1$, $\mu_e = 1$. $PL = 2$, $\eta = 0.8$, $N_0 = 1$, $I_{th} = 5$ dB, $n = 2$, $\phi = 0.3$, $\theta = 0.7$, $k = 1$, $\eta = 0.8$, $d_{SJ} = 1m$, $d_{SP} = 20m$, and $d_{SD} = 1m$.

the secrecy is more compromised, as the eavesdropper will be less impacted by the jamming power.

The two scenarios of an energy harvesting and a non-energy harvesting receiver (D) are depicted in Fig. 4.13. With $\phi = 0$, which signifies that no energy is harvested and all received power will be utilized to process the information, the messages are transmitted more securely. Consequently, no energy is stored at the receiver's storage device to be used for other tasks or to compensate for the energy lost in processing the information. Moreover, security is compromised when the receiver harvests most of the received energy ($\phi = 0.95$), leaving only a small amount of energy available to analyze the information. One can conclude from the results that there is a trade-off between the system security (reliability) and the energy level at the receiver's storage device. Therefore, to prevent a deteriorated security and an empty energy storage device, it is preferable that the receiver harvests with the proper power splitting factor, as will be illustrated in the following results. Finally, increasing the energy harvesting conversion efficiency (η) improves the security, proving the effectiveness of jamming-based energy harvesting on security.

Fig. 4.14 shows P_r^{nzc} versus I_{th} for different cases of the PS factor at D (ϕ). It is worth mentioning that at $I_{th} = -10$ dB, the value of $\phi^* = 0.43$. In this case, other values of ϕ are selected while respecting the constraint in (4.41). While comparing the P_r^{nzc} when utilizing an

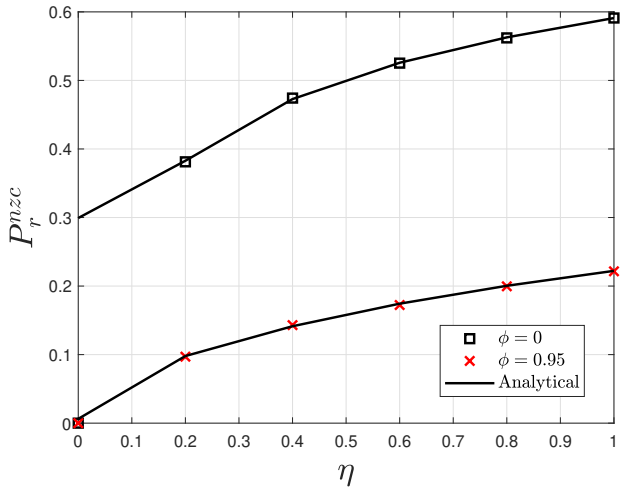

Figure 4.13: The probability of non zero secrecy capacity versus η. The main channel parameters are: $\kappa = 1$, $\mu = 1$. The wiretap channel parameters are: $\kappa_e = 1$, $\mu_e = 1$. $PL = 2$, $I_{th} = 5$ dB, $\lambda_e = 1$, $\theta = 0.6$, $N_0 = 1$, $k = 1$, $n = 2$, $d_{SJ} = 1m$, $d_{JEi} = 4m$, $d_{SP} = 20$, and $d_{SD} = 1m$.

adaptive PS factor (ϕ^*), it is concluded that ϕ^* achieves the highest privacy. This proposes that, in order to achieve the highest privacy level while satisfying the constraint in (4.41), the PS factor should be adapted at D, implying that ϕ^* produces the best privacy level. In addition, it is noticed that imposing a limit on the energy harvested at D $(P_D \geq \zeta)$ would still enhance the secrecy while assuring that there is always enough energy stored to charge its battery. In addition, a fixed PS factor of D increases the eavesdropper's risk of intercepting private information.

Fig. 4.15 highlights that the harvesting criterion at D is dependent on other network parameters, such as the location and selection of the targeted eavesdropper (k). This result shows that regardless of the selected eavesdropper (k), the optimal privacy is reached when D harvests with an adaptable PS factor ϕ, i.e., ϕ^* rather than fixed ϕ. Moreover, for the cases of ϕ^*, it is clear from the figure that the difference in the P_{rnc} for high k is smaller than the P_r^{nzc} for low k. This is due to the fact that the information privacy is more impaired when the eavesdropper is very close to S (k is low). Particularly, when k is small, D must adapt the PS factor rather than maintaining it constant.

Finally, Fig. 4.16 illustrates P_r^{nzc} versus ζ and k. The results demonstrate that when k is large and the minimal amount to be harvested at D (ζ) is low, the maximum secrecy is attained. Additionally, it is noticed that when the first or second closest eavesdropper to the transmitter S is selected, i.e., $k = 1$ or $k = 2$, the destination D should harvest with a small amount to assure

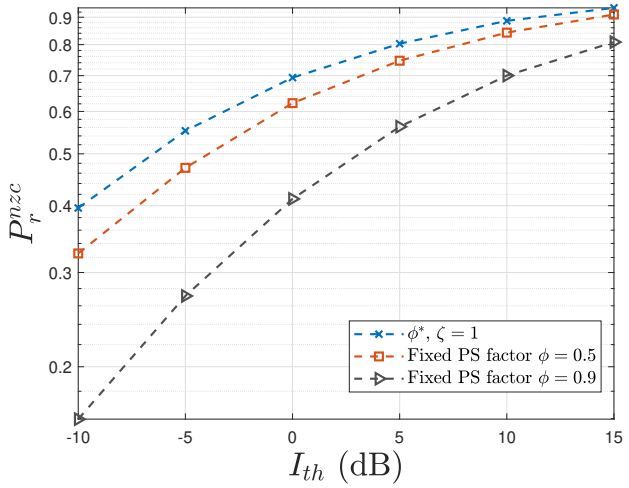

Figure 4.14: The probability of non zero secrecy capacity versus I_{th}. The main channel parameters are: $\kappa = 1$, $\mu = 1$. The wiretap channel parameters are: $\kappa_e = 1$, $\mu_e = 1$. $PL = 2$, $\eta = 0.8$, $\lambda_e = 0.1$, $\theta = 0.6$, $N_0 = 1$, $k = 1$, $n = 2$, $d_{SJ} = 1m$, $d_{JEi} = 4m$, $d_{SP} = 20$, and $d_{SD} = 1m$.

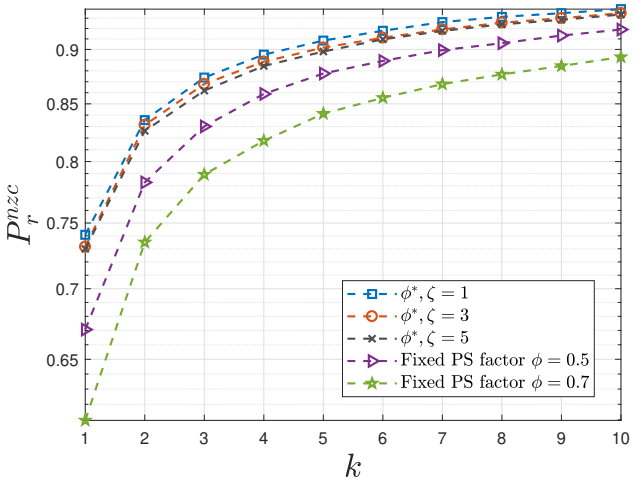

Figure 4.15: The probability of non-zero secrecy capacity versus k. The main channel parameters are: $\kappa = 1$, $\mu = 1$. The wiretap channel parameters are: $\kappa_e = 1$, $\mu_e = 1$. $PL = 2$, $\eta = 0.8$, $\lambda_e = 0.1$, $\theta = 0.9$, $n = 2$, $I_{th} = 10$ dB, $N_0 = 1$, $d_{SJ} = 1m$, $d_{JEi} = 1m$, $d_{SP} = 8m$, and $d_{SD} = 5m$.

security. This is attributed to the fact that while the lowest amount of energy required to harvest (ζ) is low, the portion remaining for decoding useful information is high resulting in higher privacy. It is worth-mentioning that in this case, the reliability of the system is high due to having a high amount of energy for processing the information $((1 - \phi)P_s)$, which will improve the link capacity. This

highlights the fact that an adaptive PS factor assists the receiver in performing a trade-off between the system reliability and the energy content at the receiver's storage device. Nevertheless, when k is large $(k = 4)$, even when the extracted energy is high owing to high ζ, higher levels of privacy can still be achieved. This implies that D may alter the PS factor and extract a larger amount of energy, which can be stored in the batteries to recharge them or conduct other tasks without compromising the system privacy.

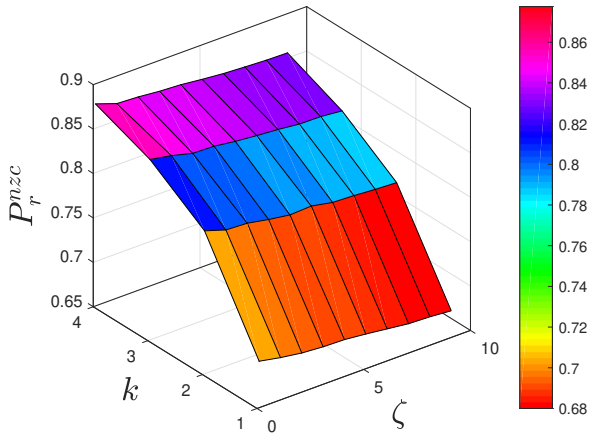

Figure 4.16: The probability of non-zero secrecy capacity versus k and ζ. The main channel parameters are: $\kappa = 1$, $\mu = 1$. The wiretap channel parameters are: $\kappa_e = 1$, $\mu_e = 1$. $PL = 2$, $\eta = 0.8$, $\lambda_e = 0.1$, $\theta = 0.6$, $n = 2$, $I_{th} = 10$ dB, $N_0 = 1$, $d_{SJ} = 1m$, $d_{JEi} = 1m$, $d_{SP} = 8m$, and $d_{SD} = 5m$.

4.8 Secrecy Analysis for EH-Enabled CRNs with Cooperative Jammer over Cascaded Rayleigh Channels

In this scenario, we propose to enhance the privacy of a CRN in the presence of multi-antenna eavesdroppers by deploying a cooperating jammer that harvests energy using the PS technique [100]. This energy is used to generate jamming signals to reduce the eavesdropper's ability to decode the information. Moreover, in regards to how eavesdroppers process the intercepted information, two scenarios are considered; colluding and non-colluding eavesdroppers. A comparison

is performed to illustrate which type is more effective in intercepting the information. For the scenario of non-colluding eavesdroppers, it is assumed that they are distributed randomly according to a homogeneous Poisson point process (HPPP). Various parameters are examined to determine their effect on PLS, including the number of antennas, the distance between nodes, the effectiveness of jamming and EH, the cascade level, and the effect of non-colluding eavesdropper density. Given this, PLS is assessed in terms of the probability of non-zero secrecy capacity (P_r^{nzc}) and the intercept probability (P_{int}).

4.9 System Model

We consider two SUs (S and D) communicate over h_{SD} channel while being threatened by several eavesdroppers attempting to intercept the messages exchanged between them through the wiretap link. Two scenarios are investigated; colluding and non-colluding eavesdroppers. At the eavesdropper, the MRC technique is used to maximize the link's reception and tapping capabilities. Furthermore, to investigate a worst-case scenario, we assume that the main link follows the cascaded Rayleigh model, while the rest of the links follow the single Rayleigh distribution [7], [67]. Given that S and D are using the underlay mode to access the licensed band, the transmission power of S should be limited to avoid deteriorating the quality of service for PUs communication. This is achieved by complying with the interference threshold tolerable at the PU receiver (P_R) through h_{SP} link. Additionally, to enhance the security of SUs' communication, an SU cooperating jammer (C_J) harvests energy from the received signals of S through the channel h_{SJ} using power splitting (PS) technique. This energy is used to generate jamming signals to impair the eavesdropper's ability to decode the messages. It is worth-noting that information about the eavesdroppers' positions relative to the source can be gained presuming that the eavesdroppers are untrusted users and lack the authorization to access the channel [94]. One can suppose that global channel state information regarding eavesdroppers is available for certain services, such as in pay-TV broadcasting services. It is worth mentioning that our system model and analysis are appropriate for modeling cognitive

vehicular networks [5]. The harvested energy at C_J is expressed as

$$E_h = \theta \eta P_s T \left| h_{SJ} \right|^2, \tag{4.44}$$

where P_s is the transmission power at S and $0 < \theta < 1$ is the PS factor. θP_s is the portion utilized for the EH process and the rest $((1-\theta)P_s)$ is used for processing the information and recharging the battery of C_J. $0 < \eta < 1$ is the energy conversion efficiency coefficient and T is the symbol duration. Given (4.44), the transmission power at C_J is given by

$$P_J = \theta \eta P_s \left| h_{SJ} \right|^2. \tag{4.45}$$

In the scope of underlay access mode, S should ensure that the transmission power is maintained below the permissible amount of interference tolerable at P_R (I_{th}) as in [66]. Given this, the jamming power in (4.45) is limited to avoid impairing the PUs' communication.

4.9.1 Colluding Eavesdroppers

Colluding eavesdroppers process the intercepted data cooperatively as it is transmitted to a centralized processor. Hence, multiple colluding eavesdroppers mimic a multi-antenna eavesdropper (E) [58] as illustrated in Fig. 4.17. Without loss of generality, we assume that the legitimate receiver

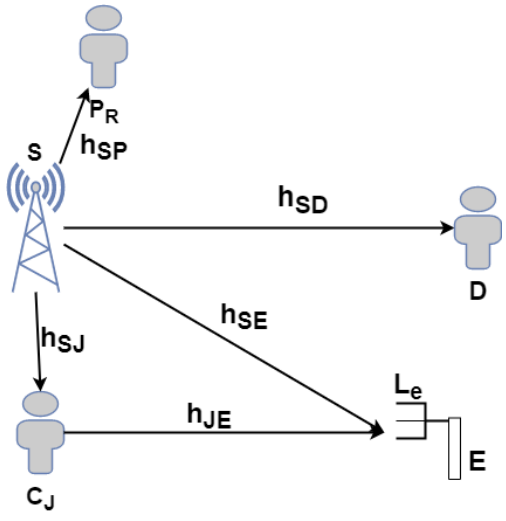

Figure 4.17: Scenario-I: Colluding Eavesdroppers.

(D) recognizes the pseudorandom sequence of the jamming signals and are thus canceled [100]. The received message at D is given by

$$y_D = \sqrt{P_s} h_{SD} x_s + n_D, \tag{4.46}$$

where P_s is the transmission power of S, x_s is the transmitted symbol, and n_D is the additive-white-Gaussian-noise (AWGN) at D with zero mean and variance N_0. Moreover, the intercepted message at the eavesdropper E is expressed as

$$y_{E_i} = \sqrt{P_s} h_{SE_i} x_s + \sqrt{P_J} h_{JE_i} x_J + n_{E_i}, \tag{4.47}$$

where x_J is the jammer transmitted symbol and h_{SE_i} is the channel between S and the i^{th} antenna of E, for $i = 1, 2, \cdots, L_e$, with L_e is the number of antennas. h_{JE_i} is the channel between C_J and the i^{th} antenna of E and n_{E_i} is the AWGN at the i^{th} antenna of E with zero mean and variance N_0. Using (4.46), the instantaneous received SNR at D is expressed as

$$\gamma_D = \frac{I_{th} \left| h_{SD} \right|^2}{N_0 \left| h_{SP} \right|^2}. \tag{4.48}$$

The SINR at E is given by

$$\gamma_{E_w} = \frac{\frac{I_{th} \left| h_{SE} \right|^2}{\left| h_{SP} \right|^2}}{P_J \left| h_{JE} \right|^2 + N_0}, \tag{4.49}$$

where $\left| h_{SE} \right|^2 = \sum_{i=1}^{L_e} \left| h_{SE_i} \right|^2$ is the combined channel power gain. Throughout this section, it is presumed that the interference is dominant at E [76]. Hence, the SINR is approximated as

$$\gamma_{E_w} \approx \frac{\frac{I_{th} \left| h_{SE} \right|^2}{\left| h_{SP} \right|^2}}{P_J \left| h_{JE} \right|^2}. \tag{4.50}$$

As mentioned earlier, h_{SD} follows the cascaded Rayleigh model. Hence, $h_{SD} = \prod_i^n x_i$, where x_i follows the Rayleigh model and n is the cascade level [66]. The probability density function (PDF) of h_{SD} is obtained using the transformed Nakagami-m distribution as in (3.94) Moreover,

the PDF of the remaining channels follow the single Rayleigh model, and thereby the PDF of their channel power gain follows the exponential distribution as

$$f_{|h_i|^2}(y) \quad = \quad \lambda_i \exp\left(-\lambda_i y\right), \tag{4.51}$$

for $i = \{SP, SJ, JE\}$. λ_i represents the corresponding fading channel parameter. In addition, since E uses the MRC technique, the PDF of $|h_{SE}|^2$ is given by [117]

$$f_{|h_{SE}|^2}(y) \quad = \quad \frac{\lambda_{SE}^M y^{M-1} \exp(-\lambda_{SE} y)}{(M-1)!}, \tag{4.52}$$

where λ_{SE} denotes the fading wiretap channel parameter.

4.9.2 Non-Colluding Eavesdroppers

In this scenario, we assume the same previously discussed system model, but with non-colluding eavesdroppers. These eavesdroppers are assumed to be distributed randomly according to a HPPP with density λ_e and each is equipped with L_e antennas. Moreover, it is presumed that the eavesdroppers are scattered in an unbounded Euclidean space of dimension U. The wiretap channel is represented by h_{SE_k} (link between S and the k^{th} eavesdropper (E_k)) as shown in Fig. 4.18. We assume that the k^{th} nearest eavesdropper to S is considered for tapping the information and for being impacted by jamming, while D can cancel them [100]. This is achieved by estimating the Euclidean distance between S and each eavesdropper. These distances are ordered in an ascending manner. Similar to the previous section, it is possible to obtain information regarding the positions related to the source [94]. The SNR at D is the same as in (4.48) and the SINR at E_k is given by

$$\gamma_{E_k} \approx \frac{\frac{I_{th}\left|h_{SE_k}\right|^2}{|h_{SP}|^2 d_k^L}}{P_J \left|h_{JE_k}\right|^2}, \tag{4.53}$$

where d_k is the distance between S and E_k and PL is the path loss exponent. d_k^{PL} is distributed as in (3.58). Assuming each eavesdropper employs MRC technique for reception, the PDF of $|h_{SE_k}|^2$

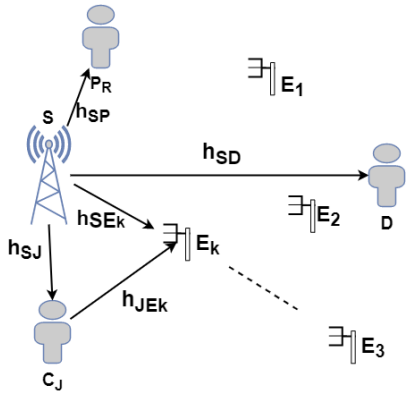

Figure 4.18: Scenario-II: Non-colluding Eavesdroppers.

is given by [117]

$$f_{|h_{SE_k}|^2}(y) = \frac{\lambda_{SE_k}^M y^{M-1} \exp(-\lambda_{SE_k} y)}{(M-1)!}. \tag{4.54}$$

4.10 PLS Analysis

In this section, PLS is evaluated in terms of the probability of non-zero secrecy capacity (P_r^{nzc}) and the intercept probability (P_{int}). Both security metrics demonstrate the channels' reliability according to the secrecy capacity C_s given by

$$C_s = \begin{cases} C_D - C_{Ej}, & \text{if } \gamma_D > \gamma_{E_j} \\ 0, & \text{if } \gamma_D \leq \gamma_{E_j} \end{cases}, \tag{4.55}$$

for $j = w, k$. $C_D = \log_2(1+\gamma_D)$ is the capacity of the main link and $C_{Ej} = \log_2(1+\gamma_{E_j})$ is the wiretap link capacity.

4.10.1 Probability of Non-Zero Secrecy Capacity

-Colluding Eavesdroppers Scenario: Here, P_r^{nzc} for the case of colluding eavesdroppers is evaluated. Given (4.55) and (4.45)-(4.50), P_r^{nzc} in (3.37) is expressed as

$$\begin{aligned} P_r^{nzc} &= 1 - P_r\left(\frac{1+\frac{I_{th}|h_{SD}|^2}{N_0|h_{SP}|^2}}{1+\frac{\frac{I_{th}|h_{SE}|^2}{|h_{SP}|^2}}{\theta\eta P_s|h_{SJ}|^2|h_{JE}|^2}} \leq 1\right) \\ &= 1 - P_r\left(|h_{SD}|^2 \leq \frac{|h_{SP}|^2|h_{SE}|^2 N_0}{\theta\eta I_{th}|h_{JE}|^2|h_{SJ}|^2}\right) \\ &= 1 - \int_0^\infty F_{|h_{SD}|^2}(z) f_Z(z) dz, \end{aligned} \tag{4.56}$$

where $Z = \frac{|h_{SP}|^2|h_{SE}|^2 q}{|h_{JE}|^2|h_{SJ}|^2}$ and $q = \frac{N_0}{\theta\eta I_{th}}$. First, the PDF of Z should be found to evaluate P_r^{nzc}. Let $Z = \frac{A}{B}$, where $A = qA'$, with $A' = |h_{SP}|^2|h_{SE}|^2$. Moreover, $B = |h_{JE}|^2|h_{SJ}|^2$. The PDF of A' is expressed as

$$f_{A'}(x) = \int_{-\infty}^{\infty} \frac{1}{|y|} f_{|h_{SP}|^2}\left(\frac{x}{y}\right) f_{|h_{SE}|^2}(y) dy. \tag{4.57}$$

Using (4.51) for $i = SP$, (4.52), and [82, Eq. (7.813.1)] and with transformation of random variables, the PDF of A is given by

$$f_A(x) = \frac{\lambda_{SP}\lambda_{SE}}{q(L_e-1)!} G_{0\,2}^{2\,0}\left(\begin{matrix} - \\ L_e-1,0 \end{matrix}\middle| \frac{\lambda_{SP}\lambda_{SE}x}{q}\right), \tag{4.58}$$

Moreover, the PDF of B is given by

$$f_B(x) = \int_{-\infty}^{\infty} \frac{1}{|y|} f_{|h_{JE}|^2}\left(\frac{x}{y}\right) f_{|h_{SJ}|^2}(y) dy. \tag{4.59}$$

Using (4.51) for $i = JE$ and $i = SJ$ and with the help of [82, Eq. (7.813.1)], (4.59) is solved as

$$f_B(x) = \lambda_{JE}\lambda_{SJ} G_{0\,2}^{2\,0}\left(\begin{matrix} - \\ 0,0 \end{matrix}\middle| \lambda_{JE}\lambda_{SJ}x\right). \tag{4.60}$$

Additionally, the PDF of Z is given by

$$f_Z(x) = \int_0^\infty y f_A(xy) f_B(y) dy. \tag{4.61}$$

Using (4.58), (4.60), and [83, eq. (2.24.1.1)], (4.61) is solved as

$$f_Z(x) = c_1 x^{-2} G_{2\,2}^{2\,2}\left({}_{0,0}^{-L_e,-1} \middle| \frac{s_1}{x} \right), \tag{4.62}$$

where $c_1 = \frac{q\lambda_{JE}\lambda_{SJ}}{\lambda_p \lambda_{SE}(L_e-1)!}$ and $s_1 = \frac{q\lambda_{JE}\lambda_{SJ}}{\lambda_p\lambda_{SE}}$. Moreover, the CDF of $|h_{SD}|^2$ can be found as in (4.16). Using (4.62), (4.16), and [83, Eq. (2.24.1.1)], (4.56) is solved as

$$P_r^{nzc} = \sum_{j=0}^{m-1} c_2 G_{2\;n+2}^{n+2\;\;2} \left({}_{\rho''}^{1-L_e-\frac{j}{n},-\frac{j}{n}} \middle| \frac{s_1 \left(\frac{m}{\Omega\sigma^{2/n}}\right)^n}{n^n} \right), \tag{4.63}$$

where $c_2 = \frac{c_1 n \beta \left(\frac{m}{\Omega\sigma^{\frac{2}{n}}}\right)^{-m+j} (m-1)! \left(\frac{q}{\lambda_p\lambda_{SE}}\right)^2 \sqrt{n}}{2j!(2\pi)^{0.5(n-1)} s_1^{1-\frac{j}{n}}}$ and $\rho'' = 0, \frac{1}{n}, \cdots, \frac{n-1}{n}, 1-\frac{j}{n}, 1-\frac{j}{n}$.

-Non-Colluding Eavesdroppers Scenario: P_r^{nzc} is reassessed for the scenario of non-colluding eavesdroppers in this section. Using (3.37), (4.48), and (4.53), P_r^{nzc} is expressed as

$$P_r^{nzc} = 1 - P_r\left(|h_{SD}|^2 \le \frac{|h_{SP}|^2 |h_{SE_k}|^2 N_0}{d_k^{PL}\theta\eta I_{th} |h_{JE_k}|^2 |h_{SJ}|^2} \right) = 1 - \int_0^\infty F_{|h_{SD}|^2}(y) f_Y(y) dy, \tag{4.64}$$

where $Y = \frac{\frac{|h_{SE_k}|^2}{d_k^{PL}}}{b\frac{|h_{JE_k}|^2 |h_{SJ}|^2}{|h_{SP}|^2}}$, with $b = \frac{\theta\eta I_{th}}{N_0}$. To find the PDF of Y, assume $Y = \frac{Q}{W}$, where $Q = \frac{|h_{SE_k}|^2}{d_k^{PL}}$ and $W = b\frac{|h_{JE_k}|^2 |h_{SJ}|^2}{|h_{SP}|^2}$. First, the PDF of Q is expressed as

$$f_Q(x) = \int_0^\infty y f_{|h_{SE_k}|^2}(xy) f_{d_k^{PL}}(y) dy. \tag{4.65}$$

Using (3.58), (4.54), and [83, Eq. (2.24.3.1)], (4.65) is solved as

$$f_Q(x) = a_1 x^{-1-\delta k} G_{\delta\;1}^{1\;\delta} \left({}_{0}^{\frac{1-L_e-\delta k}{\delta}} \middle| \frac{A_e \delta^\delta}{x^\delta \lambda_{SE_k}^\delta} \right), \tag{4.66}$$

where $a_1 = \frac{\lambda_{SE_k}^{-\delta k}\delta^{L_e+\delta k+0.5}A_e^k}{(L_e-1)!\Gamma(k)(2\pi)^{(\delta-1)0.5}}$. To find the PDF of W, assume $W = bW'$, with $W' = \frac{|h_{JE_k}|^2|h_{SJ}|^2}{|h_{SP}|^2}$. Given (4.51) and by replacing E by E_k in (4.60), and with the help of [82, Eq. (7.813.1)], the PDF of W is given by

$$f_W(x) = \frac{\lambda_{JE_k}\lambda_{SJ}}{b\lambda_p} G_{1\ 2}^{2\ 1}\left(\begin{matrix}-1\\0,0\end{matrix}\middle|\frac{\lambda_{JE_k}\lambda_{SJ}x}{b\lambda_{SP}}\right). \tag{4.67}$$

Given (4.66), (4.67), and [83, eq. (2.24.3.1)], $f_Y(x)$ is given by

$$f_Y(x) = a_2 x^{-1-\delta k} G_{1+2\delta}^{\ 2\delta\ 1+2\delta}\left(\begin{matrix}1,k,k\\ \rho'\end{matrix}\middle| s_2 x^{\delta}\right), \tag{4.68}$$

where $a_2 = \frac{a_1\lambda_{JE_k}^{\delta k}\lambda_{SJ}^{\delta k}\delta^{1.5-\delta k}}{(b\lambda_{SP})^{\delta k}(2\pi)^{1.5(\delta-1)}}$, $s_2 = \frac{\frac{\lambda_{SE_k}^{\delta}}{A_e}}{\left(\frac{\lambda_{JE_k}\lambda_{SJ}}{b\lambda_{SP}}\right)^{\delta}}$, and $\rho' = \frac{\delta-1+L_e+\delta k}{\delta}, \frac{1+\delta k}{\delta}$. Finally, substituting (4.16) and (4.68) into (4.64), P_r^{nzc} is solved as [83, eq. (2.24.3.1)]

$$P_r^{nzc} = \sum_{j=0}^{m-1} a_3 G^{\ \delta n+2\delta+1\ 2\delta}_{2\delta\ \ \delta n+2\delta+1}\left(\begin{matrix}\epsilon\\ \epsilon'\end{matrix}\middle|\frac{\left(\frac{m}{\Omega\sigma^{2/n}}\right)^{\delta n}}{s_2(\delta n)^{\delta n}}\right), \tag{4.69}$$

where $a_3 = \frac{a_2 n\beta\left(\frac{m}{\Omega\sigma^{\frac{2}{n}}}\right)^{-m+j}(m-1)!\sqrt{\delta n}s_2^{\frac{\delta k-\frac{j}{n}}{\delta}}}{2j!\delta(2\pi)^{0.5(\delta n-1)}}$, $\epsilon = \frac{1-L_e-\frac{j}{n}}{\delta^2}, \frac{\delta-1-\frac{j}{n}}{\delta^2}$, and $\epsilon' = 0,\cdots,\frac{\delta n-1}{\delta n}, \frac{\delta k-\frac{j}{n}}{\delta^2}, \frac{\delta-\frac{j}{n}}{\delta^2}, \frac{\delta-\frac{j}{n}}{\delta^2}$.

4.10.2 Intercept Probability

P_{int} defined in (3.56) is given by

$$P_{int} = P_r\left(C_s < 0\right) = 1 - P_r^{nzc}. \tag{4.70}$$

Given (4.63) and (4.69), P_{int} for both scenarios of colluding and non-colluding eavesdroppers is obtained.

4.11 Numerical Results

In this section, analytical results and Monte-Carlo simulations are presented. To account for the path loss effect, assume S operates as the reference location (see Fig. 4.19). S is located at $(0, 0)$ and the nodes (D, E, C_J and P_R) are of different distances from S. Assume $d_{XY}^{-L} = \frac{1}{2\lambda_i}$, where $X \in \{S, C_J, I_1, I_2, I_3\}$, $Y \in \{P_R, E, I_1, I_2, I_3, D, C_J\}$, and $i \in \{SP, SJ, JE, SE, SD\}$. $\lambda_{SD} = \frac{1}{2\sigma^2}$ and d_{XY} represents the distance from node X to node Y in meters (m). $I_1, I_2,$ and I_3 denote the locations of the first, second, and third obstacles in the main channel, respectively. This is to observe the effect of the cascade level on the privacy.

Fig. 4.20 represents the probability of non-zero secrecy capacity for the case of colluding eavesdroppers versus the distance between S and E (d_{SE}). It is observed that the security improves when E moves away from S. This is due to the fact that as d_{SE} becomes larger, the wiretap link's conditions get worse and E's decoding capabilities become poor. Moreover, as the conditions of the main channel deteriorate due to the rise in the cascade level (n), privacy decays. This is because a larger n suggests more obstacles between S and D, resulting in poor reception and a lower received SNR.

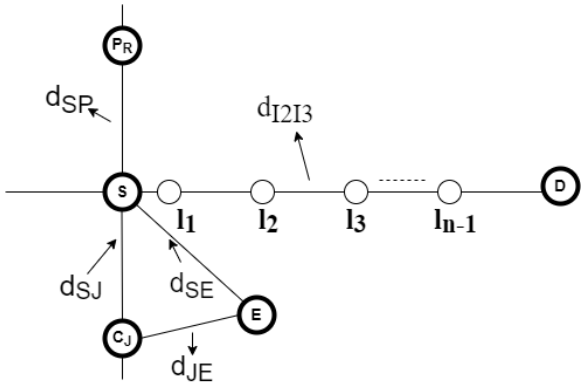

Figure 4.19: A representation of the distances between nodes.

Fig. 4.21 depicts P_r^{nzc} versus the power splitting factor at C_J (θ) and the distance between C_J and E (d_{JE}) for the case of colluding eavesdroppers. It is noticed that the security improves as θ increases. This is attributed to the fact that as the harvested energy increases (θ rises), the amount of jamming signals generated and broadcast grows, thus reducing the quality of the tapped messages at E. Moreover, as the jammer approaches E, i.e., d_{JE} reduces, the jamming impact generally increases, leading to enhanced privacy. Given this, C_J is capable of adjusting the amount of harvested

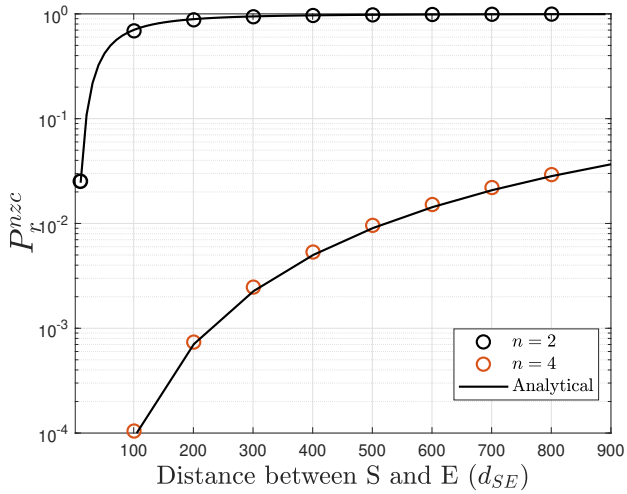

Figure 4.20: The probability of non-zero secrecy capacity (P_{rc}) versus the distance between S and E (d_{SE}) for different cascade levels (n). $d_{SP} = 200m$, $d_{SI_1} = 10m$, $d_{I_1I_2} = 10m$, $d_{I_2I_3} = 10m$, $d_{I_3D} = 10m$, $d_{JE} = 100m$, $d_{SJ} = 1m$, $L_e = 3$, $\theta = 0.6$, $\eta = 0.8$, $I_{th} = 5$ dB, and $PL = 3$.

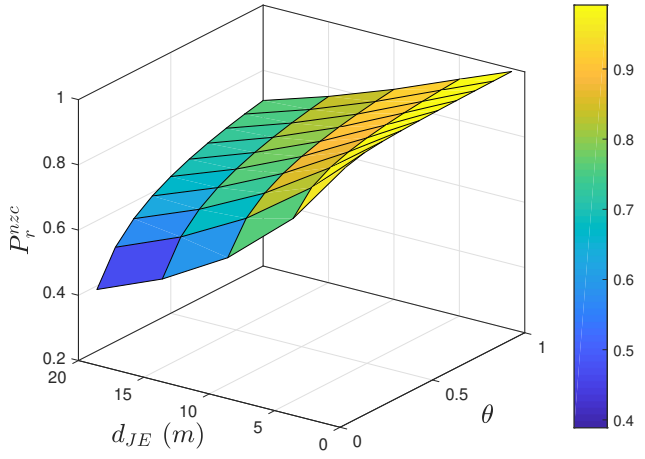

Figure 4.21: The probability of non-zero secrecy capacity (P_{rc}) versus θ and d_{JE}. $n = 2$, $d_{SE} = 50m$, $d_{SP} = 200m$, $d_{SI_1} = 10m$, $d_{I_1D} = 10m$, $d_{JE} = 20m$, $d_{SJ} = 1m$, $L_e = 2$, $I_{th} = 5$ dB, $\eta = 0.1$ and $PL = 2$.

energy, i.e., the value of θ, in response to the closeness to E. Particularly, as d_{JE} becomes larger, C_J must harvest more energy and thereby emitting more jamming power to maintain the privacy. However, as C_J gets closer to E, C_J varies the transmission power by reducing the amount of harvested energy and raising the amount left for charging its battery, i.e., $(1 - \theta)P_s$.

The PLS is assessed for the non-colluding eavesdroppers scenario in Fig. 4.22. We assume a

two-dimensional (2D) area $(U = 2)$ and a HPPP distribution of the eavesdroppers' locations. 10^5 realizations of their positions are generated in a square area of a side of 25 meters (m). The figure illustrates how security deteriorates as the density of eavesdroppers (λ_e) increases. This is due to that fact that with more eavesdroppers dispersed over the area, there is a higher probability that one will be closer to S, providing better channel conditions and thus increased interception capabilities. Additionally, regardless of the density of eavesdroppers, as the EH process efficiency improves, i.e., as η rises, the probability of a secure connection increases. This is due to the increase in the jamming power impacting E_k, demonstrating the efficiency of cooperating jamming-based energy harvesting.

Fig. 4.23 illustrates P_r^{nzc} versus θ for the case of non-colluding eavesdroppers. The results demonstrate that even when eavesdroppers are not colluding to intercept the information, the jamming process-based EH is powerful at confounding the eavesdropper and reducing its ability of interception. Moreover, the eavesdropper's selection, denoted by k, has a substantial impact on security. Specifically, selecting the first closest eavesdropper to S $(k = 1)$ has the greatest influence on reducing security. That is, it is more likely to have more reliable channel conditions and hence greater decoding capabilities, compared to selecting the fifth one $(k = 5)$.

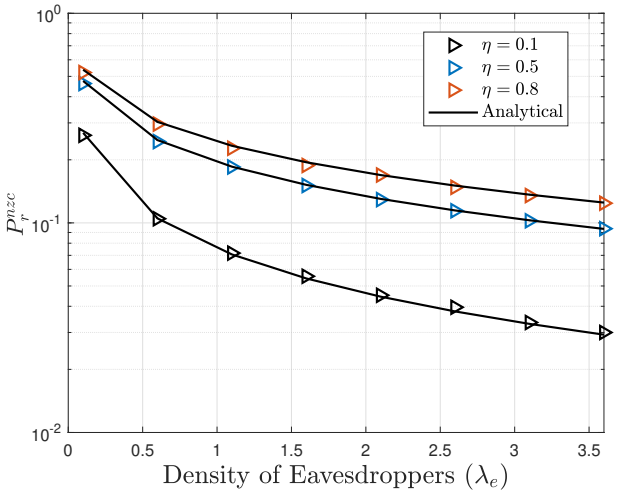

Figure 4.22: The probability of non-zero secrecy capacity (P_{rc}) versus the density of eavesdroppers (ϕ) for different values of η. $n = 2$, $d_{SE_k} = 50m$, $d_{SP} = 200m$, $d_{SI_1} = 10m$, $d_{I_1D} = 10m$, $d_{JE_k} = 100m$, $d_{SJ} = 1m$, $L_e = 3$, $I_{th} = 5$ dB, $\theta = 0.8$, $k = 1$, and $PL = 2$.

Finally, in Fig. 4.24, the intercept probability (P_{int}) against the interference threshold (I_{th}) is

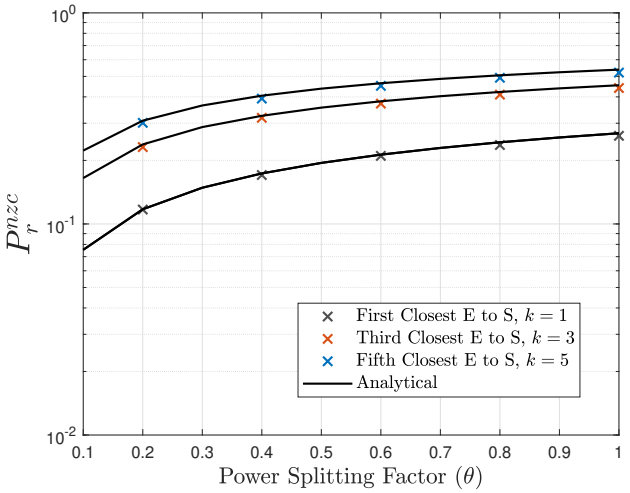

Figure 4.23: The probability of non-zero secrecy capacity (P_{rc}) versus the power splitting factor (θ) for different selections of the eavesdropper (k). $n = 2$, $d_{SE_k} = 50m$, $d_{SP} = 200m$, $d_{SI_1} = 10m$, $d_{I_1D} = 10m$, $d_{JE_k} = 100m$, $d_{SJ} = 1m$, $L_e = 3$, $I_{th} = 5$ dB, $\eta = 0.1$, $\lambda_e = 1$, and $PL = 2$.

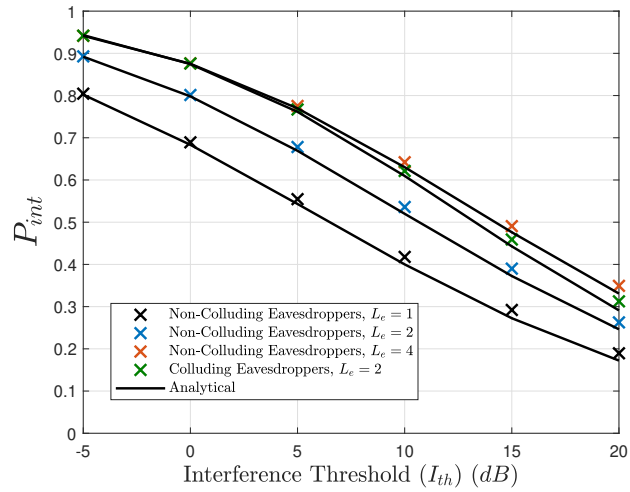

Figure 4.24: The intercept probability (P_{int}) versus the interference threshold (I_{th}). $n = 2$, $d_{SE} = 50m$, $d_{SP} = 200m$, $d_{SI_1} = 10m$, $d_{I_1D} = 10m$, $d_{JE} = 100m$, $d_{SJ} = 1m$, $k = 1$, $\eta = 0.1$, $\theta = 0.8$, $\lambda_e = 0.1$, and $PL = 2$.

depicted for the colluding and non-colluding eavesdroppers scenarios. Comparing both scenarios for $L_e = 2$, it is noticed that even though there are more eavesdroppers in the non-colluding case, the colluding eavesdroppers are more efficient at intercepting messages. This demonstrates the crucial need for incorporating colluding eavesdroppers when investigating PLS for CRNs. Furthermore, the results demonstrate an improvement in the system's privacy as I_{th} increases. This is because

an increase in I_{th} indicates that the SU source may raise its transmission power, improving the main channel's conditions in terms of received SNR. Moreover, when E_k is equipped with a greater number of antennas (L_e), privacy is severely compromised, as E_k gets more powerful and the reception at its end improves owing to the MRC.

4.12 Summery

In this chapter, we presented an underlay CRN over cascaded κ-μ channels, in which an eavesdropper poses a threat to the security of SUs. The SU destination harvests energy from the SU transmitter. Our findings indicate that security has improved as a result of the destination using the gathered energy to generate jamming signals to confuse the eavesdropper. In this scenario, PLS was examined and compared for two scenarios; an energy-harvesting and a non-energy-harvesting eavesdropper. Additionally, we discussed another case in which cooperative jamming is used to improve security over cascaded κ-μ channels with multiple non-colluding eavesdroppers. Given this scenario, we developed another model as a special case, in which users communicate via cascaded Rayleigh channels. In this case, two scenarios for the eavesdroppers' tapping capabilities are presented: colluding and non-colluding eavesdroppers. The findings show that collaborating eavesdroppers pose a higher threat to the SUs' security.

Chapter 5

Overlay CRNs- Enabled EH with AF Relays

5.1 Introduction

Recent research has focused on improving the energy efficiency of the underlying CRN through the utilization of EH. However, few studies have been conducted on employing EH for overlay CRN. For instance, in [72], a cooperation between a pair of SUs and PUs is conducted, in which the assistant SU harvests energy using PS protocol from the PUs' messages. The outage probability and the energy efficiency for both networks have been evaluated. Moreover, in [73], a TS energy harvesting process is performed by SUs, in which the SU that assists the PUs decodes and forwards the PUs messages in exchange for utilizing the licensed band. The outage probability and system throughput have been assessed in this work. Additionally, in [74], an overlay CRN was studied, in which the SU forwards the PUs messages in exchange for utilizing the bands, whereas the PU harvests energy from the received SUs' messages to improve its battery energy level. The PS factor has been optimized with the objective of improving the SUs' and PUs' communication reliability.

The main goal of this chapter is to improve the energy and spectral efficiencies of the system. Hence, we assume an overlay CRN, in which two PUs exchange messages with the assistance of SUs. Multiple SUs are assumed to be randomly distributed according to a HPPP, in which one of the SUs is selected based on the Euclidean distance. The selected SU harvests energy from

the PUs' messages by adopting the time switching protocol. Then, utilizing the gathered energy, this SU combines its own messages with the amplified PUs messages and forwards them to the destinations. The reliability of the SUs and PUs networks is investigated in terms of the outage probability. Furthermore, two optimization problems are proposed, in which the time switching and the power allocation factors are optimized. The first problem has the potential of maximizing the secondary users' rate while ensuring that the primary users' rate is maintained above a threshold, whereas the second one is proposed to maximize the sum rate of both networks.

5.2 System Model

Assume we have a PU transmitter (PU-Tx) communicating with a PU receiver (PU-Rx) as shown in Fig. 5.1. Due to the unavailability of a reliable link between the PUs, SUs are assumed to assist the PUs in forwarding their messages in exchange for the use of a licensed band. We assume that M SUs are distributed according to a homogeneous HPPP with a density of λ_e. One of these SUs will be selected based on the k^{th} nearest to PU-Tx. Moreover, this SU is permitted to harvest energy from PUs messages using the time switching (TS) protocol via the channel h_{SR}. In addition, the selected SU performs as an amplify-and-forward (AF) relay, in which it amplifies the PUs' messages and forwards them to the PU destination along with its own messages to its receiver (SU-Rx). We assume that the SUs are distributed in an unbounded Euclidean space of dimension U.

Fig. 5.2 shows the time frame of the TS-EH process. During the first time slot (ρT), the selected SU (R_k) harvests energy from the PUs messages with the energy harvested (E_s) given by

$$E_s = \frac{\rho \eta P_s T \left|h_{SR}\right|^2}{d^{PL}}, \tag{5.1}$$

where P_s is the transmission power at S, $0 < \rho < 1$ is the time switching factor, d is the distance of a randomly distributed SU from PU-Tx, PL is the path loss exponent, η represents the energy conversion efficiency coefficient, and T is the transmission time slot. Using (5.1), the transmission

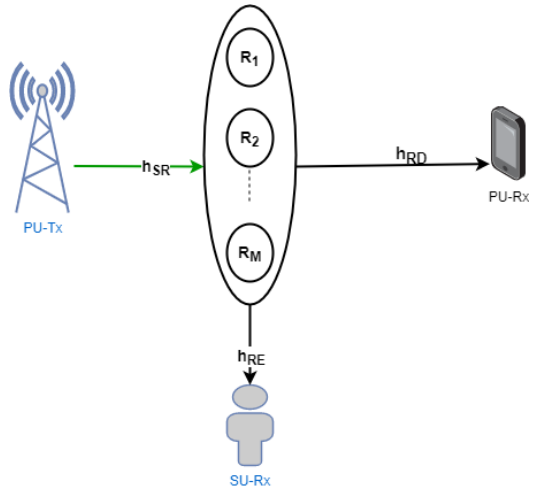

Figure 5.1: The system model.

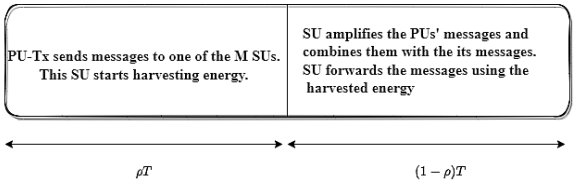

Figure 5.2: Frame structure of TS-based SWIPT in the proposed cognitive radio network.

power at R_k is given by

$$P_R = \frac{EH}{(1-\rho)T} = \frac{\rho\eta P_s \left|h_{SR}\right|^2}{(1-\rho)d^{PL}}. \tag{5.2}$$

The received message at the k^{th} random SU is given by

$$y_{R,k} = \sqrt{\frac{P_s}{d^{PL}}} h_{SR} x_p + n_R, \tag{5.3}$$

where x_p is the PUs' transmitted message and n_R is the AWGN at the SU relay with a zero mean and a variance N_0. During the second time slot $((1-\rho)T)$, the selected SU (R_k) amplifies the PUs' messages and combines them with its own messages to be transmitted. These messages are received by both receivers; PU-Rx and SU-Rx. Given this, the received message at the PU-Rx is given by

$$y_D = \beta y_{R,k} h_{RD} + \sqrt{(1-\alpha)P_R} h_{RD} x_s + n_D, \tag{5.4}$$

where x_s is the transmitted SUs messages and n_D is the AWGN at PU-Rx with a zero mean and a variance N_0. α represents a power allocation factor, in which αP_R is allocated to transmit the PUs messages, while the rest $((1-\alpha)P_R)$ is used to transfer the SUs' messages. Moreover, β is the amplification factor of R_k given by

$$\beta = \sqrt{\frac{\alpha P_R}{\frac{P_s g_{SR}}{d^{PL}} + N_0}}. \tag{5.5}$$

The noise variance in (5.5) (N_0) can be ignored compared to the term $\frac{P_s g_{SR}}{d^{PL}}$ at high SNR [72]. Hence, (5.5) can be approximated as

$$\beta \approx \sqrt{\frac{\alpha P_R}{\frac{P_s g_{SR}}{d^{PL}}}}. \tag{5.6}$$

Substituting (5.3) into (5.4), the received message at the PU-Rx is expressed as

$$y_D = \beta \sqrt{\frac{P_s}{d^{PL}}} h_{SR} x_p h_{RD} + \sqrt{(1-\alpha)P_R} h_{RD} x_s + \beta h_{RD} n_R + n_D. \tag{5.7}$$

Given (5.6) and (5.7), the instantaneous SINR at PU-Rx is expressed as

$$\gamma_D = \frac{\beta^2 g_{RD} g_{SR} \frac{P_s}{d^{PL}}}{N_0 g_{RD} \beta^2 + g_{RD(1-\alpha)P_R + N_0}}. \tag{5.8}$$

It is worth mentioning that PU-Rx treats the SUs messages as interference. Hence, substituting (5.2) and (5.6) into (5.8) and performing mathematical manipulations yields

$$\gamma_D = \frac{a \frac{g_{RD} g_{SR}}{d^{PL}}}{b g_{RD} + c \frac{g_{RD} g_{SR}}{d^{PL}} + N_0}, \tag{5.9}$$

where $a = \frac{\alpha \rho \eta P_s}{1-\rho}$, $b = \frac{N_0 \alpha \rho \eta}{1-\rho}$, and $c = \frac{(1-\alpha)\rho \eta P_s}{1-\rho}$. Moreover, the received message at SU-Rx is given by

$$y_S = \sqrt{(1-\alpha)P_R} h_{RE} x_s + n_s + \beta y_D h_{RE}, \tag{5.10}$$

where x_s is the SUs' transmitted messages and n_s is the AWGN at SU-Rx with a zero mean and a

variance N_0. Using (5.10), the received SINR at SU-Rx is given as

$$\gamma_S = \frac{q\frac{g_{RE}g_{SR}}{d^{PL}}}{eg_{RE} + w\frac{g_{RE}g_{SR}}{d^{PL}} + N_0}, \tag{5.11}$$

where $q = \frac{(1-\alpha)\rho\eta P_s}{1-\rho}$, $e = \frac{N_0\alpha\rho\eta}{1-\rho}$, and $w = \frac{\alpha\rho\eta P_s}{1-\rho}$. Accordingly, the data rate achieved at PU-Rx and SU-Rx are given, respectively, as

$$R_P = (1-\rho)T\log_2(1+\gamma_D), \tag{5.12}$$

$$R_S = (1-\rho)T\log_2(1+\gamma_S). \tag{5.13}$$

We assume that all links follow the Rayleigh fading model. Hence, the channels power gain (g_m), for $m = SR, RD, RE$ follow the exponential distribution with λ_m being the fading coefficient. The PDF and the CDF of g_m are given, respectively, as

$$f_{g_m}(x) = \lambda_m \exp(-\lambda_m x), \tag{5.14}$$

$$F_{g_m}(x) = 1 - \exp(-\lambda_m x). \tag{5.15}$$

As mentioned earlier in the chapter, in our analysis, the k^{th} nearest SU to PU-Tx will be selected to forward the messages. This is performed by measuring the Euclidean distance from PU-Tx to each of the SUs. The PDF of the path loss d^{PL} for the k^{th} nearest SU is distributed as expressed in (3.58).

5.3 Outage Probability

Recall that the outage probability (OP) represents the probability that the data rate is lower than a predetermined rate threshold (R_{thi}), for $i = p, s$. Given this, R_{thp} indicates the threshold for the PUs' link, whereas R_{ths} denotes the rate threshold for the SUs' communication. The outage

probability is given by

$$OP = P_r(R_j \leq R_{thi}), \tag{5.16}$$

for $j \in (P, S)$. In this section, the outage probability for the PUs and SUs links is evaluated to reveal the reliability of the considered communication system.

5.3.1 Outage Probability of the Primary Users' Network

Considering the outage probability to assess the PUs communication quality is significant since the PUs receive their own messages in addition to the SUs messages, which are regarded as interference. The outage probability for the PUs' link is evaluated in this section by rewriting (5.16) using (5.12) and (5.8) as

$$\begin{aligned} OP &= P_r\left(a g_{RD} g_{SR} \leq bJ g_{RD} d^{PL} + Jc g_{RD} g_{SR} + N_0 J d^{PL}\right) \\ &= P_r\left(g_{SR} \leq \frac{bJ}{a - Jc} d^{PL} + \frac{N_0 J}{(a - Jc)} L\right) \\ &= \int_0^\infty \int_0^\infty F_Y\left(c_1 z + c_2 l\right) f_Z(z) f_L(l) dz dl, \end{aligned} \tag{5.17}$$

where $J = 2^{\frac{R_{thp}}{(1-\rho)T}} - 1$, $c_1 = \frac{bJ}{a-Jc}$, $c_2 = \frac{N_0 J}{a-Jc}$, and $L = \frac{d^{PL}}{g_{RD}}$. First, one needs to obtain the PDF of the variable L as

$$f_L(x) \;\; = \;\; \int_0^\infty y f_{d^{PL}}(xy) f_{g_{RD}}(y) dy\cdot \tag{5.18}$$

Substituting (3.58) and (5.14) for $m = RD$ yields

$$f_L(x) = \frac{\delta A_e^k \lambda_{RD}}{\Gamma(k)} x^{\delta k - 1} \int_0^\infty y^{\delta k} G_{0\,1}^{1\,0}\left(\begin{matrix} - \\ 0 \end{matrix} \middle| \lambda_{RD} y\right) G_{0\,1}^{1\,0}\left(\begin{matrix} - \\ 0 \end{matrix} \middle| A_e x^\delta y^\delta\right) dy.$$

Using [83, eq. (2.24.1.1)], the PDF of L is found as

$$f_L(x) \;\; = \;\; c_3 x^{\delta k - 1} G_{\delta\,1}^{1\,\delta}\left(\begin{matrix} -k \\ 0 \end{matrix} \middle| \frac{A_e x^\delta \delta^\delta}{\lambda_{RD}^\delta}\right), \tag{5.19}$$

where $c_3 = \frac{\delta^{1.5+\delta k} A_e^k \lambda_{RD}^{-\delta k}}{\Gamma(k)(2\pi)^{(\delta-1)0.5}}$. The outage probability of the PUs' link given in (5.17) is expressed as

$$\begin{aligned} OP &= \frac{c_3 \delta A_e^k}{\Gamma(k)} \int_0^\infty \int_0^\infty \left[1 - \exp^{-\lambda_{SR}(c_1 z + c_2 l)}\right] \exp\left(-A_e z^\delta\right) z^{\delta k - 1} l^{\delta k - 1} G_{\delta\ 1}^{1\ \delta} \left(\begin{matrix} -k \\ 0 \end{matrix} \middle| \frac{A_e l^\delta \delta^\delta}{\lambda_{RD}^\delta} \right) \\ &\quad \times dz dl = 1 - \frac{c_3 \delta A_e^k}{\Gamma(k)} I_1 I_2, \end{aligned} \tag{5.20}$$

where I_1 is expressed as

$$I_1 = \int_{z=0}^\infty z^{\delta k - 1} G_{0\ 1}^{1\ 0} \left(\begin{matrix} - \\ 0 \end{matrix} \middle| \lambda_{SR} c_1 z \right) G_{0\ 1}^{1\ 0} \left(\begin{matrix} - \\ 0 \end{matrix} \middle| A_e z^\delta \right) dz. \tag{5.21}$$

Using [83, eq.(2.24.1.1)], I_1 is solved as

$$I_1 = \frac{\delta^{\delta k - 0.5}}{(2\pi)^{(\delta-1)0.5} (c_1 \lambda_{SR})^{\delta k}} G_{\delta\ 1}^{1\ \delta} \left(\begin{matrix} \Delta(\delta, 1-\delta k) \\ 0 \end{matrix} \middle| \frac{A_e \delta^\delta}{(\lambda_{SR} c_1)^\delta} \right), \tag{5.22}$$

where $\Delta(\delta, 1-\delta k) = \frac{1-\delta k}{\delta}, \frac{2-\delta k}{\delta}, \cdots, \frac{\delta - \delta k}{\delta}$. In addition, I_2 is expressed as

$$I_2 = \int_{l=0}^\infty l^{\delta k - 1} G_{0\ 1}^{1\ 0} \left(\begin{matrix} - \\ 0 \end{matrix} \middle| \lambda_{SR} c_2 l \right) G_{\delta\ 1}^{1\ \delta} \left(\begin{matrix} -k \\ 0 \end{matrix} \middle| \frac{A_e \delta^\delta l^\delta}{\lambda_{RD}^\delta} \right) dl. \tag{5.23}$$

Finally, using [83, eq.(2.24.1.1)], I_2 is solved as

$$I_2 = \frac{\delta^{\delta k - 0.5}}{(2\pi)^{(\delta-1)0.5} (c_2 \lambda_{SR})^{\delta k}} G_{2\delta\ 1}^{1\ 2\delta} \left(\begin{matrix} -k, \Delta(\delta, 1-\delta k) \\ 0 \end{matrix} \middle| \frac{A_e \delta^{2\delta}}{(\lambda_{SR} \lambda_{RD} c_2)^\delta} \right). \tag{5.24}$$

-Asymptotic Outage probability of the PUs' Link: Here, the asymptotic OP for the PUs' link is evaluated as the PU transmission power takes very high values. To attain the asymptotic OP, one must rewrite the Meijer-G function in (5.22) as

$$I_1 = \frac{D}{A^k} G_{\delta\ 1}^{1\ \delta} \left(\begin{matrix} \Delta(\delta, 1-\delta k) \\ k \end{matrix} \middle| A P_s^\delta \right), \tag{5.25}$$

where $D = \frac{\delta^{\delta k - 0.5}}{(2\pi)^{(\delta-1)0.5} l_1^{\delta k}}$, $A = \frac{A_e \delta^\delta}{(\lambda_{SR} l_1)^\delta}$, and $l_1 = \frac{b J \lambda_{SR}^{-\delta k}}{\frac{\alpha\rho\eta}{1-\rho} - J\frac{(1-\alpha)\rho\eta}{1-\rho}}$. Transforming (5.25) into its

integral form yields

$$I_1 = \frac{D}{A^k} \int_C \Gamma\left(k-s\right) \Gamma\left(1-\frac{1}{\delta}+s\right) \Gamma\left(1-\frac{2}{\delta}+s\right) \cdots \Gamma(s) A^s P_s^{\delta s} ds. \tag{5.26}$$

It is seen that as $P_s \to \infty$, $I_1 \to \infty$. Hence, the asymptotic expression of I_1 is evaluated using the residue method defined in [89] as

$$I_1^{Asymp} \approx \frac{D}{A^k} \Gamma(k) \Gamma\left(1-\frac{1}{\delta}\right) \Gamma\left(1-\frac{2}{\delta}\right). \tag{5.27}$$

Similarly, I_2 is approximated as

$$I_2^{Asymp} \approx \frac{B}{L^k} \Gamma(k) \Gamma\left(1-\frac{1}{\delta}\right) \Gamma\left(1-\frac{2}{\delta}\right), \tag{5.28}$$

where $B = \frac{\delta^{\delta k - 0.5}}{(2\pi)^{(\delta-1)0.5} l_2^{\delta k}}$, $W = \frac{A_e \delta^{2\delta}}{(\lambda_{SR}\lambda_{RD} l_2)^{\delta}}$, and $l_2 = \frac{N_0 J}{\frac{\alpha\rho\eta}{1-\rho} - J\frac{(1-\alpha)\rho\eta}{1-\rho}}$. Given (5.27) and (5.28), OP is given by

$$OP_P^{Asymp} \approx 1 - \frac{c_3 \delta A_e^k}{\Gamma(k)} I_1^{Asymp} I_2^{Asymp}. \tag{5.29}$$

It is evident from the result that the asymptotic outage probability is independent of P_s. This demonstrates that once the PU transmission power exceeds a certain level, there is no advantage to increasing it further. This is because the system no longer benefits from the power's impact on system reliability. This result will be further clarified and investigated in the numerical results section.

5.3.2 Outage Probability of the Secondary Users' Communication

Given the fact that the SU receiver also receives PUs messages that interfere with its own, it is critical to assess the SUs link's outage probability. The outage probability of the SUs link is evaluated using (5.16), which is expressed in terms of (5.11) and (5.13) as

$$OP \quad = \quad P_r\left(g_{SR} \leq d_1 \frac{d^{PL}}{g_{RE}} + d_2 d^{PL}\right), \tag{5.30}$$

where $d_1 = \frac{\epsilon N_o}{q-\epsilon w}$, $d_2 = \frac{\epsilon e}{q-\epsilon w}$, and $\epsilon = 2^{\frac{R_{ths}}{(1-\rho)T}} - 1$. Following the same procedure to find (5.20), the OP of the SUs' link is expressed as

$$OP = 1 - \frac{d_3 \delta A_e^k}{\Gamma(k)} H_1 H_2, \tag{5.31}$$

where $d_3 = \frac{\delta^{1.5+\delta k} A_e^k \lambda_{RE}^{-\delta k}}{\Gamma(k)(2\pi)^{(\delta-1)0.5}}$. H_1 and H_2 are expressed, respectively as

$$H_1 \quad = \quad \frac{\delta^{\delta k - 0.5}}{(2\pi)^{(\delta-1)0.5}\left(d_2 \lambda_{SR}\right)^{\delta k}} G_{\,1\,\delta}^{\,\delta\,1}\left(\begin{matrix}\Delta(\delta, 1-\delta k) \\ 0\end{matrix}\middle| \frac{A_e \delta^{\delta}}{(\lambda_{SR} d_2)^{\delta}}\right), \tag{5.32}$$

$$H_2 \quad = \quad \frac{\delta^{\delta k - 0.5}}{(2\pi)^{(\delta-1)0.5}\left(d_1 \lambda_{SR}\right)^{\delta k}} G_{\,1\,2\delta}^{\,2\delta\,1}\left(\begin{matrix}-k, \Delta(\delta, 1-\delta k) \\ 0\end{matrix}\middle| \frac{A_e \delta^{2\delta}}{(\lambda_{SR}\lambda_{RE} d_1)^{\delta}}\right). \tag{5.33}$$

-Asymptotic Outage probability of the SUs Link: In here, we evaluate the outage probability of the SUs link as the transmission power of the PU transmitter approaches ∞, i.e., as $P_s \to \infty$. This is to observe the effect of the PUs transmission power on the received SUs messages' quality. Setting $P_s \to \infty$ and performing the approach utilized to find the asymptotic OP for the PUs' link, the OP for the SUs' link is approximated as

$$OP_S^{Asymp} \approx 1 - \frac{d_3 \delta A_e^k}{\Gamma(k)} H_1^{Asymp} H_2^{Asymp}, \tag{5.34}$$

where H_1^{Asymp} is given as

$${H_1}^{Asymp} \approx \frac{D'}{A'^k}\Gamma(k)\Gamma\left(1 - \frac{1}{\delta}\right)\Gamma\left(1 - \frac{2}{\delta}\right), \tag{5.35}$$

with $D' = \frac{\delta^{\delta k-0.5}}{(2\pi)^{(\delta-1)b^*} l_1'^{\delta k}}$, $A = \frac{A_e \delta^{\delta}}{\left(\lambda_{SR} l_1'\right)^{\delta}}$, and $l_1' = \frac{e\epsilon \lambda_{SR}^{-\delta k}}{\frac{(1-\alpha)\rho\eta}{1-\rho} - \epsilon \frac{\alpha\rho\eta}{1-\rho}}$. Moreover, H_2^{Asymp} is expressed as

$$H_2^{Asymp} \approx \frac{B'}{L'^k} \Gamma(k) \Gamma\left(1 - \frac{1}{\delta}\right) \Gamma\left(1 - \frac{2}{\delta}\right). \tag{5.36}$$

with $B' = \frac{\delta^{\delta k-0.5}}{(2\pi)^{(\delta-1)0.5} l_2'^{\delta k}}$, $W' = \frac{A_e \delta^{2\delta}}{\left(\lambda_{SR}\lambda_{RE} l_2'\right)^{\delta}}$, and $l_2' = \frac{N_0 \epsilon}{\frac{(1-\alpha)\rho\eta}{1-\rho} - \epsilon \frac{\alpha\rho\eta}{1-\rho}}$. As seen from (5.34), when the PU transmission power is very large, the outage probability of the SUs link becomes independent of this power. This illustrates that the outage probability reaches its lowest level as P_s takes very high values. This effect will be investigated in the numerical results section.

5.4 Optimization Problems

The primary goal of this section is to improve the networks' data rate in two distinct scenarios. We begin by optimizing the time switching factor (ρ) and the power allocation factor (α) that maximize the data rate of the SUs link while respecting the PUs' rate constraint. Following that, we optimize the same parameters that maximize the sum rate ($R_S + R_P$) to enhance the reliability of both networks. It is worth noting that by optimizing ρ, one may manage the time slots dedicated to energy harvesting and the time allocated to amplifying and forwarding user' messages. Furthermore, optimizing α enables the evaluation of the amount of power required to transfer the messages of each network, and hence the amount of interference affecting each network.

5.4.1 Maximizing the Secondary Users Data Rate

In this section, the time switching factor (ρ) and the power allocation factor of R_k (α) are optimized with an objective of maximizing the SUs' rate while ensuring that the PUs' rate is maintained above a certain threshold (R_{pt}). This demonstrates that the SUs link's reliability may be improved while ensuring that the PUs' reception quality standards are met. Given this, the optimization problem is formulated as

$$\mathcal{P}1: \max_{\rho,\alpha} \quad R_S \tag{5.37}$$

$$\text{s.t.} \quad 0 < \rho < 1, \tag{5.38}$$

$$0 < \alpha < 1, \tag{5.39}$$

$$R_P \geq R_{pt}. \tag{5.40}$$

This problem is clearly a non-convex one since it is a non-linear mixed-integer optimization problem, and hence it is hard to be solved directly. Instead, it can be shown that it is a biconvex problem in ρ and α. As the term suggests, a biconvex problem is the one that is convex in α for a given value of ρ, and convex in ρ for a fixed α. This can be easily shown by several methods, such as plotting the functions on Matlab. Similar to [72], this type of problems can be solved using the algorithm described in Table 5.1. As mentioned in the table, one can use the Lagrangian approach to find the

Table 5.1: Algorithm of solving a biconvex optimization problem

Step 1	Assume G demonstrates the biconvex set of α and ρ and select an arbitrary initial point for these parameters, i.e., (α_0, ρ_0).
Step 2	For a fixed value of ρ, find the optimal value of α (α^*) for the convex problem using the Lagrangian dual method through the method of the gradient decent.
Step 3	Using α^*, search for the optimal value of ρ (ρ^*) for the convex problem using the Lagrangian dual method.

optimal value of ρ and α. The Lagrangian of $\mathcal{P}1$ can be expressed as

$$\mathcal{L}(\zeta, \xi_1, \xi_2, \xi_3) = R_S + \xi_1(\zeta - 1) + \xi_2(-\zeta) + \xi_3(R_{pt} - R_P),$$

where $\xi_1, \xi_2,$ and ξ_3 represent the dual variables associated with the constraint on ζ, for $\zeta \in (\rho, \alpha)$, and the PUs' rate in (5.40), respectively. Then, the Lagrange dual function of $\mathcal{P}1$ is expressed as

$$\mathcal{L}(\xi_1, \xi_2, \xi_3) = \max_{\zeta} \mathcal{L}(\zeta; \xi_1, \xi_2, \xi_3). \tag{5.41}$$

Using the partial derivative and the method of the gradient descent, the values of ρ^*, α^*, ξ_1, ξ_2, and ξ_3 are found.

5.4.2 Maximizing the Sum Rate

In this section, the time switching factor and the power allocation factor which maximize the sum rate $(R_S + R_P)$ are evaluated. Optimizing the sum rate has the potential to increase the reliability of both networks by lowering their outage probability. This optimization problem is formulated as

$$\mathcal{P}2: \max_{\rho,\alpha} \quad R_P + R_S \tag{5.42}$$

$$\text{s.t.} \quad 0 < \rho < 1, \tag{5.43}$$

$$0 < \alpha < 1. \tag{5.44}$$

The sum rate is a biconvex function and thus this problem can be solved using the methodology described in Table 5.1.

5.5 Numerical Results

In this section, the results of our theoretical analyses and Monte-Carlo simulations are presented. Assume a two-dimensional (2D) area $(U = 2)$ and a HPPP distribution of the relays locations. 10^5 realizations of the positions of the relays are generated in a square area of a side of 20 meters (m). Moreover, to take the distance between the nodes into account, we let $d_{xy}^{-PL} = \frac{1}{2\lambda_{xy}}$, in which d_{xy} is the distance between nodes x and y, for $xy = SR, RD, RE$.

Figure 5.3 presents the outage probability of the PUs' link versus the density of SUs. It is observed that when more SUs exist in the network, the reliability of the PUs transmission improves. This is owing to the fact that the more densely populated the area is with SUs, the more likely it is to have an SU closer to the PU transmitter with superior channel characteristics. Moreover, in contrast to the fourth nearest user $(k = 4)$, selecting the first closest SU to the PU transmitter, i.e., $k = 1$, has the greatest impact on improving the performance of the PUs' communication. That is, there is

a larger probability that the closest user will be able to effectively deliver the PUs messages.

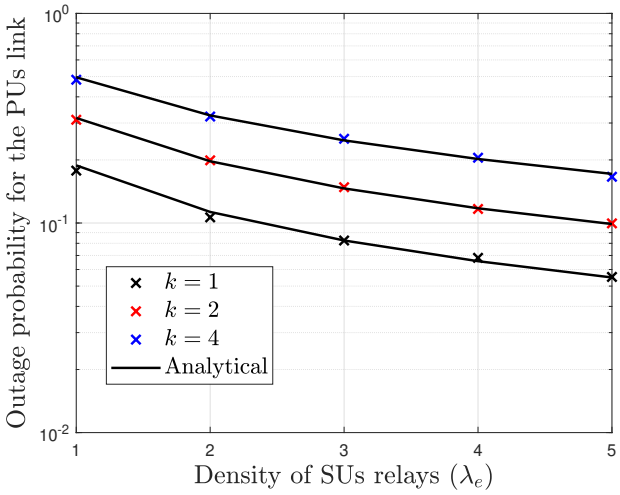

Figure 5.3: The outage probability for the PUs link versus the density of the SUs relay for different values of k. $\rho = 0.5$, $PL = 2$, $\lambda_{RD} = 0.5$, $\lambda_{SR} = 0.5$, $T = 1$, $R_{thp} = 0.5$, $P_s = 5$ dB, $\alpha = 0.8$, and $\eta = 0.8$.

Figure 5.4 illustrates the outage probability of the PUs' communication against the time switching factor (ρ). It is observed that the outage probability is a convex function of ρ. As ρ increases, demonstrating more time is allocated for harvesting energy, a higher SNR is achieved at the PU receiver and consequently a better system performance. However, beyond the minimum value of ρ, the system's reliability worsens. This depicts the scenario in which the time slot left for amplifying the PUs messages and forwarding them to the destination $(1 - \rho)$ is small. Additionally, as the energy harvesting efficiency coefficient (η) increases, the outage probability reduces. This is because a greater η indicates that the relaying SU is capable of harvesting more energy, implying that more power is available for messages' delivery.

Figure 5.5 reflects the impact of the SUs transmission on the PUs' communication. As mentioned earlier in this chapter, the PU receiver regards the SUs messages as interference. Hence, as $(1 - \alpha)$ increases, which is the portion of SU relay power dedicated to forwarding SUs messages, the PUs communication becomes more susceptible to outages. In addition, this figure depicts the effect of the fading severity level of the h_{RD} channel on the PUs' communication, as represented by λ_{RD}. It is found that when λ_{RD} increases, the fading becomes more severe, resulting in a poor reception at the PU destination.

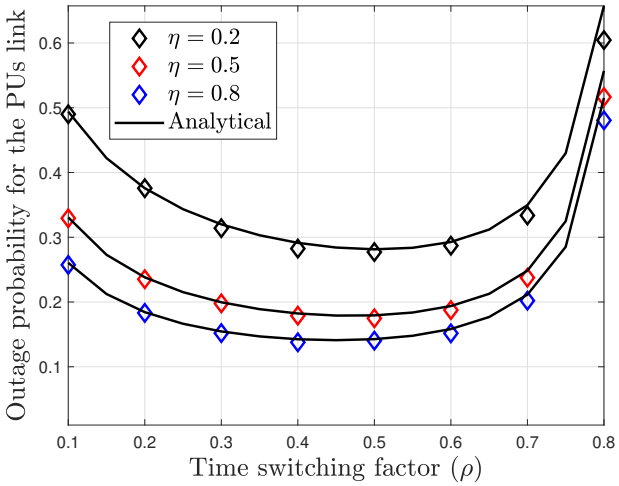

Figure 5.4: The outage probability for the PUs link versus the time switching factor for different values of η. $k = 1$, $PL = 2$, $\lambda_{RD} = 0.5$, $\lambda_{SR} = 0.5$, $T = 1$, $R_{thp} = 0.4$, $PL = 2$, $P_s = 5$ dB, $\alpha = 0.8$, and $\lambda_e = 1$.

Figure 5.6 depicts the impact of the PUs messages on the quality of the SUs' communication. As the proportion of the relay's power dedicated to PU transmission (α) increases, the probability of an outage in the SUs' communication increases. This is because as α rises, the SU receiver becomes more subject to the interference caused by the PUs transmissions. Additionally, as α increases, the portion of power assigned to the SUs' communication at the relay decreases, raising the probability of an SUs' transmission outage. However, a higher α suggests that a greater amount of the power is assigned to convey the PUs messages, resulting in a lower PUs' link outage probability. Finally, since the same relay that forwards PUs' messages also forwards SUs' messages, as the density of the SUs relays increases, the reliability of the SUs network improves.

Figure 5.7 reveals the significance of sharing in overlay CRN. In this figure, we compare the overlay CRN with direct transmission, in which we presume that the PUs can communicate directly without the assistance of SUs. As shown in the figure, when α is between 0.35 and 0.65, the overlay CRN outperforms the direct transmission since the attained outage probability is lower. This applies to both SUs and PUs networks. Moreover, it is evident that when $\alpha = 0.5$, both networks function similarly. In addition, when $\alpha < 0.5$, the SUs' communication reliability is greater than the PUs', however, when $\alpha > 0.5$, the PUs' reliability steadily improves to surpass the SUs'. This illustrates the importance of optimizing α to be able to decide how to distribute the power of the SU relay and

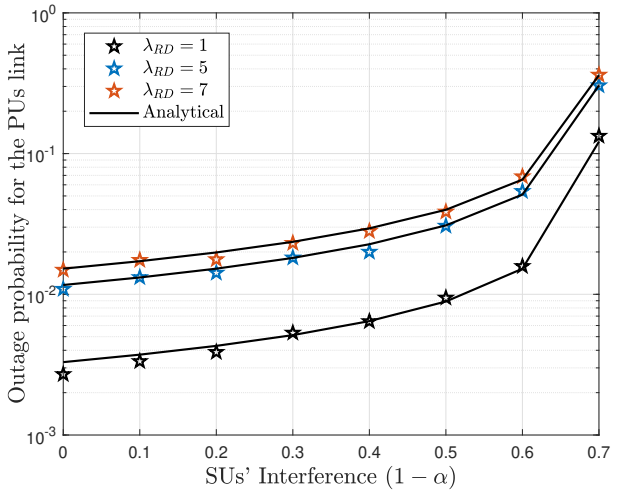

Figure 5.5: The outage probability for the PUs link versus the interference caused by the SUs transmissions. $k = 1$, $\delta = 1$, $\lambda_{SR} = 1$, $T = 1$, $R_{thp} = 0.2$, $P_s = 5$ dB, $\eta = 0.7$, $\rho = 0.6$, $\lambda_e = 100$, and $k = 1$.

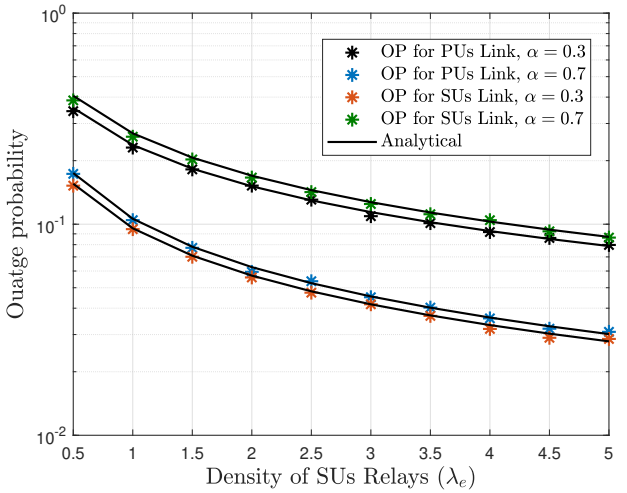

Figure 5.6: The outage probability for the PUs and SUs links versus the SUs density. $k = 1$, $PL = 2$, $\lambda_{SR} = 1$, $\lambda_{RD} = 1$, $\lambda_{RE} = 1$, $T = 1$, $R_{thp} = 0.1$, $R_{ths} = 0.1$, $P_s = 5$ dB, $\rho = 0.6$, $\eta = 0.7$, and $k = 1$.

control the interference caused by one network on another.

Figure 5.8 shows the outage probability of the SUs network versus the transmission power of the PU-Tx (P_s). It can be seen that as P_s increases, the outage probability decreases. This is because as P_s increases, the amount of energy harvested at the SU relay increases, leading to improved SUs' link reliability. In addition, the figure shows the asymptotic outage probability of the SUs' link,

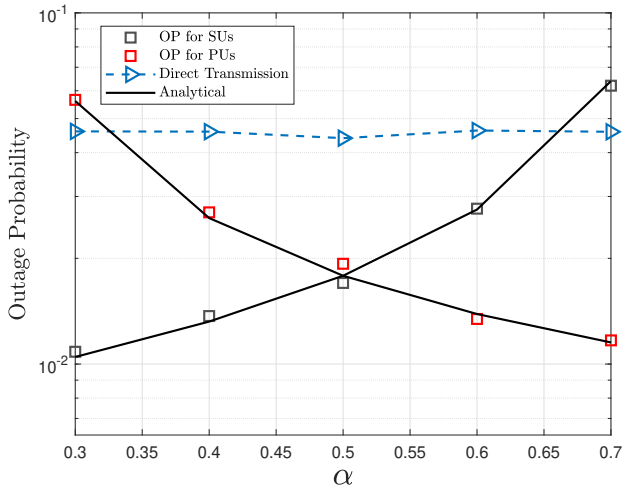

Figure 5.7: The outage probability versus α. $k = 1$, $\rho = 0.5$, $\eta = 0.2$, $\lambda_{RD} = 0.5$, $PL = 2$, $\lambda_{SR} = 0.5$, $T = 1$, $R_{thp} = 0.2$, $R_{ths} = 0.2$, $P_s = 2$ dB, $\lambda_e = 5$. $d_{SR} = 0.5m$, $d_{RD} = 0.5m$, $d_{RE} = 0.5m$, and $d_{SP(direct)} = 1m$.

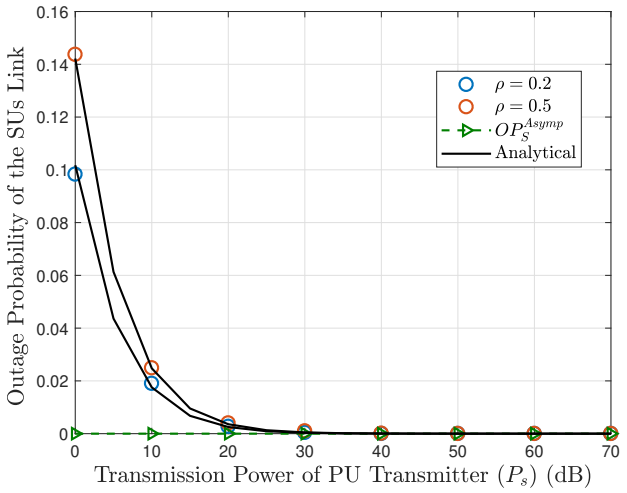

Figure 5.8: The outage probability of the SUs versus P_s. $k = 1$, $\eta = 0.2$, $\lambda_{RE} = 0.5$, $\lambda_{SR} = 0.1$, $T = 1$, $R_{ths} = 1$, $PL = 2$, $\alpha = 0.2$, and $\lambda_e = 5$.

which represents the scenario when P_s approaches ∞. It is obvious that as P_s reaches this value, the system is in optimal condition. This is due to the fact that the harvested energy will be high, and thus the received SINR will be improved, resulting in a zero outage probability. Moreover, one can notice that the outage probability agrees with the asymptotic one at high values of P_s.

Figure 5.9 illustrates the outage probability for the PUs link versus the PU transmission power P_s. As P_s increases, the PUs' communication quality improves. This is attributable to the fact

that boosting the PU-Tx transmission power increases the harvested energy at the assistant SU. As the amount of energy gathered increases, the amplification factor increases, resulting in a higher reception quality at PU-Rx. In addition, the saturation that occurs at high P_s indicates that boosting the power has no benefit after a particular level of P_s. This is owing to the belief that as P_s becomes very large, the outage probability becomes independent of this power and reaches its optimum situation, i.e. $OP \approx 0$. This is also confirmed by the agreement between the outage probability at high P_s and the asymptotic outage probability obtained in (5.34) as $P_s \to \infty$. Furthermore, despite the independence on P_s, the results demonstrate that the overlay CRN outperforms the direct transmission between PUs, i.e., without the assistance of SUs.

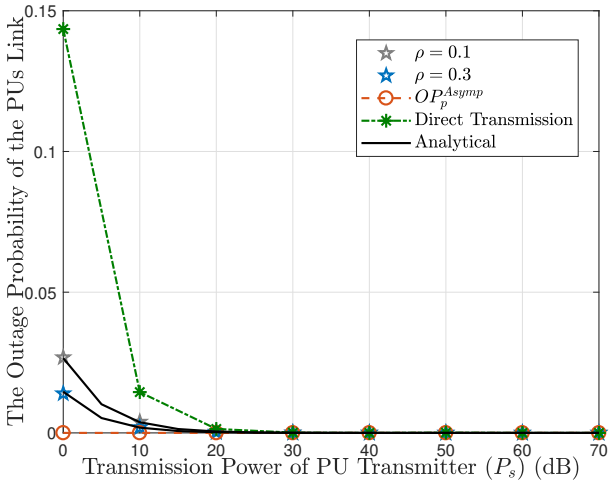

Figure 5.9: The outage probability of the PUs versus P_s. $k = 1$, $PL = 2$, $\eta = 0.9$, $d_{SR} = 0.5m$, $d_{RD} = 0.5m$, $T = 1$, $R_{thp} = 0.4$, $\alpha = 0.8$, and $\lambda_e = 5$.

Figure 5.10 depicts the SUs' link rate versus the transmission power of the PU-Tx (P_s). By comparing the fixed value of ρ and α with the optimum ones (ρ^*, α^*), it is clear that the SUs achieve the optimum link rate when ρ and α are chosen according to the optimization problem in (5.37). In addition, the results indicate the benefit of performing a joint optimization for both parameters rather than optimizing a single parameter ((α^*, $\rho = 0.4$) and (ρ^*, $\alpha = 0.95$)). Particularly, the SUs achieve the highest rate when both parameters are optimized jointly. This highlights the significant importance of having an adjustable time switching factor and power allocation factor in the EH process. An optimized α assists in determining the amount of SU relay power that should be used

for each network while controlling the interference caused by one network on another. Moreover, by optimizing ρ, one can determine the time slots assigned for the EH process and the amplifying and forwarding process. Furthermore, it is noticed that optimizing both parameters yields a result that is closer to optimizing α independently for fixed ρ. This depends on the selected values of the fixed parameters and the PUs rate threshold. To illustrate a scenario in which the joint optimization approach gets close to optimizing solely ρ, the threshold in Figure 5.11 is considered to be lower than the one in Figure 5.10 with different fixed values chosen for the single optimization scenarios. The figure indicates that when optimizing ρ, selecting lower α and R_{pt} results in rising the impact of optimizing ρ, as it gets closer to the joint optimization. Additionally, it is worth mentioning that the fixed values of ρ and α are selected from the feasibility region of problem $\mathcal{P}1$.

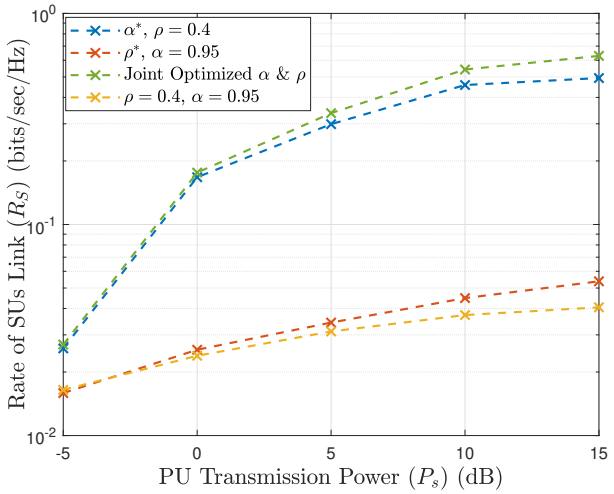

Figure 5.10: The SUs' rate link versus P_s. $k = 1$, $\eta = 0.8$, $\lambda_{RD} = 1$, $\lambda_{SR} = 0.5$, $\lambda_{RE} = 1$, $T = 1$, $R_{pt} = 0.5$, and $\lambda_e = 1$.

Figure 5.12 presents the links rates of the SUs and PUs communication against P_s. It is observed that optimizing the parameters α and ρ improves the SUs rate. Moreover, even with fixed parameters, i.e. without optimization, the PUs' rate remains greater than the threshold rate (R_{pt}). This ensures that the performance of the PUs' link is preserved above the minimum allowed level. In addition, whether the parameters are optimized or fixed, the PUs' rate remains greater than the SUs' rate. Additionally, Figure 5.13 shows both rates against P_s when α and ρ are optimized. It is concluded that regardless of the transmission power level of PU-Tx, the PUs' rate is maintained

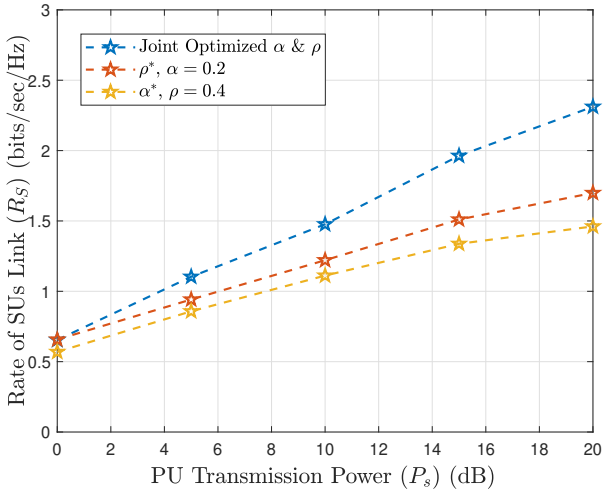

Figure 5.11: The SUs' rate link versus P_s. $k = 1$, $\eta = 0.8$, $\lambda_{RD} = 1$, $\lambda_{SR} = 0.5$, $\lambda_{RE} = 1$, $T = 1$, $R_{pt} = 0.1$, and $\lambda_e = 1$.

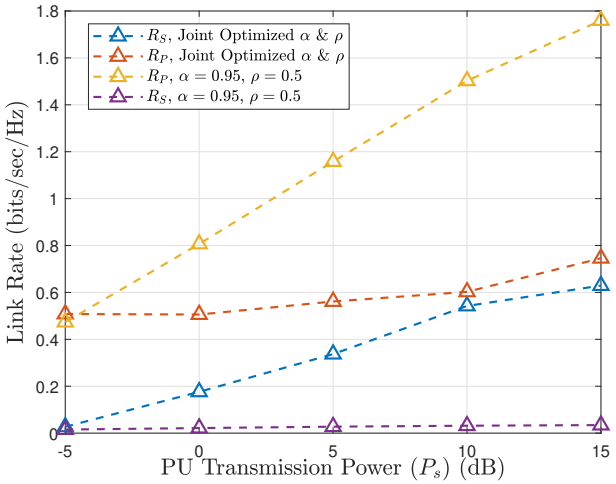

Figure 5.12: The SUs' and PUs' links rate versus P_s. $k = 1$, $\eta = 0.8$, $PL = 2$, $\lambda_{RE} = 1$, $\lambda_{RD} = 1$, $\lambda_{SR} = 0.5$, $T = 1$, $R_{pt} = 0.5$, and $\lambda_e = 1$.

above the threshold ($R_P \geq 0.5$).

As a final investigation, Figure 5.14 presents the sum-rate of both networks versus the PU transmission power (P_s). It is observed that using the time switching factor and the power allocation factor optimized in problem $\mathcal{P}2$ (ρ^* and α^*) provides the best performance when compared to fixed ρ and α. Notably, optimizing the sum rate has the advantage of simultaneously enhancing both networks' reliability, regardless of the interference imposed by one network on the other. As a result,

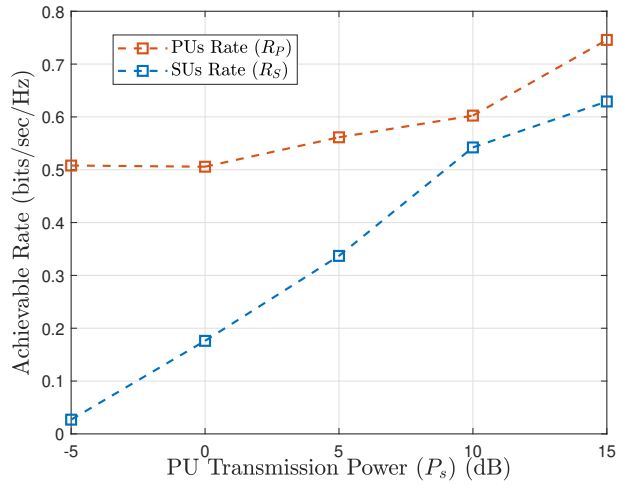

Figure 5.13: The SUs' and PUs' links rate versus P_s for joint optimized ρ and α. $k = 1$, $\eta = 0.8$, $PL = 2$, $\lambda_{RE} = 1$, $\lambda_{RD} = 1$, $\lambda_{SR} = 0.5$, $T = 1$, $R_{pt} = 0.5$, and $\lambda_e = 1$.

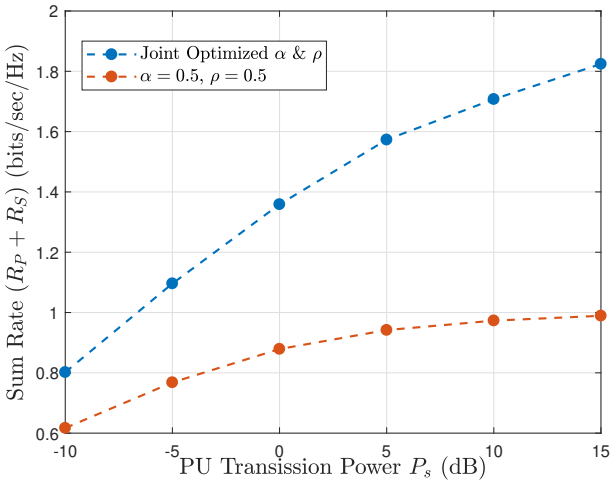

Figure 5.14: The sum rate versus P_s for different values of α and ρ. $k = 1$, $\eta = 0.8$, $\lambda_{RD} = 1$, $\lambda_{SR} = 0.5$, $\lambda_{RE} = 1$, $T = 1$, and $\lambda_e = 1$.

all users in this cooperating CRN will have stable communication.

5.6 Summery

This chapter investigates an overlay cognitive radio network with two primary users (PUs) and several secondary users (SUs). In exchange for accessing the licensed band, one of these multiple

SUs is chosen to forward the PUs messages using the harvested energy from the PU transmitter messages. Our results indicate that a higher density of these SUs is required to increase the link reliability of the PUs and SUs communication. The outage probability of both links and their asymptotic expressions have been derived. In addition, the time switching factor and the SU relay power allocation factor are optimized for two scenarios: maximizing the SUs' rate while constraining the PUs' rate, and maximizing the sum of both networks' rates. Our results demonstrate that, as compared to fixed factors, the derived optimized ones achieve the optimum performance.

Chapter 6

Conclusions and Future Works

6.1 Conclusions

Monitoring the radio spectrum, it is noticed that the spectrum usage is concentrated over certain parts of the band. On the other hand, a significant portion of the spectrum is still under-utilized due to the static frequency allocation. As the demand for spectrum usage increases, there should be a solution for these issues. Hence, CRNs were proposed to solve these problems by enabling SUs to access the bands in an opportunistic manner. As the unlicensed users seek to access the licensed bands, one of the three access modes should be used; interweave, underlay, and overlay. Threats on CRNs can be initiated from outside the network, regardless of the type of access mode. In this case, users within the coverage range of transmission are able to overhear confidential information due to the broadcasting nature of the transmission. Moreover, since SUs and PUs both reside on the same network, they need to be protected from different types of threats. All the aforementioned reasons necessitate the importance of utilizing PLS approaches to secure the data in CRNs and PLS is proved to be a reliable and effective approach to achieve the required level of secrecy. Our research has made major contributions, as evidenced by the number of publications associated with our research. Next, we briefly summarize those accomplishments.

In Chapter 3, we examined PLS in three distinct scenarios in which a three-node wiretap system was considered to operate over cascaded κ-μ fading channels. The first scenario assumed the

worst-case circumstance. Under the prospect of conspiring eavesdroppers, the second scenario assumed normal conditions, i.e., cascaded channels at all links. Additionally, in the third case, it was assumed that non-colluding eavesdroppers are attempting to intercept the confidential information. We demonstrated that security declines as the cascade level in the main channel increases or as the cascade level in the wiretap lowers. However, improving the conditions on the main channel by increasing the average received SNR at the legitimate receiver can help reduce the risk of a secrecy outage. Additionally, we compared colluding and non-colluding eavesdroppers and demonstrated that colluding eavesdroppers pose a higher security risk. PLS is studied for an underlay SIMO CRN over cascaded κ-μ fading channels with an eavesdropping risk. Both the SU destination and the eavesdropper are equipped with multiple antennas and employ MRC technique. The results demonstrate that the rise in the cascade level at the main channel impairs secrecy, demonstrating that the assumption of cascaded channels cannot be ignored, particularly when devices are moving or in dense scattering zones. The privacy may be augmented by deploying additional antennas at the legitimate receiver. Additionally, we highlighted how the constraint on transmit power can have a significant influence on secrecy when SUs access the channel via the underlay model. Our findings confirm that both the main and wiretap channel conditions have an impact on PLS. Finally, we considered a particular case of the later system model in which a SISO CRN with cascaded Rayleigh channels was assumed. We showed that the distances between nodes significantly affect security. For example, when the distance between the SU transmitter and the eavesdropper is short, the secondary user's security can be significantly compromised.

In Chapter 4, the PLS for underlay CRNs was strengthened through jamming approaches based on energy harvesting techniques over cascaded channels. We began by assuming that the SU destination performs energy harvesting while receiving messages from the SU transmitter. The destination emits jamming signals to weaken the eavesdropper's reception using the full-duplex approach. As a result of our findings, we demonstrated that the confidentiality of SU data transmission can be enhanced by increasing the proportion of energy used for jamming. Additionally, our findings highlight the trade-off between system reliability and security. Furthermore, we added a cooperating SU jammer to the system model to gather energy and broadcast jamming signals toward the

non-colluding multiple eavesdroppers. The results demonstrate that when the density of eavesdroppers rises, the security of SUs declines. Additionally, our findings suggest that in order to achieve optimal privacy, the power splitting factor should be adapted at the legitimate receiver. Finally, the study advises that the jammer should adjust the quantity of energy harvested based on the location of the most powerful eavesdropper. Additionally, we contrasted colluding and non-colluding eavesdroppers and observed that, even with a high density of non-colluding eavesdroppers, security is degraded more when colluding eavesdroppers exist.

In Chapter 5, we examined an overlay cognitive radio network with two PUs and multiple SUs. In exchange for being granted access to the licensed band, one of these multiple SUs is chosen to transfer the PUs messages using the energy harvested from the PU transmitter messages. Our findings show that a higher density of these SUs is necessary to improve the communication links reliability for both PUs and SUs. Additionally, the time switching factor and power allocation factor for the SU relays are optimized for two scenarios: maximizing the SUs' rate while restraining the PUs' rate, and maximizing the total of the two networks' rates. Our findings indicate that, when compared to fixed factors, the obtained optimized ones function optimally.

6.2 Future Works

Until this point, our research has concentrated on enhancing the security of wireless networks using cascaded channels. However, additional research is required to widen the scope of our findings. 5G techniques can be used in conjunction with the research of PLS for CRNs to enhance the security of the network or to overcome several raised obstacles. This section comprises some suggestions for future work;

Recent researches have concentrated on imbuing CRNs with intelligence via artificial intelligence techniques such as machine learning. For our work in Chapter 5, we assumed that several SUs exist and one is selected to relay the information. We might extend the study by constructing a learning-based strategy for several functions. For example, we may assume an overlay CRN with multiple transmitting SUs, and one receiving SU. Among the SUs' transmitters, there is one central node that collects historic data over time sent by the other SUs in the cooperative network. The

central node will learn the decision function based on the collected data and decide which SU will relay the messages.

Another extension to our overlay model would be to modify the SU relay's selection criterion. The revised criterion is modified to take the energy level of each SU relay into consideration. This is to assist the SU with the lowest battery energy level in harvesting energy and recharging the battery. Additionally, one can investigate PLS when all channels are subjected to cascaded fading distributions rather than single fading models. Assuming an eavesdropper is present to tap the secret information, one of the SUs may be chosen to forward the messages, while another SU is designated to send harmful signals to the eavesdroppers to safeguard the transmissions.

Multiple antennas at the transmitter and/or receiver of the main channel have been shown to improve the received SNR and hence the secrecy of the SUs' network. Thus, an interesting extension to our underlay or overlay scenarios would be to consider multiple antennas at the SUs or PUs transmitters to assist in ensuring the security of the transmission.

The final suggested future work would be to integrate the non-orthogonal multiple access (NOMA) technique with CRNs. NOMA has attracted considerable interest recently since it enables several users to share a single wireless resource concurrently. As a result, NOMA increases coverage and spectral efficiency. Additional spectral efficiency gains are possible when NOMA is combined with CRNs, as both address the issue of spectrum under-utilization. This, however, comes at the cost of rising inter-interference and intra-cell interference, which creates security issues. Thus, when developing the network, particularly over cascaded channels, PLS for CRNs-based NOMA should be examined. For instance, PLS could be examined for overlay CRN-based NOMA with multiple SUs and PUs operating over cascaded channels. SUs are deemed to be untrusted users (eavesdroppers). Based on the channel gains of the selected users, the primary and secondary users can be paired using power-domain NOMA.

Appendix A

List of Publications

-Journal Articles:

- **D. H. Tashman**, W. Hamouda and I. Dayoub, "Secrecy Analysis Over Cascaded κ -μ Fading Channels With Multiple Eavesdroppers," in IEEE Transactions on Vehicular Technology, vol. 69, no. 8, pp. 8433-8442, Aug. 2020, doi: 10.1109/TVT.2020.2995115.

- **D. H. Tashman** and W. Hamouda, "Physical-Layer Security on Maximal Ratio Combining for SIMO Cognitive Radio Networks Over Cascaded κ-μ Fading Channels," in IEEE Transactions on Cognitive Communications and Networking, vol. 7, no. 4, pp. 1244-1252, Dec. 2021, doi: 10.1109/TCCN.2021.3074178.

- **D. H. Tashman**, W. Hamouda and J. M. Moualeu, "On Securing Cognitive Radio Networks-Enabled SWIPT Over Cascaded κ-μ Fading Channels With Multiple Eavesdroppers," in IEEE Transactions on Vehicular Technology, vol. 71, no. 1, pp. 478-488, Jan. 2022, doi: 10.1109/TVT.2021.3127321.

- **D. H. Tashman** and W. Hamouda, "An Overview and Future Directions on Physical-Layer Security for Cognitive Radio Networks," in IEEE Network, vol. 35, no. 3, pp. 205-211, May/June 2021, doi: 10.1109/MNET.011.2000507.

- Ghareeb, I. and **D. H. Tashman**, "Statistical analysis of cascaded Rician fading channels", in International Journal of Electronics Letters, 8(1), 46-59, 2020.

- **D. H. Tashman** and W. Hamouda, "Cascaded κ-μ Fading Channels with Colluding and Non-Colluding Eavesdroppers: Physical-Layer Security Analysis", Future Internet, 13(8), 205, 2021.

-Conference Proceedings:

- **D. H. Tashman** and W. Hamouda, "Cascaded κ-μ Fading Channels with Colluding Eavesdroppers: Physical-Layer Security Analysis," 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), 2021, pp. 1-6, doi: 10.1109/ICCSPA49915.2021.9385753.

- **D. H. Tashman** and W. Hamouda, "Secrecy Analysis for Energy Harvesting-Enabled Cognitive Radio Networks in Cascaded Fading Channels," ICC 2021 - IEEE International Conference on Communications, 2021, pp. 1-6, doi: 10.1109/ICC42927.2021.9500621.

- **D. H. Tashman** and W. Hamouda, "Physical-Layer Security for Cognitive Radio Networks over Cascaded Rayleigh Fading Channels," GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 2020, pp. 1-6, doi: 10.1109/GLOBECOM42002.2020.9348134. Best Paper Award.

- **D. H. Tashman** and W. Hamouda, "Towards Improving the Security of Cognitive Radio Networks-Based Energy Harvesting," ICC 2022 - IEEE International Conference on Communications, accepted.

- **D. H. Tashman**, W. Hamouda and J. M. Moualeu, "Overlay Cognitive Radio networks Enabled Energy Harvesting with AF Relays." To be submitted

Bibliography

[1] M. Bouabdellah, F. E. Bouanani, P. C. Sofotasios, D. B. da Costa, H. Ben-azza, K. Mezher, and S. Muhaidat, "Intercept Probability of Underlay Uplink CRNs with Multi-Eavesdroppers," in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Istanbul, Turkey, Turkey, 2019, pp. 1–6.

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

[3] Y. Alsaba, S. K. A. Rahim, and C. Y. Leow, "Beamforming in Wireless Energy Harvesting Communications Systems: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 2, pp. 1329–1360, 2018.

[4] H. Ilhan, M. Uysal, and I. Altunbas, "Cooperative Diversity for Intervehicular Communication: Performance Analysis and Optimization," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 7, pp. 3301–3310, 2009.

[5] D. H. Tashman and W. Hamouda, "An Overview and Future Directions on Physical-Layer Security for Cognitive Radio Networks," *IEEE Network*, pp. 1–7, 2020.

[6] I. Ghareeb and D. Tashman, "Statistical analysis of cascaded rician fading channels," *International Journal of Electronics Letters*, pp. 1–14, 2018.

[7] D. H. Tashman, W. Hamouda, and I. Dayoub, "Secrecy analysis over cascaded $\kappa - \mu$ fading channels with multiple eavesdroppers," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 8433–8442, 2020.

[8] M. Bouabdellah, F. El Bouanani, P. C. Sofotasios, S. Muhaidat, D. B. Da Costa, K. Mezher, H. Ben-Azza, and G. K. Karagiannidis, "Cooperative Energy Harvesting Cognitive Radio Networks With Spectrum Sharing and Security Constraints," *IEEE Access*, vol. 7, pp. 173 329–173 343, 2019.

[9] I. Ghareeb and D. Tashman, "Statistical analysis of cascaded Rician fading channels," *Int. J. Electron. Lett.*, vol. 8, no. 1, pp. 46–59, 2020.

[10] J. Lee, J. H. Lee, and S. Bahk, "Performance Analysis for Multi-Hop Cognitive Radio Networks Over Cascaded Rayleigh Fading Channels With Imperfect Channel State Information," *IEEE Trans. Veh. Technol.*, vol. 68, no. 10, pp. 10 335–10 339, 2019.

[11] Z. Xiang, W. Yang, G. Pan, Y. Cai, and Y. Song, "Physical Layer Security in Cognitive Radio Inspired NOMA Network," *IEEE J. Sel. Top. Signal Process.*, vol. 13, no. 3, pp. 700–714, 2019.

[12] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys Tutorials*, vol. 11, no. 1, pp. 116–130, First 2009.

[13] S. Pandit and G. Singh, "Spectrum sensing in cognitive radio networks: potential challenges and future perspective," in *Spectrum sharing in cognitive radio networks*. Springer, 2017, pp. 35–75.

[14] E. Visotsky, S. Kuffner, and R. Peterson, "On collaborative detection of tv transmissions in support of dynamic spectrum sharing," in *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.* IEEE, 2005, pp. 338–345.

[15] R. Chen and J. Park, "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks," in *2006 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks*, 2006, pp. 110–119.

[16] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A Survey on Security Threats

and Detection Techniques in Cognitive Radio Networks," *IEEE Communications Surveys Tutorials*, vol. 15, no. 1, pp. 428–445, 2013.

[17] Q. Wang, K. Xu, and K. Ren, "Cooperative Secret Key Generation from Phase Estimation in Narrowband Fading Channels," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 9, pp. 1666–1674, October 2012.

[18] S. Ö. Ata, "Secrecy Performance Analysis Over Double Nakagami-m Fading Channels," in *2018 41st Int. Conf. Telecommun. Signal Process. (TSP)*, Athens, Greece, July 2018, pp. 1–4.

[19] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the Security of Cognitive Radio Networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3790–3795, Aug. 2015.

[20] H. Choi, D. Ron, M. Sengly, and J. Lee, "Energy-neutral wireless sensor network based on swipt in wireless powered communication networks," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–7.

[21] X. Di, K. Xiong, P. Fan, and H. Yang, "Simultaneous wireless information and power transfer in cooperative relay networks with rateless codes," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 2981–2996, 2017.

[22] B. Talha and M. Pätzold, "Channel Models for Mobile-to-Mobile Cooperative Communication Systems: A State of the Art Review," *IEEE Vehicular Technology Magazine*, vol. 6, no. 2, pp. 33–43, June 2011.

[23] A. Kaur and J. Malhotra, "Cascade Fading Channel Models for Wireless Communication-A Survey," *International Journal of Computer Applications*, vol. 89, no. 14, pp. 22–25, 2014.

[24] A. A. Boulogeorgos, P. C. Sofotasios, B. Selim, S. Muhaidat, G. K. Karagiannidis, and M. Valkama, "Effects of RF Impairments in Communications Over Cascaded Fading Channels," *IEEE Trans. Commun.*, vol. 65, no. 11, pp. 8878–8894, Nov. 2016.

[25] A. Bhowal and R. S. Kshetrimayum, "End to end performance analysis of M2M cooperative

communication over cascaded α-μ channels," in *2017 9th Int. Conf. Commun. Syst. Networks (COMSNETS)*, Bangalore, India, Jan. 2017, pp. 116–122.

[26] S. Ö. Ata, "Secrecy performance analysis over cascaded fading channels," *IET Commun.*, vol. 13, no. 2, pp. 259–264, Jan. 2019.

[27] A. Bekkali, S. Zou, A. Kadri, M. Crisp, and R. V. Penty, "Performance Analysis of Passive UHF RFID Systems Under Cascaded Fading Channels and Interference Effects," *IEEE Trans. Wireless Commun.*, vol. 14, no. 3, pp. 1421–1433, March 2015.

[28] Y. Alghorani, G. Kaddoum, S. Muhaidat, and S. Pierre, "On the Approximate Analysis of Energy Detection Over $n*$Rayleigh Fading Channels Through Cooperative Spectrum Sensing," *IEEE Wireless Commun. Lett.*, vol. 4, no. 4, pp. 413–416, Aug. 2015.

[29] Z. Hadzi-Velkov, N. Zlatanov, and G. K. Karagiannidis, "Level Crossing Rate and Average Fade Duration of the Multihop Rayleigh Fading Channel," in *2008 IEEE Int. Conf. Commun.*, Beijing, China, May 2008, pp. 4451–4455.

[30] K. Peppas, F. Lazarakis, A. Alexandridis, and K. Dangakis, "Cascaded generalised-K fading channel," *IET commun.*, vol. 4, no. 1, pp. 116–124, Jan. 2010.

[31] F. Yilmaz and M. Alouini, "Product of the Powers of Generalized Nakagami-m Variates and Performance of Cascaded Fading Channels," in *GLOBECOM 2009 - 2009 IEEE Global Telecommun Conf.*, Honolulu, HI, USA, Nov. 2009, pp. 1–8.

[32] P. C. Sofotasios, L. Mohjazi, S. Muhaidat, M. Al-Qutayri, and G. K. Karagiannidis, "Energy Detection of Unknown Signals Over Cascaded Fading Channels," *IEEE Antennas and Wireless Propag. Lett.*, vol. 15, pp. 135–138, May 2016.

[33] 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, May 2018.

[34] Y. Alghorani, G. Kaddoum, S. Muhaidat, S. Pierre, and N. Al-Dhahir, "On the Performance of Multihop-Intervehicular Communications Systems Over n$*$Rayleigh Fading Channels," *IEEE Wireless Commun. Lett.*, vol. 5, no. 2, pp. 116–119, April 2016.

[35] M. D. Yacoub, "The $\kappa - \mu$ distribution and the $\eta - \mu$ distribution," *IEEE Antennas Propag. Mag.*, vol. 49, no. 1, pp. 68–81, Feb. 2007.

[36] G. K. Karagiannidis, N. C. Sagias, and P. T. Mathiopoulos, "N $*$ nakagami: A novel stochastic model for cascaded fading channels," *IEEE Transactions on Communications*, vol. 55, no. 8, p. 1453, 2007.

[37] J. Salo, H. M. El-Sallabi, and P. Vainikainen, "The distribution of the product of independent rayleigh random variables," *IEEE Transactions on Antennas and Propagation*, vol. 54, no. 2, pp. 639–643, Feb 2006.

[38] E. J. Leonardo and M. D. Yacoub, "Product of α-μ variates," *IEEE Wireless Communications Letters*, vol. 4, no. 6, pp. 637–640, 2015.

[39] ——, "Statistics of the product of arbitrary α-μ variates with applications," in *Personal, Indoor, and Mobile Radio Communication (PIMRC), 2014 IEEE 25th Annual International Symposium on*. IEEE, 2014, pp. 73–76.

[40] O. S. Badarneh, S. Muhaidat, P. C. Sofotasios, S. L. Cotton, K. Rabie, and D. B. da Costa, "The nfisher-snedecor $\mathcal{F}$ cascaded fading model," in *2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Oct 2018, pp. 1–7.

[41] X. Liu, "Probability of strictly positive secrecy capacity of the Rician-Rician fading channel," *IEEE Wireless Communications Letters*, vol. 2, no. 1, pp. 50–53, 2013.

[42] ——, "Probability of strictly positive secrecy capacity of the Weibull fading channel," in *2013 IEEE Global Communications Conference (GLOBECOM)*, Dec 2013, pp. 659–664.

[43] 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, July 2015.

[44] X. Liu, "Strictly positive secrecy capacity of log-normal fading channel with multiple eavesdroppers," in *2014 IEEE International Conference on Communications (ICC)*, June 2014, pp. 775–779.

[45] H. Lei, I. S. Ansari, G. Pan, B. Alomair, and M. Alouini, "Secrecy Capacity Analysis Over $\alpha - \mu$ Fading Channels," *IEEE Communications Letters*, vol. 21, no. 6, pp. 1445–1448, June 2017.

[46] L. Kong, H. Tran, and G. Kaddoum, "Performance analysis of physical layer security over α-μ fading channel," *Electronics Letters*, vol. 52, no. 1, pp. 45–47, 2015.

[47] J. M. Moualeu, D. B. da Costa, W. Hamouda, U. S. Dias, and R. A. A. de Souza, "Physical Layer Security Over α-κ-μ and α-η-μ Fading Channels," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 1025–1029, Jan. 2019.

[48] M. Srinivasan and S. Kalyani, "Secrecy capacity of $\kappa - \mu$ shadowed fading channels," *IEEE Communications Letters*, vol. 22, no. 8, pp. 1728–1731, Aug 2018.

[49] J. M. Moualeu and W. Hamouda, "On the Secrecy Performance Analysis of SIMO Systems Over $\kappa - \mu$ Fading Channels," *IEEE Commun. Lett.*, vol. 21, no. 11, pp. 2544–2547, Nov. 2017.

[50] J. Sun, H. Bie, X. Li, J. Zhang, G. Pan, and K. M. Rabie, "Secrecy Performance Analysis of SIMO Systems Over Correlated $\kappa - \mu$ Shadowed Fading Channels," *IEEE Access*, vol. 7, pp. 86 090–86 101, June 2019.

[51] J. M. Moualeu, D. B. da Costa, F. J. Lopez-Martinez, W. Hamouda, T. M. N. Ngatched, and U. S. Dias, "Secrecy Analysis of a TAS/MRC Scheme in $\alpha - \mu$ Fading Channels," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2019, pp. 1–6.

[52] L. Kong, S. Vuppala, and G. Kaddoum, "Secrecy Analysis of Random MIMO Wireless Networks Over α-μ Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 11 654–11 666, Dec 2018.

[53] L. Yang, M. O. Hasna, and I. S. Ansari, "Physical Layer Security for TAS/MRC Systems With and Without Co-Channel Interference Over η–μ Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 12 421–12 426, Dec 2018.

[54] H. Lei, H. Zhang, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and K. A. Qaraqe, "Secrecy Outage Performance for SIMO Underlay Cognitive Radio Systems With Generalized Selection Combining Over Nakagami-m Channels," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 10 126–10 132, Dec 2016.

[55] S. Ö. Ata, "Physical layer security over cascaded Rayleigh fading channels," in *2018 26th Signal Processing and Communications Applications Conference (SIU)*. IEEE, 2018, pp. 1–4.

[56] R. Singh and M. Rawat, "Unified Analysis of Secrecy Capacity Over N $*$ Nakagami Cascaded Fading Channel," in *2018 18th International Symposium on Communications and Information Technologies (ISCIT)*. IEEE, 2018, pp. 422–427.

[57] L. Kong, Y. Ai, J. He, N. Rajatheva, and G. Kaddoum, "Intercept Probability Analysis over the Cascaded Fisher-Snedecor $\mathcal{F}$ Fading Wiretap Channels," in *2019 16th International Symposium on Wireless Communication Systems (ISWCS)*, Aug 2019, pp. 672–676.

[58] D. H. Tashman and W. Hamouda, "Cascaded κ-μ fading channels with colluding eavesdroppers: Physical-layer security analysis," in *2020 Int. Conf. Commun. Signal Process. their Appl. (ICCSPA)*, Sharjah, United Arab Emirates, 2021, pp. 1–6.

[59] D. Tashman, W. A. Hamouda, and J. M. Moualeu, "On securing cognitive radio networks-enabled swipt over cascaded-fading channels with multiple eavesdroppers," *IEEE Transactions on Vehicular Technology*, 2021.

[60] H. Zhao, H. Liu, Y. Liu, C. Tang, and G. Pan, "Physical layer security of maximal ratio combining in underlay cognitive radio unit over Rayleigh fading channels," in *2015 IEEE Int. Conf. Commun. Software Networks (ICCSN)*, Chengdu, China, June 2015, pp. 201–205.

[61] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the Security of Cognitive Radio Networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3790–3795, Aug 2015.

[62] H. Lei, C. Gao, I. S. Ansari, Y. Guo, Y. Zou, G. Pan, and K. A. Qaraqe, "Secrecy Outage Performance of Transmit Antenna Selection for MIMO Underlay Cognitive Radio Systems Over Nakagami-m Channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2237–2250, March 2017.

[63] H. Zhao, Y. Tan, G. Pan, Y. Chen, and N. Yang, "Secrecy Outage on Transmit Antenna Selection/Maximal Ratio Combining in MIMO Cognitive Radio Networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10 236–10 242, Dec 2016.

[64] S. Chetry and A. Singh, "Physical Layer Security of Outdated CSI Based CRN," in *2018 9th Int. Conf. Comput., Commun. Networking Technol. (ICCCNT)*, Bangalore, India, July 2018, pp. 1–5.

[65] A. Singh, M. R. Bhatnagar, and R. K. Mallik, "Physical Layer Security of a Multiantenna-Based CR Network With Single and Multiple Primary Users," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 11 011–11 022, 2017.

[66] D. H. Tashman and W. Hamouda, "Physical-Layer Security for Cognitive Radio Networks over Cascaded Rayleigh Fading Channels," in *GLOBECOM 2020 - 2020 IEEE Global Commun. Conf.*, Taipei, Taiwan, 2020, pp. 1–6.

[67] D. H. Tashman and W. Hamouda, "Physical-Layer Security on Maximal Ratio Combining for SIMO Cognitive Radio Networks over Cascaded κ – μFading Channels," *IEEE Transactions on Cognitive Communications and Networking*, pp. 1–1, 2021.

[68] A. Singh, M. R. Bhatnagar, and R. K. Mallik, "Secrecy Outage Performance of SWIPT Cognitive Radio Network With Imperfect CSI," *IEEE Access*, vol. 8, pp. 3911–3919, 2020.

[69] P. M. Quang, T. T. Duy, and V. N. Quoc Bao, "Performance evaluation of underlay cognitive radio networks over Nakagami-m fading channels with energy harvesting," in *2016 Int. Conf. Adv. Technol. Commun. (ATC)*, 2016, pp. 108–113.

[70] R. Song, X. Tang, D. Wang, D. Zhai, W. Xu, and B. Li, "Joint Wireless Power and Information Transfer for Primary Secure Transmission," in *2019 11th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, 2019, pp. 1–5.

[71] J. Zhang, G. Pan, and H. Wang, "On physical-layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system," *IEEE Access*, vol. 4, pp. 3887–3893, 2016.

[72] Z. Wang, Z. Chen, B. Xia, L. Luo, and J. Zhou, "Cognitive Relay Networks With Energy Harvesting and Information Transfer: Design, Analysis, and Optimization," *IEEE Transactions on Wireless Communications*, vol. 15, no. 4, pp. 2562–2576, 2016.

[73] D. S. Gurjar, H. H. Nguyen, and H. D. Tuan, "Wireless Information and Power Transfer for IoT Applications in Overlay Cognitive Radio Networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3257–3270, 2019.

[74] K.-Y. Hsieh, F.-S. Tseng, M.-L. Ku, and C.-Y. Hsu, "Information and energy cooperation in overlay hierarchical cognitive radio networks," in *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2018, pp. 274–279.

[75] D. H. Tashman and W. Hamouda, "Secrecy Analysis for Energy Harvesting-Enabled Cognitive Radio Networks in Cascaded Fading Channels," in *ICC 2021 - IEEE Int. Conf. Commun.*, 2021, pp. 1–6.

[76] D. Tashman, W. A. Hamouda, and J. M. Moualeu, "On Securing Cognitive Radio Networks-Enabled SWIPT over Cascaded-Fading Channels with Multiple Eavesdroppers," *IEEE Transactions on Vehicular Technology*, pp. 1–1, 2021.

[77] J. M. Moualeu and W. Hamouda, "Secrecy performance analysis over mixed α-μ and κ-μ fading channels," in *2018 IEEE Wireless Commun. Networking Conf. (WCNC)*, Barcelona, Spain, 2018, pp. 1–6.

[78] H. Lei, C. Gao, I. S. Ansari, Y. Guo, G. Pan, and K. A. Qaraqe, "On Physical-Layer Security

Over SIMO Generalized-K Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 7780–7785, 2016.

[79] J. M. Moualeu, P. C. Sofotasios, D. B. da Costa, W. Hamouda, U. S. Dias, and S. Muhaidat, "Physical-Layer Security over Generalized SIMO Multipath Fading Channels," in *2019 Int. Conf. Adv. Commun. Technol. Networking (CommNet)*, Rabat, Morocco, 2019, pp. 1–6.

[80] J. M. Moualeu, D. B. da Costa, F. J. Lopez-Martinez, W. Hamouda, T. M. N. Nkouatchah, and U. S. Dias, "Transmit Antenna Selection in Secure MIMO Systems Over $\alpha - \mu$ Fading Channels," *IEEE Trans. Commun.*, vol. 67, no. 9, pp. 6483–6498, 2019.

[81] J. M. Moualeu, W. Hamouda, and F. Takawira, "Intercept Probability Analysis of Wireless Networks in the Presence of Eavesdropping Attack With Co-Channel Interference," *IEEE Access*, vol. 6, pp. 41 490–41 503, 2018.

[82] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*. Academic press, 2007.

[83] A. Prudnikov, Y. Brychkov, and O. Marichev, "Integrals series: More special functions, volume iii of integrals and series," *New York: Gordon and Breach Science Publishers*, 1990.

[84] J. Proakis and M. Salehi, *Digital Communications, 5th ed. New York*. McGraw-Hill, 2008.

[85] V. Adamchik and O. Marichev, "The algorithm for calculating integrals of hypergeometric type functions and its realization in REDUCE system," in *Proceedings of the international symposium on Symbolic and algebraic computation*. ACM, 1990, pp. 212–224.

[86] M. K. Simon and M.-S. Alouini, *Digital communication over fading channels*. John Wiley & Sons, 2005, vol. 95.

[87] A. M. Mathai, *A handbook of generalized special functions for statistical and physical sciences*. Oxford University Press, USA, 1993.

[88] C. D. Bodenschatz, "Finding an H-function distribution for the sum of independent H-function variates ," Ph.D. dissertation 1992.

[89] H. Chergui, M. Benjillali, and S. Saoudi, "Performance Analysis of Project-and-Forward Relaying in Mixed MIMO-Pinhole and Rayleigh Dual-Hop Channel," *IEEE Communications Letters*, vol. 20, no. 3, pp. 610–613, March 2016.

[90] K. Jiang, T. Jing, Y. Huo, F. Zhang, and Z. Li, "SIC-Based Secrecy Performance in Uplink NOMA Multi-Eavesdropper Wiretap Channels," *IEEE Access*, vol. 6, pp. 19 664–19 680, April 2018.

[91] S. Jia, J. Zhang, H. Zhao, and R. Zhang, "Relay Selection for Improved Security in Cognitive Relay Networks With Jamming," *IEEE Wireless Commun. Lett.*, vol. 6, no. 5, pp. 662–665, Oct. 2017.

[92] M. Milisic, M. Hamza, and M. Hadzialic, "Outage and symbol error probability performance of L-branch maximal-ratio combiner for generalized κ- μ fading," in *ELMAR, 2008. 50th International Symposium*, vol. 1. IEEE, 2008, pp. 231–236.

[93] J. Proakis and M. Salehi, "Digital Communications, (McGrawHill, New York, 2008)," *Google Scholar*.

[94] A. Singh, M. R. Bhatnagar, and R. K. Mallik, "Secrecy outage of a simultaneous wireless information and power transfer cognitive radio system," *IEEE Wireless Communications Letters*, vol. 5, no. 3, pp. 288–291, 2016.

[95] R. Su, Y. Wang, and R. Sun, "Destination-assisted jamming for physical-layer security in swipt cognitive radio systems," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, 2018, pp. 1–6.

[96] M. Haenggi, "On distances in uniformly random networks," *IEEE Transactions on Information Theory*, vol. 51, no. 10, pp. 3584–3586, 2005.

[97] B. Ji, Y. Li, S. Chen, C. Han, C. Li, and H. Wen, "Secrecy Outage Analysis of UAV Assisted Relay and Antenna Selection for Cognitive Network under Nakagami-m Channel," *IEEE Trans. Cognit. Commun. Networking*, pp. 1–1, 2020.

[98] N. A. Khalek and W. Hamouda, "From Cognitive to Intelligent Secondary Cooperative Networks for the Future Internet: Design, Advances, and Challenges," *IEEE Network*, pp. 1–8, 2020.

[99] H. Lei, H. Zhang, I. S. Ansari, Z. Ren, G. Pan, K. A. Qaraqe, and M. Alouini, "On Secrecy Outage of Relay Selection in Underlay Cognitive Radio Networks Over Nakagami-m Fading Channels," *IEEE Trans. Cognit. Commun. Networking*, vol. 3, no. 4, pp. 614–627, 2017.

[100] M. Bouabdellah, F. El Bouanani, and M. Alouini, "A PHY Layer Security Analysis of Uplink Cooperative Jamming-Based Underlay CRNs With Multi-Eavesdroppers," *IEEE Trans. Cognit. Commun. Networking*, vol. 6, no. 2, pp. 704–717, 2020.

[101] J. M. Moualeu, W. Hamouda, and F. Takawira, "Secrecy Performance of Generalized Selection Diversity Combining Scheme with Gaussian Errors," in *2018 IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Chicago, IL, USA, 2018, pp. 1–5.

[102] J. M. Moualeu and W. Hamouda, "Performance analysis of secure communications over α-μ/κ-μ fading channels," in *2017 12th Int. Conf. Comput. Eng. Syst. (ICCES)*, Cairo, Egypt, 2017, pp. 473–478.

[103] C. Jiang, Y. Chen, and K. J. R. Liu, "Data-Driven Optimal Throughput Analysis for Route Selection in Cognitive Vehicular Networks," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 11, pp. 2149–2162, 2014.

[104] A. Pandey, S. Yadav, D. T. Do, and R. Kharel, "Secrecy Performance of Cooperative Cognitive AF Relaying Networks With Direct Links Over Mixed Rayleigh and Double-Rayleigh Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15 095–15 112, 2020.

[105] H. Lu, Y. Chen, and N. Cao, "Accurate approximation to the PDF of the product of independent Rayleigh random variables," *IEEE Antennas and Wireless Propagation Letters*, vol. 10, pp. 1019–1022, 2011.

[106] T. D. Ponnimbaduge Perera, D. N. K. Jayakody, S. K. Sharma, S. Chatzinotas, and J. Li, "Simultaneous wireless information and power transfer (swipt): Recent advances and future challenges," *IEEE Communications Surveys Tutorials*, vol. 20, no. 1, pp. 264–302, 2018.

[107] J. Lee, "Full-Duplex Relay for Enhancing Physical Layer Security in Multi-Hop Relaying Systems," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 525–528, 2015.

[108] T. Riihonen, S. Werner, and R. Wichman, "Optimized gain control for single-frequency relaying with loop interference," *IEEE Trans. Wireless Commun.*, vol. 8, no. 6, pp. 2801–2806, 2009.

[109] J. Lee, "Self-Interference Cancelation Using Phase Rotation in Full-Duplex Wireless," *IEEE Trans. Veh. Technol.*, vol. 62, no. 9, pp. 4421–4429, 2013.

[110] C. Zhong, H. A. Suraweera, G. Zheng, I. Krikidis, and Z. Zhang, "Wireless Information and Power Transfer With Full Duplex Relaying," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3447–3461, 2014.

[111] R. Tan, Y. Gao, H. He, and Y. Cao, "Secrecy Performance of Cognitive Radio Sensor Networks with an Energy-Harvesting based Eavesdropper and Imperfect CSI," in *2018 Asian Hardware Oriented Secur. Trust Symp. (AsianHOST)*, 2018, pp. 80–85.

[112] Y. Zou, X. Wang, and W. Shen, "Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack," in *2013 IEEE Int. Conf. Commun. (ICC)*, 2013, pp. 2183–2187.

[113] A. A. Boulogeorgos, P. C. Sofotasios, B. Selim, S. Muhaidat, G. K. Karagiannidis, and M. Valkama, "Effects of RF Impairments in Communications Over Cascaded Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 11, pp. 8878–8894, 2016.

[114] X. Chen, L. Guo, X. Li, C. Dong, J. Lin, and P. T. Mathiopoulos, "Secrecy Rate Optimization for Cooperative Cognitive Radio Networks Aided by a Wireless Energy Harvesting Jammer," *IEEE Access*, vol. 6, pp. 34 127–34 134, 2018.

[115] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Comput. networks*, vol. 50, no. 13, pp. 2127–2159, 2006.

[116] M. Bouabdellah, F. E. Bouanani, P. C. Sofotasios, D. B. da Costa, K. Mezher, H. Benazza, S. Muhaidat, and G. K. Karagiannidis, "Physical Layer Security For Dual-hop SWIPT-Enabled CR Networks," in *2019 16th Int. Symp. Wireless Commun. Syst. (ISWCS)*, 2019, pp. 629–634.

[117] R. Duan, M. Elmusrati, R. Jantti, and R. Virrankoski, "Capacity for Spectrum Sharing Cognitive Radios with MRC Diversity at the Secondary Receiver under Asymmetric Fading," in *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, 2010, pp. 1–5.