Secrecy Outage Analysis of Cognitive NOMA System with Control-Jamming

M.Tech. Thesis

By
KAJAL YADAV
2002102004

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY INDORE
JUNE 2022

Secrecy Outage Analysis of Cognitive NOMA System with Control-Jamming

A THESIS

Submitted in partial fulfillment of the
requirements for the award of the degree
of
Master of Technology

By
KAJAL YADAV

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY INDORE
JUNE 2022

INDIAN INSTITUTE OF TECHNOLOGY INDORE

CANDIDATE'S DECLARATION

I hereby certify that the work which is being presented in the thesis entitled **Secrecy Outage Analysis of Cognitive NOMA System with Control-Jamming** in the partial fulfillment of the requirements for the award of the degree of **MASTER OF TECHNOLOGY** and submitted in the **DEPARTMENT OF ELECTRICAL ENGINEERING, Indian Institute of Technology Indore**, is an authentic record of my own work carried out during the time period from August 2020 to June 2022 under the supervision of Dr. Prabhat Kumar Upadhyay, Professor, Discipline of Electrical Engineering.

The matter presented in this thesis has not been submitted by me for the award of any other degree at this or any other institute.

Kajal Yadav

30-05-2022

Signature of the student with date

KAJAL YADAV

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

30-05-2022

Signature of the Supervisor of

M.Tech. thesis (with date)

Dr. PRABHAT KUMAR UPADHYAY

Ms. Kajal Yadav has successfully given her M.Tech. Oral Examination held on 06-June-2022.

Signature of Supervisor of M.Tech. thesis
Date: 6-6-2022

Convener, DPGC
Date:06/06/2022

Signature of PSPC Member #1
Date: 06/06/2022

Signature of PSPC Member #2
Date: 06-June-2022

ACKNOWLEDGEMENTS

I would like to thank my supervisor, Dr. Prabhat Kumar Upadhyay, Professor, Department of Electrical Engineering, IIT Indore, for his constant encouragement, support, and guidance throughout the project. His unique perspective on things and relentless pursuit of perfection have had a profound impact on me and have significantly transformed me. I consider myself extremely fortunate to be one of his master's students.

I would like to thank my PSPC members, Dr. Trapti Jain, Professor, Department of Electrical Engineering, IIT Indore, and Dr. Surya Prakash, Associate Professor, Department of Computer Science and Engineering, IIT Indore, for providing their crucial insights into the assessment of this work during the research.

I am grateful to Dr. Vipul Singh, Head of Department - Electrical Engineering, for providing all the technical and administrative assistance needed to complete the project successfully and efficiently.

I would like to express my heartfelt gratitude to the Ph.D. scholars Mr. Chandan Singh and Mr. Alok Kumar Shukla; without their support and belief in me, this would not have been possible.

I am grateful to my friends and classmates at IIT Indore for their encouragement and assistance.

I am thankful to IIT Indore for giving me such an experience of a lifetime.

Last but not least, I want to thank God and my parents for giving me opportunities.

DEDICATION

I would like to dedicate this work to my beloved mother and father and my family.

Abstract

Wireless communication has advanced significantly over the last couple of decades. The exponential boom of mobile traffic and high-rate data communication services can also bring about additional spectrum scarcity problems in fifth-generation technologies. That's why several novel technologies for fifth-generation (5G) and beyond wireless communication have been developed. Non-orthogonal multiple access (NOMA) and cognitive radio (CR) are two concepts that have been envisioned as promising candidates to improve spectrum efficiency.

NOMA is a different way of using multiplexing to share the spectrum among multiple users. It uses power domain multiplexing to allow different users to share a single resource block. NOMA outperforms traditional Orthogonal Multiple Access (OMA) in terms of spectrum efficiency, connectivity, latency, and fairness.

It is also known that CR, in which secondary users (SUs) intelligently change their operating settings to access the spectrum band occupied by primary users (PUs), in an opportunistic manner, makes more efficient use of the wireless spectrum. There are currently three main CR paradigms: 1) Interweave 2) Underlay; and 3) Overlay.

The combination of NOMA and CR is known as cognitive NOMA (CNOMA), and it has demonstrated the ability to meet the criteria for 5G and beyond networks.

Traditionally, the protection of information in wireless networks has been done through cryptography. However, this may not be viable in energy-limited systems since the encryption protocols require high computational capability. Physical layer security (PLS) is a promising and effective

solution for addressing the risk of information leakage in future wireless communication systems.

In our work, we proposed a Control-Jamming (CJ)-aided overlay cognitive NOMA system. Here we have used the Decode and Forward (DF) relaying technique. A mathematical expression has been derived for the secrecy outage probability (SOP) and the strictly positive secrecy capacity (SPSC) metrics. This expression is based on the Nakagami-*m* fading model. We found a closed-form expression for the asymptotic behavior of the SOP equation. This provides us with more insights. The derived performance measures were validated using Monte-Carlo simulations. The proposed system models' performance has also been evaluated in the scenario of jamming. Here, we have looked at the difference in performance between jamming and non-jamming cases. The jamming case performed better than the non-jamming case. It is clear from the results that the CJ is an efficient solution to ensure PLS. In order to make our proposed system model more realistic, we can use energy harvesting. Energy harvesting models are more efficient. Furthermore, future work on the CJ-aided CNOMA network with imperfect SIC and CSI conditions can be done, which will be useful for realistic implementations.

CONTENT

LIST OF PUBLICATIONS ---------- **XI**

LIST OF FIGURES ---------- **XIII**

NOMENCLATURE ---------- **XV**

ACRONYMS ---------- **XVII**

Chapter 1: Introduction ---------- **1**

1.1 Overview ---------- **1**

1.2 Evolution of Cellular Systems ---------- **1**

1.3 Characteristics and Applications of 5G ---------- **6**

1.4 Technologies in 5G ---------- **8**

1.5 Objective of Study ---------- **10**

1.6 Organization of the Thesis ---------- **11**

Chapter 2: Review of Past Work ---------- **13**

Chapter 3: Secrecy Outage Analysis of Cognitive NOMA System with Control-Jamming ---------- **17**

3.1 Introduction ---------- **17**

3.2 Organization of Chapter ---------- **17**

3.3 System Model ---------- **17**

3.4 Performance Analysis ---------- **22**

Chapter 4: Results and Discussion ---------- **29**

Chapter 5: Conclusions and Future Scope ---------- **33**

5.1 Conclusion ---------- **33**

5.2 Future Scope ---------- **33**

REFERENCES ---------- **35**

LIST OF PUBLICATIONS

[1] **K. Yadav**, P. K. Upadhyay, and J. M. Moualeu, "Secrecy Outage Analysis of Cognitive NOMA System with Control-Jamming," under preparation.

[2] A. K. Shukla, J. Sharanya, **K. Yadav**, and P. K. Upadhyay, “Exploiting SWIPT Enabled IoT-based Coordinated Direct and Relay Transmission with Non-Orthogonal Multiple Access,” Revised version to be submitted in *IEEE Sensors Journal*.

LIST OF FIGURES

1.1 Evolution of Technology from 1G to 5G 2

1.2 Basic diagram of NOMA 9

3.1 System Model 18

3.2 Transmission Block Structure for overlay cognitive NOMA system 19

4.1 SOP vs Δ_S (in dB) for non-jamming case 29

4.2 SOP vs Δ_S (in dB) for jamming case 30

4.3 SPSC vs Δ_S (in dB) for non-jamming case 31

4.4 SPSC vs Δ_S (in dB) for jamming case 31

4.5 SOP vs a_1 for both jamming and non-jamming case 32

NOMENCLATURE

$f_X(x) = Probability\ density\ function\ (PDF)\ of\ a\ random\ variable\ X.$

$F_X(x) = Cumulative\ distribution\ function\ (CDF)\ of\ a\ random\ variable\ X.$

$P_S = Transmit\ power\ of\ base\ station.$

$h_{ij} = Channel\ coefficient.$

$|h_{ij}|^2 = Channel\ gain.$

$m_{ij} = Fading\ parameter.$

$\Omega_{ij} = Average\ fading\ power.$

$y_i^j = Signal\ recived\ at\ i_{th}\ node\ in\ j_{th}\ trasmission\ phase.$

$P_R = Transmit\ power\ at\ relay.$

$x_s = Transmitted\ signal\ by\ the\ S.$

$n_R = AWGN\ variable.$

$\Delta_S = Transmit\ SNR\ for\ node\ S.$

$a_1, a_2 = Power\ allocation\ coeficients\ for\ x_S\ and\ x_R\ respectively.$

$\Delta_R = Transmit\ SNR\ at\ node\ R.$

$R_{th} = Threshold\ Rate.$

$C_D, C_Q = Secrecy\ capacity\ for\ users\ D\ and\ Q\ respectively.$

ACRONYMS

AF - Amplify and Forward

AMPS - Advanced Mobile Phone System technology

AWGN - Additive White Gaussian Noise

CDF - Cumulative Distribution Function

CDMA - Code-Division Multiple Access

CDRT - Coordinated Direct and Relay Transmission

CJ - Control-Jamming

CNOMA - Cognitive NOMA

CR - Cognitive Radio

CSI - Channel State Information

DF - Decode-and-Forward

EDGE - Enhanced Data rates for GSM Evolution

ESC - Ergodic Sum Capacity

FD - Full Duplex

FDMA - Frequency Division Multiple Access

GPRS - General Packet Radio Service

GPS - Global Positioning System

GSM - Global System for Mobile communication

HD - Half Duplex

IoT - Internet of Things

IT - Information Transmission

LTE - Long-Term Evolution

MMS - Multimedia Message

MRC - Maximum Ratio Combining

NOMA - Non-Orthogonal Multiple Access

OFDM - Orthogonal Frequency-Division Multiplexing

OMA - Orthogonal Multiple Access

OP - Outage Probability

PDA - Personal Digital Assistant

PDF - Probability Density Function

PIC - Parallel Interference Cancellation

PLS - Physical Layer Security

PR - Primary Receiver

PT - Primary Transmitter

QoS - Quality of Service

RF - Radio Frequency

RFID - Radio-Frequency Identification

SIC - Successive Interference Cancellation

SINR - Signal-to- Interference Plus-Noise Ratio

SNR - Signal-to-Noise Ratio

SOP - Secrecy Outage Probability

SPSC - Strictly Positive Secrecy Capacity

SR - Secondary Receiver

ST - Secondary Transmitter

TD-SCDMA - Time Division Synchronous Code Division Multiple Access

UMTS - Universal Mobile Telecommunication System.

VPN - Virtual Private Networks

WCDMA - Wideband Code Division Multiple Access

Wi-Fi - Wireless Fidelity

Wi-Max - Worldwide Interoperability for Microwave Access

WWWW - Wireless World Wide Web

Chapter 1: Introduction

1.1 Overview

Telecommunications and networking have been and will continue to be key technologies in humanity's and technology's growth. Since 1980, when the mobile cellular era began, mobile communications have undergone significant changes and expanded dramatically. Each generation has a unique set of norms, abilities, practices, and characteristics that distinguish it from the one before it. The first generation (1G) of mobile wireless communication networks were analogue and only used for voice calls. Users can send and receive text messages using the second generation (2G) of digital technology. Third-generation (3G) mobile technology offers increased data transmission speeds, more space for storage, and enhanced multimedia capabilities. The fourth-generation (4G) of wireless mobile internet allows for faster and more reliable connections than ever before. It also boosts bandwidth while saving money on resources. Fifth-generation (5G) cellular technology will herald a new era in the cellular market by revolutionizing the use of mobile phones by providing extremely high bandwidth. Users have never had access to technology with as many advanced features as they will with 5G. This technology is quickly becoming the most in-demand and valuable on the market [1].

1.2 Evolution of Cellular Systems

Since 1981, cellular wireless networks have evolved rapidly, with each new mobile generation appearing more advanced than the last. Let's have a look at the various stages of wireless communication technology evolution:

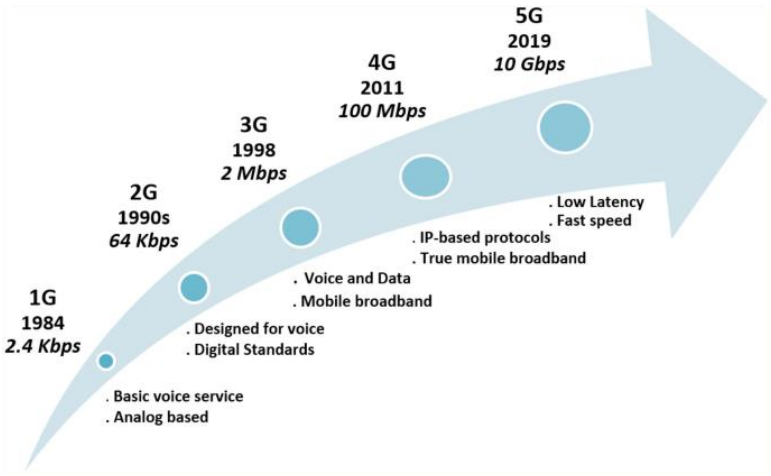

Figure 1.1: Evolution of technology from 1G to 5G [2].

1) **First Generation (1G):** NTT launched the first commercially automated 1G cellular network in Japan in 1979, and Bell Labs in the United States in 1984. 1G networks were designed for voice only and used analogue protocols with speeds of only 2.4 Kbps. 1G allowed for the use of multiple cell sites as well as the ability to transfer calls from one site to the next as the user moved between cells during a conversation. It was used for voice services and was based on AMPS. The AMPS system used FDMA and were frequency modulated with a channel capacity of 30 kHz and a frequency band of 824-894 MHz. Its basic characteristics are as follows:

- Provides data speed of 2.4 kbps.
- All of your calls will be connected in one country.
- Analogue switching.
- Voice quality is poor due to interference.
- Phone size is not convenient to carry.
- Security is a major concern.
- Very low spectrum efficiency.

Radio calls are easily overheard by third parties when they're replayed in radio towers. It has poor voice links, no security, and low capacity.

2) **Second Generation (2G):** The second generation of GSM phones, which first appeared in the late 1980s, is a well-known and highly reliable type of phone. It transmits voice using digital signals. This technology's primary focus was on digital signals, and it provides services for delivering text and picture messages at low speeds (in kbps). It has a frequency range of 30 to 200 kHz. In addition to 2G, 2.5G systems use packet-switched and circuit-switched domains and offer data rates of up to 144 kbps, such as GPRS, CDMA, and EDGE. The following are the primary characteristics of 2G:
   - Data transmission speed up to 64kbps.
   - Digital system.
   - Text messages and MMS service is possible.
   - Capacity and quality are enhanced.
   - Unable to deal with large amounts of data, such as videos.
   - To make mobile phones work, strong digital signals were required.
3) **Third Generation (3G):** 3G was introduced in 2000 and is based on GSM. The aim of this technology was to deliver fast data. Using packet switching, the original technology was improved to allow data rates of up to 14 Mbps and higher. It makes use of a Wide Band Wireless Network to improve clarity. It also provides data services, television/video access, and new services such as Global Roaming. It operates at 2100 MHz and has a bandwidth of 15-20 MHz, which is used for high-speed internet service and video chatting. The following are the primary characteristics of 3G:
   - Speed of 2 Mbps.
   - Known as smartphones.

- Data transfer rates have been increased to ensure that audio and video files can be handled smoothly.
- Email communication is possible.
- Enhanced security, video conferencing, and 3D gaming.
- High cost for 3G license services.
- Building infrastructure for 3G is difficult.
- High bandwidth required.
- Costly 3G phones.

In Europe, the 3G mobile system was known as UMTS, while the American 3G variant was known as CDMA2000. Also, the IMT2000 has accepted a new 3G standard from China, i.e., TD-SCDMA. WCDMA is the UMTS air interface technology.

4) **Fourth Generation (4G):** With 4G, you can experience blistering speeds when downloading files up to 100Mbps. 4G includes all of the features of 3G plus additional services such as Multi-Media Newspapers, enhanced TV viewing, and the ability to send data much more quickly than previous generations [3]. LTE is a type of 4G technology that is classified as being of high speed. 4G is a QoS and rate requirement set by future applications such as Wireless Broadband Access, Multimedia MMS, Video Chat, Mobile TV, HDTV Content, Digital Video Broadcasting (DVB), minimum services such as voice and data, and other bandwidth-intensive services. The following are the primary characteristics of 4G:

- Speeds ranging from 10Mbps to 1Gbps are possible.
- Streaming video of high quality.
- Combination of Wi-Fi and Wi-Max.
- More secure communication.
- Provides a wide variety of services at any time and from any location as needed by the user.
- Increased MMS.

- Low per-bit cost.
- Battery usage is increasing.
- Implementation is difficult.
- Expensive hardware is required.

5) **Fifth Generation (5G):** The Fifth Generation (also known as 5G) began in the late 2010s. 5G technology has the potential to significantly improve connectivity and coverage. The global WWWW will be the primary focus of 5G. It's a completely unrestricted wireless communication system. With 5G technology, mobile operating systems can handle unprecedented amounts of data and high-volume phone calls. The future of 5G technology is bright as it can handle cutting-edge technology and provide customers with invaluable handsets. Perhaps 5G technology will take over the global market in the coming days. The ability of 5G technologies to support software and consulting is remarkable. To provide high connectivity, the 5G network employs router and switch technology. 5G technology allows nodes within a building to connect to the internet via a combination of wired and wireless network connections. 5G technology will soon enable a mobile phone that works in a similar way to a PDA, and the entire office will be available to us. In the near future, in less than six seconds, we will be able to download a full-length HD movie, compared to the seven minutes it takes for 4G and more than an hour for 3G. Furthermore, video calls will be so realistic that we will feel as if we are talking to the person on the other side of the screen. 5G is a high-throughput, wide-coverage packet-switched wireless system. OFDM and millimeter wireless are used in 5G wireless, allowing for a data transmission rate of 20 Mb/s and a frequency range of 2-8 GHz.

   The uncertainty surrounding 5G is due to the fact that this is still largely a concept and that the wireless industry has not yet agreed

on a new network standard. However, there are important objectives that we hope to achieve through 5G:

- Fast data transfer speed: 4G networks can now achieve peak download speeds of 1 gigabit per second, but this is rarely achieved in practice. For 5G, this increases to 10 Gbps.
- Extremely low latency: The time it takes for one device to send a packet of data to another is called "latency". 4G has a delay of about 50ms, while 5G has a delay of about 1ms. This is of great importance for industries, and self-driving cars.
- A world that is more "connected": Over the next decade, IoT (connected cars, smart homes, etc.) is likely to explode, requiring networks that can support billions of connected devices. 5G provides users with the capacity and bandwidth they need.

While this technology is still far from being realized, it has the capability to absolutely extrude the manner in which we engage with Wi-Fi devices, from smartphones to vehicles we drive.

1.3 Characteristics and Applications of 5G

The following features are included in the current 5G technology trend:

- 5G technology provides connection speeds of up to 25 Mb/s.
- 5G technology provides mobile users with high resolution and two-way high bandwidth sharing.
- 5G technology enables large-scale data transfer at gigabit speeds and supports approximately 65,000 connections.
- With 5G technology, upload and download speeds have reached record highs.
- 5G generation additionally helps VPN.
- 5G terminals aid software programs that describe radio and modulation schemes.

- The improvement of 5G cellular networks is taken into consideration to be targeted on consumer devices. For example, the advanced billing interface of the 5G era makes it extra appealing and effective.
- 5G technology networks provide a wide range of improved connectivity around the world. The device has to be capable to accessing multiple wireless technologies of Wi-Fi technology on an equal time, and the tool have to be capable of integrate different flows from different technology.
- Vertical handover is impractical when there are multiple technologies, operators, and service providers and should be avoided.
- In 5G, every community is chargeable for managing consumer mobility, and end devices make the final selection among the numerous wireless / access points to network carriers for a selected service. This option is based on mobile phone open intelligent middleware.
- A great feature of 5G is remote diagnostics. This gives users a better, faster solution.

Applications for 5G are far beyond our imagination. Some of the 5G applications are:

- Logistics and Transportation: Efficient use of RFID tags, real-time GPS tracking and reporting, and efficient monitoring to minimize the risk of theft or misplacement of items.
- Smart Cities: Smart metropolis packages which include site visitors management, instant climate updates, nearby broadcasts, power management, clever grids, smart avenue lighting, water assets management, crowd management, and emergency response can leverage dependable 5G Wi-Fi networks to growth operability.

- Smart Farming: Farmers can track and effortlessly control the location of their herd by using smart RFID sensors and GPS technology. For irrigation control, and power management, they can use smart sensors.
- Healthcare and mission-vital applications: 5G era enables physicians to carry out superior medical file methods through the use of dependable wireless networks related to the opposite side of the world. People with persistent infections will benifit from clever gadgets and real-time monitoring. Smart scientific gadgets, which include wearables, constantly screen the patient's situation and set off alarms in an emergency. Hospitals and paramedics can be notified in crisis situations and take the necessary steps to facilitate diagnosis and treatment.
- Self-driving: With 5G wireless networks, self-driving cars are no longer far from reality. High-performance, low-latency wireless network connectivity is important for autonomous driving.

1.4 Technologies in 5G

Engineers took a fundamentally different approach to wireless network design to meet the demanding requirements laid out in the international specification for 5G. A number of key technologies (including Massive MIMO and Beamforming), as well as the use of OFDM, a highly spectral-efficient modulation technique, and the mm-Wave spectrum, contribute to the improved performance of 5G New Radio.

1. Massive MIMO: MIMO (multiple-input, multiple-output) is a radio access technology. It uses multiple antennas at the transmitter and also at the receiver to improve the radio link's quality, throughput, and capacity. MIMO employs spatial

diversity and spatial multiplexing techniques to send separate and independently encoded data signals, referred to as "streams," over the same time period and frequency resource.

Many modern wireless and RF technologies, such as Wi-Fi and LTE, use MIMO.

In order to deliver the required data rates and support the high number of connections, 5G networks will rely heavily on network densification as they roll out, especially in urban areas. Massive MIMO combined with beamforming technology allows for highly targeted use of spectrum, eliminating current performance bottlenecks, supporting a larger number of users in the cell, and improving the end-user experience in densely populated areas.

2. NOMA: Users are multiplexed in the power domain in non-orthogonal multiplexing. Using SIC, at the transmitter, different users are superimposed and separated at the receiver. In several ways, NOMA outperforms traditional OMA.

   It increases the number of users that can be served at the same time, allowing for massive connectivity.

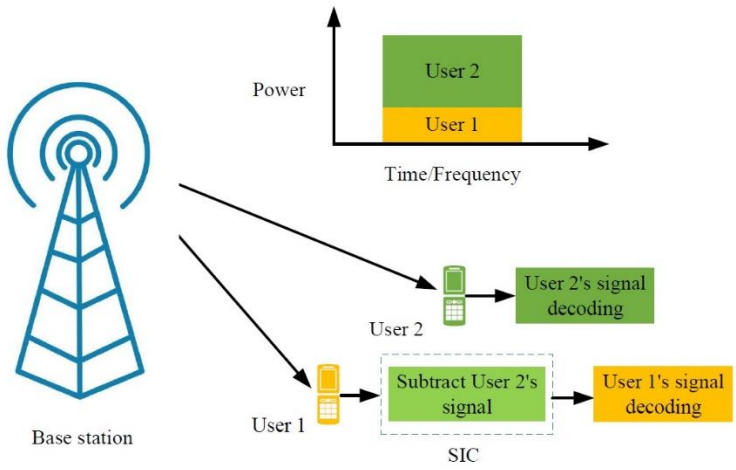

Figure 1.2: Basic diagram of NOMA [27].

Due to simultaneous transmission, a user does not need to go through a scheduled time slot to transmit their data, resulting in lower latency.

NOMA can maintain user fairness and a diverse range of service quality by balancing power between strong and weak users.

NOMA provides higher cell-edge throughput and thus improves the cell-edge user experience by allocating more power to a weak user.

3. Millimeter-wave (mm-wave) technology: The term mm-Wave refers to a portion of the RF spectrum with a very short wavelength that lies between 24GHz and 100GHz. Because this part of the spectrum is largely untapped, the goal of mm-wave technology is to significantly increase the available bandwidth. 5G mm-Wave is a ground-breaking cellular technology that allows users to access massive bandwidth.

   Another advantage of this short wavelength is that, despite the shorter transmission distance, it can transfer data even faster.

   It can be a critical component of 5G for powering data in sports stadiums, shopping complexes, or other places where data congestion is an issue.

1.5 Objective of Study

Our main goal is to investigate the NOMA system's secrecy performance in the presence of an eavesdropper. To our best knowledge, there have been few works regarding performance analysis of PLS in jammer aided CNOMA systems. The major contributions are as follows:

- We proposed a CJ-aided overlay cognitive NOMA system where the primary receiver (D) adopts MRC to combine the information from the primary transmitter (S) and relay (R).
- First, we obtain the SNR for each user. Then, closed-form expressions for the SOP are derived. MRC introduces difficulties in deriving the SOP.
- Based on the derived SOP expressions for the system for both non-jamming and jamming cases considering Nakagami-*m* fading, we showcase that, using a jammer to confuse the eavesdropper helps in improving the SOP of the system.
- To get further insight, we also derived asymptotic SOP expression at high SNR regime and SPSC expression for this system model.
- Finally, analytical results are corroborated by Monte-Carlo simulation results, and it shows the superiority of employing jamming approaches over without jamming approaches.

1.6 Organization of the Thesis

A chapter-wise breakup of the present work is as follows:

Chapter 1 provides an overview of wireless communication networks and their evolution over the last few decades. Some basic features of 5G, its applications, and some radio access technologies of 5G are also described.

Chapter 2 deals with the literature review and past work that has been done on NOMA, CR, and PLS. It mentions the novel contribution of the authors in the past to predict the types of challenges in 5G communication.

Chapter 3 describes the system model for the CJ-aided overlay cognitive NOMA system using DF relaying technique. Further, the

performance analysis of the CJ-aided overlay cognitive NOMA system is carried out with perfect SIC.

Chapter 4 gives the numerical and simulation outcomes to investigate the effect of the jammer on the secrecy and overall performance of the NOMA system.

Chapter 5 concludes and summarizes the research work and, comprehensive discussions based on the results obtained are presented. This chapter also discusses the scope of future work.

Chapter 2: Review of Past Work

Two promising technologies in 5G wireless networks are NOMA and CR. NOMA is a different way of using multiplexing to share the spectrum among multiple users. It uses power domain multiplexing to allow different users to share a single resource block. NOMA outperforms traditional OMA [3]. CR is a promising solution to tackle spectrum scarcity problem. In CR, secondary user (SU) can also exist at the same frequency band with licensed primary users (PUs) [4]. The integration of NOMA with CR can be termed as Cognitive-NOMA (CNOMA) [5], [6].

Innumerable CNOMA-based studies have been conducted because they provide more efficient spectrum utilization. Low latency, massive connectivity, and high throughput are the advantages of the intelligent spectrum sharing of CNOMA [7]. The authors in [8], studied CR inspired NOMA model. In this, they have analyzed the performance of fixed-power-allocation NOMA (F-NOMA) and cognitive-radio-inspired NOMA (CR-NOMA). PU is the weak user who experiences poor channel conditions and has a higher priority, while SU experiences good channel conditions and has a lower priority, and target reception quality for PU is guaranteed. NOMA signal is sent by the transmitter to the PU and SU.

In [9], the authors incorporated the underlay cognitive NOMA system with two users, in which an FD relay transmits information to the far user, and at the same time, the base station (BS) transmits information to the near user. The authors in [10], investigated an overlay cognitive NOMA system. Here, ST works as a relay and helps in forwarding the PR's and the SR's signals using the NOMA principle. First, the PT will send its signal to PR and ST and in the second phase, ST will help in transmitting the primary and secondary messages simultaneously.

The authors of [11] proposed a two-user cooperative NOMA-FD system in which a dedicated FD relay supports information transmission to the user having poor channel conditions. Under the realistic assumption of imperfect SIC, the achievable OP of both users and ESC are investigated, and exact analytical expressions are derived.

The authors of [12] introduced NOMA in CDRT, in which a base station (BS) communicates directly with user 1 while only communicating with user 2 through a relay. Both outage probability and ergodic sum capacity have analytical expressions. When compared to NOMA in non-coordinated direct and relay transmission (nCDRT), the proposed NOMA in CDRT provides a significant performance boost.

If we share the single time-frequency resource block with multiple users, it can impose a secrecy challenge. Because of the broadcasting nature of wireless communication, secrecy issues have continuously grown over the years, making secure communication in the existence of eavesdroppers a challenge. Conventional encryption methods employ cryptographic algorithms to achieve communication authentication and security [13]–[15]. These traditional security approaches are not efficient enough to be employed in 5G networks because they require high computational capability, and these approaches are not energy efficient. The cryptographic approach provides binary-level security. To improve overall security strength in 5G networks, a promising solution is PLS technique [16], [17]. PLS uses the inherent characteristics of wireless channels such as noise, fading, etc. to guarantee message confidentiality at the receiver. That's why the implementation of PLS in NOMA networks has drawn more attention in recent years [18]. In [19], the authors have investigated the basic principle of PLS and introduced some existing PLS techniques. After that, the unique features of IoT are explained. After that, they presented a comprehensive review of challenges faced by the PLS protocol in IoT. Then, three PLS solutions are proposed, which can be

implemented with IoT soon. To minimize the SOP of a cooperative relay network, different jamming selection techniques and relay optimization techniques are investigated in [20], [21]. Authors in [22] have investigated PLS for NOMA systems, by using AF and DF relaying protocols. Moreover, the authors in [23], investigated PLS for a NOMA-based downlink hybrid satellite-terrestrial relay network by using AF relaying technique in the presence of an eavesdropper. For the satellite link, Shadowed-Rician fading is adopted, and Nakagami-m fading is adopted for terrestrial links. By deriving closed-form expressions for SOP and SPSC, authors have investigated secrecy performance. Jammer-aided cooperative NOMA system is investigated in [24]. One relay is used as a jammer. Max-min relay selection and random relay selection strategies are considered. SOP performance is analyzed for both the relay selection strategies.

Chapter 3: Secrecy Outage Analysis of Cognitive NOMA System with Control-Jamming

3.1 Introduction

The overlay cognitive NOMA system model is described in this chapter. A NOMA system model with control-jamming and DF Relay Networks was proposed. We used one base station, one relay, two users, one eavesdropper, and one jammer in the proposed system model. Furthermore, we assume that all receiver nodes are aware of the complete CSI of all links. The signal from the base station and the relay is received in two phases by the receiver nodes. At receiver nodes, diversity combining will be used. Switched combining, selection combining, maximum-ratio combining, and equal-gain combining are examples of diversity combining techniques. We used the maximum-ratio combining diversity technique in our research. The performance of the system is analyzed by deriving the secrecy outage probability, and Strictly Positive Secrecy Capacity over Nakagami-*m* fading channels.

3.2 Organization of Chapter

The remaining chapter is organized as follows: In Section 3.3, the system model and the end-to-end SINRs are shown for the Cognitive NOMA system. Section 3.4 gives closed-form expressions for both users' SOP and SPSC over Nakagami-*m* fading channels.

3.3 System Model

In this section, we provided a full description of the system model and afterward, derived end-to-end SINR for jamming and non-jamming cases.

We considered an overlay cognitive NOMA system with one primary transmitter (PT) S, one primary receiver (PR) D, one secondary transmitter (ST) R, one secondary receiver (SR) Q, one eavesdropper (E), and one jamming node (J), as shown in Fig. 1. ST is working as a relay. The jamming node sends out an interference signal in order to reduce the SINR of the eavesdropper link. We assumed that all these nodes were operating in HD mode. Because the direct link is missing from S to E, the eavesdropper attempts to intercept the information transmitted by the relay. There is a direct link between S and D, which is considered to improve performance at D. The relay node employs DF relaying to send the detected symbols to two NOMA users, D and Q. It is assumed that all channels will experience Nakagami-m fading.

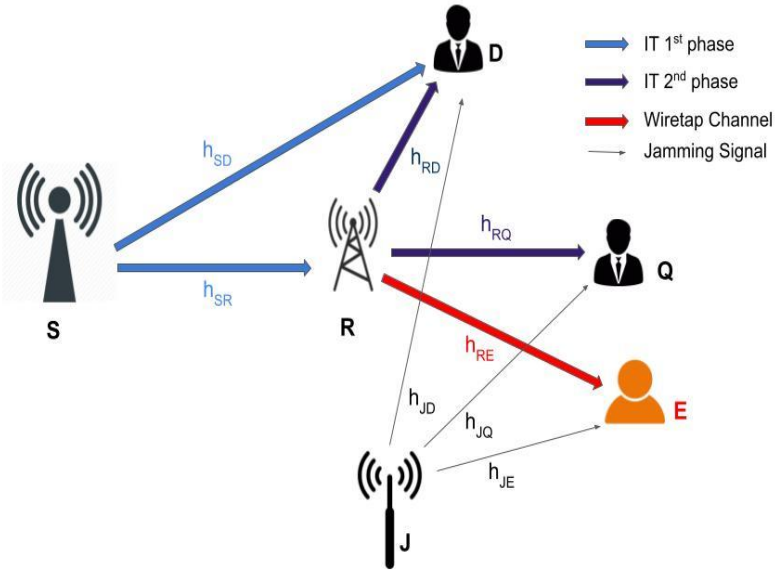

Figure 3.1: System model.

We denote the channel coefficient by h_{ij} where $i \in \{S, R, J\}, j \in \{R, D, Q, E\}$ with $i \neq j$. The channel gain $|h_{ij}|^2$ follows the gamma distribution with parameters m and Ω. Zero mean additive white

Gaussian noise (AWGN) with N_0 variance is assumed for all channels. Assume that the entire communication time slot is normalized to be unity. In the first half-time duration, transmission from S to D and S to R will take place. Next, the information transmission (IT) process from R to D and R to Q is conducted in the remaining half-time duration T/2 along with jamming from J to E.

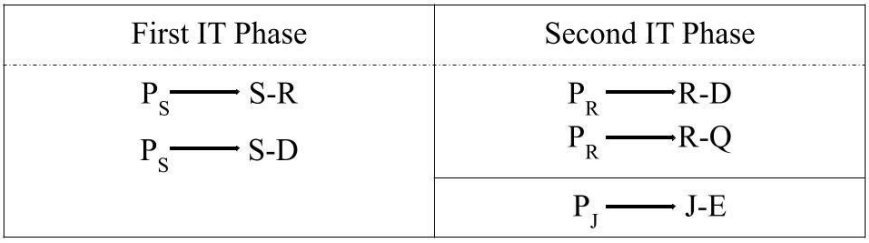

Figure 3.2: Transmission block structure for overlay CNOMA system.

3.4.1 Channel Model: The cumulative distribution function (CDF) and probability density function (PDF) of a random variable X are denoted by $F_X(.)$ and $f_X(.)$. For $i \in \{S, R, J\}$ and $j \in \{R, D, Q, E\}$ with $i \neq j$, the respective PDF and CDF of $|h_{ij}|^2$ with the fading severity m_{ij} and average power Ω_{ij} can be given as

$$f_{|h_{ij}|^2}(x) = \left(\frac{m_{ij}}{\Omega_{ij}}\right)^{m_{ij}} \frac{x^{m_{ij}-1}}{\Gamma(m_{ij})} e^{-\frac{m_{ij}}{\Omega_{ij}}x}, \quad (1)$$

$$F_{|h_{ij}|^2}(x) = \frac{1}{\Gamma(m_{ij})} \Upsilon\left(m_{ij}, \frac{m_{ij}}{\Omega_{ij}}x\right). \quad (2)$$

3.4.2 First IT phase (t_1): In the first IT phase, signal received at R and D is given by

$$y_R = h_{SR}\sqrt{P_S}x_S + n_R, \quad (3)$$

$$y_D^{t_1} = h_{SD}\sqrt{P_S}x_S + n_D^{t_1}, \quad (4)$$

where x_S is the transmitted signal by the S, n_R and $n_D^{t_1}$ are AWGN variables, and $\mathbb{E}[|x_S|^2] = 1, \mathbb{E}[.]$ represents the expectation distribution, P_S is the average transmit power of S.

Therefore, received SNR at R for decoding x_S is given by

$$\gamma_R = \Delta_S |h_{SR}|^2, \tag{5}$$

and through direct link, SNR at D for detecting x_S is given by

$$\gamma_D^{t_1} = \Delta_S |h_{SD}|^2, \tag{6}$$

where $\Delta_S \triangleq \frac{P_S}{N_0}$ represents transmit SNR for node S.

3.4.3 Second IT phase (t_2): R will use the DF strategy in the second IT phase. In this relaying strategy, first node R will attempt to decode the primary signal x_S. Then, it will combine its own signal x_R with signal x_S to form a superimposed signal $r(t)$ after successfully decoding signal x_S. In specific, the ST transmits

$$r(t) = \sqrt{P_R a_1} x_S + \sqrt{P_R a_2} x_R, \tag{7}$$

where a_1 and a_2 are power allocation coefficients for x_S and x_R respectively, where $a_1 + a_2 = 1$ and $a_1 \geq a_2$, transmission power at relay R is P_R and we assume $P_R = P_S$.

Received signal at D and Q in second IT phase are given by

$$y_D^{t_2} = h_{RD}(\sqrt{P_R a_1} x_S + \sqrt{P_R a_2} x_R) + n_D^{t_2}, \tag{8}$$

$$y_Q^{t_2} = h_{RQ}(\sqrt{P_R a_1} x_S + \sqrt{P_R a_2} x_R) + n_Q^{t_2}, \tag{9}$$

where $n_D^{t_2}$ and $n_Q^{t_2}$ are AWGN variables at D and Q, respectively.

From the received signal at D, it will directly decode x_S, because more power is allocated to x_S. So the SINR corresponding to the decoding of x_S at D is given by

$$\gamma_D^{t_2} = \frac{\Delta_R |h_{RD}|^2 a_1}{\Delta_R |h_{RD}|^2 a_2 + 1}, \tag{10}$$

with $\Delta_R = \frac{P_R}{N_0}$ representing the transmit SNR at node R. At D, the signals from the relaying and direct links are combined using MRC. So, the received SINR at D is given by

$$\gamma_D = \Delta_S |h_{SD}|^2 + \frac{\Delta_R |h_{RD}|^2 a_1}{\Delta_R |h_{RD}|^2 a_2 + 1}. \quad (11)$$

From the received signal $y_Q^{t_2}$, Q will first decode x_S and then apply SIC to decode x_R. x_S must be subtracted from $y_Q^{t_2}$ before the decoding of x_R is carried out.

Therefore, the SINR corresponding to the decoding of x_S at Q is given by

$$\gamma_Q^S = \frac{\Delta_R |h_{RQ}|^2 a_1}{\Delta_R |h_{RQ}|^2 a_2 + 1}. \quad (12)$$

At Q, we've assumed that perfect SIC is used. The SINR at Q to detect its message x_R is given by

$$\gamma_Q^R = \Delta_R |h_{RQ}|^2 a_2. \quad (13)$$

We used the worst-case scenario in which E has multiuser detection capability, as we did in [22]. Parallel interference cancellation (PIC) will be used by Eavesdropper to distinguish the superimposed mixture of signals.

a) Non-jamming case: In this case, the eavesdropper tries to wiretap the data from the R. The received signal at E is given by

$$y_{RE} = h_{RE}\left(\sqrt{P_R a_1} x_S + \sqrt{P_R a_2} x_R\right) + n_E. \quad (14)$$

As a result, received SINRs at E for detecting user D and Q's message symbols can be given as

$$\gamma_E^S = \Delta_R |h_{RE}|^2 a_1, \quad (15)$$

$$\gamma_E^R = \Delta_R |h_{RE}|^2 a_2. \quad (16)$$

b) Jamming case: The eavesdropper attempts to wiretap the data from the R in this case as well. The jammer, on the other hand, sends out an intentional interference signal to confuse the eavesdropper. The signal received at E is given by

$$y_E = y_{RE} + y_{JE}, \tag{17}$$

$$y_E = h_{RE}\left(\sqrt{P_R a_1}x_S + \sqrt{P_R a_2}x_R\right) + n_E + h_{JE}\sqrt{P_J}x + n_E, \tag{18}$$

where P_J is the transmit power of jamming node and x is the jamming signal. The received SINRs at E for detecting user D and Q's message symbols can be written as

$$\gamma_{EJ}^{S} = \frac{\Delta_R|h_{RE}|^2 a_1}{\Delta_J|h_{JE}|^2+2}, \tag{19}$$

$$\gamma_{EJ}^{R} = \frac{\Delta_R|h_{RE}|^2 a_2}{\Delta_J|h_{JE}|^2+2}, \tag{20}$$

where $\Delta_J \triangleq \frac{P_J}{N_0}$ represents the transmit SNR at node J.

3.4 Performance Analysis

3.4.1 Capacity: The channel capacity, *C*, is the maximum rate at which information can be transmitted through a channel. The Shannon–Hartley theorem applies the channel capacity concept to an AWGN channel with B Hz bandwidth and signal-to-noise ratio $\frac{S}{N}$.

$$C = B\ \log_2\left(1 + \frac{S}{N}\right) \text{ bits per second.} \tag{21}$$

The rates of x_S and x_R over legitimate channels as R uses the DF protocol are given by

$$C_S = \frac{1}{2}\log_2(1 + \min\{\gamma_R, \gamma_D\}), \tag{22}$$

$$C_R = \frac{1}{2}\log_2(1 + \gamma_Q^R). \tag{23}$$

Meanwhile, the rates of x_S and x_R over eavesdropping channel are

1. Non-Jamming Case:

$$C_{E-i} = \frac{1}{2}\log_2(1 + \gamma_E^i). \tag{24}$$

2. Jamming Case:

$$C_{E-i}^{J} = \frac{1}{2}\log_2(1 + \gamma_{EJ}^i), \tag{25}$$

so,

$$C_E = \{C_{E-i}, C_{E-i}^{J}\}, \tag{26}$$

where $i \in \{S, R\}$. It should be noted that difference of the capacity between the main link channel and the wiretap link channel is known as secrecy capacity, which must be non-negative [25]. As a result, the secrecy capacity for users D and Q can be given as

$$C_D = [C_S - C_E]^+, \tag{27}$$

$$C_Q = [C_R - C_E]^+, \tag{28}$$

where $[x]^+ = \max\{0, x\}$.

3.4.2 Secrecy Outage Probability (SOP): This section examines the secrecy performance for eavesdropping D and Q signals. In addition, we provide analysis for the asymptotic SOP. SOP occurs when a user's secrecy capacity is less than a predefined threshold R_{th}. Superimposed signals are transmitted to users in NOMA based networks. As a result, an outage occurs when any user fails to meet the threshold rate. As a result, the mathematical expression for SOP is as follows

$$P_{out}^{SOP} = Pr\left[C_D < R_{th}, C_Q < R_{th}\right]. \tag{29}$$

3.4.2.1 Non-Jamming Case: From equation (22), (23), (24), (27) and (28), SOP expression can be formulated as

$$P_{out}^{SOP} = 1 - \Pr\left[\frac{1 + \min\{\gamma_R, \gamma_D\}}{1 + \gamma_E^S} > C_{th}, \frac{1 + \gamma_Q^R}{1 + \gamma_E^R} > C_{th}\right],$$

$$= 1 - P_1, \tag{30}$$

where $C_{th} = 2^{2R_{th}}$. A closed form expression for (30) is still difficult to find. Therefore, we consider the following upper bound $\gamma_D < \Delta_S |h_{SD}|^2 + \frac{a_1}{a_2}$ for high SNR regime. Therefore, obtained upper bound for P_1 is given as

$$P_1 < \Pr\left[\gamma_R > \alpha, \gamma_D > \alpha, \gamma_Q^R > \beta\right], \tag{31}$$

where $\alpha = (C_{th} - 1) + C_{th}\gamma_E^S$ and $\beta = (C_{th} - 1) + C_{th}\gamma_E^R$. On further simplification, P_1 is given by

$$P_1 < \Pr\left[\begin{matrix}|h_{RQ}|^2 > A|h_{RE}|^2 + B, |h_{SR}|^2 > C|h_{RE}|^2 + D, \\ |h_{SD}|^2 > E|h_{RE}|^2 + F\end{matrix}\right], \quad (32)$$

where $A = C_{th}, B = \frac{C_{th}-1}{\Delta_R a_2}, C = \frac{C_{th}a_1\Delta_R}{\Delta_S}, D = \frac{C_{th}-1}{\Delta_S}, E = \frac{C_{th}a_1\Delta_R}{\Delta_S}$ and $F = \frac{C_{th}-1-\frac{a_1}{a_2}}{\Delta_S}$.

Therefore,

$$P_1 < \int_0^{\infty} \left[1 - F_{|h_{RQ}|^2}(Ax + B)\right]\left[1 - F_{|h_{SR}|^2}(Cx + D)\right] \left[1 - F_{|h_{SD}|^2}(Ex + F)\right] f_{|h_{RE}|^2}(x)\, dx. \quad (33)$$

By using (2) and with the aid of [26, Eq. (3.351.1)] into (33), we get

$$1 - F_{|h_{SR}|^2}(Cx + D) = e^{-\frac{m_{SR}}{\Omega_{SR}}(Cx+D)} \sum_{k=0}^{m_{SR}-1} \left(\frac{m_{SR}}{\Omega_{SR}}\right)^k \frac{1}{k!}(Cx + D)^k. \quad (34)$$

Using the same approach as in (34), the final expression of P_1 can be obtained as

$$P_1 < k_1 k_2 k_3 \frac{1}{\Gamma(m_{RE})}\left(\frac{m_{RE}}{\Omega_{RE}}\right)^{m_{RE}} (\delta - 1)! \left(\frac{m_{RE}}{\Omega_{RE}} + H_1\right)^{-\delta}, \quad (35)$$

where $\delta = i + j + n + m_{RE}$, k_1, k_2 and k_3 are given respectively by

$$k_1 = e^{-\frac{m_{SR}}{\Omega_{SR}}(D)} \sum_{k=0}^{m_{SR}-1} \left(\frac{m_{SR}}{\Omega_{SR}}\right)^k \frac{1}{k!} \sum_{i=0}^{k} \binom{k}{i} D^{k-i} C^i, \quad (36)$$

$$k_2 = e^{-\frac{m_{SD}}{\Omega_{SD}}(F)} \sum_{l=0}^{m_{SD}-1} \left(\frac{m_{SD}}{\Omega_{SD}}\right)^l \frac{1}{l!} \sum_{j=0}^{l} \binom{l}{j} F^{l-j} E^j, \quad (37)$$

$$k_3 = e^{-\frac{m_{RQ}}{\Omega_{RQ}}(B)} \sum_{M=0}^{m_{RQ}-1} \left(\frac{m_{RQ}}{\Omega_{RQ}}\right)^l \frac{1}{M!} \sum_{n=0}^{M} \binom{M}{n} B^{M-n} A^n, \quad (38)$$

and $H_1 = C\frac{m_{SR}}{\Omega_{SR}} + E\frac{m_{SD}}{\Omega_{SD}} + A\frac{m_{RQ}}{\Omega_{RQ}}$.

Finally, the SOP expression of the proposed system is obtained by substituting (35) in (30).

3.4.2.2 Jamming Case: By using equation (19), (20) in (25) and by utilizing (27) and (28), SOP expression can be formulated as

$$P_{out,J}^{SOP} = 1 - \Pr\left[\frac{1+\min\{\gamma_R,\gamma_D\}}{1+\gamma_{EJ}^{S}} > C_{th}, \frac{1+\gamma_Q^R}{1+\gamma_{EJ}^{R}} > C_{th}\right],$$

$$= 1 - P_2. \tag{39}$$

Here, we adopt the following upper bound $\gamma_D < \Delta_S|h_{SD}|^2 + \frac{a_1}{a_2}$, $\gamma_{EJ}^{S} < a_1$ and $\gamma_{EJ}^{R} < a_2$. Therefore, obtained upper bound for P_2 is given by

$$P_2 < \Pr\left[\gamma_R > \alpha_J, \gamma_D > \alpha_J, \gamma_Q^R > \beta_J\right], \tag{40}$$

where $\alpha_J = (C_{th} - 1) + C_{th}\gamma_{EJ}^{S}$ and $\beta_J = (C_{th} - 1) + C_{th}\gamma_{EJ}^{R}$. Note that the variables $\gamma_R, \gamma_D \; and \; \gamma_Q^R$, in (40), are not correlated, so on further simplification, P_2 is given by

$$P_2 < \Pr[|h_{SD}|^2 > a]\; Pr[|h_{SR}|^2 > b]\; Pr\left[|h_{RQ}|^2 > c\right], \tag{41}$$

$$P_2 < P_{21}P_{22}P_{23}, \tag{42}$$

where $a = \frac{\alpha_J - \frac{a_1}{a_2}}{\Delta_S}, b = \frac{\alpha_J}{\Delta_S} \; and \; c = \frac{\beta_J}{\Delta_R a_2}$. We start by deriving an analytical expression for P_{21} which can be rewritten as

$$P_{21} = Pr[|h_{SD}|^2 > a], \tag{43}$$

$$= \int_a^{\infty} \frac{1}{\Gamma(m_{SD})} \left(\frac{m_{SD}}{\Omega_{SD}}\right)^{m_{SD}} x^{m_{SD}-1} e^{-\frac{m_{SD}}{\Omega_{SD}}x} dx. \tag{44}$$

With the aid of [26, Eq. (3.351.1)], we get

$$P_{21} = e^{-\frac{m_{SD}}{\Omega_{SD}}a} \sum_{k=0}^{m_{SD}-1} \left(\frac{m_{SD}}{\Omega_{SD}}\right)^k \frac{1}{k!} a^k. \tag{45}$$

Similarly, $P_{22} \; and \; P_{23}$ are given respectively by

$$P_{22} = e^{-\frac{m_{SR}}{\Omega_{SR}}b} \sum_{k=0}^{m_{SR}-1} \left(\frac{m_{SR}}{\Omega_{SR}}\right)^k \frac{1}{k!} b^k\,, \tag{46}$$

$$P_{23} = e^{-\frac{m_{RQ}}{\Omega_{RQ}}c} \sum_{k=0}^{m_{RQ}-1} \left(\frac{m_{RQ}}{\Omega_{RQ}}\right)^k \frac{1}{k!} c^k. \tag{47}$$

Finally, the analytical expression of the SOP for the proposed system with jamming can be obtained by plugging (45)–(47) into (42) and then into (39).

3.4.3 Strictly Positive Secrecy Capacity (SPSC) Analysis: The SPSC is defined as the probability that the secrecy capacity is positive. To learn more about the existence of secrecy, the SPSC expression is obtained. The SPSC expression can be given by

$$SPSC = 1 - SOP|_{R_{th}=0},$$
$$= Pr\left[C_D > 0, C_Q > 0\right]. \quad (48)$$

3.4.3.1 Non-Jamming Case: In this scenario, the SPSC is obtained by

$$SPSC_{WJ} = Pr\left[\gamma_R > \gamma_E^S, \gamma_D > \gamma_E^S, \gamma_Q^R > \gamma_E^R\right],$$
$$= \int_0^\infty \left[1 - F_{|h_{RQ}|^2}(x)\right]\left[1 - F_{|h_{SR}|^2}(Tx)\right]$$
$$\left[1 - F_{|h_{SD}|^2}(Ux - V)\right] f_{|h_{RE}|^2}(x)\, dx. \quad (49)$$

By using (2) and with the aid of [26, Eq. (3.351.1)] into (49), we get

$$SPSC_{WJ} = \frac{k_1 k_2 k_3}{\Gamma(m_{RE})}\left(\frac{m_{RE}}{\Omega_{RE}}\right)^{m_{RE}} (\vartheta - 1)! \left(\frac{m_{RE}}{\Omega_{RE}} + H_2\right)^{-\vartheta}, \quad (50)$$

where $\vartheta = k + j + M + m_{RE}$, $T = \frac{\Delta_R a_1}{\Delta_S}, U = \frac{\Delta_R a_1}{\Delta_S}, V = \frac{a_1}{a_2 \Delta_S}$, and k_1, k_2 and k_3 are given by

$$k_1 = \sum_{k=0}^{m_{SR}-1} \left(\frac{m_{SR}}{\Omega_{SR}}\right)^k \frac{1}{k!} T^k, \quad (51)$$

$$k_2 = e^{\frac{m_{SD}}{\Omega_{SD}} V} \sum_{l=0}^{m_{SD}-1} \left(\frac{m_{SD}}{\Omega_{SD}}\right)^l \frac{1}{l!} \sum_{j=0}^{l} \binom{l}{j} (-V)^{l-j}\, U^j, \quad (52)$$

$$k_3 = \sum_{M=0}^{m_{RQ}-1} \left(\frac{m_{RQ}}{\Omega_{RQ}}\right)^M \frac{1}{M!}, \quad (53)$$

and $H_2 = T\frac{m_{SR}}{\Omega_{SR}} + U\frac{m_{SD}}{\Omega_{SD}} + \frac{m_{RQ}}{\Omega_{RQ}}$. It should be noted that the R→E link parameters dominate the proposed system's secrecy performance for non-jamming case.

3.4.3.2 Jamming Case: In the presence of a jammer, the analytical expression of the SPSC is given by

$$SPSC_J = Pr\left[\gamma_R > a_1, \gamma_D > a_1, \gamma_Q^R > a_2\right], \quad (54)$$
$$= \Pr\left[|h_{SD}|^2 > z_1\right] Pr\left[|h_{SR}|^2 > z_2\right] Pr\left[|h_{RQ}|^2 > z_3\right], \quad (55)$$
$$= P_{31} P_{32} P_{33}, \quad (56)$$

where $z_1 = \frac{a_1 - \frac{a_1}{a_2}}{\Delta_s}$, $z_2 = \frac{a_1}{\Delta_S}$ and $z_3 = \frac{1}{\Delta_R}$.

From (55), it is evident that the value of P_{31} is always equal to 1 since the value of a_2 cannot be greater than 1. After further simplification, the expressions of P_{32} and P_{33} can be expressed as

$$P_{32} = e^{-\frac{m_{SR}}{\Omega_{SR}} z_2} \sum_{k=0}^{m_{SR}-1} \left(\frac{m_{SR}}{\Omega_{SR}}\right)^k \frac{1}{k!} (z_2)^k, \tag{57}$$

$$P_{33} = e^{-\frac{m_{RQ}}{\Omega_{RQ}} z_3} \sum_{k=0}^{m_{RQ}-1} \left(\frac{m_{RQ}}{\Omega_{RQ}}\right)^k \frac{1}{k!} (z_3)^k. \tag{58}$$

By inserting (57) and (58) into (56), we get the analytical expression of the SPSC for jamming case. From this derived expression of the SPSC, it can observed that underlying secrecy performance is independent of the S →D link, but is rather governed by the parameters of the S → R link.

3.4.4 Asymptotic SOP Analysis: This section obtains expression for asymptotic SOP in the high SNR region to gain more insight.

3.4.4.1 Non-Jamming Case: The asymptotic SOP is calculated under the assumption that $\Delta_S = \Delta_R = \Delta_J \to \infty$. Therefore, the analytical expression of the SOP in (30) can be expressed as

$$SOP_{WJ}^{\infty} \approx 1 - \int_0^{\infty} \left[1 - F_{|h_{RQ}|^2}(Ax + B)\right] \left[1 - F_{|h_{SR}|^2}(Cx + D)\right] \left[1 - F_{|h_{SD}|^2}(Ex + F)\right] f_{|h_{RE}|^2}(x)\, dx, \tag{59}$$

and

$$F_{|h_{SR}|^2}(Cx + D) = \frac{1}{\Gamma(m_{SR})} \Upsilon\left(m_{SR}, \frac{m_{SR}}{\Omega_{SR}}(Cx + D)\right), \tag{60}$$

with $\Upsilon(\cdot,\cdot)$ being the lower incomplete Gamma function defined in [26, Eq. (8.350.1)]. At high SNR and with the aid of $\Upsilon(n, z) \approx \frac{z^n}{n}$, (60) can be approximated as

$$F_{|h_{SR}|^2}(Cx + D) \approx \frac{1}{m_{SR}\Gamma(m_{SR})} \left(\frac{m_{SR}}{\Omega_{SR}}\right)^{m_{SR}} \sum_{j=0}^{m_{SR}} \binom{m_{SR}}{j} D^{m_{SR}-j} C^j x^j. \tag{61}$$

Using the same approach to obtain (61), the other two CDF expressions in (59) can be approximated as

$F_{|h_{SD}|^2}(Ex+F) \approx$

$$\frac{1}{m_{SD}\Gamma(m_{SD})}\left(\frac{m_{SD}}{\Omega_{SD}}\right)^{m_{SD}} \sum_{i=0}^{m_{SD}} \binom{m_{SD}}{i} F^{m_{SD}-i} E^i x^i, \quad (62)$$

$F_{|h_{RQ}|^2}(Ax+B) \approx$

$$\frac{1}{m_{RQ}\Gamma(m_{RQ})}\left(\frac{m_{RQ}}{\Omega_{RQ}}\right)^{m_{RQ}} \sum_{k=0}^{m_{RQ}} \binom{m_{RQ}}{k} B^{m_{RQ}-k} A^k x^k. \quad (63)$$

So, using (61), (62) and (63) in (59) and after some manipulations, the asymptotic SOP expression is obtained and is independent of the transmit SNR demonstrating a zero diversity gain.

3.4.4.2 Jamming Case: In what follows, we approximate the SOP expression in (39) as

$$SP_J^{\infty} = 1 - P_{21}P_{22}P_{23}, \quad (64)$$

where

$$P_{21} = Pr[|h_{SD}|^2 > a] = \frac{1}{\Gamma(m_{SD})}\left(\frac{m_{SD}}{\Omega_{SD}}\right)^{m_{SD}} \int_a^{\infty} x^{m_{SD}-1} e^{-\frac{m_{SD}}{\Omega_{SD}}x}\, dx. \quad (65)$$

At high SNR, P_{21} can be approximated as

$$P_{21} \approx 1 - \frac{1}{m_{SD}\Gamma(m_{SD})}\left(\frac{a \times m_{SD}}{\Omega_{SD}}\right)^{m_{SD}}. \quad (66)$$

Similarly P_{22} and P_{23} can be approximated as

$$P_{22} \approx 1 - \frac{1}{m_{SR}\Gamma(m_{SR})}\left(\frac{b \times m_{SR}}{\Omega_{SR}}\right)^{m_{SR}}, \quad (67)$$

$$P_{23} \approx 1 - \frac{1}{m_{RQ}\Gamma(m_{RQ})}\left(\frac{c \times m_{RQ}}{\Omega_{RQ}}\right)^{m_{RQ}}, \quad (68)$$

where a, b and c have been defined after (42). By substituting (66)-(68) into (64), the asymptotic SOP expression at high SNR is obtained. As $SOP_J^{\infty} \propto \frac{1}{\Delta^{G_d}}$ with $G_d = \min(m_{SD}, m_{SR}, m_{RQ})$ being the diversity gain.

Chapter 4: Results and Discussion

The numerical results in this section are used to analyze the impact of the jammer on the secrecy performance of the NOMA system, and Monte-Carlo simulation is used to back up the findings. We have fixed $\Delta_S = \Delta_R = \Delta_J$. The threshold rate R_{th} is defined in bit per sec per hertz (bps/Hz). Herein, we set the following $m_{SD} = m_{SR} = m_{RQ} = m_{RE} = 2$ as fading severity parameters, $\Omega_{SD} = 2, \Omega_{SR} = 1, \Omega_{RQ} = 1, \Omega_{RE} = 0.01$ as average power of the multipath components.

In figure 4.1, we have plotted SOP versus Δ_S (in dB) curves for the non-jamming case for three different values of threshold rate i.e., $R_{th} = 3,5,8$ bps/Hz. Analytical curves are followed by Monte-Carlo simulation results for both the lower and higher values of SNR, as can be seen in the graph.

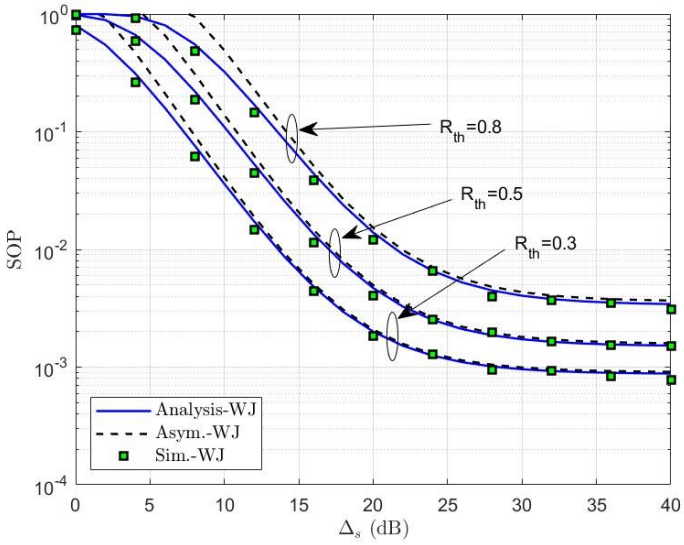

Figure 4.1: SOP vs Δ_S (in dB) for non-jamming case.

It is observed from the graph that for higher value of R_{th} SOP performance degrades because the occurrence of outage event increases with increase in the value of R_{th}. The SOP curve tends to have a constant value for higher SNR values.

Figure 4.2 exhibits the performance of the SOP against Δ_S in the case of jammer. This graph is plotted for three different values of threshold rate i.e., $R_{th} = 3,5,8$ bps/Hz.

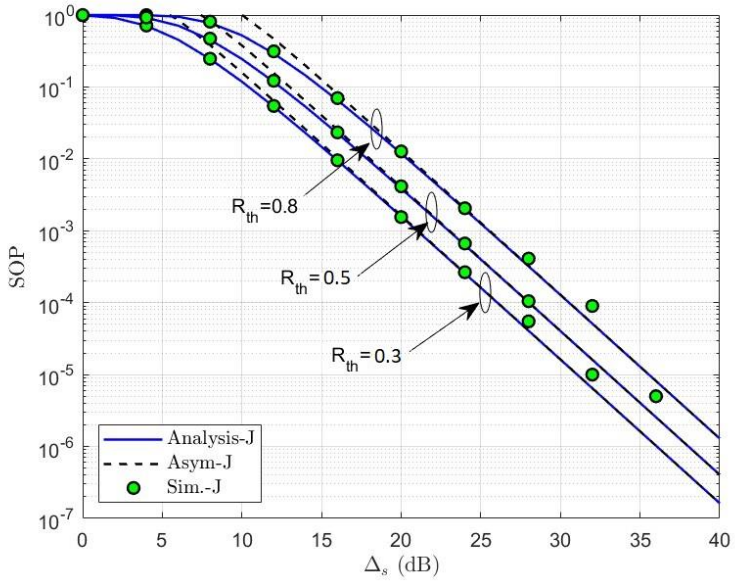

Figure 4.2: SOP vs Δ_S (in dB) for jamming case.

It is clear from the graph that, SOP curve is constantly decreasing. So, we can state that the jamming provides better SOP performance than the non-jamming case. We observe that, SOP performance attained at lower threshold rate is better as compared to higher threshold rate. At high SNR, jamming suppresses the deleterious effect, unlike in Figure 4.1, leading to an error floor.

Figure 4.3-4.4 exhibits the performance of the SPSC against Δ_S for the case of non-jamming and jamming, respectively. Curve 4.3 (for non-the jamming case), is drawn by setting $m_{RE} = 2$, $\Omega_{RE} = 0.01, \Omega_{RE} = 1, \Omega_{RE} = 2$ and the curve 4.4 (for jamming case), is drawn by setting $m_{SR} = 2$, $\Omega_{SR} = 0.1, \Omega_{SR} = 1, \Omega_{SR} = 2$. It can be observed from the curves that for smaller value of average SNR Ω_{RE}, better SPSC performance is achieved in non-jamming case. This is because, if we increase the value of Ω_{RE}, it will positively affect the capability of the

eavesdropper, which results in a decrease in the SPSC value. And in the case of the jammer, for large value of average SNR Ω_{SR} (which is tantamount to improving the channel between S and R), better performance is achieved.

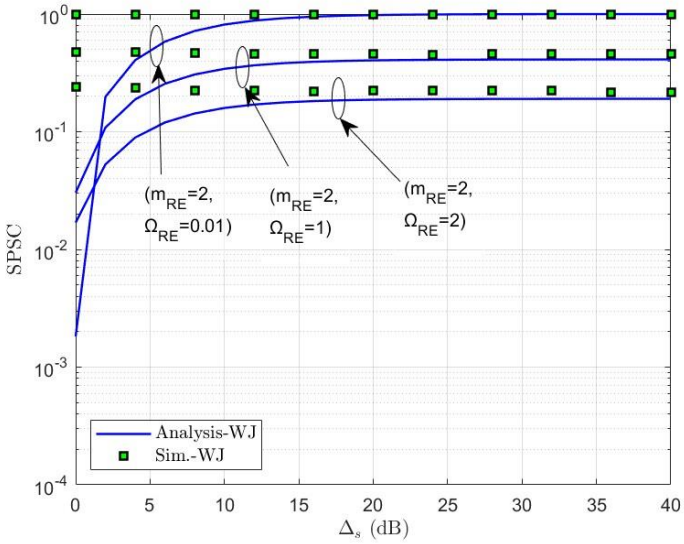

Figure 4.3: SPSC vs Δ_S (in dB) for non-jamming case.

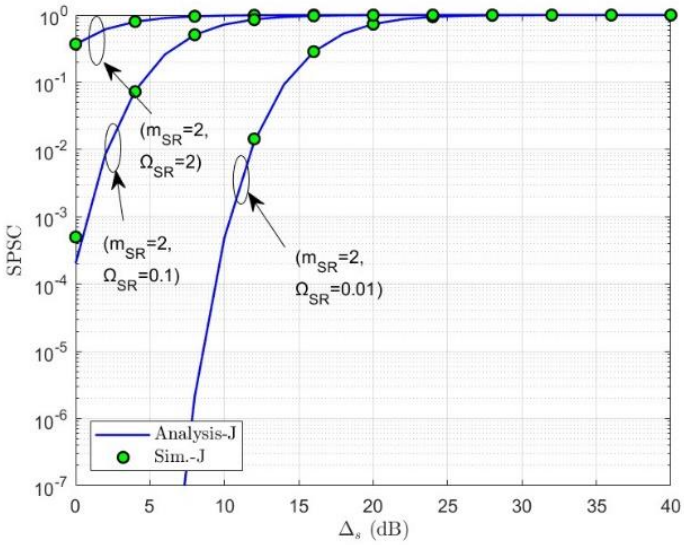

Figure 4.4: SPSC vs Δ_S (in dB) for jamming case.

Figure 4.5 shows the impact of variation of the power allocation coefficient a_1 on the SOP for both jamming and non-jamming case, for two different values of $\Delta_S = 20, 30$ dB. For $\Delta_S = 30\ dB$, SOP performance

is better than that for $\Delta_S = 20\ dB$ because $\Delta_S = \Delta_J$, and with the increase in the value of Δ_J the impact of jammer increases, and it will deteriorate the SNR at the eavesdropper so the overall SOP performance will be improved. But for a fixed value of Δ_S, as the value of a_1 increases, the power allocated for the transmission of x_R decreases. This is because of the fact that the received SNR at Q for x_R depends on a_2, and $a_2 = 1 - a_1$. Therefore, the probability of correctly decoding x_R is low. And this degrades the SOP performance.

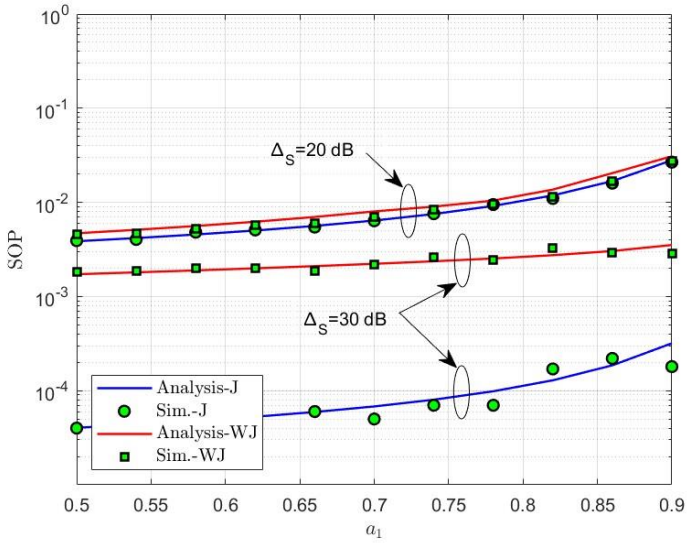

Figure 4.5: SOP vs a_1 for both jamming and non-jamming case.

Chapter 5: Conclusions and Future Scope

5.1 Conclusion

In chapter 3, the performance analysis of the CJ-aided overlay cognitive NOMA system is carried out by deriving the SOP, SPSC expressions and asymptotic SOP in closed-form over Nakagami-*m* fading channels. Furthermore, closed-form expressions for performance metrics such as SOP, SPSC, and asymptotic SOP of the proposed system model are implemented in MATLAB. From simulation results, it is observed that the secrecy outage performance for the system with jammer is better than the system without jammer. Further, it is observed that SOP for non-jamming case saturates at high SNR while SOP for jamming case proportionally improves with SNR. Finally, the simulated SOP and SPSC values obtained from Monte Carlo simulations agree well with the theoretical values. Therefore, the derived expressions are validated using simulations as well.

5.2 Future Scope

The following is a summary of the scope of future work:

- The performance of the CJ-aided overlay cognitive NOMA system model is carried out by not considering energy harvesting model. However, in practical scenarios, energy harvesting models are more efficient.
- In order to make our proposed system model more spectrally efficient, FD technique can be employed. So, performance analysis can be carried out by considering the FD mode at relay.
- We can consider the cases of imperfect SIC and CSI conditions, which is useful for realistic implementations.

REFERENCES

[1] J. A. del Peral-Rosado, R. Raulefs, J. A. López-Salcedo and G. Seco-Granados, "Survey of Cellular Mobile Radio Localization Methods: From 1G to 5G," *IEEE Commun. Surveys and Tuts*., vol. 20, no. 2, pp. 1124-1148, Second quarter 2018.

[2] Attaran, M., "The impact of 5G on the evolution of intelligent automation and industry digitization" *J. of Ambient Intell. Human Comput.* (2021).

[3] K. F. Jasim, and I. F. Al-Shaikhli, "Mobile technology generations and cryptographic algorithms: Analysis study," *4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT),* pp. 50-55, 2015.

[4] G. I. T siropoulos et al., "Radio resource allocation techniques for efficient spectrum access in cognitive radio networks," *IEEE Commun. Surveys and Tuts*., vol. 18, no. 1, 1st Qrtr., pp. 824–847, 2016.

[5] F. Li, H. Jiang, R. Fan, and P. Tan, "Cognitive non-orthogonal multiple access with energy harvesting: An optimal resource allocation approach," *IEEE Trans. Veh. Technol*., vol. 68, no. 7, pp. 7080-7095, July 2019.

[6] L. Yang et al., "Cooperative non-orthogonal layered multicast multiple access for heterogeneous networks," *IEEE Trans. Commun*., vol. 67, no. 2, pp. 1148–1165, Feb. 2019.

[7] Z. Ding, M. Peng, and H. V. Poor, "Cooperative non-orthogonal multiple access in 5G systems," *IEEE Commun. Lett*., vol. 19, no. 8, pp. 1462–1465, Aug. 2015.

[8] Z. Ding, P. Fan, and H. V. Poor, "Impact of user pairing on 5G nonorthogonal multiple access downlink transmissions," *IEEE Trans. Veh. Technol*., vol. 65, no. 8, pp. 6010-6023, Aug. 2016.

[9] M. M. Mohammadi, B. K. Chalise, A. Hakimi, Z. Mobini, H. A. Suraweera and Z. Ding, “Beamforming design and power allocation for full-duplex non-orthogonal multiple access cognitive relaying,” *IEEE Trans. On Commun.*, vol. 66, no. 12, pp. 5952-5965, Dec. 2018.

[10] L. Lv, Q. Ni, Z. Ding and J. Chen, “Application of non-orthogonal multiple access in cooperative spectrum sharing networks over nakagami- m fading channels,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5506-5511, June 2017.

[11] C. Zhong and Z. Zhang, "Non-Orthogonal Multiple Access With Cooperative Full-Duplex Relaying," *IEEE Commun. Lett.*, vol. 20, no. 12, pp. 2478-2481, Dec. 2016.

[12] J. Kim and I. Lee, "Non-Orthogonal Multiple Access in Coordinated Direct and Relay Transmission," *IEEE Commun. Lett*., vol. 19, no. 11, pp. 2037-2040, Nov. 2015.

[13] N. Yang, et al., “Safeguarding 5G wireless communication networks using physical layer security,” *IEEE Commun. Mag*., vol. 53, no. 4, pp. 20–27, Apr. 2015.

[14] B. Schneier, “Description of a new variable-length key, 64-bit block cipher (blowfish),” *Fast Softw. Encryption Cambridge Security Workshop*, Cambridge, U.K., pp. 191–204, Dec. 1993.

[15] B. Schneier, “Applied cryptography: Protocols, algorithms, and source Code in C,” Indianapolis, IN, USA: Wiley, 1996.

[16] Y. Liu, H. H. Chen, and L. Wang, “Physical layer security for next generation wireless networks: Theories, technologies, and challenges,” *IEEE Commun. Surveys and Tuts*., vol. 19, no. 1, pp. 347-376, Firstquarter 2017.

[17] Y. W. Hong, P. C. Lan, and C. C. Kuo, “Enhancing physical layer secrecy in multiantenna wireless systems: An overview of signal processing approaches,” *IEEE Signal Proc. Mag.*, vol. 30, no. 5, pp. 29–40, Sept. 2013.

[18] A. Mukherjee et al., “Principles of physical layer security in multiuser wireless networks: A survey,” *IEEE Commun. Surveys and Tuts*., vol. 16, no. 3, pp. 1550–73, 3rd Quarter 2014.

[19] Sun, Li, and Qinghe Du., “A review of physical layer security techniques for Internet-of-Things: Challenges and solutions,” *Entropy 20,* no. 10, 2018.

[20] T. M. Hoang, T. Q. Duong, N. Vo, and C. Kundu, “Physical layer security in cooperative energy harvesting networks with a friendly jammer,” *IEEE Commun. Lett.*, vol. 6, no. 2, pp. 174-177, April 2017.

[21] H. Webb et al., “Secrecy outage analysis in energy harvesting relay networks with a friendly jammer,” *4th International Conference on Recent Advances in Signal Processing, Telecommunications and Computing (SigTelCom),* pp. 45-49, 2020.

[22] J. Chen, L. Yang, and M. S. Alouini, “Physical layer security for cooperative NOMA systems,” *IEEE Trans. Veh. Technol.,* vol. 67, no. 5, pp. 4645-4649, May 2018.

[23] V. Bankey, V. Singh, and P. K. Upadhyay, “Physical layer secrecy of NOMA-based hybrid satellite-terrestrial relay networks,” *IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1-6, 2020.

[24] C. Yu, H. Ko, X. Peng, W. Xie, and P. Zhu, “Jammer-aided secure communications for cooperative NOMA systems,” *IEEE Commun. Lett*., vol. 23, no. 11, pp. 1935-1939, Nov. 2019.

[25] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[26] I. S. Gradshteyn, and I. M. Ryzhik, *Tables of Integrals, Series and Products*, 6th ed. New York: Academic Press, 2000.

[27] M. Zeng and P. Nguyen and O. Dobre and H. Vincent Poor and H Poor, “Physical Layer Security for NOMA Systems”, Feb. 2020.