UNIVERSITY OF CALIFORNIA SAN DIEGO

Performance Analysis of Modern Communication Networks under Hostile Environment

A dissertation submitted in partial satisfaction of the
requirements for the degree
Doctor of Philosophy

in

Electrical Engineering (Communication Theory and Systems)

by

Turki Yousef A Alkhamees

Committee in charge:

Professor Laurence B. Milstein, Chair
Professor Pamela C Cosman
Professor William S Hodgkiss Jr.
Professor Xinyu Zhang

2024

The Dissertation of Turki Yousef A Alkhamees is approved, and it is acceptable in quality and form for publication on microfilm and electronically.

University of California San Diego

2024

DEDICATION

To My Family

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AWGN	Additive White Gaussian Noise
ASER	Average Symbol Error Rate
BS	Base Station
CCI	Co-Channel Interference
CDF	Cumulative Distribution Function
CR-NOMA	Cognitive Radio-Non-Orthogonal Multiple Access
CRN	Cognitive Radio Network
CSI	Channel State Information
D2D	Device-to-Device
DOF	Degrees of Freedom
DOS	Denial of Service
ED	Energy Detection
ED-ENP	Energy Detection with Estimated Noise Power
ENP	Estimated Noise Power
FBMC-FMT	Filter Bank Multi-Carrier - Filtered Multitone
Hz	Hertz
ICI	Inter-Carrier Interference
ISI	Inter-Symbol Interference
LOS	Line of Sight
MIMO	Multiple-Input Multiple-Output
mmWave	Millimeter-Wave

MC	Multi-Carrier
DoS	Non-Line of Sight
PCA	Pilot Contamination Attack
PDF	Probability Density Function
PJA	Pilot Jamming Attack
PSD	Power Spectral Density
PU	Primary User
PUE	Primary User Emulation
PPP	Poisson Point Process
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
Rx	Receiver
SER	Symbol Error Rate
SINR	Signal-to-Interference-plus-Noise Ratio
SIR	Signal-to-Interference Ratio
SNR	Signal-to-Noise Ratio
SP	Sensing Period
SS	Spectrum Sensing
SSDF	Spectrum Sensing Data Falsification
SU	Secondary User
Tx	Transmitter

ACKNOWLEDGEMENTS

Throughout my Ph.D. journey, doubts often arose, whether concerning ideas, concepts, or the paths chosen. However, the only certainty that remains is the profound gratitude and appreciation owed to those who have contributed not only to my journey, but also to shaping my vision of the future.

First and foremost, I would like to express my deepest gratitude to my parents. They mean everything to me; they are not just a chapter in my life, but the entire book of my life. They are my eyes through which I perceive the world and my lungs through which I breathe life itself.

I also extend heartfelt thanks to my wonderful sisters, spectacular big brother, and amazing wife for their prayers, encouragement, and endless support. I consider myself incredibly fortunate to be a member of this remarkable family.

I would like to express my utmost gratitude to my advisor, Professor Milstein, for his time and patience. Throughout my journey, I never felt lacking in confidence or direction, thanks to his infinite support and guidance. Honestly, his contributions have not only impacted my journey but have also profoundly shaped my way of thinking.

Huge thanks go to Professor Pamela C Cosman, Professor William S Hodgkiss Jr., Professor Xinyu Zhang, and Professor Bhaskar Rao, I really appreciate the help and feedback from my dissertation, qual, and prelim exams.

Lastly but not least, I would like to thank my past and current lab mates, all of my friends here in San Diego, California, United States, and Saudi Arabia for their support and friendship.

Chapter 2 and Appendix A are, in part, a reprint of the paper, T. Y. Alkhamees and L. B. Milstein, "A Different Approach for Sensing Disruption," in *IEEE Access*, vol. 11, pp. 86431-

86443, 2023, doi: 10.1109/ACCESS.2023.3304244. The dissertation author is the primary researcher and author of this paper.

Chapter 3 and Appendix B are, in part, a reprint of the paper, T. Y. Alkhamees and L. B. Milstein, "Impact of Sharing Disruption in MC CR-NOMA," in *IEEE Access*, vol. 11, pp. 82871-82881, 2023, doi: 10.1109/ACCESS.2023.3300659. The dissertation author is the primary researcher and author of this paper.

Chapter 4 is, in part, a reprint of the paper, “Error Analysis for Multicarrier Transmission of Device-to-Device in Millimeter-Wave Communication”, to be submitted to *IEEE Transactions on Vehicular Technology*. The dissertation author is the primary researcher and author of the paper.

VITA

2014 Bachelor of Science in Electrical Engineering, King Saud University, Riyadh, Saudi Arabia.

2018 Master of Science in Electrical Engineering, University of Southern California, Los Angeles.

2024 Doctor of Philosophy in Electrical Engineering (Communication Theory and Systems), University of California San Diego.

PUBLICATIONS

T. Y. Alkhamees and L. B. Milstein, "A Different Approach for Sensing Disruption," in *IEEE Access*, vol. 11, pp. 86431-86443, 2023, doi: 10.1109/ACCESS.2023.3304244.

T. Y. Alkhamees and L. B. Milstein, "Impact of Sharing Disruption in MC CR-NOMA," in *IEEE Access*, vol. 11, pp. 82871-82881, 2023, doi: 10.1109/ACCESS.2023.3300659.

T. Y. Alkhamees and L. B. Milstein, “Error Analysis for Multicarrier Transmission of Device-to-Device in Millimeter-Wave Communication”, submitted to IEEE *Transactions* on *Vehicular Technology.*

.

ABSTRACT OF THE DISSERTATION

Performance Analysis of Modern Communication Networks under Hostile Environment.

by

Turki Yousef A Alkhamees

Doctor of Philosophy in Electrical Engineering (Communication Theory and Systems)

University of California San Diego, 2024

Professor Laurence B. Milstein, Chair

Most modern communication networks suffer from both intentional and unintentional interference. In this dissertation, we investigate three separate issues in modern wireless communication networks: sensing disruption attacks on cognitive radio networks (CRNs), sharing disruption attacks on cognitive radio non-orthogonal multiple access (CR-NOMA), and error analysis in millimeter-wave (mmWave) communication under unintentional interference environments.

In the first problem, we propose a different approach for sensing disruption attacks in CRNs. We examine the optimal strategy for an intelligent adversary who aims to manipulate busy bands so that they appear to be free. This approach involves contaminating noise power measurements, as demonstrated through a two-step sensing scheme that combines energy detection with noise power estimation by secondary users. We demonstrate that the optimal strategies for sensing link disruptions include equal-power and partial-band flipping, from deriving the maximum average number of missed detections under specific power constraints of the adversary.

Secondly, we examine the vulnerabilities of spectrum sharing in a CR-NOMA network, proposing a new type of attack termed sharing disruption. This attack disrupts the channel estimation phase, leading to a denial-of-service (DoS) for secondary users. We derive the optimal power allocation to maximize disruption, calculating the maximum average number of DoS bands under specific adversary power constraints. Additionally, we compare optimal power allocation with uniform power allocation.

Lastly, we investigate the error performance of mmWave bands in the presence of unintentional interference. This analysis is motivated by the anticipated increase in number of users in near future. We examine M-ary quadrature amplitude modulation ($M-QAM$) across Nakagami$-m$ channels, taking into account the impacts of directional antennas and blockage. We derive the average probability of error with employing a stochastic geometry framework that provide different insights for mmWave networks, particularly in device-to-device (D2D) communications.

Chapter 1 :

Introduction

1.1 Background and Motivation:

In modern days, most technologies in the wireless communication industry aim to solve the challenge of spectrum scarcity. The reason for this challenge is the dramatic increase in the number of users over the past decades. In response to this rising demand, many technologies have emerged to optimize the use of available spectrum or to operate on newly unlicensed bands.

Cognitive radio network (CRN) is one these technologies that was proposed to solve the spectrum scarcity dilemma by efficiently utilizing the spectrum [1]. One paradigm of CRN is to enable unlicensed users, known as secondary users (SUs), to access the spectrum without interfering with licensed users, known as primary users (PUs) [1],[2]. To achieve this, the SUs need to engage in spectrum sensing (SS), which requires them to detect the activity of PUs. Many detection techniques have been studied to sense the bands, such as energy detector (ED), matched filter detector, and cyclostationary detector. These techniques are discussed in references [3] and [4]. The simplest of these techniques is ED. However, ED leads to the problem of noise uncertainty [5], which has led researchers to study combination of energy detection with estimated noise power (ED-ENP) as in [1,6,7,8]. Past studies have used outdated noise samples from previous sensing periods to estimate noise power levels, a process known as the estimated noise power (ENP), as in [6], and [8]. An alternative method involves a random training phase that achieves nearly optimal performance [7]. Nevertheless, all these techniques can have vulnerabilities that may be targeted by adversaries to disrupt the SS, highlighting the importance of examining the these techniques under malicious activities. For more insight, see references [9,10,11].

Another technology is known as, cognitive radio non-orthogonal multiple access (CR-NOMA) which, is combining CR with non-orthogonal multiple access (NOMA) [12,13,14,15,16]. The goal of that is to increase the network capacity, and hence to utilize the spectrum more efficiently. Research about CR-NOMA has been extensively studied [15,16,17,18]. However, Ding et al. [17] investigated the impacts of user pairing in CR-NOMA by ensuring the quality of service (QoS) for PUs. Following this study, many researchers have expanded on this foundation by applying CR-NOMA strategies in multiple-input multiple-output (MIMO) environments [18] and investigating power allocation in multi-carrier (MC) NOMA systems [19]. These studies typically assume perfect channel state information (CSI), an ideal scenario that is not realistic. In fact, [20] evaluated the performance of downlink NOMA systems with imperfect CSI. Furthermore, [15], suggested that challenges in resource allocation within CR-NOMA, given imperfect CSI, remain an open problem, presenting a significant obstacle that could be exploited by adversaries to diminish system performance.

The adoption of millimeter-wave (mmWave) technology, operating at frequencies starting around 28 GHz, for 5G and future 6G communications can help solve the spectrum scarcity problem [21]. In most countries, mmWave bands were licensed for military applications or left unlicensed [21]. Integrating them into the cellular communication is set to enhance the total throughput [22]. However, as the number of users is expected to rise, the challenges such as blockage and higher path losses become more apparent on the performance as shown, in [22,23,24]. Consequently, evaluating the error analysis is essential to improve the reliability and efficiency of these networks as the number of user increases.

Due to the solutions of the spectrum scarcity problem, intentional (also known as adversarial interference) or unintentional interference can be introduced. Intentional interference is orchestrated by adversaries seeking to disrupt communication links. One example is the adversary launching jamming techniques. For more details on other examples, see [25] and [26]. The implications of intentional interference extend beyond academic concerns, posing real threats to public safety, including terrorism, vandalism, and other crimes.

The imperfections and limitations of modern communication systems can show the importance of examining both types of interference. The importance lies in conducting worst-case scenario analyses. The reason behind this is to help develop more robust technologies that ensure reliable and secure communication.

1.2 Dissertation Organization:

Chapter 2 introduces a different type of sensing disruption known as flipped attacks. The sensing disruption happens by flipping the busy bands, making them look free to the SUs. The mechanism of sensing disruption is illustrated via a two-step sensing scheme. An optimal strategy for flipped attacks is studied. Lastly, analytical and numerical results illustrate the efficiency of attacks on system parameters.

Chapter 3 explores the vulnerabilities of spectrum sharing in CR-NOMA networks. Also, it introduces a new type of attack that can cause denial of service (DoS) for several SUs in CR-NOMA. An analytical expression for the average probability of DoS is studied. Additionally, a disruption strategy involving optimal power allocation is discussed. To conclude, a comparison between uniform and optimal power allocation by the adversary is provided.

Chapter 4 examines the error performance of mmWave communications within dense interference environments. Using a stochastic geometry approach, the probability of error and the

Laplace transform of the aggregate interference are studied. Specifically, the average probability of error for $M-QAM$ is derived over the Nakagami$-m$ channel. Finally, the impact of directional antennas and blockages on error performance in mmWave device-to-device (D2D) networks is illustrated.

Chapter 2 :

Attacks Optimization of CR

2.1 Introduction:

SS introduces vulnerabilities in CRNs [9,10,11], which adversaries may exploit through various attacks, such as spectrum sensing data falsification (SSDF) and Primary User Emulation (PUE). In SSDF attacks, adversaries pose as SUs, and send signals that affect global decisions. These attacks are typically driven by motives of either vandalism, which aims to overload the Fusion Center (FC) with incorrect reports of busy bands; or exploitation, aiming to flood the FC with false reports about free bands [27]. On the other hand, PUE attacks occur during the SU's sensing period, termed as sensing disruption. Reference [28,29] have shown that PUE attacks can significantly affect the performance of CRNs. For example, one method involves sending a Gaussian signal into unoccupied bands to degrade the accuracy of SS at the SUs. Comprehensive details on these attacks and their countermeasures are illustrated in [9,10,11].

The focus of this study is on disrupting the sensing period in CRNs, specifically targeting the busy bands and changing their status to appear free. These so-called flipping attacks have not been extensively examined in the literature, which has predominantly concentrated on sensing disruptions of free bands to make them appear occupied, known as spoofing attacks [30,31,32]. Flipping attacks are particularly hurts the performance of CRNs in two different manners: they not only cause interference between SUs and PUs, undermining the fundamental principles of CRNs, but they also lead to the misclassification of the bands, consequently decreasing the total network throughput.

The outline of this chapter is as follows: Section 2.2 presents preliminaries and general formulation. The optimal strategy for flipping busy bands is described in Section 2.3. The numerical results are presented in Section 2.4, and Section 2.5 summaries this chapter.

2.2 Preliminaries and General Formulation:

In this chapter, we assume the spectral range of interest consists of U bands, the same as the number of SUs, to achieve a worst-case scenario analysis. We examine the impact of an adversary on a CRN where there are at least U SUs that adopt an ED-ENP. Note that the adversary intends to disrupt the sensing slot. Furthermore, U bands are divided into two sets of bands: a set of sensed-free bands (B_{free}) and a set of sensed-busy bands (B_{busy})

In Section 2.1.1, we discuss the two-step sensing protocol presented in [6]. The performance of an ED-ENP when an adversary is present is evaluated in Section 2.1.2. The assumptions regarding the knowledge available to an intelligent adversary and the framework of the attacks are presented in Section 2.1.3.

2.2.1 Two-Step Sensing:

The two-step sensing procedure is proposed in the IEEE 802.22 [34] and ECMA 392 [35] standards, which use sporadic long sensing periods (SPs) for fine sensing, and more frequent short SPs for fast sensing, as illustrated in Figure 2.1. A detailed description of the two-step detection scheme is shown in Figure 2.2, where a high-precision detection algorithm such as a feature detector is employed in the fine-SP mode. If a given band is sensed as being free during the fine-SP mode, the noise power level is estimated. These bands are denoted as B_{ENP}. A simple radiometer was implemented in the fast-SP mode. Therefore, the bands that are sensed as free

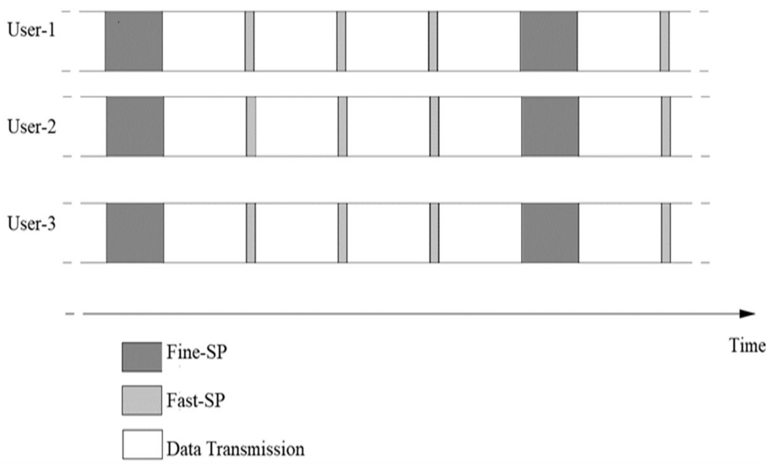


Figure 2.1:The proposed Two step sensing in the IEEE 802.22 scheduling mechanism [34].

can be expressed as $B_{free} = B_{ENP} \cup B_{fast}$, where B_{fast} is the set of sensed-free bands in the fast-SP mode.

Based on [34] and [35], the SUs in the network are either in fine-SP mode or fast-SP mode. The rationale behind this was to avoid measurements of overlapping for the SUs. Note that various key parameters of the system, such as sensing schedule and type of sensing, are publicly known [34,35]. Therefore, an adversary can be aware of this sensing mechanism and use this information to degrade the performance of the CRN.

2.2.2 Performance of an Energy Detector with Estimated Noise Power (ED-ENP):

The detection of a signal in an additive white Gaussian noise (AWGN) channel was investigated in [36]. The energy of the received waveform at the k^{th} band (i.e., the k^{th} SU), $r_k(t)$, was measured over the bandwidth W (*Hz*) and approximated as follows:

$$\frac{2}{N_0}\int_0^T [r_k(t)]^2\,dt \approx \frac{1}{\sigma_{k,n}^2}\sum_{i=1}^{N}\left|y_i^{(k)}\right|^2 = Y_{ED}^{(k)}, \tag{2.1}$$

where N_0 is the one-sided noise power spectral density (PSD) and $\sigma_{k,n}^2 = N_0 W$. The summation in (2.1) from [36] was approximated as a Gaussian statistic; therefore, we have the following detection problem:

$$\begin{aligned} H_0: &\quad y_i^{(k)} = n_i^{(k)} \\ H_1: &\quad y_i^{(k)} = x_i^{(k)} + n_i^{(k)} \end{aligned}, \tag{2.2}$$

where $x_i^{(k)}$ is the i-th signal sample, the noise samples $n_i^{(k)} \sim \mathcal{CN}\ (0, 2\sigma_{k,SS}^2)$ are i.i.d., and H_0 and H_1 are the "signal absent" and "signal present" hypotheses, respectively. The ED test statistic, $Y_{ED}^{(k)}$, has either a central chi-square (χ^2) probability density function (PDF) with $2N$ degrees of freedom (DOF) or a noncentral χ^2 PDF with $2N$ DOF [36]. For a given desired probability of a false alarm, denoted as p_{FA}^{DES}, threshold K was set based on the Neyman-Pearson criterion. This is only possible if the noise power is known [1,3,4]. If the SU estimates the noise power, the presence of an intelligent adversary can contaminate the estimate. Therefore, the test

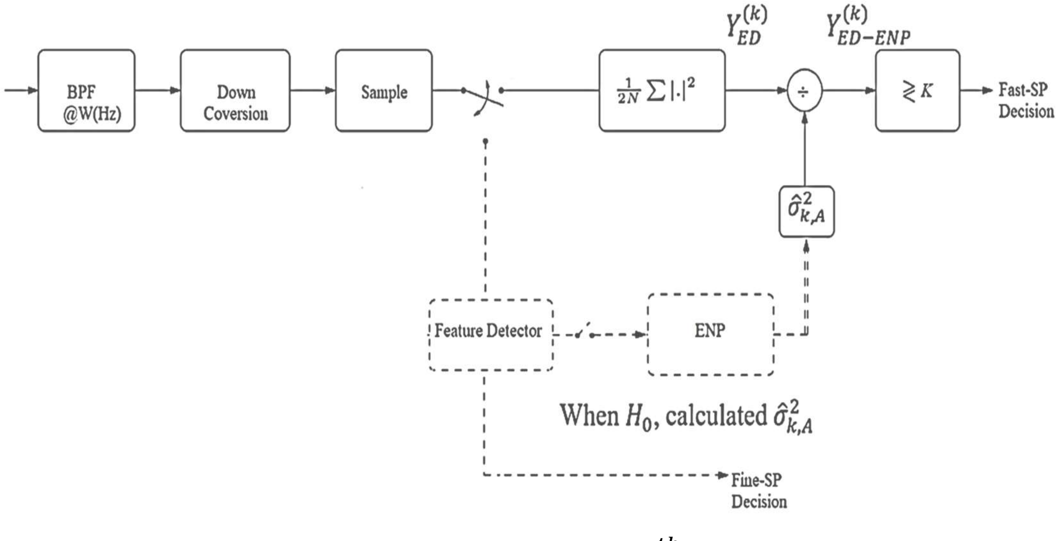


Figure 2.2: Two-step Detection scheme of the k^{th} SU that is proposed in [6].

statistic of ED-ENP for the k^{th} SU can be derived by modifying the result of [6], to include the presence of an intelligent adversary, as shown below:

$$Y_{ED-ENP}^{(k)} = \frac{1}{\hat{\sigma}_{k,A}^{2}} \left(\frac{1}{2N}\right) \sum_{i=1}^{N} \left|y_i^{(k)}\right|^2 \gtrless K$$

$$= \frac{Y_{ED}^{(k)}}{\hat{\sigma}_{k,A}^{2}} = \frac{\left(\frac{1}{2N}\right) \sum_{i=1}^{N} \left|y_i^{(k)}\right|^2}{\frac{1}{2M} \sum_{i=1}^{M} \left|n_{-i}^{(k)} + \alpha_k j_{-i}^{(k)}\right|^2} \gtrless K, \qquad (2.3)$$

where $M = WT_{fine}$ is the number of samples in the fine-SP mode, and $N = WT_{fast}$ is the number of samples in the fast-SP mode, T_{fine} is the fine-SP time interval, and T_{fast} is the fast-SP time interval. Also note that the term $\hat{\sigma}_{k,A}^{2}$ in (2.3) is a maximum likelihood estimate (MLE) of the noise power. For simplicity, we assume that the samples y_i for $i < 0$, are those in which the SUs estimate the noise power. In this way, y_{-i} is described as an outdated sample, where ideally it contains only the "noisy sample" (i.e., the noise and adversary samples only), and is given by, $n_{-i} + \sqrt{\alpha_k} j_{-i}$, for $i = \{1, .., M\}$. The thermal noise after the bandpass filter is modeled as zero-mean complex additive Gaussian noise at the k^{th} band (i.e., $\sim\mathcal{CN}\left(0, 2\sigma_{k,n}^{2}\right)$). In addition, the adversary signal after the bandpass filter is distributed as $\sim\mathcal{CN}\left(0, 2\alpha_k P_{k,A}\right)$, and is transmitted to the k^{th} allowable (i.e., free) band during the fine-SP mode, where α_k is the path loss factor between the intelligent adversary and the k^{th} SU. Also, note that the term $P_{k,A}$ is the power of the adversary signal in the k^{th} band. In this chapter, we assume that the path loss factor, α_k, is constant across all bands (i.e., $\alpha_k = \alpha$) and is assumed to be known to the adversary. This assumption is common in the literature on CRN attacks and examples can be found in [9] and [11]. The adversary and the noise signals are assumed to be independent of each other. It can be shown that for a long observation interval, $\hat{\sigma}_{k,A}^{2} \sim \chi^2$ with $2M$ DOF and a scale parameter equal to $\sigma_{k,ENP}^{2}$ [37].

One of the popular models used in the literature [1,3,6], assumes that the PU signal is a Gaussian signal, with a PDF of $\sim\mathcal{CN}(0, 2S_k)$, where $2S_k$ is the power of the PU signal on the k^{th} band and the signal-to-noise-ratio (SNR) is denoted by $\gamma_k \triangleq S/\ \sigma_{k,SS}^2$ of the PU in the k^{th} band.

Because both $\hat{\sigma}_{k,A}^2$ and $Y_{ED}^{(k)}$ have a central chi-square distribution, the ratio of these two distributions in (2.3), with proper scaling, is a central $\mathcal{F}$-distribution [6,38,39]. Therefore, the false alarm probability of ED-ENP, $p_{FA,ED-ENP}^{(k)}$, and the detection probability of ED-ENP, $p_{D,ED-ENP}^{(k)}$, can be expressed as regularized incomplete beta functions as shown below [40]:

$$p_{FA,ED-ENP}^{(k)} = Pr\left\{Y_{ED-ENP}^{(k)} > K \mid H_0\right\} = \tilde{B}\left(M, N, \frac{1}{Kw+1}\right), \tag{2.4}$$

$$p_{D,ED-ENP}^{(k)} = Pr\left\{Y_{ED-ENP}^{(k)} > K \mid H_1\right\} \ = \tilde{B}\left(M, N, \frac{1}{K\left(\frac{w}{(1+\gamma)}\right)+1}\right), \tag{2.5}$$

where $\tilde{B}(u, v, z) = \frac{1}{B(u,v)} \int_0^z x^{u-1}\,(1-x)^{v-1} dx$, $B(u, v)$ is defined as the beta function $B(u, v) = \Gamma(u)\,\Gamma(v)/\Gamma(u+v)$, and $w \triangleq (N/M)\left(\sigma_{k,ENP}^2/\sigma_{k,SS}^2\right)$. For large N and M, the probabilities $p_{FA,ED-ENP}^{(k)}$ in (2.4) and $p_{D,ED-ENP}^{(k)}$ in (2.5) can be expressed using a Gaussian approximation as follows [40]:

$$p_{FA,ED-EN}^{(k)} \ \approx Q\left(\frac{K-\frac{\sigma_{k,SS}^2}{\sigma_{k,ENP}^2}}{\frac{\sigma_{k,SS}^2}{\sigma_{k,ENP}^2}\sqrt{\frac{M+N}{MN}}}\right) = \ Q\left(\frac{K}{\frac{\sigma_{k,SS}^2}{\sigma_{k,ENP}^2}\sqrt{\frac{M+N}{MN}}} - \frac{1}{\sqrt{\frac{M+N}{MN}}}\right), \tag{2.6}$$

$$p_{D,ED-E}^{(k)} \quad \approx Q\left(\frac{K-\ \frac{\sigma_{k,SS}^2}{\sigma_{k,ENP}^2}(1+\gamma)}{\frac{\sigma_{k,SS}^2}{\sigma_{k,ENP}^2}\,(1+\gamma)\sqrt{\frac{M+N}{MN}}}\right) = \ \mathrm{Q}\left(\frac{K}{\frac{\sigma_{k,SS}^2}{\sigma_{k,ENP}^2}\,(1+\gamma)\sqrt{\frac{M+N}{MN}}} - \frac{1}{\sqrt{\frac{M+N}{MN}}}\right). \tag{2.7}$$

It is challenging to design a detector if the PU signal has an unknown deterministic waveform. However, the probability of detection can be approximated as in (2.7) if the PU SNR is in the low-SNR regime (for more details, see [6]). Note that the false alarm probability is similar to that of detecting a Gaussian signal because no PU is present. Therefore, for the remainder of this paper, we consider only the case of a PU signal as a complex Gaussian waveform. Note that the noise power of the k^{th} SU during the fine-SP mode is equal to $\sigma_{k,ENP}^2 = \sigma_{k,n}^2\left(1 + \alpha_k P_{k,A}/\ \sigma_{k,n}^2\right)$, whereas the noise power during the fast-SP mode is $\sigma_{k,SS}^2 = \ \sigma_{k,n}^2$. If there are no attacks (i.e., $P_{k,A} = 0$), then $\sigma_{k,ENP}^2 = \ \sigma_{k,n}^2$.

However, a perfect estimate of noise power is impossible in two-step sensing (i.e., $\sigma_{k,ENP}^2 \neq \sigma_{k,n}^2$) [1,5,6]. This implies that there is some residual error when estimating $\hat{\sigma}_{k,A}^2$. In [5], the approach used is a more practical model; that is, the noise process is assumed to be Gaussian, but the variance is off by some factor. As in [5], we can model the same approach for two-step sensing because $Y_{ED-E}^{(k)}$ is also approximately a Gaussian random variable, and we can say that the ratio $\sigma_{k,SS}^2/\sigma_{k,ENP}^2$ can be bounded, as $\sigma_{k,SS}^2/\sigma_{k,ENP}^2 \in [1/\rho_k,\ \rho_k]$, for any positive value of ρ_k, where ρ_k is a parameter that quantifies the size of the residual error value of the ratio between $\sigma_{k,SS}^2$ and $\sigma_{k,ENP}^2$. When $\rho_k = 1$, robust detection can be achieved. For $\rho_k \neq 1$, the robustness of detection cannot be achieved at SUs [1,2,5,6] in a low SNR regime. Therefore, a noise uncertainty problem may arise in the detection scheme. Even if the SU observes an infinite number of samples, the robustness of the detection cannot be guaranteed because of a phenomenon known as the SNR wall [5]. The SNR wall is defined as the minimum value of the SNR at which it is impossible to detect values below it, even when the number of observed samples approaches infinity.

In this chapter, for simplicity, we assume that the actual noise variance is identical across all bands, that is $\sigma^2_{k,n} = \sigma^2_n$. Therefore, the residual error is also the same across all the bands, which means $\rho_k = \rho$. In addition, the SNR of the PUs is assumed to be the same across all the bands so that $\gamma_k = \gamma$. All of these assumptions lead to a more tractable solution.

Note that even in the absence of an adversary, there will be missed detections of the busy bands owing to the residual error from estimating the noise power, the probability of which is $p_{MD} = 1 - \min_{\sigma^2_{k,SS}/\sigma^2_{k,ENP}\in[1/\rho,\rho]} p^{(k)}_{D,ED-} \quad = 1 - Q\left(\frac{K- \ (1+\gamma)/\rho}{(1+\gamma)/\rho\sqrt{\frac{M+N}{MN}}}\right) = \Phi\left(\frac{K- \ (1+\gamma)/\rho}{(1+\gamma)/\rho\sqrt{\frac{M+N}{MN}}}\right)$, where $\Phi(\cdot)$ is the cumulative distribution function of the standard normal distribution. For the remainder of this chapter, we express $p_{MD} = \Phi\left(\frac{K- \ (1+\gamma)/\rho}{(1+\gamma)/\rho\sqrt{\frac{M+N}{MN}}}\right)$.

2.2.3 Framework for Flipping Attacks:

We assume that the intelligent adversary knows the receiver structure, type of standard, sensing time, desired probability of false alarm of the SUs, p^{DES}_{FA}, and status of the U bands. Additionally, to ensure the adversary's goal of flipping as many bands as possible, we assume that all the U bands are ENP bands. ENP bands refer to the available free bands during the fine-SP mode. These U bands should be the same in number as the SUs, as seen in [30,31,41]. The adversary cannot precisely estimate/learn all of the aforementioned information that is assumed above. However, it is commonly assumed in the literature [30,31,32,33,41] that the adversary has full knowledge of at least some information. Therefore, the results of this chapter present a worst-case analysis and provide an upper bound for the SS disruption.

Note that the number of missed detections of busy bands is equivalent to the number of flipped bands. This occurs because a missed detection happens when the PU signal is not detected, which can be caused by inaccurate noise power estimation. When the adversary contaminates the estimated noise power, the band is flipped, resulting in it no longer being considered busy by the PU. Our main focus is on determining the average number of missed detections, denoted by B_f.

Lemma.1: Let us now define q_k as the probability of missed detection in the k^{th} band. In addition, let $B = \{1, 2, 3, \ldots, U\}$ be the set of bands available for sensing, and initially assume that all of them are busy when the SUs sense them in fast-SP mode (i.e., $|B_{busy}| = U$). Then, B_f can be expressed as the sum of the individual missed detection probabilities for each band, as shown below in (2.8):

$$B_f = \sum_{k=1}^{U} q_k \tag{2.8}$$

Proof: Let X_k $(k = 1, 2, \ldots, U)$ be a binary random variable, such that $X_k = 1$ indicates that the k^{th} band is successfully flipped to be free, and $X_k = 0$ indicates that the attempt to flip the k^{th} band was unsuccessful (i.e., sensed to be busy). Therefore, the expected value of the sum of X_k over all k values was the average number of missed detections.

$$B_f = E\{\sum_{k=1}^{U} X_k\} = \sum_{k=1}^{U} E\{X_k\} = \sum_{k=1}^{U} q_k \tag{2.9}$$

■

The objective of the adversary in the flipping attacks with a total power P_A, is to maximize the average number of missed detections of the SUs during the fast-SP mode, subject to the adversary contaminating the ENP bands during the fine-SP mode. Hence, we have the following optimization problem:

$$\max_{P_{k,A},\forall k\in\{1,..U\}} \quad \sum_{k=1}^{U} q_k, \tag{2.10}$$

$$s.t \;\; P_{k,A} \geq 0, \forall k \in \{1,..U\}, \sum_{k=1}^{U} P_{k,A} = P_A.$$

A defense strategy for SUs is to employ a more robust detector in the fine-SP mode. However, implementing this strategy comes at the cost of a longer sensing period, resulting in a reduced throughput.

2.3 Optimization of Flipping Attacks:

In this section, we analyze the optimal strategy for sensing link disruption under the assumption that both the number of ENP bands and the number of busy bands equals U, the total number of bands. We then consider a more realistic case, in which the number of ENP bands differs from the number of busy bands.

2.3.1 Optimal Sensing Disruption for Flipping Attacks:

As discussed earlier, from (2.7), we can directly determine that the flipping probability is equivalent to q_k, which can be shown to be

$$q_k = 1 - p_{D,ED-ENP}^{(k)} = \Phi\left(\frac{K - \frac{\sigma_{k,SS}^2}{\sigma_{k,ENP}^2}(1+\gamma)}{\frac{\sigma_{k,SS}^2}{\sigma_{k,ENP}^2}(1+\gamma)\sqrt{\frac{M+N}{MN}}}\right) = \Phi\left(\frac{K}{\frac{1}{\left(\frac{\alpha P_{k,A}}{\sigma_n^2}+\rho\right)}(1+\gamma)\sqrt{\frac{M+N}{MN}}} - \frac{1}{\sqrt{\frac{M+N}{MN}}}\right). \tag{2.11}$$

The spoofing probability p_k, from (2.6), can be expressed as,

$$p_k = p_{FA,ED-ENP}^{(k)} = Q\left(\frac{K - \frac{\sigma_{k,SS}^2}{\sigma_{k,ENP}^2}}{\frac{\sigma_{k,SS}^2}{\sigma_{k,ENP}^2}\sqrt{\frac{M+N}{MN}}}\right). \tag{2.12}$$

From (2.12), the adversary should increase $\sigma_{k,SS}^{2}$ to spoof free bands. In other words, the adversary should jam during the SP-fast mode, similar to the techniques described in [30,31,32]. It is evident that there exists a trade-off between spoofing and flipping attacks.

By substituting (2.11) into (2.10), we formulate the optimal sensing link disruption as follows:

$$\max_{P_{k,A},\forall k\in\{1,..U\}} \quad \sum_{k=1}^{U}\Phi\left(\frac{a}{\frac{1}{\left(P_{k,A}+\rho\right)}(1+\gamma)}+b\right), \tag{2.13}$$

$$s.t\ \ P_{k,A}\geq 0,\forall k\in\{1,..U\},\ \sum_{k=1}^{U}P_{k,A}=P_{A},$$

where $a\triangleq\frac{K}{\sqrt{\frac{M+N}{MN}}}$, and $b\triangleq\frac{-1}{\sqrt{\frac{M+N}{MN}}}$. The optimization problem in (2.13) is convex, because the objective and inequality constraints are both convex [42]. Using the Karush–Kuhn–Tucker (KKT) conditions, the optimal power flipping allocation of (2.12) yields the following solution:

$$P_{k,A}^{*}=\begin{cases}\frac{P_{A}}{u}, & k\in\varphi_{\mathrm{A}}\\ 0, & otherwise\end{cases}, \tag{2.14}$$

where $\varphi_{\mathrm{A}}\triangleq\left\{k\mid\lambda_{k}^{*}=0,P_{k,A}^{*}>0\right\}$ are the flipped bands caused by the adversary's flipping power, and λ_{k}^{*} is the Lagrangian multiplier. Note that u is the number of flipped bands (See Appendix A.1).

The technique described in (2.14) is known as uniform power allocation and is widely employed, as seen in previous works [29,30,31]. However, the key distinction lies in the result of the approach, which involves flipping the busy band, whereas the other techniques spoof the free bands. Additionally, in (2.14), from the adversary's point of view, equal flipping power allocation is optimal because the adversary is not aware of the system parameter values, in particular, a, b, γ, and ρ for each band.

2.3.2 Optimal Number of Flipping Bands:

The optimal number of flips in (2.14) is unclear. To see this, let the value of the objective function given in (2.13) for the optimal solution given in (2.14) as a function of u be as follows:

$$f(u) = (U-u)\,\Phi\left(\frac{a\,\rho}{(1+\gamma)} + b\right) + u\,\Phi\left(\frac{a\left(\frac{\alpha P_A}{u\,\sigma_n^2}+\rho\right)}{(1+\gamma)} + b\right). \tag{2.15}$$

Then, the terms in (2.15) can be interpreted as the probability of a missed detection in each band, multiplied by the number of occurrences of each. This probability is enhanced by the inaccuracy of the noise power estimate and/or the presence of an adversary. We now replace u with the real continuous variable x (i.e., $x \in \mathbb{R}^+$). The extreme-value theorem in [43] states if $f(x)$ is continuous on a closed interval $[1, U]$, it must hit its maximum and minimum on that interval. To find the extreme point x^*, we solve $f'(x) = 0$. Thus, the optimal number of flipped bands u^*, is $\lfloor x^* \rfloor$ or $\lceil x^* \rceil$. The derivative of $f(x)$ is given by (2.16):

$$f'(x) = \Phi\left(\frac{a\left(\alpha\frac{P_A}{\sigma_n^2}\right)}{(1+\gamma)\,x} + \frac{a\rho}{(1+\gamma)} + b\right) - p_{MD} - \frac{a\left(\alpha\frac{P_A}{\sigma_n^2}\right)}{(1+\gamma)\,x\,\sqrt{2\pi}}\,e^{-\frac{1}{2}\left(\frac{a\left(\alpha\frac{P_A}{\sigma_n^2}\right)}{(1+\gamma)\,x} + \frac{a\rho}{(1+\gamma)} + b\right)^2}. \tag{2.16}$$

Note that setting $f'(x) = 0$, results in a nonlinear equation, which means that the expression x^* cannot be derived directly. However, the result in Appendix A.2 shows that $f'(x) > 0,\ for\ 0 \leq x < \infty$ (i.e., $f(x)$ continuously increases as x increases for $x > 0$). In other words, when the number of flipped bands increases, the average number of missed detections also increases. Note that, while the adversary attacks the ENP bands during the fine-SP mode, the consequence of flipping busy bands is observed during the fast-SP mode. Previously, it was assumed that ENP and busy bands were the same as the total number of bands. Because this will not always be the case, we now evaluate the case in which $|B_{ENP}|$ and $|B_{busy}|$ are different. As a result, x^* is upper bounded by $|B_{ENP}|$ or $|B_{busy}|$, depending on which of them is smaller. This can be expressed as follows:

-When $|B_{ENP}| \geq |B_{busy}|$, then x^* is upper bounded by $|B_{busy}|$, because it is impossible to flip more than number of busy bands, regardless of how many bands the adversary attacks. If P_A is sufficiently large to contaminate all ENP bands (i.e., $P^*_{k,A} \leq P_A \,/\, |B_{busy}|$), the optimal strategy is full-band flipping. That is, the flipping power is identically distributed and can be expressed as:

$$f(x^*)|_{x^*=|B_{busy}|} = |B_{busy}|\Phi\left(\frac{a\left(\frac{\alpha P_A}{|B_{busy}|}+\rho\right)}{1+\gamma} + b\right). \qquad (2.17)$$

However, if the number of busy bands increase, the result is flipping a portion of the busy bands (i.e., partial-band flipping). This case can be mathematically expressed as follows:

$$f(x^*)|_{x^*<|B_{busy}|} = x^*\Phi\left(\frac{a\left(\frac{\alpha P_A}{\sigma_n^2 x^*}+\rho\right)}{1+\gamma} + b\right) + \left(|B_{busy}| - x^*\right)p_{MD}. \qquad (2.18)$$

-When $|B_{ENP}| < |B_{busy}|$, the adversary's goal is to flip all busy bands, but this cannot be done because the adversary cannot contaminate more than the ENP bands. Thus, x^* cannot be greater than $|B_{ENP}|$, which shows that the attack strategy is partial-band flipping. From Appendix A.2, $f(x)$ continuously increases as x increases for $x \geq 0$; thus, the maximum of $f(x)$ is achieved when $x^* = |B_{ENP}|$, as shown below:

$$f(x) = |B_{ENP}|\Phi\left(\frac{a\left(\frac{\alpha\,P_A}{\sigma_n^2|B_{ENP}|}+\rho\right)}{(1+\gamma)} + b\right) + \left(|B_{busy}| - |B_{ENP}|\right) p_{MD}. \qquad (2.19)$$

Based on the analysis provided, we can conclude that it is impossible for SUs to be flipped more than the number of busy bands, whereas the adversary cannot contaminate more than the number of ENP bands. Therefore, the maximum average number of missed detections B_f, is given by

$$B_f = u^*\,\Phi\left(\frac{a\left(\frac{(\,\alpha\,P_A/\sigma_n^2)}{u^*}+\rho\right)}{(1+\gamma)} + b\right) + \left(|B_{busy}| - u^*\right) p_{MD}. \qquad (2.20)$$

Overall, the ratio $\frac{(\,\alpha\,P_A/\sigma_n^2)}{u^*}$ in (2.20) plays an important role in the optimal strategy for sensing link disruption. Furthermore, with sufficiently large adversary power, full-band flipping is optimal, as long as $|B_{ENP}| \geq |B_{busy}|$. Otherwise, the partial-band flipping is optimal.

2.3.3 Average Number of Missed Detection due to the Adversary Presence:

In the absence of an adversary (i.e., $u^* = 0$), the average number of missed detections in (2.20), caused by the residual error from estimating the noise power, is equals to $|B_{busy}|p_{MD}$. To demonstrate the effect of flipping attacks dominated by the adversary, we define the average number of missed detections primarily because of the presence of the adversary as

$$\Delta B_f = B_f - |B_{busy}|p_{MD}. \qquad (2.21)$$

When we substitute B_f in (2.20) into (2.21), we have

$$\Delta B_f = u^* \left(\Phi\left(\frac{a\left(\frac{P_A}{u^*} + \rho\sigma_n^2/\alpha\right)}{\sigma_n^2/\alpha(1+\gamma)} + b \right) - p_{MD} \right). \tag{2.22}$$

Here, in the case of partial-band flipping, ΔB_f is proportional to the adversary power, P_A, and can be expressed as:

$$\Delta B_f = \frac{a\, P_A}{(1+\gamma)\sigma_n^2/\alpha\ \sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{a\left(c^* + \rho\sigma_n^2/\alpha\right)}{\sigma_n^2/\alpha\,(1+\gamma)} + b\right)^2}. \tag{2.23}$$

To illustrate the intuition behind (2.23), consider (2.16) and define $c^* = P_A/x^*$. This allows us to express the derivative of the function $f'(x^*)$ as:

$$f'(x^*) = \Phi\left(\frac{a\left(c^* + \frac{\rho\sigma_n^2}{\alpha}\right)}{\frac{\sigma_n^2}{\alpha(1+\gamma)}} + b \right) - p_{MD} - \frac{a\, c^*}{(1+\gamma)\sigma_n^2/\alpha\,\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{a\left(c^* + \rho\sigma_n^2/\alpha\right)}{(1+\gamma)\sigma_n^2/\alpha} + b\right)^2}. \tag{2.24}$$

If at $f'(x^*) = 0$, then (2.24) can be simplified as:

$$\Phi\left(\frac{a\left(c^* + \rho\sigma_n^2/\alpha\right)}{\sigma_n^2/\alpha(1+\gamma)} + b \right) - p_{MD} = \frac{(a\, c^*) e^{-\frac{1}{2}\left(\frac{a\left(c^* + \frac{\rho\sigma_n^2}{\alpha}\right)}{\frac{(1+\gamma)\sigma_n^2}{\alpha}} + b\right)^2}}{\frac{(1+\gamma)\sigma_n^2}{\alpha}\sqrt{2\pi}}. \tag{2.25}$$

In (2.25), when $N, M, \gamma, \rho, \alpha, \sigma_n^2$, and p_{FA}^{DES} are fixed, then $c^*$is determined. Moreover, the optimal flipping power required for each of the flipping bands mentioned in the previous section is equivalent to c^*. Recall that $\lfloor x^* \rfloor$ or $\lceil x^* \rceil$ is equal to u^*, a positive finite number that can be expressed as, $u^* = P_A/c^*$. Finally, substituting (2.25) into (2.22), we obtain:

$$\Delta B_f = P_A/c^* \left(\frac{a\, c^*}{(1+\gamma)\sigma_n^2/\alpha\, \sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{a\left(c^* + \rho\sigma_n^2/\alpha\right)}{(1+\gamma)\sigma_n^2/\alpha} + b\right)^2} \right)$$

$$= \frac{a\, P_A}{(1+\gamma)\sigma_n^2/\alpha\, \sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{a(c^* + \rho\sigma_n^2/\alpha)}{(1+\gamma)\, \sigma_n^2/\alpha} + b\right)^2} . \tag{2.26}$$

Table 2.1: Main Notations for Chapter 2.

U	Total number of bands.	B_f	Average number of flipped bands.
M	Number of samples during fine-SP.	ΔB_f	Average number of flipped bands due to the Adversary.
N	Number of samples during fast-SP.	$\lvert B_{busy} \rvert$	Number of busy bands during fast-SP.
$\sigma_{k,ENP}^2$	Noise power during fine-SP mode on the k^{th} band.	$\lvert B_{ENP} \rvert$	Number of ENP bands during fine-SP.
$\hat{\sigma}_{k,A}^2$	Estimated noise power on the k^{th} band.	$\sigma_{k,SS}^2$	Noise power during fast-SP mode on the k^{th} band.
P_A	Total flipping power	$P_{k,A}$	Power flipping allocation on the k^{th} band.
σ_n^2	Noise Variance (true value).	γ	SNR of the PU.
ρ	Residual error parameter from estimating $\hat{\sigma}_{k,A}^2$.	α	Path Loss factor
q_k	Flipping probability on the k^{th} band.	p_k	Spoofing probability on the k^{th} band.
u	Number of flipped bands	K	Threshold.

In conclusion, for the case $|B_{ENP}| > |B_{busy}|$, the adversary will not utilize more power than c^* in each ENP band. If the adversary has excess power, it would look for more ENP bands to contaminate until all the ENP bands are contaminated. In the other case, when $|B_{ENP}| < |B_{busy}|$, according to the discussion in Section III-B, the optimal number of flipped bands cannot be greater than $|B_{ENP}|$. Even when the adversary increases the flipping power, there are no additional contaminated ENP bands.

2.4 Numerical Results:

In this section, the optimal sensing disruption technique is demonstrated through numerical simulations. The adversary performs equal power flipping across the ENP bands because there is no knowledge of the system parameters such as N, M, γ, p_{FA}^{DES}, and ρ. We employed equal power flipping with varying system parameter values to evaluate flipping optimization. Without loss of generality, we assume that $\sigma_n^2 = 1$ and $\alpha = 1$. Finally, it is desirable to compare flipping attacks with existing sensing disruptions.

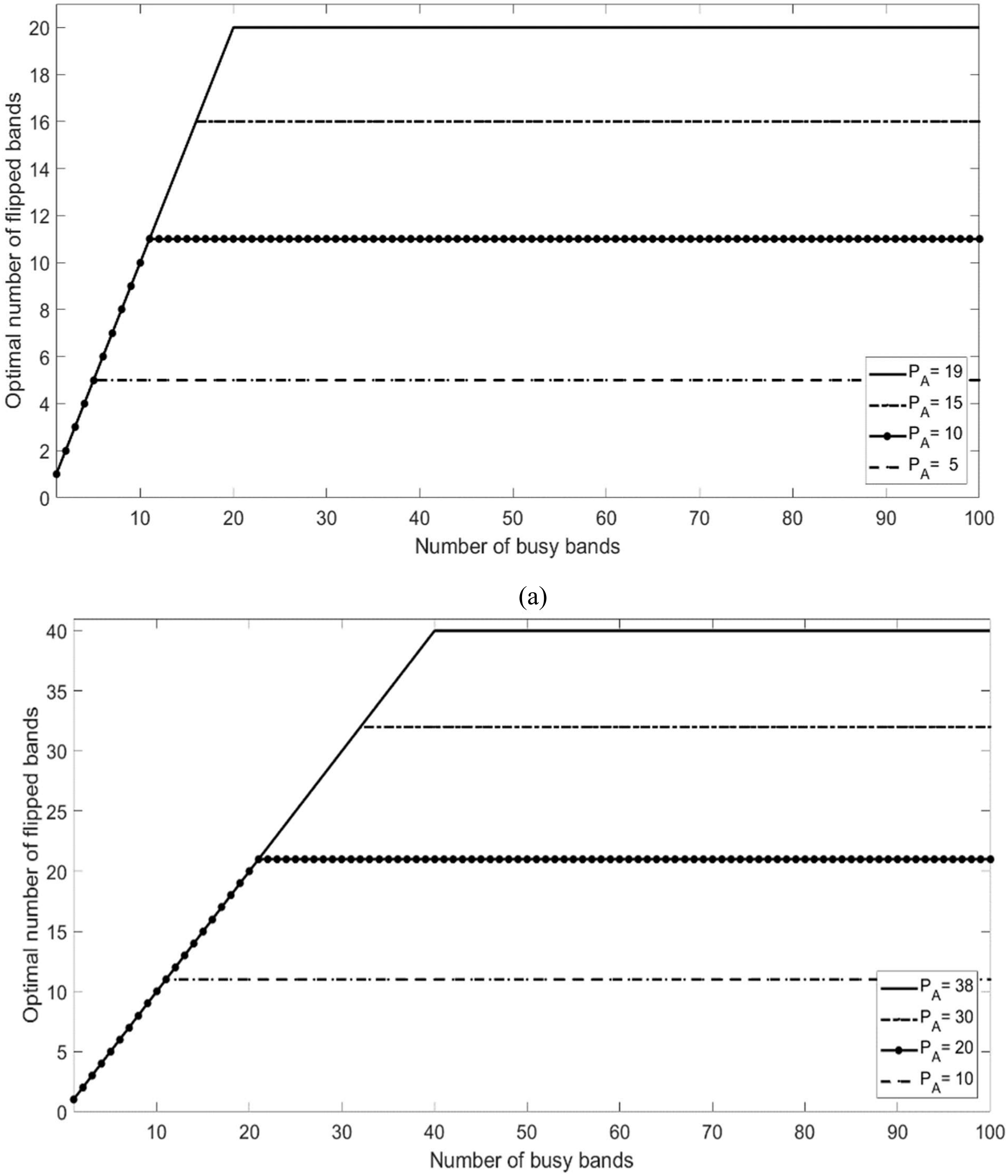
2.4.1 Optimal Number of Flipped bands u^*:

We demonstrate how the optimal number of flipped bands, u^*, varies with $|B_{busy}|$ for different values of $|B_{ENP}|$, γ, and P_A. Figure 2.3 shows u^* versus $|B_{busy}|$, where the curves are parameterized by P_A for various ENP bands. The remaining system parameters are set as follows: $p_{FA}^{DES} = 0.05$, $\rho = 1$, $N = 100$ and $M = 10N$. In Figure 2.3, each curve exhibits a knee, that shows a shift from full-band flipping to partial- band flipping. The region to the left of the knee indicates that u^*equals the number of busy bands. As discussed in Section III, if the number of ENP bands is greater than the number of busy bands, and the adversary has sufficient power to contaminate the ENP measurements of the available SUs, the optimal strategy is to flip all busy bands. To the right of the knee, we have $|B_{busy}| > |B_{ENP}|$; thus, $u^*$is upper bounded by $|B_{ENP}|$, and even if the flipping power increases, the adversary cannot contaminate more than the number of ENP bands. Thus, the optimal flipping strategy is partial-band flipping. In the second case, the partial-band flipping region occurs when $|B_{ENP}| > |B_{busy}|$, but P_A is not sufficiently large to contaminate all available ENP bands. Thus, the optimal flipping strategy is to flip a fraction of busy bands. With the same setup as in Figure 2.3, Figure 2.4 shows that γ of the PUs' signals plays an important role in degrading u^*, regardless of the number of bands that the adversary attacks. Comparing Figure 2.4(b) with Figure 2.4(a) for the same values of u^*,and $|B_{ENP}|$, we see that Figure 2.4(a) utilizes a smaller value of P_A than Figure 2.4(b) to flip the same number of busy bands. This is because γ in Figure 2.4(a) was lower than that in Figure 2.4(b). Finally, each curve exhibits a knee, which is determined by $|B_{ENP}|$ and $|B_{busy}|$.

2.4.2 The effect of System Parameters:

In Figure 2.5, Figure 2.6, and Figure 2.7, we operate in the region to the right of the knee of Figure 2.3, which means that the optimal strategy for the adversary is partial-band flipping. In particular, we operate in the region where $|B_{ENP}| > |B_{busy}|$. In these figures, u^* is plotted versus P_A, with different system parameter setup values. From Appendix A.2, it is clear that u^*increases as P_A increases, up to the point where all ENP bands are contaminated.

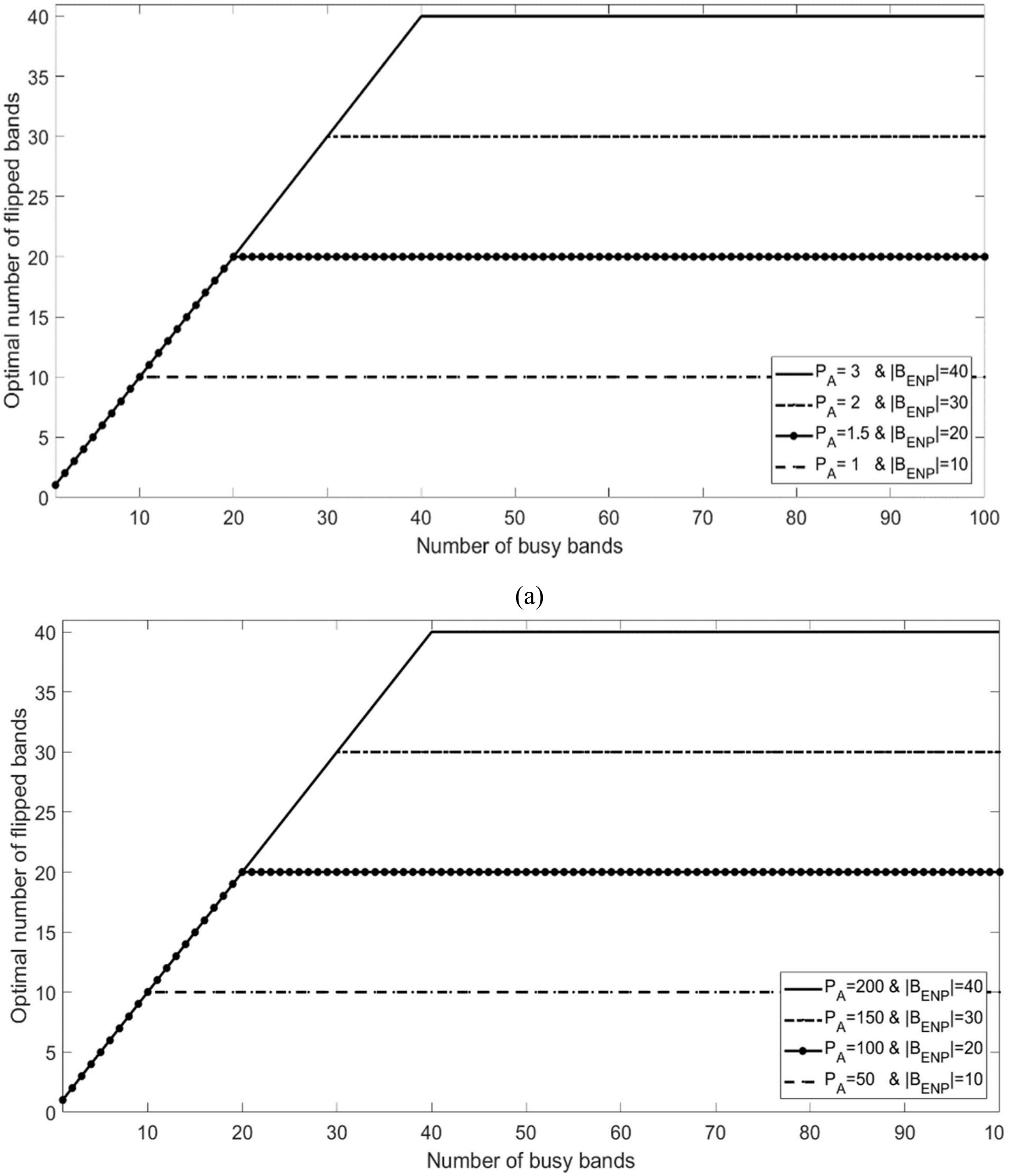
In Figure 2.5, we set $N = 100$; $M = 10N$ and $\rho = 1$, and plot u^* for different values of γ, as well as different values of the desired probability of false alarm p_{FA}^{DES}. Note that each value of p_{FA}^{DES} corresponds to a different threshold value. Figure 2.5 (a) shows that when $\gamma = 0\ dB$, u^*increases as P_A increases. This is reasonable, because increasing the flipping power implies attacking more ENP bands. As a result of γ increasing, u^* significantly decreases, as shown in Figure 2.5 (b). In both Figure 2.5 (a) and Figure 2.5 (b), if p_{FA}^{DES} decreases, then the adversary can utilize less power for flipping over the same $|B_{ENP}|$, resulting in flipping more of the busy bands. The reason is that the threshold, K, increases, so that it is harder to detect the busy bands.



(a)

(b)

Figure 2.3: Optimal number of flipped bands u^* versus the number of busy bands $|B_{busy}|$: (a) $|B_{ENP}| = 20$. (b) $|B_{ENP}| = 40$.



(a)

(b)

Figure 2.4: Optimal number of flipped bands u^* versus the number of busy bands $|B_{busy}|$:(a) $\gamma = -3dB$. (b) $\gamma = 3dB$.

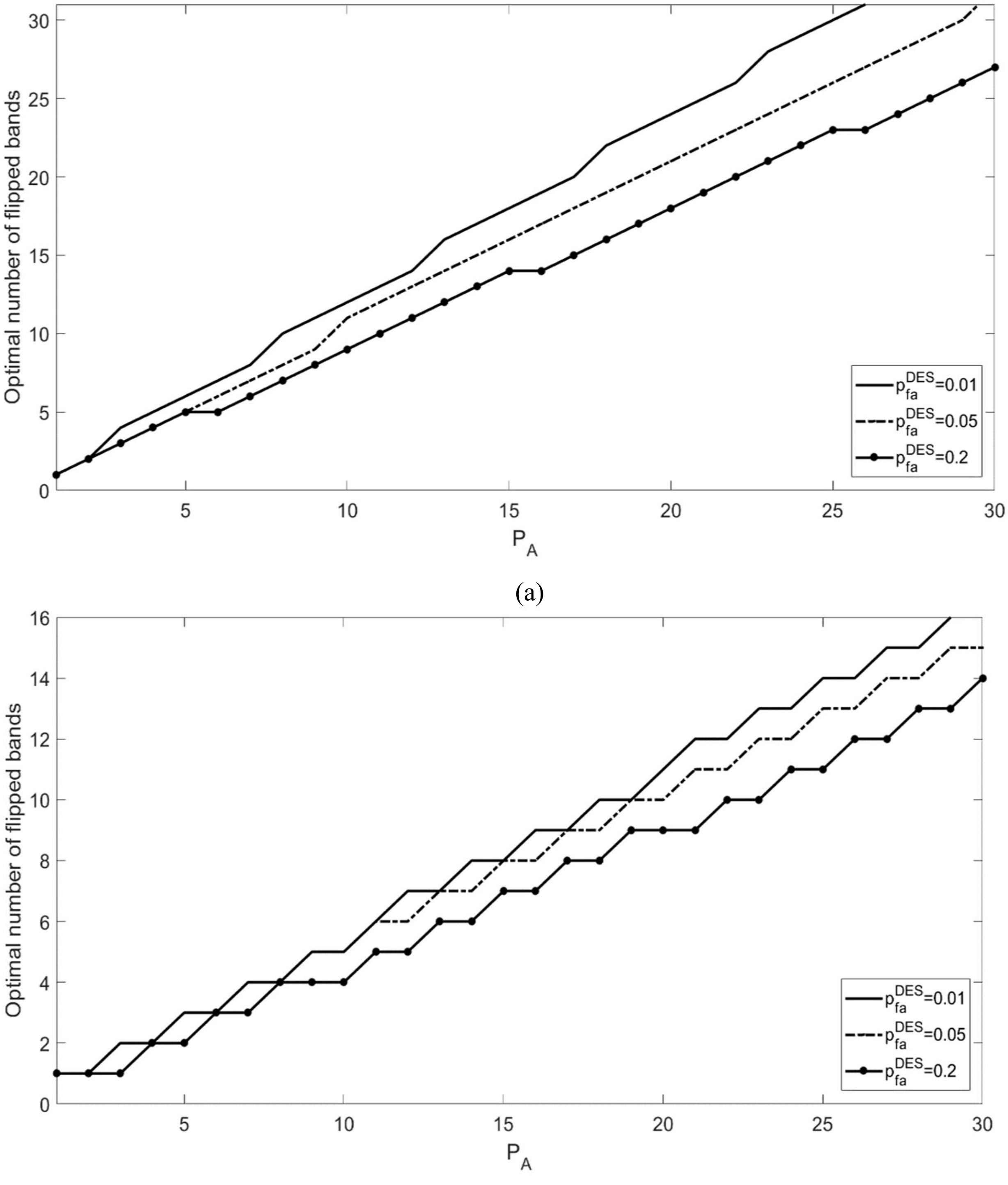
As shown in Figures 2.6(a) and 2.6(b), we plot u^* for different values of N and M, but we set $p_{FA}^{DES} = 0.05, \gamma = 0dB$, and $\rho = 1$. The results show that u^* increased as N decreased, as seen in Figure 2.6 (a). This is because the more samples the SUs observe during fast-SP, the more correct the decisions the SU makes regarding the busy bands. In contrast, Figure 2.6 (b) shows that as M increases, u^* also increased. This is because an increase in M implies that the SUs estimate the contaminated noise power more effectively.

In Figures 2.7 (a) and 2.7 (b), u^* is plotted for different values of γ and ρ, with the other parameters set as follows: $p_{FA}^{DES} = 0.05$, $N = 100$ and $M = 10N$. Clearly, u^* increases when ρ increases because robust detection can no longer be guaranteed at the SUs, as shown in both Figure 2.7 (a) and Figure 2.7 (b). However, if γ increases, as shown in Figure 2.7 (b), u^* decreases compared to Figure 2.7 (a) because the SNR of the PU increases; thus, the SUs can better detect the busy bands.

In conclusion, the optimal number of flipped bands is affected by $p_{FA}^{DES}, N, M, \gamma$, and ρ. This implies that the optimal flipping power allocation is also affected by these parameters, because $P_{k,A}^* = P_A/u^*$.

2.4.3 Average Number of Missed Detections B_f :

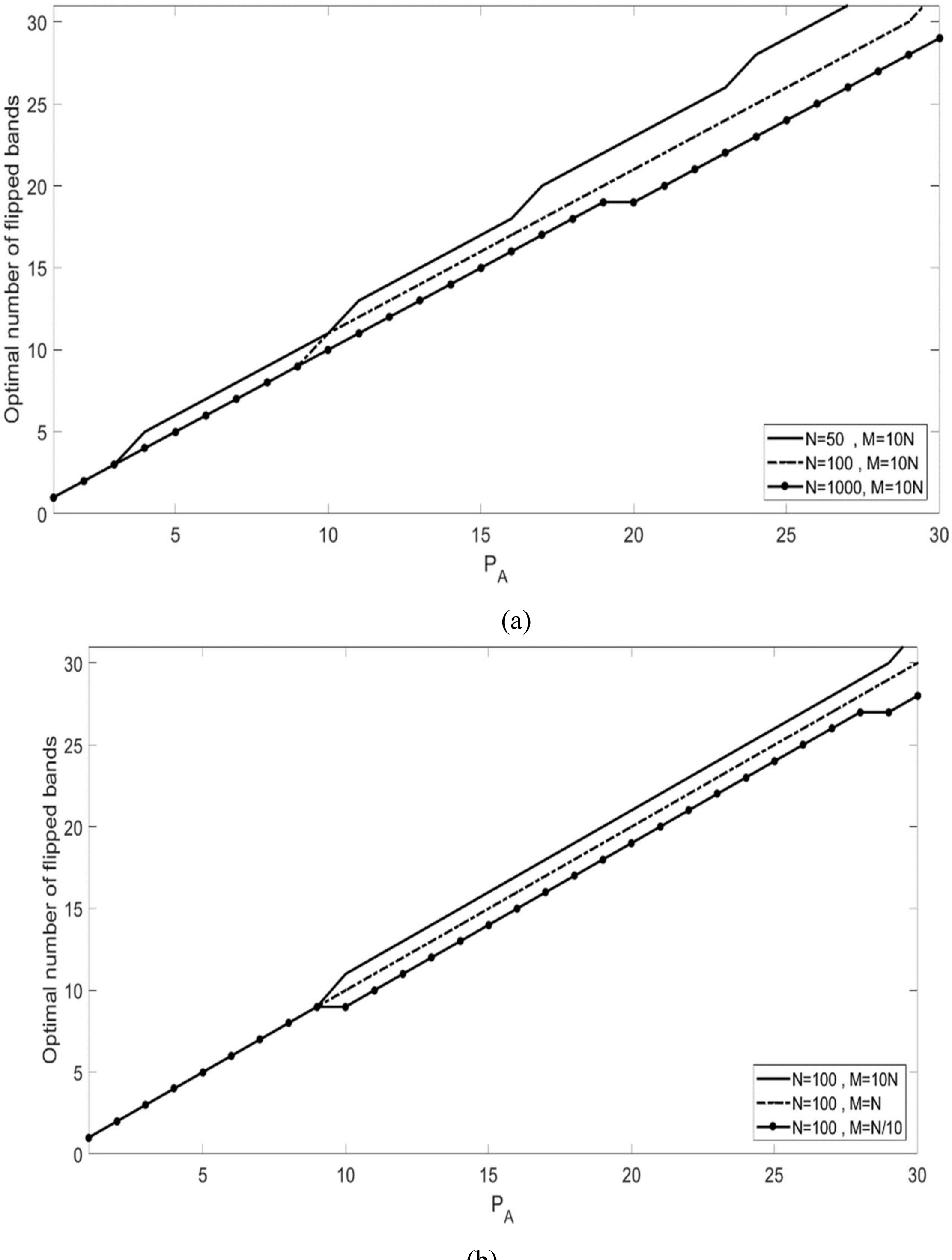
Figure 2.8 shows the plots of B_f versus $|B_{busy}|$, where the curves are parameterized by ρ. In Figure 2.8 (a) $P_A = 10$, and in Figure 2.8 (b)$P_A = 38$. The other parameters were set to $N = 100$, $M = 10N$, $p_{FA}^{DES} = 0.05$ and $\gamma = 0$ dB. The interpretation of each knee in the curves in Figure 2.8 is that full- band flipping becomes partial-band flipping, for the same reasons as those in Figure 2.3. As shown in Figure 2.8, when the slope of the curve is 45^o, we are in the full-band



(a)

(b)

Figure 2.5: Optimal number of flipped bands u^*versus P_A: (a) $\gamma = 0dB$ (b) $\gamma = 3dB$.



(a)

(b)

Figure 2.6: Optimal number of flipped bands u^*versus P_A for different values of: (a) N (b) M.

.

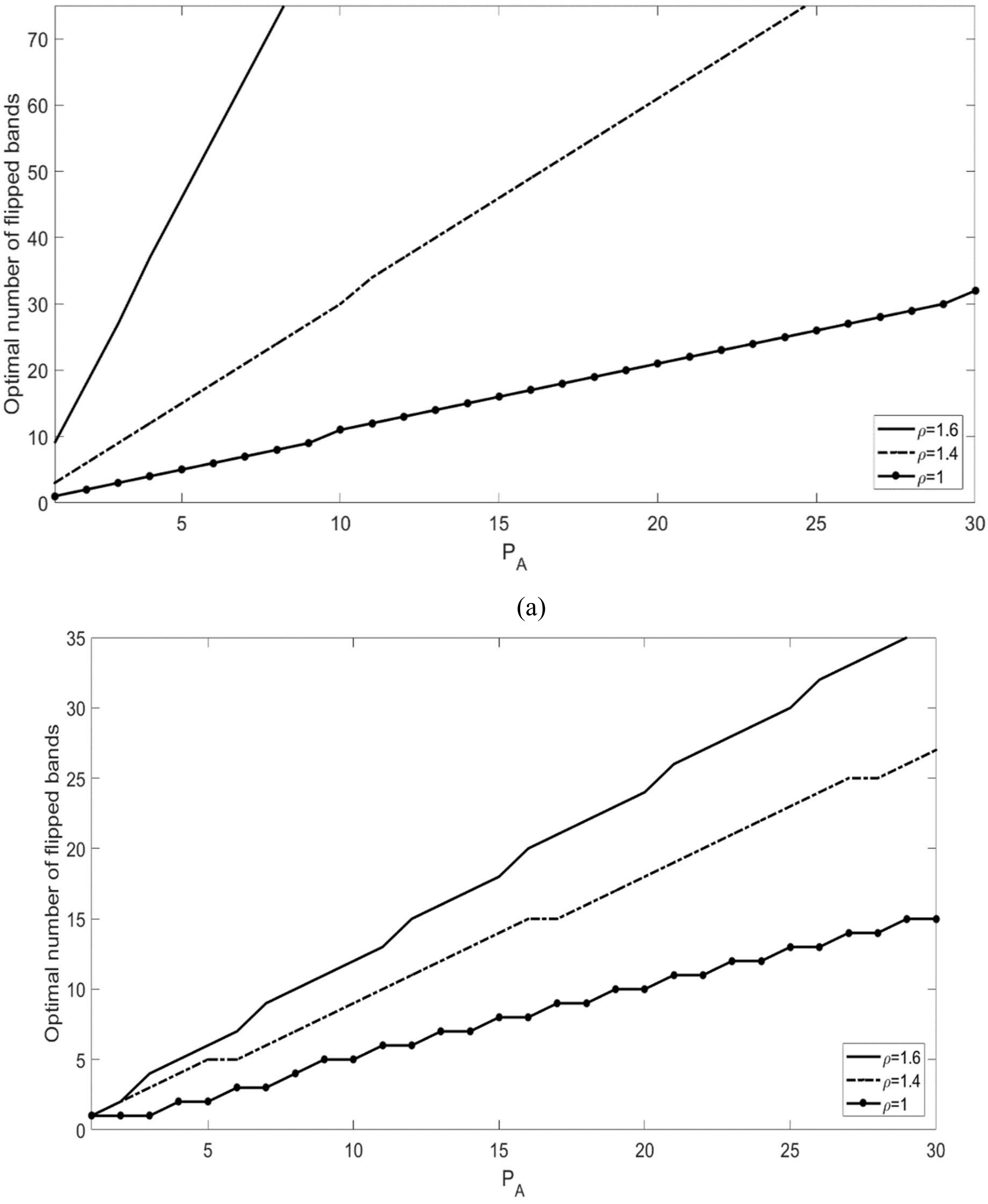
flipping region (i.e., $u^* = |B_{busy}|$). In this region, the missed detections of the busy bands are owing to both the presence of the adversary and $\rho \neq 1$, as shown in (2.20). When the slope of B_f

flipping region (i.e., $u^* = |B_{busy}|$). In this region, the missed detections of the busy bands are owing to both the presence of the adversary and $\rho \neq 1$, as shown in (2.20). When the slope of B_f

is determined only by p_{MD}, the slope only increases linearly with ρ. It should be noted that Figure 2.8 (b) has a larger full-band region than Figure 2.8 (a). This is because the adversary increases P_A to contaminate all the available ENP bands.

2.4.4 Average Number of Missed Detections Primarily due to the Presence of the Adversary ΔB_f :

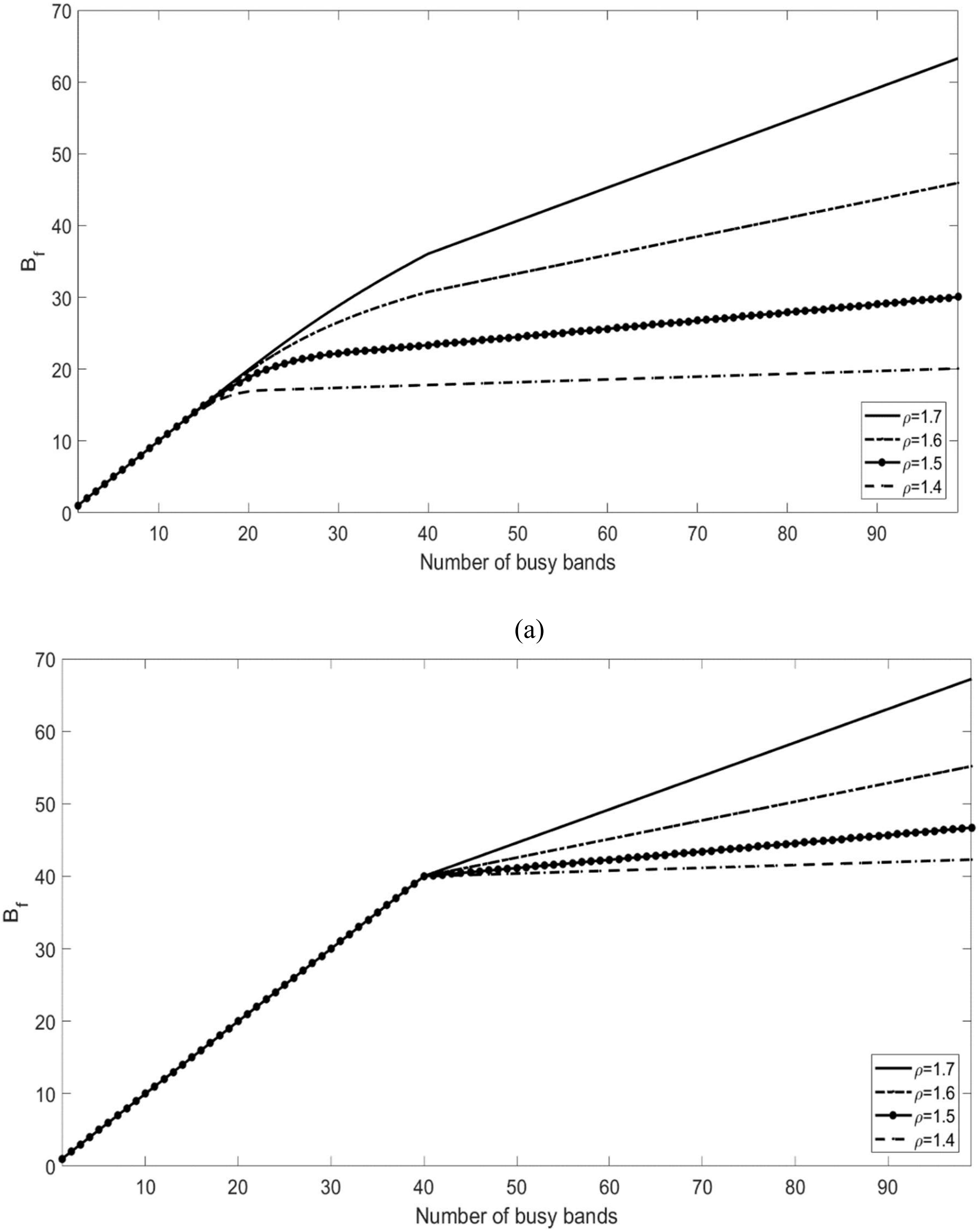
In Figure 2.9, ΔB_f is plotted for the case of $|B_{ENP}| \geq |B_{busy}|$. The remaining parameters were set as $N = 100$, $M = 10N$, $\gamma = 0\ dB$ and $\rho = 1$. The interpretation of each knee in the curves in Figure 2.9 is equivalent to that in Figure 2.3. The difference between Figure 2.8 and Figure 2.9 is in the value of ρ, which shows that in the partial-band region, ΔB_f in Figure 2.9 becomes constant when $|B_{busy}|$ increases, compared with B_f in Figure 2.8. Note that an increase in P_A, leads to an increase in ΔB_f, as discussed in Section III-C. A comparison between Figure 2.9(b) and Figure 2.9(a) shows that increasing p_{FA}^{DES} results in a decrease in K. For the same flipped power, ΔB_f is more significant in Figure 2.9 (b) than in Figure 2.9 (a). This provides an advantage to the adversary in spreading less flipping power over ENP bands. In Figure 2.10, ΔB_f is plotted against P_A, with $N = 100$, $M = 10N$, and various values of p_{FA}^{DES}, γ and ρ. Additionally, we operated in the partial-band region, particularly when $|B_{ENP}| \geq |B_{busy}|$.



(a)

(b)

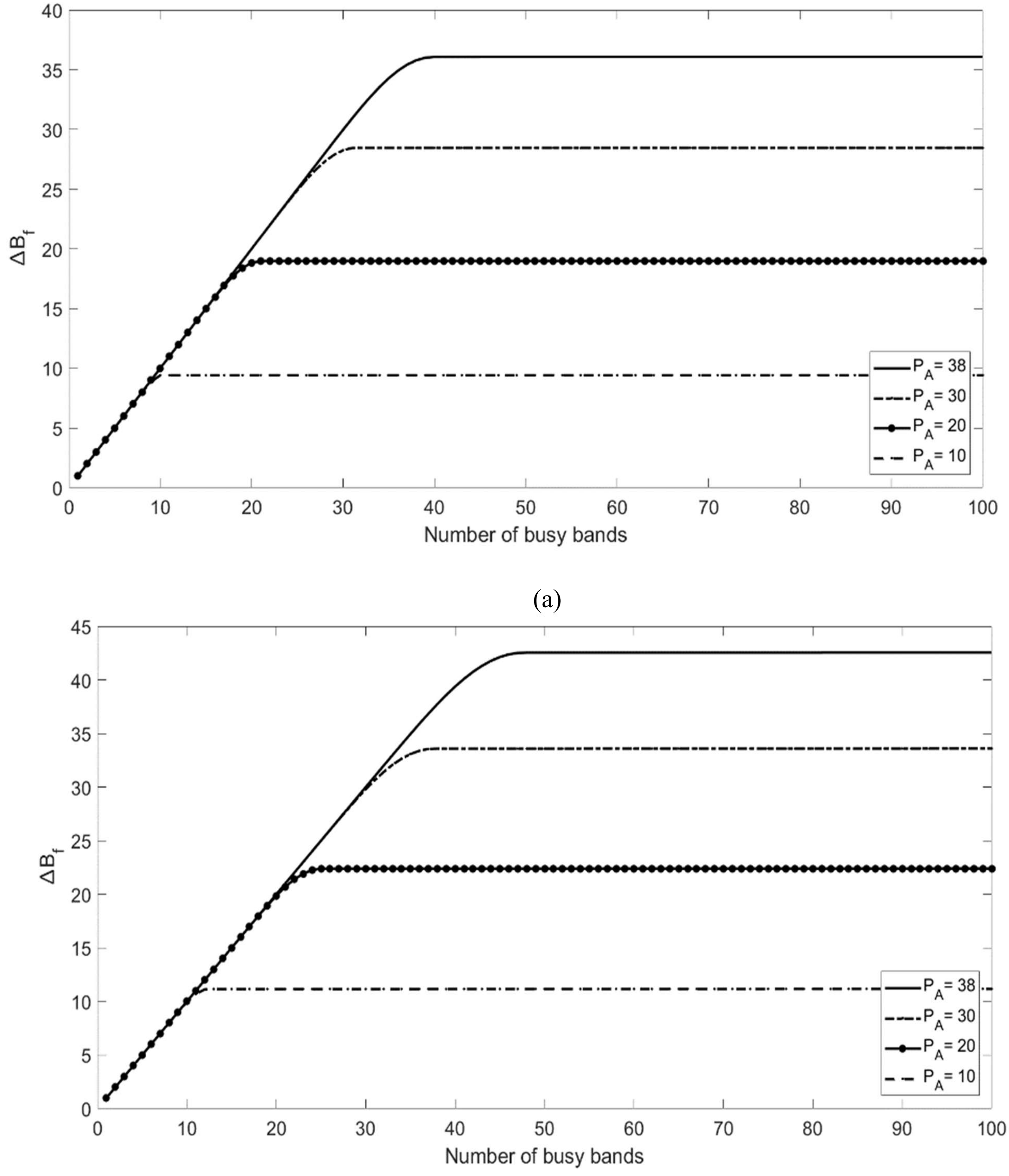
Figure 2.7: Optimal number of flipped bands u^*versus P_A: (a) $\gamma = 0dB$ (b) $\gamma = 3dB$.



(a)

(b)

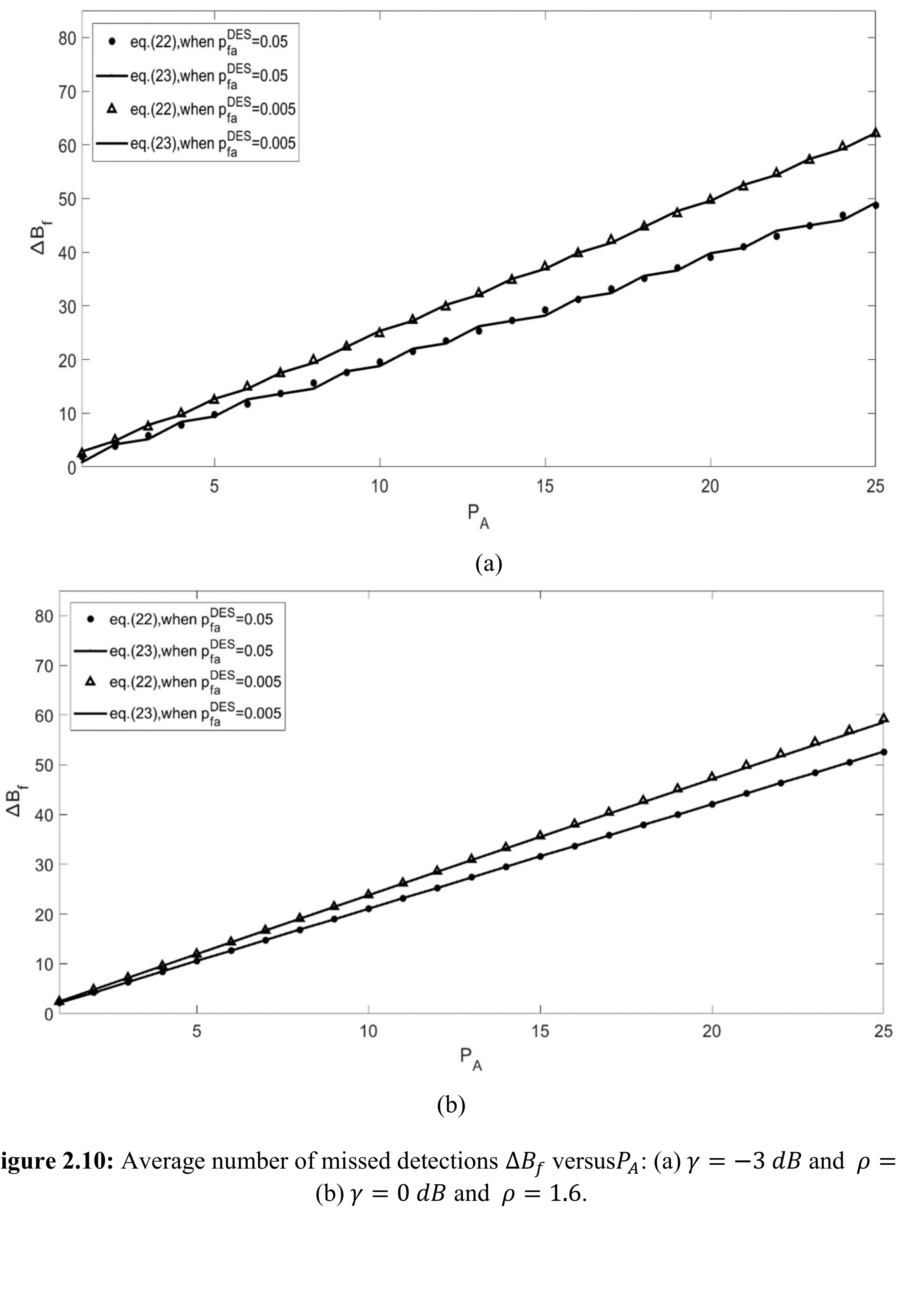
Figure 2.8:Average number of missed detections B_f versus the number of buys bands: (a)$P_A = 10$ (b) $P_A = 38$.



(a)

(b)

Figure 2.9: Average number of missed detections ΔB_f versus the number of buys bands: (a) $p_{FA}^{DES} = 0.05$ (b) $p_{FA}^{DES} = 0.005$.



(a)

(b)

Figure 2.10: Average number of missed detections ΔB_f versusP_A: (a) $\gamma = -3\ dB$ and $\rho = 1$ (b) $\gamma = 0\ dB$ and $\rho = 1.6$.

Figure 2.10 shows that ΔB_f linearly increases when the P_A increases. In addition, we can see that ΔB_f of (2.23) is consistent with (2.22), for both Figures 2.10 (a) and 2.10 (b).

2.5 Summary

In this chapter, we observed that increasing the flipping power allows the adversary to flip more bands, up to the point where all ENP bands are contaminated. Additionally, we observe that an increase in the threshold, ρ, or the number of samples during fine-SP (i.e., M) increases the chance of successful flipping attacks, while a decrease in the number of samples during fast-SP (i.e., N) also increases flipping attacks. Furthermore, we establish that for the given system parameters (ρ, N, M, and p_{FA}^{DES}), ΔB_f is proportional to flipping power.

2.6 Acknowledgements:

The text of this chapter is, in part, a reprint of the paper, T. Y. Alkhamees and L. B. Milstein, "A Different Approach for Sensing Disruption," in *IEEE Access*, vol. 11, pp. 86431-86443, 2023, doi: 10.1109/ACCESS.2023.3304244. The dissertation author is the primary researcher and author of this paper.

Chapter 3 :

Attacks Optimization of CR-NOMA

3.1 Introduction:

The imperfect CSI poses a challenge in evaluating the performance of CR-NOMA, as mentioned earlier. However, in general, the vulnerability of the CSI is studied in the literature, as in [25, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53]. In one type of attack, the pilot contamination attack (PCA), adversaries send a mimic pilot signal to mislead the base stations or access points. PCA has two main objectives: contaminating the channel estimation phase to enhance eavesdropping, as in [46, 47], or spoofing legitimate users, as outlined in [48, 49]. Zhou et al. [46] first introduced PCA within physical-layer security. Furthermore, [47] has examined PCA's impact on massive MIMO systems. The aim was to minimize the sum rate of downlink transmissions and affect secrecy performance.

Another type of attack, the pilot jamming attack (PJA), disrupts channel measurements by sending jamming signals during the estimation phase, as in [50] and [51]. Additionally, studies [52] and [53] combined PJA with jamming the data phase, resulting in minimized system performance.

The difference between PCA and PJA stems from their objectives, influenced by the system's security model and performance metrics. Additional details on pilot attacks and countermeasures are available in [25,44].

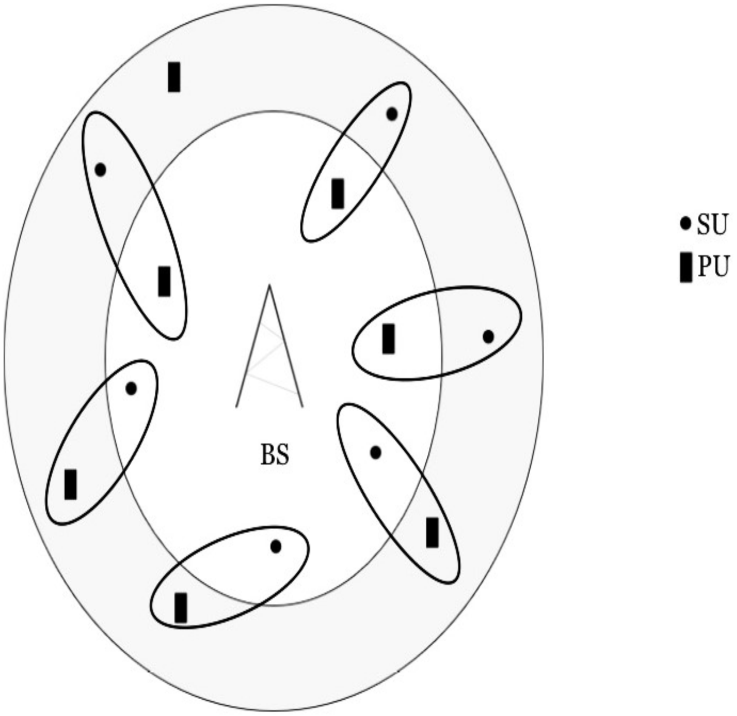


Figure 3.1: An illustration of MC CR-NOMA.

An adversary can also take advantage of pilot attacks to disrupt the CR-NOMA system. The adversary aims to cause a DoS to the SU. To complete the loop, the adversary needs to implement PJA because the adversary's goal is not to listen to users' messages or to impersonate the SUs, because no secrecy protocol is implemented in the system. Therefore, in this chapter, PJA in a CR-NOMA system can be a more effective attack than PCA.

Another motivation to discuss is that most of the current research on NOMA systems focuses on the mechanisms of possible attacks and proposed detection schemes to detect these attacks, without examining the optimal attack strategies. For example, in [25] and [54], the authors pointed out the possibility of a DoS attack or spoofing attacks if there is a large disruption of the PCA in different scenarios.

The primary focus of this study is to design an intelligent adversary attack that causes a DoS to multiple SUs. These are types of DoS attacks because the intelligent adversary desires to denial the SUs from utilizing the bands. DoS attacks destroy the main purposes of MC CR-NOMA, which include spectrum efficiency and massive connectivity [13,14].

The outline of this chapter is as follows: Section 3.2 presents the preliminaries and general formulation. The downlink outage performance is described in Section 3.3. The numerical results are presented in Section 3.4, and Section 3.5 summaries this chapter.

3.2 Preliminaries and General Formulation:

In this section, we discuss the framework of the communication model. Subsequently, we present assumptions regarding the knowledge available to an adversary, followed by an overview of the attack mechanism. Finally, we address the problem formulation related to DoS attacks.

3.2.1 Communication Model:

Consider a downlink MC CR-NOMA system with U clusters. In each of the U clusters, the PU and SU are grouped together to serve in the same frequency band (or subcarrier), following the NOMA principle [12,14], and different groups are allocated to different frequency bands [19], as shown in Figure 3.1. We also assume that the system employs time-domain duplexing (TDD).

Spectrum sharing in MC CR-NOMA is obtained by constraining the power allocated to the SU on each band (cluster), to meet the QoS of the PU [12,17]. This means that the BS needs to divide power allocation into two goals. The first is the PU’s reliable reception, and the second is the opportunistic transmission to the SU’s [15]. As result of that, the key advantage of CR-NOMA its ability to achieve a balance between throughput and fairness [14].

To perform CR-NOMA, the BS transmits a superimposed signal to both the SU and PU in the k^{th} cluster (i.e., band), as follows [13,15]:

$$x_k(n) = \sqrt{P_{k,T}}\left(a_{k,p}\ s_{k,p}(n) + a_{k,s}\ \ s_{k,s}(n)\right). \tag{3.1}$$

where $s_{k,p}(n)$and $s_{k,s}(n)$ denote the transmitted data signal from the BS to the PU and the SU in the k^{th} band, respectively. Also, the total transmitted power is denoted by $P_{k,T}$ at the k^{th} band. The terms $a_{k,p}^2$ and $a_{k,s}^2$correspond to the power allocation coefficients of the PU and the SU, respectively, with a constraint of $a_{k,p}^2\ + a_{k,s}^2 = 1$. For each cluster k, $\forall k = \{1, \dots, U\}$, and user i, $\forall i \in \{p, s\}$, that is either the PU or SU, respectively, the channel from the BS to the user is represented as $\underline{g}_{k,i} = \sqrt{\beta_{k,i}}\underline{h}_{k,i}$, where $\underline{h}_{k,i} \sim \mathcal{CN}(0,1\,)$, and $\beta_{k,i}$ denotes the large-scale fading expressed as $\beta_{k,i} = d_{k,i}^{-\alpha}$. Here, $d_{k,i}$ is the distance between the BS and user i at the cluster k. The parameter α represents the path loss exponent.

MC CR-NOMA [19] is a technique that aims to allocate power among users (i.e., PU and SU) within each band. This power allocation relies on the availability of the users' CSI at the BS. In other words, the BS needs to estimate the CSIs from all clusters and separate the pilot signals of each user in each cluster, whether it's a PU or SU. In order to guarantee that the BS gives higher priority to the PUs, as in [18] and [55]. The PUs in the cell must transmit a designated pilot signal to the BS. If we assume that the CSI of the i^{th} user in the k^{th} cluster is estimated at the BS, similar to [55], then from the orthogonality principle, the minimum mean square error (MMSE) estimate [37], denoted as, $\underline{\hat{h}}_{k,i}$ which has a distribution of, $\mathcal{CN}\left(0, 1 - \sigma_{\varepsilon_{k,i}}^2\right)$, where $\sigma_{\varepsilon_{k,i}}^2 = \sigma_{w_{BS}}^2/(\beta_{k,i} + \sigma_{w_{BS}}^2)$. The term $\sigma_{w_{BS}}^2$ is due to the thermal noise at the BS, which is distributed as $\sim \mathcal{CN}\left(0, \sigma_{w_{BS}}^2\right)$.

The intended received signal for users in the k^{th}band is shown in [20] with an imperfect channel estimate. Considering that NOMA is a special case of CR systems, as mentioned in [17], and assuming the channel reciprocity holds, similar to [18] and [55], then the intended received signals for the PU and SU can be expressed as follows, respectively:

$$\begin{aligned} y_{k,p}(n) &= g_{k,p}\, x_k(n) + w_{k,p}(n) \\ &= \left(\underline{\hat{h}}_{k,p} + \underline{\varepsilon}_{k,p}\right)\sqrt{\beta_{k,p}P_{k,T}}\left(a_{k,p}\, s_{k,p}(n) + a_{k,s}\, s_{k,s}(n)\right) + w_{k,p}(n), \end{aligned} \tag{3.2}$$

$$\begin{aligned} y_{k,s}(n) &= g_{k,s}\, x_k(n) + w_{k,s}(n) \\ &= \left(\underline{\hat{h}}_{k,s} + \underline{\varepsilon}_{k,s}\right)\sqrt{\beta_{k,s}P_{k,T}}\left(a_{k,p}\, s_{k,p}(n) + a_{k,s}\, s_{k,s}(n)\right) + w_{k,s}(n), \end{aligned} \tag{3.3}$$

where $w_i(n)$ is the received background noise sample at either the PU or SU, and each one is a zero-mean complex Gaussian with variance $\sigma^2_{w_{k,i}}$, for $i \in \{p, s\}$.

3.2.2 Attack Model:

In MC CR-NOMA, constructing PJAs for multiple clusters (i.e., users) appears to be a more practical and simple form of attack than PCAs. This is because a single adversary cannot simultaneously eavesdrop on multiple legitimate user messages. Moreover, there is always a possibility that an adversary cannot know exactly the pilot signal (sequence) of a legitimate user. Therefore, the adversary transmits a jamming signal during the channel estimation phase at the BS.

In this chapter, we assume that the adversary knows the total number of bands U, and the targeted SINR of users. We further assume that the adversary is synchronized with the user signal during channel estimation, which is a common assumption in pilot attacks [45,46,48,47,49,51,52,53]. In addition, we assume that the adversary has full knowledge of the distances between the BS and the users in accordance with pilot attacks, as in [45,46,48,49,51,52].

In practice, the adversary will not know the aforementioned information. However, it is widespread in electronic warfare literature (see [25,26,44,45]), to assume that the adversary has full knowledge of at least some information, and this allows the adversary to inflict worst-case performance. Therefore, this chapter emphasized worst-case analysis, which is an upper bound for the spectrum sharing disruption. Note that the worst-case analysis is from the perspective of legitimate users (i.e., SUs), whereas it is considered optimal jamming on the side of the adversary (i.e., intentional interference).

The authors of [20] indicated that the parameter $\sigma^2_{\varepsilon_{k,p}}$, defined in the previous subsection, indicates the quality of channel estimation. Based on this, the adversary's goal of degrading the quality of the channel estimate implies that the adversary needs to increase $\sigma^2_{\varepsilon_{k,p}}$. The channel estimate of the k^{th} PU is a modified result from the previous subsection to include the adversary, as shown below:

$$\underline{h}_{k,p} = \underbrace{\underline{\hat{h}}_{k,p}}_{estimated\ chann\quad coefficient} + \overbrace{\underline{\varepsilon}_{k,p} + \underline{g}_{k,A}\, z_{k,A}}^{effective\ nosie}, \tag{3.4}$$

where the channel coefficient from the adversary-to-BS is assumed to have a Rayleigh distribution. This means that $\underline{g}_{k,A} = \sqrt{\beta_{k,A}}\,\underline{h}_{k,A}$, where $\underline{h}_{k,A} \sim \mathcal{CN}\ (0,1)$, and $\beta_{k,A} = d_{k,A}^{-\alpha}$. Finally, $d_{k,A}$ denotes as the distance between the BS and the adversary. Note that $\underline{\varepsilon}_{k,p}$ is still the error term, which is modeled as a complex Gaussian random variable distributed as in [20].

From [56], for a given Gaussian channel and Gaussian target signal, the worst-case jamming scenario occurs when a Gaussian signal is transmitted. To accomplish this, the adversary must transmit a complex Gaussian signal on the k^{th} band distributed as $\underline{z}_{k,A} \sim \mathcal{CN}\big(0, P_{k,A}\big)$, where $P_{k,A}$ is the adversary power in the k^{th} band. The adversary signal is assumed to be independent of both $\underline{\varepsilon}_{k,p}$ and $\underline{h}_{k,p}$. It is also assumed that the adversary signal is independent of $\underline{h}_{k,A}$. Conditioned on $\underline{h}_{k,A}$, we apply the linear MMSE principle [37]. Therefore, the variance is obtained by modifying the variance from the previous subsection 3.2.1 to include the adversary and is given by

$$var(\underline{\hat{h}}_{k,p}) = var(\underline{h}_{k,p}) - var\left(\underline{\varepsilon}_{k,p} + \sqrt{\frac{\beta_{k,A}}{\beta_{k,p}}}\, \underline{h}_{k,A}\, \underline{z}_{k,A}\right)$$

$$= 1 - \overbrace{\left(\frac{(\sigma_{wBS}^2 + \beta_{k,\,A}\ |\underline{h}_{k,A}|^2 P_{k,A})}{\beta_{k,p} + (\sigma_{wBS}^2 + \beta_{k,\,A}\ |\underline{h}_{k,A}|^2 P_{k,A})}\right)}^{\sigma_{\varepsilon_{k,pA}}^2}. \tag{3.5}$$

3.2.3 Problem Formulation:

In the context of MC CR-NOMA, to launch DoS attacks on the SUs within each band means that the PUs will only use those bands. To achieve this, the adversary aims to influence the BS to allocate most of the transmitted power in the k^{th} cluster (i.e., band) solely for the PU's (i.e., $a_{k,s}^2 = 0$). This can be illustrated by the expression for the outage probability of the SU. Consider the single-carrier CR-NOMA case as an example, which can be obtained from [17] as follows:

$$\mathbb{P}_{out,SU}^{(k)} = Pr\left\{\left(a_{k,s}^2 = 0\right) \cup \left(\underline{\gamma}_{k,s} < \theta_{k,SU}, a_{k,s}^2 \neq 0\right)\right\}$$

$$= Pr\left\{a_{k,s}^2 = 0\right\} + Pr\left\{\underline{\gamma}_{k,s} < \theta_{k,SU}, a_{k,s}^2 \neq 0\right\}, \tag{3.6}$$

where $\underline{\gamma}_{k,s}$ is the instantaneous SINR of the SU in the k^{th} band. In (3.6), $\theta_{k,SU}$ is the SU's targeted SINR in the k^{th} band. An outage event at the SU is defined as the union of two events. Two scenarios can describe these events. The first scenario is that sufficient QoS is not guaranteed to the PU, which results in the SU not being able to be served. The second scenario arises when $\underline{\gamma}_{k,s}$ falls below $\theta_{k,SU}$, provided that the SU has been served and the QoS requirements for the PU are fulfilled. Clearly, in (3.6), $Pr\left\{a_{k,s}^2 = 0\right\}$ can be expressed as a DoS probability of the SU in the

k^{th} band, because it is the event where the PU is unable to share the spectrum with the SU, and these bands are called DoS bands. We are interested in the average number of DoS bands, denoted by B_A.

Note that a DoS event occurs both when the SU is a cell-edge user and when the SU is a cell-center user. The reason for this is that the PU must always be served with higher priority compared to the SU. In this way, the PU outage performance was evaluated as a worst-case scenario, as modeled in reference [18] and [55]. This assumption also results in the SU having a similar outage expression for both the cell-edge SU and the cell-center SU. For more details, see [55].

For simplicity, the targeted SINR of the PUs is assumed to be the same across all bands, so that $\theta_{k,PU} = \theta_{PU}$. Therefore, the targeted SINR of the SUs is also the same across all bands, which means $\theta_{k,SU} = \theta_{SU}$.

Let us now define $\mathbb{P}_{DoS}^{(k)}$ as the probability of a DoS in the k^{th} band. Additionally, let $B = \{1, 2, 3, \dots, U\}$ be the set of bands available to be shared between users, and assume that all users' CSI are known and noisy at the BS. Then, B_A can be expressed as the sum of the individual DoS probabilities in each band, as shown below in (3.7):

$$B_A = \sum_{k=1}^{U} \mathbb{P}_{DoS}^{(k)}. \tag{3.7}$$

In the next step, we need to formulate an optimal sharing disruption over U bands. The objective of an adversary with total power P_A is to maximize the average number of DoS bands of (3.7); hence, we have the following optimization problem:

$$\max_{P_{1,A},\dots,P_{U,A}} \quad \sum_{k=1}^{U} \mathbb{P}_{DoS}^{(k)}, \tag{3.8}$$

$$s.t \;\; P_{k,A} \geq 0 \text{ for } k = 1, \dots, U, \sum_{k=1}^{U} P_{k,A} = P_A.$$

3.3 Outage Performance of the Downlink Transmission:

In this section, we analyze the performance of the downlink transmission. To begin with, we present the probability of a DoS at the SU when an adversary is present. Subsequently, we formulate the result of the DoS probability into the optimization problem. We then suggest two power allocation techniques for the adversary to implement.

3.3.1 Performance when an Adversary is Present:

If the adversary jams the PU channel estimation at the BS, as in (3.5), then the intended received signal at the PU can be derived by modifying the result of (3.2) to include the presence of an adversary, as shown below:

$$y_{k,p}(n) = g_{k,pA}\, x_k(n) + w_{k,p}(n) = \left(\underline{\hat{h}}_{k,p} + \underline{\varepsilon}_{k,p} + \sqrt{\beta_{k,A}/\beta_{k,p}}\, \underline{h}_{k,A}\ \underline{z}_{k,A}\right)$$

$$\times \sqrt{\beta_{k,p}P_{k,T}}\left(a_{k,p}\, s_{k,p}(n) + a_{k,s}\, s_{k,s}(n)\right) + w_{k,p}(n). \qquad (3.9)$$

To meet the QoS requirements for the PU, the BS first needs to allocate power to the PU [12,14,15]. This means that the BS needs to adjust the choices of the power allocation coefficients such that the QoS of the PU is satisfied. From (3.10), the SINR of the PU in the k^{th} band can be expressed as follows:

$$\underline{\gamma}_{k,p} = \frac{\beta_{k,p} a_{k,p}^2 \left|\underline{\hat{h}}_{k,p}\right|^2}{\beta_{k,p}\left(a_{k,s}^2 \left|\underline{\hat{h}}_{k,p}\right|^2 + \sigma_{\varepsilon_{k,pA}}^2\right) + \rho_k}, \qquad (3.10)$$

where $\rho_k = \sigma_{w_{k,p}}^2 / P_{k,T}$. Note that, in (3.10), the numerator is the desired signal of the PU in the k^{th} band. The denominator represents the intra-cluster interference, imperfection of the channel estimation including the adversary, and received noise sample at the PU. Note that inter-cluster interference is beyond the scope of this study. However, the rejection techniques for inter-cluster interference are suggested as in [55] or [57], and for more details see [12,13,14].

In line with references [17,18,55,57], when the QoS requirements for PUs are not fulfilled, a significant portion of the transmitted power is allocated to the PU. To be more specific, the PU outage event is defined as the failure to meet the QoS requirements, represented by $\underline{\gamma}_{k,p} < \theta_{PU}$. Then, by substituting (3.10) with the PU outage event, we obtain,

$$\frac{\beta_{k,p} a_{k,p}^2 \left|\underline{\hat{h}}_{k,p}\right|^2}{\beta_{k,p}\left(a_{k,s}^2 \left|\underline{\hat{h}}_{k,p}\right|^2 + \sigma^2_{\varepsilon_{k,pA}}\right) + \rho_k} < \theta_{PU}. \tag{3.11}$$

If we now substitute $a_{k,p}^2 = 1 - a_{k,s}^2$, then with some algebraic manipulation, we have

$$\frac{\left|\underline{\hat{h}}_{k,p}\right|^2 - \theta_{PU}\left[\sigma^2_{\varepsilon_{k,pA}} + \frac{\rho_k}{\beta_{k,p}}\right]}{\left|\underline{\hat{h}}_{k,p}\right|^2 (1 + \theta_{PU})} > a_{k,s}^2. \tag{3.12}$$

Hence, (3.12) implies that the maximal transmit power that can be allocated to the SU in the k^{th} band is given by

$$a_{k,s}^2 = \max\left\{0, \frac{\left|\underline{\hat{h}}_{k,p}\right|^2 - \theta_{PU}\left[\sigma^2_{\varepsilon_{k,pA}} + \frac{\rho_k}{\beta_{k,p}}\right]}{\left|\underline{\hat{h}}_{k,p}\right|^2 (1 + \theta_{PU})}\right\}. \tag{3.13}$$

Note that $a_{k,s}^2$ is a function of the channel coefficient of the k^{th} PU. This indicates that the power allocated to the SU is constrained to satisfy the QoS requirements of the PU. From (3.13), we can conclude that a DoS to the SU in the k^{th} band (i.e., $a_{k,s}^2 = 0$) can occur when $\left|\underline{\hat{h}}_{k,p}\right|^2 < \theta_{PU}\left[\sigma^2_{\varepsilon_{k,pA}} + \rho_k/\beta_{k,p}\right]$. This means that the BS have to allocate all of its available power to the PU to satisfy the QoS. To study the outage performance at the SU, in particular, the probability of DoS at the SU in the k^{th} band, conditioned upon $\left|\underline{h_{k,A}}\right|^2$, is defined as

$$\mathbb{P}_{DoS}^{(k)} = Pr\left\{a_{k,s}^2 = 0\right\}$$

$$= Pr\left\{\left|\underline{\hat{h}}_{k,p}\right|^2 < \theta_{PU}\ \left[\sigma^2_{\varepsilon_{k,pA}} + \frac{\rho_k}{\beta_{k,p}}\right]\right\}$$

$$= 1 - e^{-\left(\frac{\theta_{PU}\left[\sigma^2_{\varepsilon_{k,pA}} + \frac{\rho_k}{\beta_{k,p}}\right]}{\left(1-\sigma^2_{\varepsilon_{k,pA}}\right)}\right)}, \tag{3.14}$$

because $\underline{\hat{h}}_{k,p}$ follows a complex Gaussian distribution; thus, in (3.15), $\left|\underline{\hat{h}}_{k,p}\right|^2$ follows an exponential distribution with parameters $\left(1 - \sigma^2_{\varepsilon_{k,pA}}\right)$. Let $\eta_k \triangleq \sigma^2_{\varepsilon_{k,pA}} + \frac{\rho_k}{\beta_{k,p}}$, $\underline{Y_k} \triangleq \left|\underline{h_{k,A}}\right|^2$, and $\overline{P_k} \triangleq \mathbb{E}_{\underline{Y_k}}\left\{\mathbb{P}^{(k)}_{DoS}\right\}$. Then, by averaging (3.14) over $\underline{Y_k}$, we obtain the total probability of DoS at the SU, given by

$$\overline{P_k} = \int_0^{\infty} Pr\left\{\underline{Y_k} < \eta_k\theta_{PU}\ \middle|\ \underline{Y_k} = z_k\right\} f_{\underline{Y_k}}(z_k)dz_k$$

$$= 1 - \frac{\beta^2_{k,p}}{\theta_{PU}P_{k,A}\,\beta_{k,A}\,[\beta_{k,p}+\rho_k]+\beta^2_{k,p}}\,e^{-\left(\frac{\theta_{PU}\,A_2}{\beta^2_{k,p}}\right)}, \tag{3.15}$$

where $A_2 = \beta_{k,p}\,\rho_k + \sigma^2_{w_{BS}}\left(\beta_{k,p} + \rho_k\right)$. For the derivations of $\overline{P_k}$ see Appendix B.1.

As a sanity check, if the estimation was error-free, meaning that $\sigma^2_{\varepsilon_{k,pA}} = 0$. Then, (3.15) is equivalent to the result in [17]. In addition, consider the case where only the adversary is absent (i.e., $P_{k,A} = 0$). Thus, the DoS probability of the k^{th} band can be expressed as

$$\mathbb{P}^{(k)}_{DoS}(0) = 1 - e^{-\left(\frac{\theta_{PU}\,A_2}{\beta^2_{k,p}}\right)}. \tag{3.16}$$

Substituting (3.15) into (3.4), the optimal spectrum sharing disruption can be formulated as

$$\max_{P_{1,A},\dots,P_{U,A}} \quad \textstyle\sum_{k=1}^{U}\left(1 - \frac{1}{P_{k,A}\,\beta_{k,A}\,\tilde{a}_k+1}\,e^{-\left(\tilde{a}_k\sigma^2_{w_{BS}}+\,\tilde{b}_k\right)}\right), \tag{3.17}$$

$$s.t\ P_{k,A} \geq 0, \text{ for } k = 1, \dots, U, \textstyle\sum_{k=1}^{U} P_{k,A} = P_A,$$

where $\tilde{a}_k \triangleq \frac{\theta_{PU}[\beta_{k,p}+\ \rho_k]}{\beta^2_{k,p}}$ and $\tilde{b}_k \triangleq \frac{\theta_{PU}\,\rho_k}{\beta_{k,p}}$.

3.3.2 Optimal Power Allocation:

Note that (3.17) is a convex optimization problem, since the objective, inequality constraint, and equality constraint all are convex. By applying the KKT conditions [42], the optimal power allocated at k^{th} band can be expressed as shown below:

$$P_{k,A}^{*} = \begin{cases} \mu_k, & \mathbb{P}_{DoS}^{(k)}(0) < 1 - \frac{v^*}{\tilde{a}_k\, \beta_{k,A}} \\ 0, & \mathbb{P}_{DoS}^{(k)}(0) \geq 1 - \frac{v^*}{\tilde{a}_k\, \beta_{k,A}} \end{cases}, \tag{3.18}$$

where,

$$\mu_k = \sqrt{\frac{1-\mathbb{P}_{DoS}^{(k)}(0)}{\tilde{a}_k\, \beta_{k,A} v^*}} - \frac{1}{\tilde{a}_k\, \beta_{k,A}}, \tag{3.19}$$

and v^* satisfies the constraint $\sum_{k=1}^{U} P_{k,A}^{*} = P_A$, which is an increasing function of $1/\sqrt{v^*}$. This function can be computed using the bisection method (see Appendix B.2). When the optimal strategy of spectrum sharing disruption is implemented, the adversary efficiently allocates jamming power in each band. This implies that the adversary approaches the full-band jamming strategy.

3.3.3 Equal-Power Allocation:

A more realistic case is when the adversary has no prior knowledge of the terms $\beta_{k,A}$, $\tilde{a}_k$, $\tilde{b}_k$ or $\sigma_{w_{BS}}^2$. In this case, the optimal $P_{k,A}$ that maximizes (3.19) is the equal-power strategy. Similar to Appendix B.2, fulfilling the complementary slackness condition yields only two cases. In these cases, all terms (i.e., $\beta_{k,A}$, $\tilde{a}_k$, $\tilde{b}_k$ and $\sigma_{w_{BS}}^2$) are assumed to be the same in each band for some k, where $k \in \{1,2,\ldots,U\}$, and for the rest of the bands $P_{k,A} = 0$. Therefore, the optimal spectrum sharing disruption power allocation is as follows:

$$P_{k,A}^{*} = \begin{cases} \frac{P_A}{u}, & k \in \varphi_{\mathrm{A}} \\ 0, & otherwise \end{cases}, \tag{3.20}$$

where $\varphi_A \triangleq \{k \mid P_{k,A}^{*} > 0\}$ is expressed as a set of DoS bands caused by the adversary. By definition, the cardinality of φ_A is u $(0 < u \leq U)$, which represents the number of DoS bands. In this case, the adversary's goal is to increase the DoS to as many bands as possible. Because there

Table 3.1: Main Notations for Chapter 3.

U	Total number of bands (clusters).	B_A	Average number of DoS bands.
$\beta_{k,i}$	Large-scale fading between the BS and i at the k^{th} band, where $i \in \{s, p, A\}$.	$\mathbb{P}_{DoS,SU}^{(k)}$	Probability of DoS in the k^{th} band. .
$d_{k,i}$	Distance from the BS to i on the k^{th} band, where $i \in \{s, p, A\}$.	$\underline{\gamma}_{k,i}$	Instantaneous SINR of user i at the k^{th} band, where $i \in \{s, p\}$.
$\underline{h}_{k,i}$	Small-scale fading between the BS and i at the k^{th} band, where $i \in \{s, p, A\}$.	$P_{k,T}$	Transmitted power from the BS to the users in the k^{th} band.
$a_{k,i}^{2}$	Amount of power allocated to i user, where $i \in \{s, p\}$.	$P_{k,A}$	Jamming power from the adversary to the BS on the k^{th} band.
θ_{PU}	Targeted SINR of the PU.	P_A	Total jamming power of the adversary.
$\hat{\underline{h}}_{k,i}$	Estimated channel of user i at the k^{th} band, where $i \in \{s, p\}$.	$\underline{\varepsilon}_{k,i}$	Error of channel estimation of user i at the k^{th} band, where $i \in \{s, p\}$.
u	Number of DoS bands	$\mathbb{P}_{DoS}^{(k)}(0)$	DoS probability of the k^{th} band due to absent of the adversary.
$\sigma_{w_{k,i}}^{2}$	Variance of the received background noise for user i, where $i \in \{s, p\}$.	$\sigma_{w_{BS}}^{2}$	Variance due to the thermal noise at the BS.
Note that, A: Adversary, s: SU, and p: PU.			

are U allowable bands, the optimal number of DoS bands, u^*, is upper bounded by U. Hence, the optimal strategy is to jam all available bands, U, which means that

$$P_{k,A}^* = \frac{P_A}{U}, \qquad k = 1, \dots, U. \tag{3.21}$$

Full-band jamming is optimal (i.e., $u^* = U$) when the adversary has a sufficiently large P_A. Otherwise, the partial-band jamming is optimal.

3.4 Numerical Results:

In this section, the optimal sharing disruption technique is illustrated using numerical simulations. For simplicity, in these simulations, we assume that the BS transmits fixed power in each cluster (i.e., $P_{k,T} = P_T/U$). In addition, we assume that the noise variance of all PUs is the same as the noise variance at the BS, that is $\sigma^2_{w_{1,p}} = \sigma^2_{w_{2,}} = \cdots = \sigma^2_{w_{u,p}} = \cdots = \sigma^2_{w_{U,p}} = \sigma^2_{w_{BS}} = N_0$. The small-scale fading is assumed to be Rayleigh fading for both the PUs and the adversary. Finally, it is desirable to compare CR-NOMA pilot attacks with existing OMA pilots attacks. However, the unconventional nature of CR-NOMA pilot attacks makes it difficult to formulate a meaningful metric for direct comparison.

3.4.1 DoS Probability $\mathbb{P}_{DoS}^{(k)}$:

The parameters used in the simulations were set as follows: $N_0 = -64$ dBm, $P_{k,T} = 30$ dBm, $d_{k,A} = \frac{1}{2}$ km, and $\alpha = 2$. Monte Carlo simulation results were averaged over 10^6 independent trials. Figures 3.2 and 3.3 plot $\mathbb{P}_{DoS,\ SU}^{(k)}$ versus $P_{k,A}$, where the curves are parameterized for various values of θ_{PU} and $d_{k,p}$, respectively. Both Figures 3.2 and 3.3 show that $\mathbb{P}_{DoS,\ SU}^{(k)}$ increased when $P_{k,A}$ increased up to the point where the k^{th} band approached full-band jamming (i.e., full-band DoS attack). Furthermore, the numerical results obtained from (3.16) were matched with the Monte Carlo simulations. In addition, Figure 3.2 illustrates the impact of θ_{PU} on the DoS probability in a single-carrier CR-NOMA. As shown in Figure 3.2, when θ_{PU} increased, the DoS probability also increased. This is because the targeted data rate of the PU increases, in which case the bandwidth to be shared with the SU decreases. This means that the adversary needs to utilize less power to launch a full-band DoS attack when the targeted data rate of the PU increases. Figure 3.3 shows the effect of PU distance on $\mathbb{P}_{DoS}^{(k)}$ in CR-NOMA. The results show that $\mathbb{P}_{DoS}^{(k)}$ shifts to full-band DoS faster as well. This was because the free-space loss factor increased. Therefore, the adversary needs to use less power than when the PU distance is relatively shorter. We conclude that each curve undergoes a shifting transition to a full-band DoS, and the shift is determined by θ_{PU}, $d_{k,p}$, and other parameters, as illustrated in the next section.

3.4.2 Average Number of DoS bands B_A :

We illustrate the impact of system parameters on the average number of DoS bands. Figure 3.4 shows plots of B_A versus the available total number of bands, where the curves are parameterized by P_A for different values of $d_{k,A}$. The other parameters were set as follows: $N_0 = -64$ dBm, $P_{k,T} = 30$ dBm, $\theta_{PU} = 1$, and $\alpha = 2$. The PUs are distributed over a circular ring, where the distance vector is denoted as $\boldsymbol{d}_p = [d_{1,p}, d_{2,p}, \dots, d_{U,p}]$, $d_{k,p} \in [0,1\text{km}]$.The curves in Figure 3.4 show the transition from full-band jamming to partial-band jamming. The reason for full-band jamming is that the adversary has a sufficiently large P_A to launch a PJA on all the available bands. In this case, each curve B_A is equal to the available number of bands (i.e., the slope is 45^o) because of the presence of both the adversary and the system parameters. The second case is the partial-band jamming region because the adversary's total power was not large enough to cause a DoS attack on all available SUs. Because of the insufficient power of the adversary, the

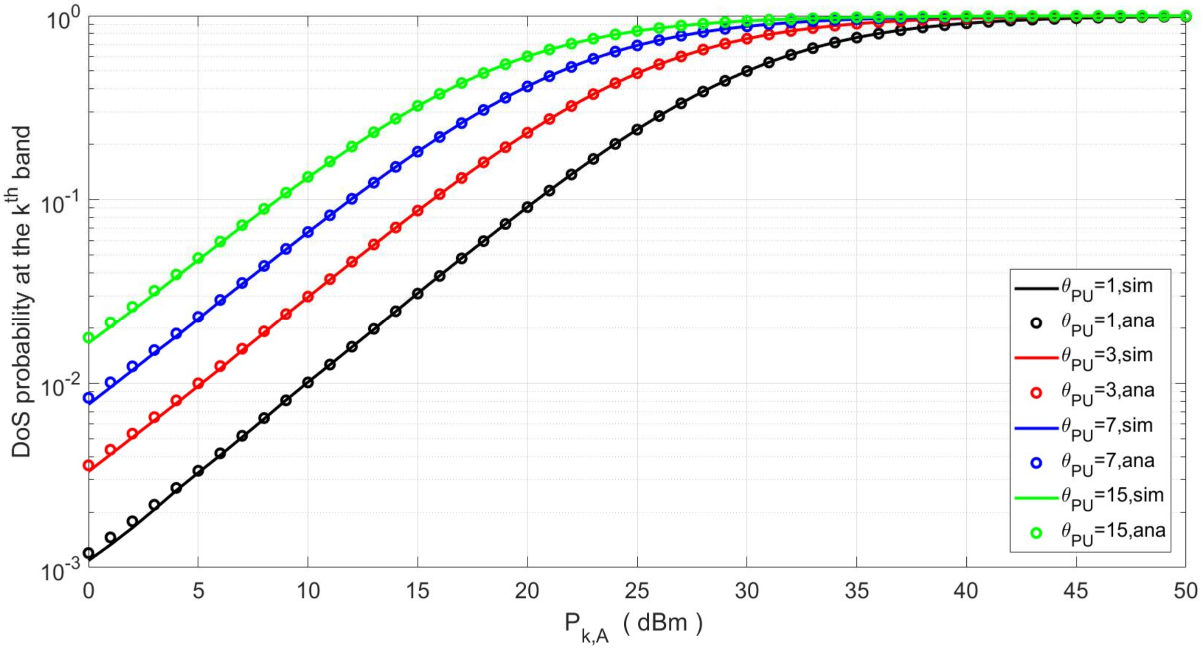


Figure 3.2: DoS probability at the k^{th}band $\mathbb{P}_{DoS,\ SU}^{(k)}$ versus the adversary power in the k^{th} band $P_{k,A}$(dBm).

slope decreases, as shown in Figure 3.4. In this case, the value of the slope was determined solely by the system parameters. Therefore, the result shows that the adversary jammed a fraction of the available bands.

An increase in P_A, leads to an increase in B_A, as shown in Figures 3.4 (a) and 3.4 (b). This is expected because, as shown in Figures 3.2 and 3.3, when the adversary power in the k^{th} band increases, the probability of DoS also increases. Comparing Figure 3.4 (b) with Figure 3.4 (a), we see that when $d_{k,A}$ increases for the same value of P_A, Figure 3.4 (a) outperforms Figure 3.4 (b) in terms of B_A. This is because the adversary in Figure 3.4 (a) is closer to the BS during the PJA than in Figure 3.4 (b).

In Figures 3.5 and 3.6, B_A is plotted versus P_A, for various values of $P_{k,T}$ and N_0, respectively, and the remaining parameters are the same as in Figure 3.4. The only difference was that $U = 100$, where previously, we set $U = 1$, because we considered a single-carrier CR-

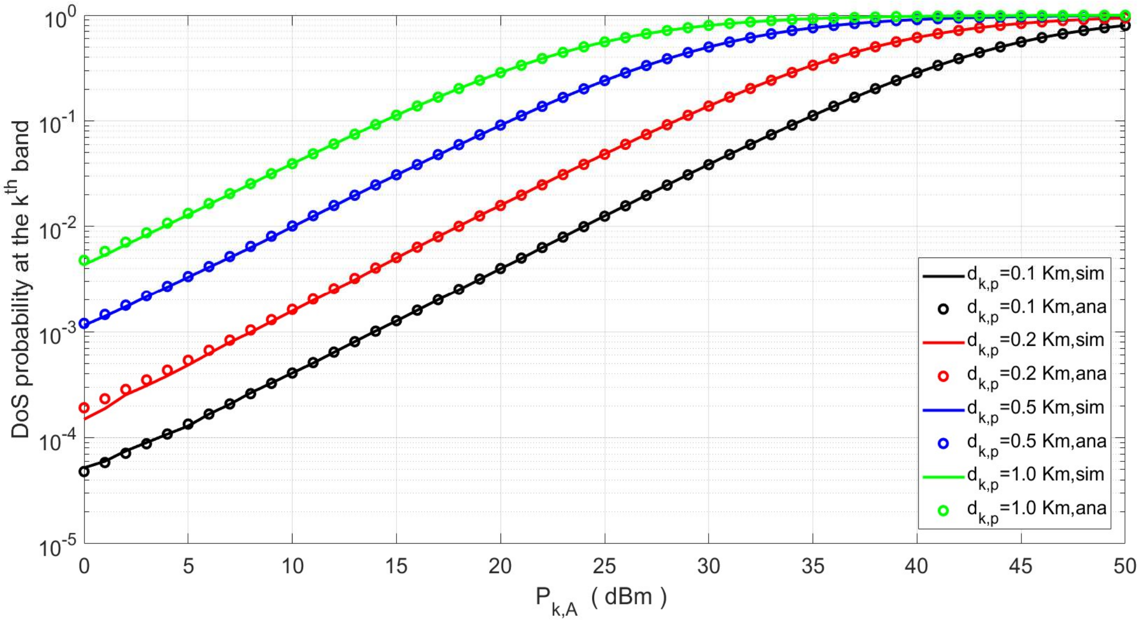
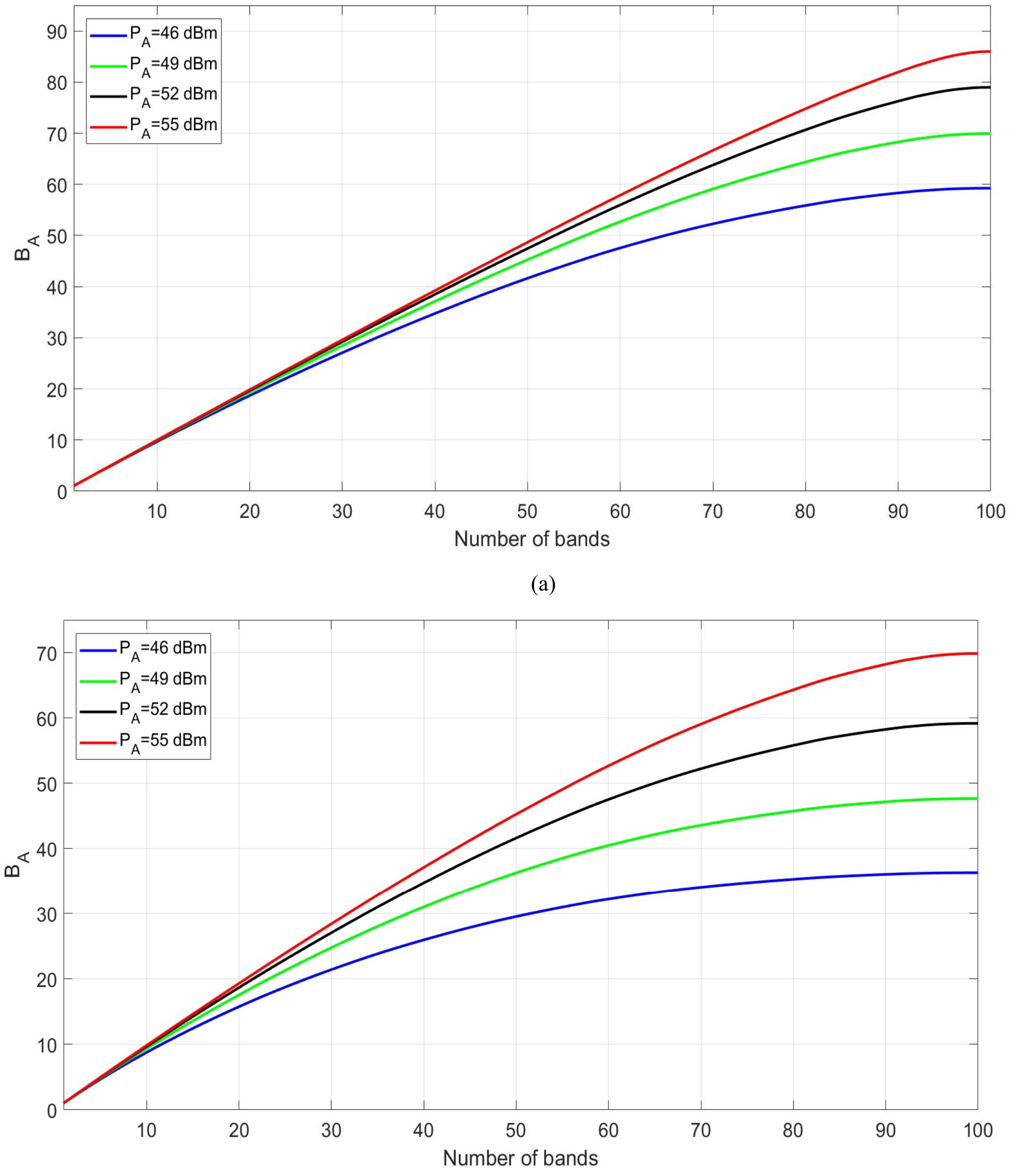


Figure 3.3: DoS probability at the k^{th}band $\mathbb{P}^{(k)}_{DoS,\ SU}$ versus the adversary power in the k^{th}band $P_{k,A}$(dBm).

NOMA. As expected, Figures 3.5 and 3.6 show that B_A increases when P_A increases. Note that in both Figures 3.5 and 3.6, B_A is almost constant in the low P_A region. From Figures 3.2 and 3.3, we know that the adversary needs the power to be around $P_A = 30$ dBm for an adversary to cause a DoS attack. However, for an MC CR-NOMA system, the adversary would need to use even higher power levels to achieve a successful DoS attack. Furthermore, the use of equal-power is not the best strategy for an adversary with a low power budget. As shown in Figure 3.5, $P_{k,T}$ decreases, B_A starts at a higher value, and as a result, B_A continues to shift faster to full-band jamming than the other curves. However, for the high P_A regime, the difference between the values of $P_{k,T}$ shows that the value of B_A is unnoticeable. This is because the adversary has a very high total power to disrupt spectrum sharing. In contrast, in Figure 3.6, when N_0 increases, B_A starts at a higher value. In addition, B_A shifts faster toward full-band jamming. The observations in Figure 3.5 are the same as those in Figure 3.6, and the reasons for these observations in Figure 3.6 are the same as those in Figure 3.5. In conclusion, $P^*_{k,A}$ allocation is affected by θ_{PU}, $d_{k,A}$, $d_{k,p}$, $P_{k,T}$ and N_0.



(a)

(b)

Figure 3.4: Average number of DoS bands B_A versus the number of bands: (a) $d_{k,A} = 1/2\ Km$ (b) $d_{k,A} = 1\ Km$.

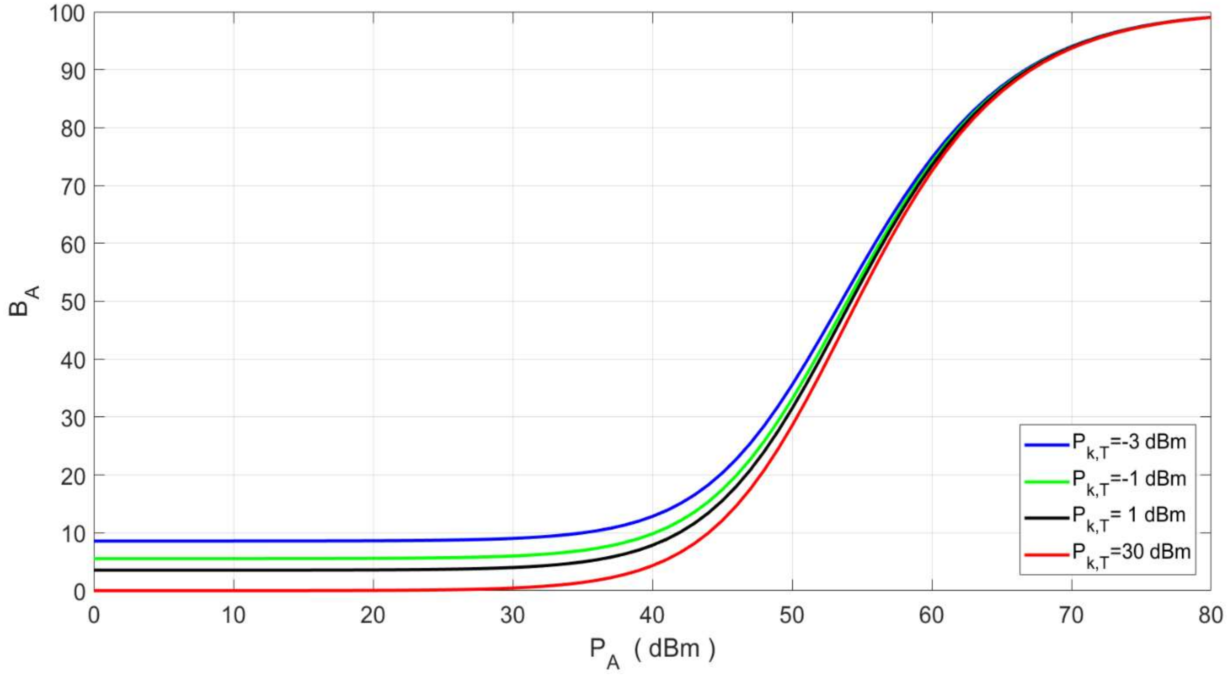


Figure 3.5: Average number of DoS bands B_A versus P_A for different values of $P_{k,T}$.

3.4.3 Equal-power VS optimal power allocation:

The effect of the power allocation algorithm on the average number of DoS bands is shown in Figure 3.7. In particular, an adversary employs two strategies: optimal power allocation and equal -power allocation. In Figure 3.7, the parameters follow the same setup as those shown in Figure 3.4. In the low P_A region, there is a slight difference between the two strategies. This is because to conduct a full-band DoS attack for a single band, the adversary needs to have approximately 5 dB power, as shown in Figures 3.2 and 3.3. If there are U bands, the adversary may not have sufficient power to disturb all U bands in either strategy. As P_A increases, the difference between the two strategies becomes noticeable. Specifically, the terms $P_{k,T}$, $\sigma^2_{w_{k,p}}$ and $\theta_{k,PU}$ do not vary in each band. However, the increase between the two strategies is around at most 3 DoS bands for the

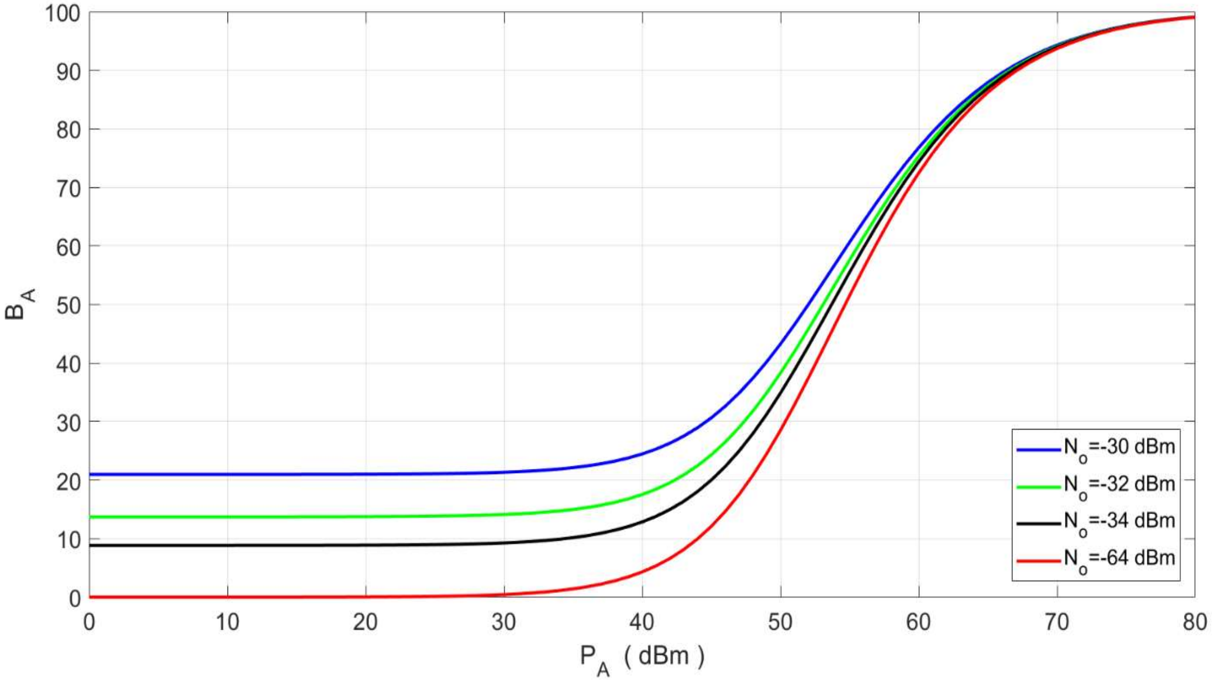


Figure 3.6: Average number of DoS bands B_A versus P_A for different values of N_0.

.

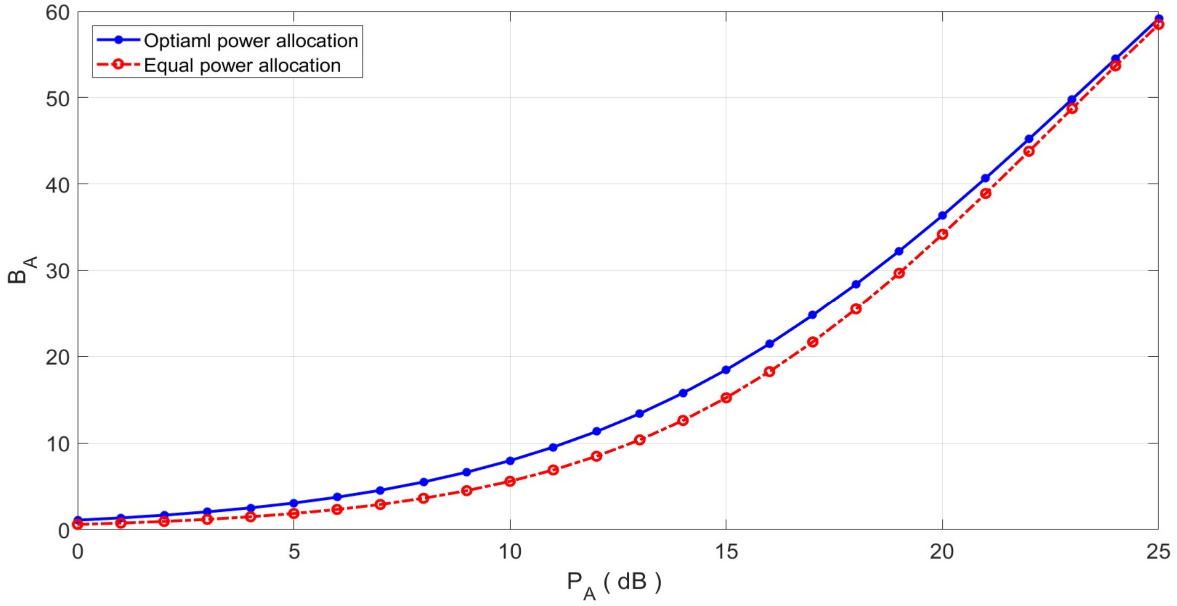


Figure 3.7: Average number of DoS bands B_A versus P_A.

same P_A. This is because the optimal allocated power in each band is based on the values of $\beta_{k,A}$, $\tilde{a}_k$, $\tilde{b}_k$ and $\sigma_{w_{BS}}^2$ as expressed in (3.20). This implies that effective DoS attacks can be conducted when the adversary is aware of the environment. As P_A is further increased, both strategies shift from partial-band jamming to full-band jamming; hence, the curves match each other at a sufficiently high P_A. This illustrates that the adversary should increase the power budget, rather than attempt to learn the values of $\beta_{k,A}$, $\tilde{a}_k$, $\tilde{b}_k$ and $\sigma_{w_{BS}}^2$. However, if the adversary increases the power, it is very likely that the BS will be able to detect these attacks.

3.5 Summary

In this chapter, we can summarize the key points from our analysis that is increasing the adversary power enables the adversary to cause a full-band DoS attack. An increase in the targeted SINR, distance of PUs, or N_o, increases the chances of successful DoS attacks. A decrease in the distance of the adversary or the transmitted power also increases the chance of a successful full DoS attack. For the given system parameters ($d_{k,p}$, $d_{k,A}$, N_o, P_T, and θ_{PU}), B_A is proportional to the total adversary power, and the optimal power strategy outperforms the equal-power strategy.

3.6 Acknowledgements:

The text of this chapter is, in part, a reprint of the paper, T. Y. Alkhamees and L. B. Milstein, "Impact of Sharing Disruption in MC CR-NOMA," in *IEEE Access*, vol. 11, pp. 82871-82881, 2023, doi: 10.1109/ACCESS.2023.3300659. The dissertation author is the primary researcher and author of this paper.

Chapter 4 :

Error Analysis of mmWave network

4.1 Introduction:

According to the measurements of [22] and [24], there are significant differences in path loss models for both line-of-sight (LOS) and non-line-of-sight (NLOS) propagation. These differences are primarily due to blockage. There are many ways to incorporate blockage models, such as 3GPP, random shape, and LOS ball; for more details, see [58].

The performance analysis of mmWave communications, including coverage probability and average capacity rate, has been extensively investigated. These investigations consider the impact of blockage as shown in [60, 61, 62, 63, 64, 65, 66, 67]. The authors of [60] utilized a rectangular Boolean scheme to model obstacles. In fact, the result of [60] shows that the LOS probability function aligns with the 3GPP suburban model. This model was further extended as shown in [61]. The extension involved a stochastic geometry approach to model interference and evaluate coverage performance. Later on, the framework served as the baseline for modeling and analyzing mmWave systems, as described in [58]. In addition, [62] considered beam misalignment, and derived corresponding system performance metrics. Interference in mmWave communication systems, or in communication systems in general, is modeled using stochastic geometry. This is because of the mathematical flexibility of the stochastic geometry [68,69,70,71]. That allows the system performance metrics to be derived in a tractable and straightforward manner.

In the context of D2D networks utilizing mmWave communication, [62] analyzed system throughput assuming self-blocking. Moreover, [63] explored the outage probability in a D2D mmWave network by varying the heights and widths of obstacles. Additionally, [64] analyzed outage performance, accounting for hardware distortion. However, these studies predominantly focused on coverage probability and often overlooked the network's error performance.

Before filling this gap, some studies have investigated the error performance of mmWave bands. In terms of multi-hop relaying [65], the error performance and coverage rate of mmWave communication bands were studied. Additionally, the impact of blockage on diversity and coding gains for mmWave communication was analyzed in [66] only for the desired link. In [67], an error analysis of mmWave cellular networks was derived. All of these studies assumed the binary communication case (i.e., the modulation order is equal to 2). Owing to their bandwidth efficiency, most modern communication systems use high-order M-ary quadrature amplitude modulation $(M - QAM)$.

There are many waveforms and modulation formats for 5G communication [72], one of which is the filter bank multicarrier-filtered multitone (FBMC-FMT) [73]. Although the FBMC can effectively reduce out-of-band leakage, it is vulnerable to co-channel interference (CCI). Error analysis of a communication system under CCI has been investigated under many assumptions, such as binary phase-shift keying $(BPSK)$ [74] and QAM [75,76]. Not only does the stochastic geometry approach enable coverage analysis, but it also serves as a very useful tool for error analysis, as demonstrated in [68,69,77,78,79,80,81]. The utility of this approach arises from practical difficulties in characterizing aggregate interference directly; evaluating the distributions of the sums and products of random variables can be exceedingly complex [69]. In fact, in [77],

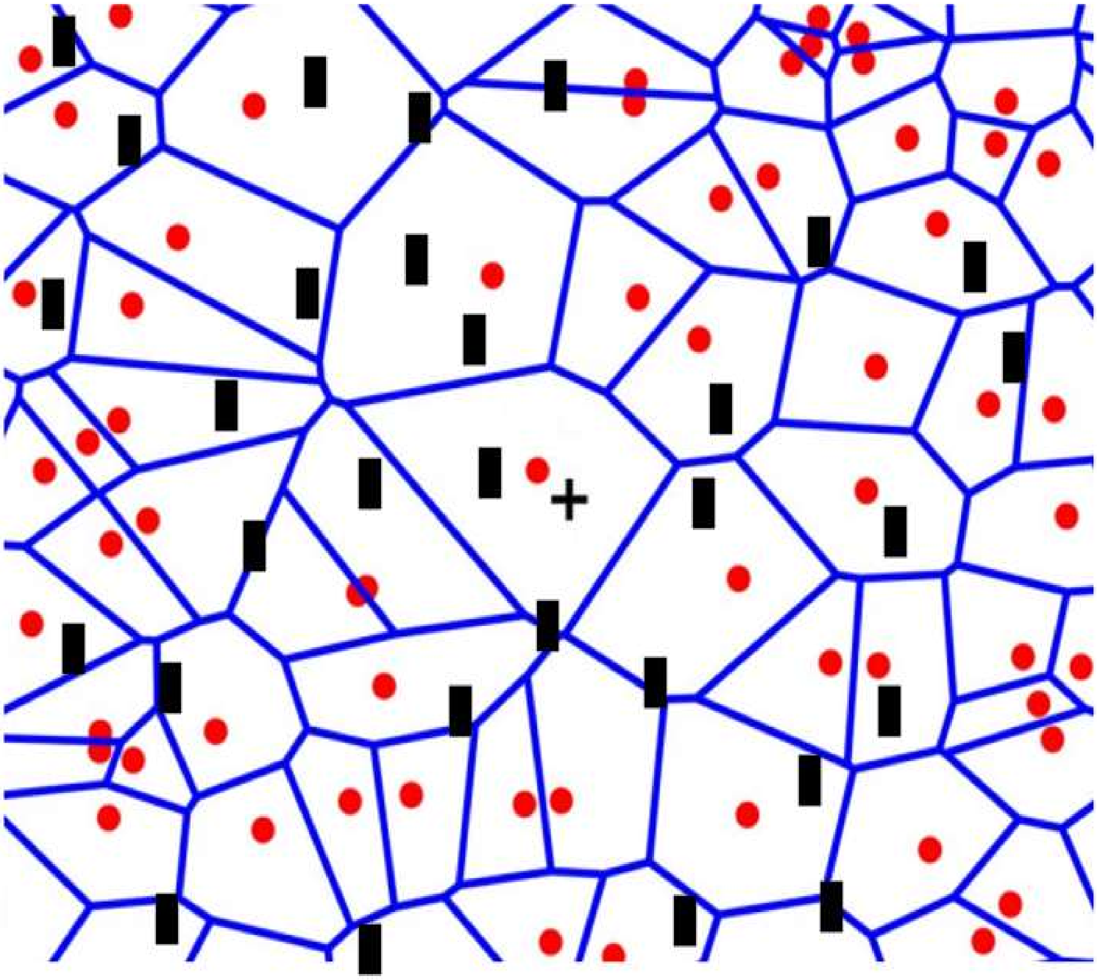


Figure 4.1: Illustration of network model.

the authors introduced the concept of an equivalent-in-distribution to represent the aggregate interference. This relies on the assumption that the sum of the interferences can be modeled as a sum of randomly scaled Gaussians, leading to more tractable formulations for error analysis.

Therefore, this chapter aims to investigate the error performance of mmWave communication within a dense interference environment. Such focus is important for ensuring the effective throughput and reliability of networks in the near future, as the number of mmWave network users is expected to increase.

The structure of this chapter is organized as follows: Section 4.2 introduces the preliminaries and general formulation. Section 4.3 details the error rate analysis. Numerical results are provided in Section 4.4, while Section 4.5 offers the summary of the chapter.

4.2 System Model and General Formulation:

In this section, we discuss the frameworks of the network model and the transceiver model. Additionally, we present the assumptions regarding the channel and the directional antenna model.

4.2.1 Network Model:

Consider an mmWave single-cell D2D network as shown in Figure 4.1. The transmitters are shown as red dots, the receiver is represented as a cross, and the blockages are represented as rectangles. There are M_c orthogonal subcarriers are allocated over the total frequency band of W (Hz). Each D2D pair can access these subcarriers, subject to resource allocation involving power distribution and adaptive modulation and is served by a base station (BS) in a time-slot manner. The transmitter D2D pair locations follow a homogeneous Poisson point process (PPP) represented as ϕ, with density parameter λ. In all D2D networks, there is a fixed distance between the transmitter and receiver devices.

In an mmWave network, the transmitted waveforms are more susceptible to blockage effects during propagation compared to lower frequency bands. These blockages can impact both LOS and NLOS links. The blockage phenomena were modeled similarly to the baseline mmWave system model in [58]. Then, the propagation path between the transmitter Tx and receiver Rx can be classified as either LOS or NLOS. Mathematically, the probability of LOS, representing a propagation path is similar to that described in [59],

$$P_L(r) = e^{-\beta} \ , \tag{4.1}$$

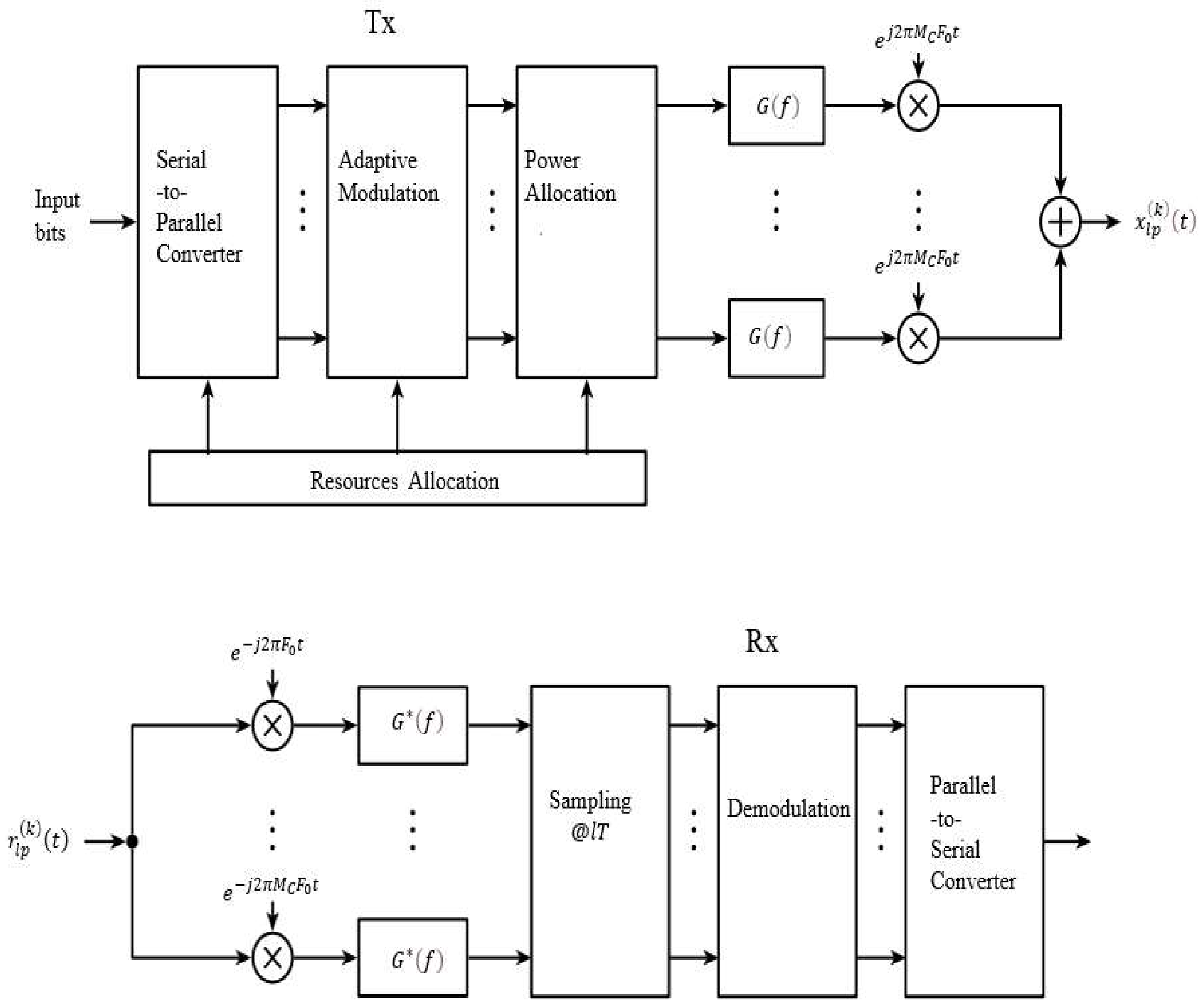


Figure 4.2: Transceiver of FBMC-FMT.

where r is the fixed distance between the k^{th} D2D pair (i.e., Tx and Rx) and m^{th} subcarrier, and β denotes as the blockage parameter. The probability of NLOS for a specific propagation path is given in [59] as

$$P_N(r\ ) = 1 - P_L(r) = 1 - e^{-\beta r}. \tag{4.2}$$

The LOS probabilities of different D2D transmitters can be assumed to be independent, as indicated in [60]. In this way, the D2D transmitters can be categorized into two separate non-homogeneous PPPs, according to the propagation paths to the k^{th} D2D receiver. One is from the

LOS transmitters, characterized as ϕ_L, where the intensity is $\lambda P_L(r)$.The other is from the NLOS transmitters, represented as ϕ_N , where the intensity is $\lambda P_N(r)$. Note that the blockage parameter, β, depends on many factors, such as the width and length of the blockers. Additionally, β varies depending on the density of the region, as summarized in [5]. For instance, $\beta = 1/100$ is taken from the UT Austin building topology, while $\beta = 1/200$ is used in suburban areas according to the 3GPP blockage model. Another value for the blockage parameter, $\beta = 1/141.4$, was proposed in [60].

4.2.2 Transmitter (Tx):

Consider an FBMC-FMT system that assigns W (*Hz*) across M_c orthogonal frequency bands, denoted as $m = \{1, 2, 3\ \dots\ M_c\}$. Accordingly, the spacing of the subcarriers can be denoted as $F_0 = W/M_c$ [75]. The Tx in this multicarrier system is shown in Figure 4.2. Each signal is modulated using square $M - QAM$ modulation, which is performed by the m^{th} subcarrier of the k^{th} Tx. Note that $1/T$ represents the symbol rate. The l^{th} complex modulated symbol on the m^{th} subcarrier from the k^{th} Tx is indicated by $X_{m,l}^{(k)}$, where the variance $Var\left[X_{m,l}^{(k)}\right] = \frac{1}{2}\mathbb{E}\left\{\left|X_{m,l}^{(k)}\right|^2\right\}$ is normalized to unity. Thus, the low-pass equivalent signal in the time domain for the k^{th} Tx of a multicarrier system, denoted $x_{lp}^{(k)}(t)$, is formulated as follows:

$$x_{lp}^{(k)}(t) = \sum_{m=1}^{M_c} \sqrt{p_m^{(i)}\, T} \sum_l X_{m,l}^{(k)}\, g(t - lT)\, e^{j2\pi m F_0 t}, \tag{4.3}$$

where $p_m^{(i)}$ represents the power of the m^{th} subcarrier of the k^{th} Tx; and $g(t)$ is the pulse shaping at the Tx. Note that $G(f)$ is the Fourier transform of filter $g(t)$. Combining the pulse shaping and matched filter, it results in$|G(f)|^2$, forming a Nyquist pulse characterized with a roll-off factor of

$0 < \rho \leq 1$. To avoid intercarrier interference (ICI), F_0 is set as $(1+\rho)/T$. Note that most components of the transceiver, as well as the assumptions, are similar to those described in [75].

4.2.3 Channel Model:

The results of the measurements show that the mmWave channel suffers from multipath, particularly in NLOS links [23,24]. In contrast, LOS links have a direct path that dominates over the relatively smaller contribution of the multipath, specifically when a directional antenna is implemented. However, to align with previous studies such as [60,61,62,63,64,65,66], the Nakagami$-m$ distribution has been widely used for modeling and analyzing performance metrics in mmWave communications. Consequently, the small-scale fading from the k^{th} Tx to the k^{th} Rx on the m^{th}subcarrier is represented as, $h_{k,m}^{(k)}$, but with differing fading severity parameters for both links [60,61,62,63,64,65,66]. This differentiation is crucial for effectively representing the differences between the LOS and NLOS links. The corresponding fading power gain $\left|h_{k,m}^{(k)}\right|^2$ is distributed as a normalized Gamma, given that the link is at distance r, as shown below:

$$\left|h_{k,m}^{(k)}\right|^2 \sim \begin{cases} Gamma(m_L, m_L) & LOS, \\ Gamma(m_N, m_N) & NLOS, \end{cases} \tag{4.4}$$

where m_L and m_N represent the fading severity parameters for the LOS and NLOS, respectively. Note that Nakagami$-m$ equals Rayleigh when $m = 1$, implying that there is no dominant component. Larger values of m indicate the presence of a dominant component, showing less severe fading conditions. This causes the channel to behave in a more deterministic manner.

Because the path loss depends on the propagation distance and operating frequency, different path loss exponents are applied to the LOS and NLOS links. Given that k^{th} the transmitter and k^{th} receiver are separated by distance r, their path loss at the m^{th} subcarrier $\Omega^{(k,m)}$ is given by

$$\Omega^{(k,m)} = \begin{cases} \Omega_L(r) = L_L(r)^{-\nu_L} & LOS, \\ \Omega_N(r) = L_N(r)^{-\nu_N} & NLOS, \end{cases} \tag{4.5}$$

where L_L, L_N are the path loss intercepts of LOS and NOLS links, respectively. Interestingly, the path loss for both the LOS and NLOS links can be the same when a similar reference distance, r_{ref} is applied, (e.g., $r_{ref} = 1$). Under this assumption, we have $L_L = L_N = L_0 = \left(\lambda_c / \left(4\pi r_{ref}\right)\right)^2$, where λ_c is the wavelength, as indicated in [23]. The LOS and NLOS path loss exponents, ν_L and ν_N, respectively, typically satisfy $\nu_N > \nu_L > 0$ in mmWave communication path loss models [23,24]. This chapter also incorporates the path loss models similar to many studies, such as [60,61,62,63,64,65,66].

4.2.4 Directional Antenna Model:

To simplify the analysis, we assumed the implementation of a two-sector model similar to that in [60] and [65]. The two-sector model is also part of the baseline mmWave system model presented in [58]. This model considers a main lobe gain M_S and a side lobe gain m_S. The directional gain, denoted as $A(\Theta_S)$, is a function of the azimuth angle Θ_S for $S \in \{Tx, Rx\}$:

$$A(\Theta_S) = \begin{cases} M_S & if\ |\Theta_S| \leq \theta \\ m_S & otherwise \end{cases}. \tag{4.6}$$

The value of the main lobe gain is inversely proportional to the half-power beamwidth ($HPBW$), meaning that as θ increases, M_S decreases. This inverse relationship is due to the fact that a wider observation angle of the antenna results in a reduced directional gain.

In this chapter, we assumed perfect beam alignment for the desired signal link. This means that the total directivity gain for the k^{th} D2D pair, denoted as $A_{tot}^{(k,k)}$, is the product of the transmitting antenna gain $A(\Theta_{Tx_k})$ and the receiving antenna gain $A(\Theta_{Rx_k})$, which results in $A_{tot}^{(k,k)} = M_{Tx_k} M_{Rx_k}$. However, beam misalignment errors, is beyond the scope of this chapter, for more insight see [61].

For the interfering link, k^{th}receiver and i^{th} transmitter steering angles are independently and uniformly distributed over $[-\pi, \pi]$. The total directivity gain $A_{tot}^{(i,k)} = A(\Theta_{T_i})\, A(\Theta_{R_k})$, can be modeled as a discrete random variable as follows:

$$A_{tot}^{(i,k)} = \begin{cases} a_1 = M_{Tx_i} M_{Rx_k} & w.p.\ b_1 = \xi_T \xi_R, \\ a_2 = M_{Tx_i} m_{Rx_k} & w.p.\ b_2 = \xi_T (1 - \xi_R), \\ a_3 = m_{Tx_i} M_{Rx_k} & w.p.\ b_3 = (1 - \xi_T)\xi_R, \\ a_4 = m_{Tx_i} m_{Rx_k} & w.p. b_4 = (1 - \xi_T)(1 - \xi_R), \end{cases}, \tag{4.7}$$

where a_z is a possible outcome of the total directivity gain. Additionally, the terms b_z represent the assigned probability for the possible outcome, where $z \in \{1,2,3,4\}$, $\xi_T \triangleq \left(\frac{\Theta_{Tx_i}}{2\pi}\right)$ and $\xi_R \triangleq \frac{\Theta_{Rx_k}}{2\pi}$. Note that the omnidirectional antenna for both Tx and Rx has no impact on the total directional gain (i.e., $\xi_T = 1$ and $\xi_R = 1$).

4.2.5 Receiver (Rx):

Under the assumption that the D2D receiver has full knowledge of the channel state information (CSI), it is also assumed that a block fading channel model is employed. In this model, it was assumed that the signal passed through a channel characterized by flat and slow fading. Additionally, it is assumed that multipath fading independently affects different transmitters [75]. The signal from the i^{th} Tx reaches the k^{th} Rx with a time delay denoted as $\tau_k^{(i)}$. When $i \neq k$, it is uniformly distributed within the interval [0, T). Additionally, denote the random phase shift as $\theta_k^{(i)}$, which is assumed to have a uniform distribution between $-\pi$ and π.

It is further assumed that a coherent Rx is employed to ensure perfect bit synchronization for the desired signal, that is, $\tau_k^{(k)} = 0$ and $\theta_k^{(k)} = 0$. After the down conversion, the lowpass equivalent signal from to the k^{th} Rx, as shown in Figure 4.2, is given by,

$$r_{lp}^{(k)}(t) = \; I_{D,k}^{(k)}(t) + I_{I,L}(t) + I_{I,N}(t) + n^{(k)}(t), \tag{4.8}$$

where $n^{(k)}(t)$ represents the AWGN at the k^{th} Rx, characterized by a two-sided power spectral density N_0. The energy of the m^{th} subcarrier of the k^{th} Tx is given by $E_m^{(k)} = p_m^{(k)}T$, and the rest of terms in (4.8) are defined as follows:

-$Desired\ signal$:

$$I_{D,k}^{(k)}(t) = \; \sum_{m=1}^{M_c} \sqrt{A_{tot}^{(k,k)} E_m^{(k)} \varOmega^{(k,m)}} h_{k,m}^{(k)} \sum_l X_{m,k}^{(l)} \, g(t - lT) e^{j\left(2\pi m F_0 t + \theta_k^{(k)}\right)}, \tag{4.9A}$$

-$LOS\ Interfernce\ signal$:

$$I_{I,L}(t) = \sum_{r_i \in \phi_L \backslash \{k\}} \sum_{m=1}^{M_c} \sqrt{\, A_{tot}^{(i,k)} E_m^{(i)} \varOmega_L(r_i)} h_{k,m}^{(i)} \sum_l X_{m,i}^{(l)} g\left(t - lT - \tau_k^{(i)}\right) e^{j\left(2\pi k F_0 t + \theta_k^{(i)}\right)}, \tag{4.9B}$$

-$NLOS\ Interfernce\ signal$:

$$I_{I,N}(t) = \sum_{r_i \in \phi_N \backslash \{k\}} \sum_{m=1}^{M_c} \sqrt{A_{tot}^{(i,k)} E_m^{(i)} \varOmega_N(r_i)} \; h_{k,m}^{(i)} \sum_l X_{m,i}^{(l)} g\left(t - lT - \tau_k^{(i)}\right) e^{j\left(2\pi k F_0 t + \theta_k^{(i)}\right)}. \tag{4.9C}$$

For the n^{th} subcarrier, with the l^{th} received symbol is set to zero, the output of the matched filter yields many terms and is given by,

$$Y_n^{(k)}[0] = \int_{-\infty}^{\infty} \, r^{(k)}(t) e^{-j2\pi n F_0 t} g^*(t) \, dt = Q_D + Q_{I,N} + Q_{I,L} + N_k[0], \tag{4.10}$$

where $N_k[l]$ is the output noise term given by $\int_{-\infty}^{\infty} \, n^{(k)}(t) e^{-j2\pi n \;_0 t} g^*(t - lT) \, dt \, t$, and it is distributed as a zero-mean complex Gaussian with a second moment denoted as $\sigma_{n_0}^2 = N_0 \int_{-\infty}^{\infty} \, |g(t)|^2 \, dt = N_0$ [75]. Taking into account that $\tau_k^{(k)} = 0$, $\int_{-\infty}^{\infty} \, |g(t)|^2 \, dt = 1$, and denote that $g\left(-lT - \tau_k^{(i)}\right) = g_{l,k}^{(i)}$; then the rest of the terms in (4.10) can be expressed as follows:

$$Q_D^{(k)} = \int_{-\infty}^{\infty} I_{D,k}^{(k)}(t)\ e^{-j2\pi n\ {}_{0}t} g^*(t)\, dt = \sqrt{A_{tot}^{(k,k)} E_n^{(k)} \Omega^{(k,n)}} h_{k,n}^{(k)} X_{n,k}^{(0)}, \quad (4.11)$$

$$Q_{I,L} = \int_{-\infty}^{\infty} I_{I,L}(t)\ e^{-j2\pi n\ {}_{0}t} g^*(t)\, dt = \sum\nolimits_{r_i \in \phi_L \backslash \{k\}} \sqrt{A_{tot}^{(i,k)}\ E_n^{(i)} \Omega_L(r_i)}\ h_{k,n}^{(i)} e^{j\theta_k^{(i)}} \sum\nolimits_l X_{n,i}^{(l)} g_{l,k}^{(i)}, \quad (4.12)$$

$$Q_{I,N} = \int_{-\infty}^{\infty} I_{I,N}(t)\, e^{-j2\pi n F_0 t} g^*(t)\, dt = \sum\nolimits_{r_i \in \phi_N \backslash \{k\}} \sqrt{A_{tot}^{(i,k)}\ E_n^{(i)} \Omega_N(r_i)}\ h_{k,n}^{(i)} e^{j\theta_k^{(i)}} \sum\nolimits_l X_{n,i}^{(l)} g_{l,k}^{(i)}. \quad (4.13)$$

4.3 Rate Error Analysis:

In this section, we evaluate the error probability of the m^{th} subcarrier and the k^{th} D2D receiver. Note that CCI is now referred to as the aggregate interference. Initially, the aggregate interference components in (4.12) and (4.13) show that there are in-phase and quadrature components, denoted by:

$$Q_{I,L} = \sum\nolimits_{r_i \in \phi_L \backslash \{k\}} \sqrt{A_{tot}^{(i,k)}\ E_n^{(i)} \Omega_L(r_i)}\ h_{k,n}^{(i)} \left(Y_{i,n,k}^{(Re)} + j\, Y_{i,n,k}^{(Im)} \right), \quad (4.14)$$

$$Q_{I,N} = \sum\nolimits_{r_i \in \phi_N \backslash \{k\}} \sqrt{A_{tot}^{(i,k)}\ E_n^{(i)} \Omega_N(r_i)}\ h_{k,n}^{(i)} \left(Y_{i,n,k}^{(Re)} + j\, Y_{i,n,k}^{(Im)} \right), \quad (4.15)$$

where $Y_{i,n,k}^{(Re)} = \left(\sum_l Re\left\{ X_{n,i}^{(l)} \right\} g_{l,k}^{(i)} \right) cos\left(\theta_k^{(i)} \right) + \left(\sum_l Im\left\{ X_{n,i}^{(l)} \right\} g_{l,k}^{(i)} \right) sin\left(\theta_k^{(i)} \right)$ and $Y_{i,n,k}^{(Im)} = \left(\sum_l Im\left\{ X_{n,i}^{(l)} \right\} g_{l,k}^{(i)} \right) cos\left(\theta_k^{(i)} \right) - \left(\sum_l Re\left\{ X_{n,i}^{(l)} \right\} g_{l,k}^{(i)} \right) sin\left(\theta_k^{(i)} \right)$, are the real and imaginary term, respectively. Then, the aggregate interference can be represented as:

$$I_{agg} = \left(Q_{I,N}^{(Re)} + Q_{I,L}^{(Re)} \right) + j\left(Q_{I,N}^{(Im)} + Q_{I,L}^{(Im)} \right). \quad (4.16)$$

To consider the implications of I_{ag} , we condition the network geometry ((i.e., $r \in \phi_q, \forall q \in \{L, N\}$), total directivity gain (i.e., $A_{tot}^{(i,k)}$), and channel gains (i.e., $h_{k,n}^{(k)}$and $h_{k,n}^{(i)}$). Even under these conditions, I_{agg} does not have a closed-form expression owing to its pulse shape. To compensate for this, numerical integration approximation techniques have been employed in references [74] and [76]. Additionally, the characteristic function of I_{agg} was approximated using a power series in [75]. To examine the interference in dense environments, we modeled the aggregated interference signal using a Gaussian signaling approximation. This approach is justified by the assumption that each interference link operates close to its capacity [79], yielding a worst-case scenario of interference.

4.3.1 SER Expression via Gaussian Signaling Approximation for the Aggregate Interference:

Obtaining the interference terms in (4.16) is often a challenging task. However, as discussed in [82], some researchers have employed a Gaussian signaling approximation to model the aggregated interference. In addition, [79,80, 81] applied the Gaussian signaling approximation with a stochastic geometry approach. This approximation assumes that the symbol from each interferer is drawn independently from a complex Gaussian distribution with a unit energy. For example, the i^{th} transmitter in n^{th} subcarrier and l^{th} symbol is distributed as $\tilde{J}_{n,l}^{(i)} \sim \mathcal{CN}(0,1)$. Consequently, the symbols at the k^{th} D2D receiver output can be represented as,

$$J_{n,k}^{(i)} = \left(\sum_{l} \tilde{J}_{n,l}^{(i)} g_{l,k}^{(i)}\right) e^{j\theta_k^{(i)}}, \tag{4.17}$$

leading to (4.14) and (4.15) to become

$$Q_{I,L} = \sum_{r_i \in \phi_L \setminus \{k\}} \sqrt{A_{tot}^{(i,k)}\, E_n^{(i)} \Omega_L(r_i)}\, h_{k,n}^{(i)} J_{n,k}^{(i)} = \sum_{r_i \in \phi_L \setminus \{k\}} Q_{n,k,L}^{(i)}, \tag{4.18}$$

and

$$Q_{I,N} = \sum_{r_i \in \phi_N \setminus \{k\}} \sqrt{A_{tot}^{(i,k)} E_n^{(i)} \Omega_N(r_i)}\, h_{k,n}^{(i)} A_{tot}^{(i,k)} J_{n,k}^{(i)} = \sum_{r_i \in \phi_N \setminus \{k\}} Q_{n,k,N}^{(i)}. \tag{4.19}$$

In this chapter, the raised-cosine pulse is considered for Nyquist pulses because it is widely used in the literature (e.g., [74] and [75]). When we condition on ϕ_q, $h_{k,n}^{(i)}$, and $A_{tot}^{(i,k)}$, where $q \in \{L, N\}$, we can derive the variance of $J_{n,l}^{(i)}$ for the raised-cosine pulse, as shown in [74]:

$$Var\left(J_{n,l}^{(i)}\right) = \frac{1}{2}\mathbb{E}\left\{\left|\left(\sum_l \tilde{J}_{n,l}^{(i)} g_{l,k}^{(i)}\right)e^{j\theta_k^{(i)}}\right|^2\right\} = \sum_l \mathbb{E}\left\{\left|\tilde{J}_{n,l}^{(i)}\right|^2\right\} \mathbb{E}\left\{\left|g_{l,k}^{(i)}\right|^2\right\} = (1-\rho/4). \qquad (4.20)$$

Now, $Q_{n,k,q|\phi_q, A_{tot}^{(i,k)}, h_{k,n}^{(i)}}^{(i)} \sim \mathcal{CN}\left(0,\ \sigma_{I,q,i}^2\right)$ for $q \in \{L, N\}$, where the variance of each link is $\sigma_{I,q,i}^2 = \Omega_q(r_i)E_n^{(i)}A_{tot}^{(i,k)}\left|h_{k,n}^{(i)}\right|^2(1-\rho/4)$. The different interference links are assumed to be independent. Thus, $Q_{I,q|\phi_q, A_{tot}^{(i,k)}, h_{k,n}^{(i)}} \sim \mathcal{CN}\left(0,\ \sigma_{I,q}^2\right)$, where $\sigma_{I,q}^2 = \sum_i\ \sigma_{I,q,i}^2$.

Conditioning on ϕ_L, ϕ_N, $h_{k,n}^{(k)}$, $A_{tot}^{(i,k)}$, and $h_{k,n}^{(i)}$ results in the decision statistic in (10) with a Gaussian distribution. This simplifies the SER evaluation for general $M-QAM$ in aggregated interference with AWGN to depend solely on SINR, which is expressed as follows:

$$\Upsilon_k^{(q)} = \frac{\left|h_{k,n}^{(k)}\right|^2}{\sigma_{I,N}^2/\left(\Omega_q(r)E_n^{(k)}\right) +\ \sigma_{I,L}^2/\left(\Omega_q(r)E_n^{(k)}\right) + 1/\gamma^{(q)}}$$

$$= \begin{cases} \dfrac{\left|h_{k,n}^{(k)}\right|^2}{\sigma_{I,N}^2/\left(\Omega_L(r)E_n^{(k)}\right) + \sigma_{I,L}^2/\left(\Omega_L(r)E_n^{(k)}\right) + 1/\gamma} & LOS, \\ \dfrac{\left|h_{k,n}^{(k)}\right|^2}{\sigma_{I,N}^2/\left(\Omega_N(r)E_n^{(k)}\right) + \sigma_{I,L}^2/\left(\Omega_N(r)E_n^{(k)}\right) + \left(r^{(v_N - v_L)}\right)/\gamma} & NLOS, \end{cases} . \qquad (4.21)$$

In (4.21), aggregate interference can be denoted as, $i_{agg} =\ \sigma_{I,N}^2 +\ \sigma_{I,L}^2$, and $A_k^{(i)} = A_{tot}^{(i,k)}/(M_{Tx_k}M_{Rx_k})$. The SNR for the LOS is $\gamma^{(L)} = \gamma \triangleq \frac{E_n^{(k)}\left(M_{Tx_k}M_{Rx_k}\right)L_0(r^{-v_L})}{\sigma_{n_0}^2}$ and the SNR for the NLOS is $\gamma^{(N)} = \frac{E_n^{(k)}\left(M_{Tx_k}M_{Rx_k}\right)L_0\ (r^{-v_N})}{\sigma_{n_0}^2} \triangleq \gamma\left(r^{(v_L - v_N)}\right)$. Note that i_{agg} is a random variable. Without loss of generality, conditioned on $r \in \phi_q$, $h_{k,n}^{(k)}$, and i_{agg}, the SER is denoted by $\mathcal{E}$ for a coherent detector using a square $M-QAM$ modulation scheme, and is given in [83] as

$$\mathcal{E}\left(r \in \phi_q, h_{k,n}^{(k)}, i_{agg}\right) = 2w\ erfc\left(\sqrt{\alpha \Upsilon_k^{(q)}}\right) - w^2 erfc^2\left(\sqrt{\alpha \Upsilon_k^{(q)}}\right), \tag{4.22}$$

where, $w = \left(\frac{\sqrt{\mathcal{M}_{k,m}}-1}{\sqrt{\mathcal{M}_{k,m}}}\right)$,and $\alpha = \frac{3/2}{\mathcal{M}_{k,m}-1}$ are modulation-dependent weighting factors. It should be noted that by adjusting the variables w and α, the SER for various modulation schemes and constellation sizes can be determined, as demonstrated in [84].

Because $\left|h_{k,n}^{(k)}\right|^2$follows a normalized gamma distribution (i.e., $Gamma\left(m_q\right)$, for $q \in \{L, N\}$), the author in [85] introduced a valuable technique to average the SER expression in (4.22) over $\left|h_{k,n}^{(k)}\right|^2$ and a random variable, i_{agg}, as follows:

$$ASER\ \left(r \in \phi_q\right) = \mathbb{E}_{h_{k,n}^{(k)}, i_{agg}}\left\{\mathcal{E}\left(r \in \phi_q, h_{k,n}^{(k)}, i_{agg}\right)\right\}$$

$$= \mathbb{E}_{\left|h_{k,n}^{(k)}\right|^2, i_{agg}}\left\{2w\ erfc\left(\sqrt{\alpha \Upsilon_k^{(q)}}\right)\right\} - \mathbb{E}_{h_{k,n}^{(k)}, i_{agg}}\left\{w^2 erfc^2\left(\sqrt{\alpha \Upsilon_k^{(q)}}\right)\right\}. \tag{4.23}$$

This averaging in (4.23) can be applied to the two terms separately, as illustrated in [85]. The terms are as follows:

$$\mathbb{E}_{\left|h_{k,n}^{(k)}\right|^2, i_{agg}}\left\{2w\ erfc\left(\sqrt{\Upsilon_k^{(q)}}\right)\right\} = 2w\ - \frac{4w\Gamma\left(m_q\ + \frac{1}{2}\right)}{\pi\Gamma\left(m_q\right)}$$

$$\times \int_0^\infty \frac{e^{-s\left(1+\frac{m_q}{\alpha\gamma^{(q)}}\right)}}{\sqrt{s}} \mathcal{L}_{i_{agg}}\left(\frac{m_q}{\alpha\Omega_q(r)E_n^{(i)}}\ s\right) {}_1F_1\left(1 - m_q; \frac{3}{2}, s\right) ds\ \triangleq P_I \tag{4.24A}$$

and

$$\mathbb{E}_{h_{k,n}^{(k)}, i_{agg}}\left\{w^2 erfc^2\left(\sqrt{\Upsilon_k^{(q)}}\right)\right\}$$

$$= w^2 - \left(\frac{4w^2 m_q}{\pi}\right)\int_0^\infty e^{-s\frac{m_q}{\alpha\gamma^{(q)}}} \mathcal{L}_{i_{agg}}\left(\frac{m_q}{\alpha\Omega_q(r)E_n^{(i)}}\ s\right)$$

$$\times \int_0^{\frac{\pi}{4}} {}_1F_1\left(1+m_q\,;2,-s/\sin^2(\vartheta)\right)\frac{d\vartheta}{\sin^2(\vartheta)}\;ds\;\triangleq P_{II}, \tag{4.24B}$$

where $\mathcal{L}_{i_{agg}}(.)$ is the Laplace transform (LT), ${}_1F_1(a;b,x)$ is the Kummer confluent hypergeometric function; and $q \in \{L,N\}$. The LT of the aggregate interference is discussed in the next subsection.

4.3.2 LT of i_{agg}:

Reference [60] derived an aggregate interference term in accordance with the baseline mmWave system model presented in [58] under the assumption that the minimum path loss governs the association rule. Based on an association rule, the exclusion and inclusion regions of interference can be established. For more details on the association rules, see [68,69,70,71]. However, because the distance was fixed in this chapter, the max-SINR association was adopted, implying that no exclusion region for interferers was considered [70]. We employ common stochastic geometry techniques, as found in [68], [70], and [18], to derive the LT of aggregate interference, denoted as $\mathcal{L}_{i_{agg}}(s)$ which as shown below,

$$\mathcal{L}_{i_{agg}}(s) = \mathbb{E}\{e^{-si_{agg}}\} = \mathbb{E}\left\{e^{-s\sigma_{I,N}^2}\right\}\mathbb{E}\left\{e^{-s\sigma_{I,L}^2}\right\}$$

$$= \mathbb{E}\left\{\prod_{r_i\in\phi_N\setminus\{k\}} e^{-s\left(\Omega_N(r_i)E_n^{(i)}\left|h_{k,n}^{(i)}\right|^2 A_k^{(i)}\left(1-\frac{\rho}{4}\right)\right)}\right\}\mathbb{E}\left\{\prod_{r_i\in\phi_L\setminus\{k\}} e^{-s\left(\Omega_L(r_i)E_n^{(i)}\left|h_{k,n}^{(i)}\right|^2 A_k^{(i)}\left(1-\frac{\rho}{4}\right)\right)}\right\}. \tag{4.25}$$

Given that $i_{agg} = \sigma_{I,N}^2 + \sigma_{I,L}^2$, the separation of expectations arises from the independence between ϕ_N and ϕ_L. Therefore, we can calculate these two terms individually by substituting $\sigma_{I,N}^2$ and $\sigma_{I,L}^2$. To do this, we used the probability generating functional (PGFL) of a PPP in [68] as follows:

$$\mathbb{E}\left\{e^{-s\sigma_{I,N}^2}\right\} = \mathbb{E}\left\{\prod_{r_i\in\phi_N\setminus\{k\}} e^{-s\left(\Omega_N(r_i)E_n^{(i)}\left|h_{k,n}^{(i)}\right|^2 A_k^{(i)}\left(1-\frac{\rho}{4}\right)\right)}\right\}$$

$$= \exp\left(-2\pi \int_0^\infty \mathbb{E}_{A_k}\left\{1-\mathbb{E}_{h_{k,n}}\left\{e^{-s\left(1-\frac{\rho}{4}\right)\Omega_N(t)E_n\left|h_{k,n}\right|^2 A_k}\right\}\right\}\lambda P_N(t\,)tdt\right). \quad (4.26)$$

Note that in (4.26), the integral limit is owing to the max-SINR association, as mentioned earlier. Given that $h_{k,n}$ follows a Nakagami-m distribution, and A_k is assumed to be a Bernoulli random variable, their LTs can be straightforwardly evaluated, as seen in [60] and [58], and is given by the following:

$$\mathbb{E}_{A_k}\left\{1-\mathbb{E}_{h_{k,n}}\left\{e^{-s\left(1-\frac{\rho}{4}\right)\Omega_N(t)E_n\left|h_{k,n}\right|^2 A_k}\right\}\right\} = \sum_{z=1}^{4} b_z\left(1-\frac{1}{\left(1+s\left(1-\frac{\rho}{4}\right)\Omega_N(t)E_n\,\bar{a}_z/m_N\right)^{m_N}}\right), \quad (4.27)$$

where $\bar{a}_z = a_z/M_{Tx_k}M_{Rx_k}$. Calculating the LT of NLOS interference links involves substituting (4.27) into (4.26) as follows:

$$\mathbb{E}\left\{e^{s\,\sigma_{I,N}^2}\right\} = \exp\left(-2\pi\lambda\sum_{z=1}^{4} b_z\int_0^\infty D\left(m_N, s\left(1-\frac{\rho}{4}\right)\Omega_N(t)E_n\bar{a}_z\right)P_N(t\,)tdt\,\right), \quad (4.28)$$

where $D(v,x) = 1-\frac{1}{(1+x/v)^v}$. Because the calculation of the LT of LOS interference links is similar to the NLOS case, the LT of LOS interference can be expressed as,

$$\mathbb{E}\left\{e^{s\,\sigma_{I,L}^2}\right\} = \left\{\prod_{r_i\in\phi_L\backslash\{k\}} e^{-s\left(\Omega_L(r_i)E_n^{(i)}\left|h_{k,n}^{(i)}\right|^2 A_k^{(i)}(1-\rho/4)\right)}\right\}$$

$$= \exp\left(-2\pi\lambda\sum_{z=1}^{4} b_z\int_0^\infty D\left(m_L, s\left(1-\frac{\rho}{4}\right)\Omega_L(t)E_n\bar{a}_z\right)P_L(t\,)tdt\right). \quad (4.29)$$

Finally, the LT of i_{agg} is expressed as a multiplication of (4.28) and (4.29), and is given by the following:

$$\mathcal{L}_{i_{agg}}(s) = \mathbb{E}\left\{e^{s\,\sigma_{I,N}^2}\right\}\mathbb{E}\left\{e^{s\,\sigma_{I,L}^2}\right\} = \exp(-2\pi\lambda\sum_{z=1}^{4} b_z\ [V_L(z,s,r)+V_N(z,s,r)]), \quad (4.30)$$

where,

$$V_L(z,s,r) = \int_0^\infty D\left(m_L, s\left(1-\frac{\rho}{4}\right)\Omega_L(t)E_n\bar{a}_z\right)P_L(t)tdt, \quad (4.31)$$

$$V_N(z,s,r) = \int_0^\infty D\left(m_N, s\left(1-\frac{\rho}{4}\right)\Omega_N(t)E_n\bar{a}_z\right)P_N(t)tdt. \quad (4.32)$$

4.3.3 Total ASER:

The previous analysis involved averaging the SER over $h_{k,n}^{(k)}$, and the aggregate interference. The only remaining task is to obtain the average SER of (4.24A) and (4.24B) over the LOS and NLOS scenarios of the desired link. To accomplish this, we separately evaluate the $ASER$ for both the LOS and NLOS scenarios (i.e., $ASER\ (r \in \phi_L)$ and $ASER\ (r \in \phi_N)$), from the previous section. In the final step, we combine these probabilities to calculate the average $ASER$ over the LOS and NLOS scenarios of the desired link.

Starting from the last step, we denote the entire set of error events where the k^{th} Rx is connected by either an LOS link *or* an NLOS link, from the k^{th} Tx, with a fixed distance, r. The $ASER$ can then be expressed as follows:

$$ASER = ASER\ (r \in \phi_L)P_L(r) + ASER\ (r \in \phi_N)P_N(r), \tag{4.33}$$

where $P_L(r)$ and $P_N(r)$ are defined in Section II-A. The term $ASER\ \left(r \in \phi_q\right)$ is defined as the occurrence of an SER associated with a transmitter of the desired link in ϕ_q for $q \in \ \{L, N\}$. Based on the discussion in Section II-A, it has been established that the desired link of the k^{th} Rx is served by either an LOS link or an NLOS link from the k^{th} Tx. This insight allowed us to categorize the set of error events into two disjoint subsets, enabling the separation of $ASER_L$and $ASER_N$. This is analogous to the baseline model in [58] or when the beam is misaligned [61], with the difference being that these studies are focused on coverage events, while here we are dealing with error events. Starting with $ASER\ (r \in \phi_L)$, it is expressed as:

$$ASER\ (r \in \phi_L) = P_{I|L} - P_{II|L}. \tag{4.34}$$

The terms $P_{I|L}$ and $P_{II|L}$ represent the conditional SER in (4.24A) and (4.24B), respectively, given that the desired link has an LOS scenario and is given by

$$P_{I|L} = 2w - \frac{4w\Gamma\left(m_L\ + \frac{1}{2}\right)}{\pi\Gamma(m_L)} \int_0^\infty \frac{e^{-s\left(1+\frac{m_L}{\alpha\,\gamma}\right)}}{\sqrt{s}}$$

$$\times \exp\left(-2\pi\lambda \textstyle\sum_{z=1}^{4} b_z\left(V_L^{(L)} + V_N^{(L)}\right)\right) {}_1F_1\left(1 - m_L; \tfrac{3}{2}, s\right) ds \qquad (4.35A)$$

and

$$P_{II|L} = w^2 - \left(\frac{4w^2 m_L}{\pi}\right) \int_0^\infty e^{-s\frac{m_L}{\alpha\,\gamma}} \exp\left(-2\pi\lambda \sum_{z=1}^{4} b_z\left(V_L^{(L)} + V_N^{(L)}\right)\right)$$

$$\times \textstyle\int_0^{\frac{\pi}{4}} {}_1F_1(1 + m_L\,; 2, -s/\sin^2(\vartheta)) \frac{d\vartheta}{\sin^2(\vartheta)}\ ds, \qquad (4.35B)$$

where,

$$V_N^{(L)} = V_N\left(z, \frac{m_L/\alpha}{E_n^{(k)}\Omega_L(r)}\ s, t\right) = \textstyle\int_0^\infty D\left(m_N, \bar{a}_z(1 - \rho/4)\left(\frac{r^{v_N}}{t^{v_L}}\right) \frac{m_L}{\alpha SIR^{(k,i)}} s\right) P_N(t\,)tdt \quad (4.36)$$

$$V_L^{(L)} = V_L\left(z, \frac{m_L/\alpha}{\Omega_L(r)E_n^{(k)}}\ s, r\right) = \textstyle\int_0^\infty D\left(m_L, \bar{a}_z\left(1 - \frac{\rho}{4}\right)\left(\frac{r}{t}\right)^{v_L} \frac{m_L}{\alpha SIR^{(k,i)}} s\right) P_L(t\,)tdt, \qquad (4.37)$$

where $SIR^{(k,i)} = \frac{E_n^{(k)}}{E_n^{(i)}}$. Given that the desired link has an LOS link (i.e., $\left|h_{k,m}^{(k)}\right|^2 \sim Gamma(m_L, m_L)$ and $\Omega^{(k,m)} = \Omega_L(r)$), substituting the LT of i_{agg} found in (4.30), as $\mathcal{L}_{i_{agg}}\left(\frac{m_L}{\alpha\Omega_L(r)E_n^{(k)}} s\right)$ into (24A) and (24B), this results in (4.35A) and (4.35B). This substitution yields two terms, $V_L^{(L)}$ and $V_N^{(L)}$, as shown in (4.36) and (4.37). These terms correspond to $V_L(z, s, r)$ in (4.31) and $V_N(z, s, r)$ in (4.32), respectively. This illustrates the interference component arising from both the LOS and NLOS transmitters, given that the desired link has an LOS link.

A similar procedure is then employed for the NLOS scenario of the desired link as follows:

$$ASER_N = P_{I|N} - P_{II|N}, \qquad (4.38)$$

Similar to the LOS case, the terms $P_{I|N}$ and $P_{II|N}$ conditioned on the desired link have an NLOS (i.e., $\left|h_{k,m}^{(k)}\right|^2 \sim Gamma(m_N, m_N)$ and $\Omega^{(k,m)} = \Omega_N(r)$) and are given by

$$P_{I|N} = 2w - \frac{4w\Gamma\left(m_N\ + \frac{1}{2}\right)}{\pi\Gamma(m_N)} \int_0^{\infty} \frac{exp\left(-s\left(1 + \frac{m_N r^{(v_N - v_L)}}{\alpha\,\gamma}\right)\right)}{\sqrt{s}}$$

$$\times\, exp\left(-2\pi\lambda \textstyle\sum_{z=1}^{4} b_z\left(V_L^{(N)} + V_N^{(N)}\right)\right) {}_1F_1\left(1 - m_N; \frac{3}{2}, s\right) ds\,, \quad (4.39A)$$

Table 4.1: Main Notations for Chapter 4

$h_{k,m}^{(i)}$	Small-scale fading from the i^{th} Tx to the k^{th} Rx on m^{th}subcarrier.	$SIR^{(k,i)}$	Signal-to-interference ratio from the i^{th} Tx to the k^{th} Rx.
$P_N(r\ )$	Probability of a propagation path being NLOS with distance r.	$P_L(r\ )$	Probability of a propagation path being LOS with distance r.
$E_n^{(i)}$	Energy on the m^{th} subcarrier of the k^{th}.	$X_{m,l}^{(k)}$	l^{th} complex modulated symbol on the m^{th}subcarrier of the k^{th} Tx.
ρ	Roll-off factor of the Nyquist pulse.	β	Blockage parameter.
ϕ_q	Poisson point process for $q \in \{L, N\}$.	v_q	path loss exponents parameters for $q \in\ \{L, N\}$.
$\gamma^{(q)}$	SNR for the k^{th} D2D pair for $q \in \{L, N\}$.	m_q	fading severity parameters for $q \in\ \{L, N\}$.
$A_{tot}^{(i,k)}$	Total directivity gain from the i^{th} Tx to the k^{th} Rx.	$\Omega_q^{(k,m)}(r)$	Path loss of the k^{th} D2D pair at the m^{th} subcarrier for $q \in \{L, N\}$ with distance r.
Note that, L: LOS, and N: NLOS.			

and

$$P_{II|N} = w^2 - \left(\frac{4w^2 m_N}{\pi}\right)\int_0^{\infty} exp\left(-s\frac{m_N r^{(v_N - v_L)}}{\alpha\,\gamma}\right) exp\left(-2\pi\lambda \sum_{z=1}^{4} b_z\left(V_L^{(N)} + V_N^{(N)}\right)\right)$$

$$\times \int_0^{\frac{\pi}{4}} {}_1F_1\left(1 + m_N\, ; 2, -\frac{s}{sin^2(\vartheta)}\right) \frac{d\vartheta}{sin^2(\vartheta)}\, ds, \tag{4.39B}$$

where,

$$V_N^{(N)} = V_N\left(z, \frac{m_N/\alpha}{E_n^{(k)} \Omega_N(r)}\, s, r\right) = \int_0^\infty D\left(m_N, \bar{a}_z \left(1 - \frac{\rho}{4}\right)\left(\frac{r}{t}\right)^{v_N} \frac{m_N}{\alpha SIR^{(k,i)}}\, s\right) P_N(t\,)tdt, \tag{4.40}$$

$$V_L^{(N)} = V_L\left(z, \frac{m_N/\alpha}{E_n^{(k)} \Omega_N(r)} s\,, r\right) = \int_0^\infty D\left(m_L, \bar{a}_z \left(1 - \frac{\rho}{4}\right)\left(\frac{r^{v_L}}{t^{v_N}}\right) \frac{m_N}{\alpha SIR^{(k,i)}} s\right) P_L(t\,)tdt. \tag{4.41}$$

4.4 Numerical Results:

This section presents the error probability for mmWave D2D communication. For simplicity, we assume that each transmitter device transmits at a fixed power, that $SIR^{(k,i)} = SIR$, and that the roll-off factor of the raised-cosine pulse shape is equal to unity (i.e., $\rho = 1$). In addition, the path loss exponents for LOS and NLOS are $v_L = 2$ and $v_N = 3.3$, respectively. The directional antenna gains are listed in Table 4.2.

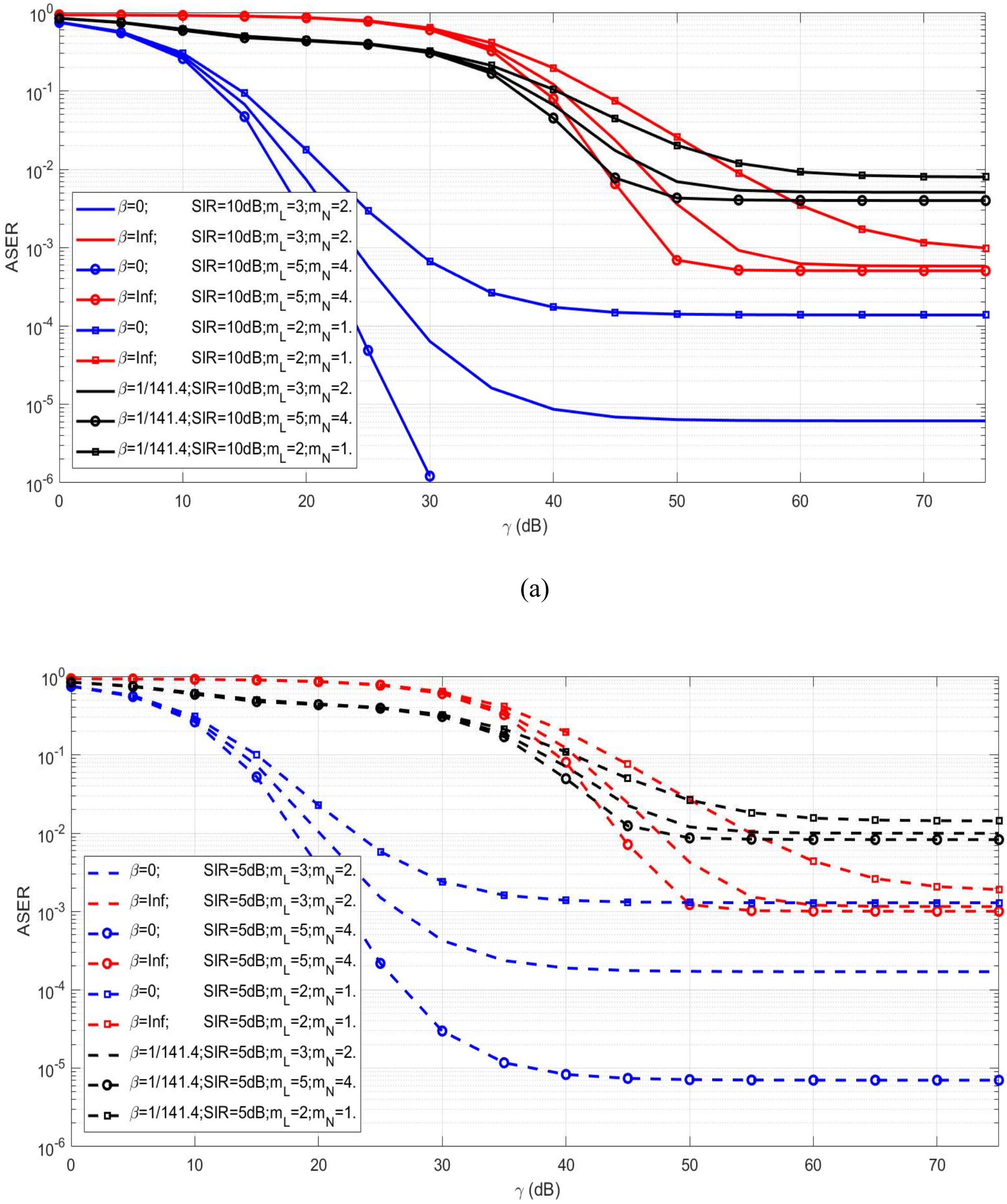
Table 4.2: Directional Antenna Gain

$HPBW$	$M_{Tx} = M_{Rx}$	$m_{Tx} = m_{Rx}$	$\xi = \xi_T = \xi_R$
10.9^o	$24.5\ dBi$	$-3\ dBi$	$109/3600$
30^o	$18\ dBi$	$-3\ dBi$	$1/12$
omnidirectional (360^o)	$0\ dBi$	$0\ dBi$	1

In Figures 4.3, the simulation parameters are set as follows: $r = 100$ m, $16QAM$, $HPBW = 10.9^o$, and $\lambda = 9 \times 10^{-6}$. Figures 4.3 presents the analytical average symbol error rate (ASER) as a function of γ, with curves parameterized for various values of β, m_L, m_N, and SIR. As expected, ASER decreases as γ increases, reaching a point where it becomes almost independent of γ at high SNR levels. Additionally, a lower SIR, as shown in Figure 4.3.(b) yields a worse performance than a higher SIR, as shown in Figure 4.3.(a), particularly around the γ-independent region (i.e., at higher SNR levels). This outcome is anticipated because the system performance becomes interference-limited and is thus predominantly dependent on the SIR.

Moreover, an increase in the fading severity parameters caused the channel to act in a more deterministic manner. The blockage parameter, β, plays a crucial role, as illustrated in Figures 4.3. Two extreme cases are highlighted: $\beta = 0$ for the LOS case where all links, both desired and interfering, are LOS; and $\beta = Inf$ for the NLOS case where all links are NLOS. Both scenarios exhibit better performance than when $\beta = 1/141.4$, in which all links (i.e., both desired and interfering) are subject to blockage at high γ levels, shifting toward an interference-limited region. Interestingly, the difference in the fading severity parameters is negligible in a noise-limited environment, specifically at low γ values. Moreover, in such an environment, NLOS cases generally performed worse than both LOS cases and those with $\beta = 1/141.4$. This is because the system performance in noise-limited scenarios is more significantly determined by the received SNR, denoted as $\gamma^{(L)}$ or $\gamma^{(N)}$. Generally, the difference between $\gamma^{(L)}$ and $\gamma^{(N)}$ depends on r, but always $\gamma^{(L)} > \gamma^{(N)}$, because in mmWave communication, $\nu_N > \nu_L$ must be satisfied [5].

Figure 4.4 is plotted with the following parameters: $r = 100\,\text{m}$, $16QAM$, $HPBW = 10.9^o$, $m_L = 2, m_N = 3$ and $\lambda = 9 \times 10^{-6}$, incorporating various blockage parameters and SIR values. The blockage parameter values were determined based on the discussion in Section II-A. In the noise-limited scenario, the blockage parameter β determines the system's performance tendency toward the LOS regime, as depicted by the blue curves in Figure 4.4, or the NLOS regime, as represented by the red curves in Figure 4.4. As β decreases, for a given distance r, the



(a)

(b)

Figure 4.3: Average symbol error rate $ASER$ versus γ with different values of β, m_L, and m_N: (a) $SIR = 10.$ (b) $SIR = 5.$

probability of LOS, $P_L(r\ )$, increases. Notably at lower SNR levels, smaller β values correspond to improved ASER. Furthermore, in an interference-limited scenario, β has a negligible effect on the interference links at higher SIR values. However, as the SIR decreases, the interference links become more susceptible to the blockage effect.

Similarly, Figure 4.5 is plotted with a fixed SIR of $0dB$, varying the $HPBW$ and β values. As the $HPBW$ widened, as shown in Table I, the total directivity gains decreased, particularly at low γ. Conversely, as the $HPBW$ widens, the k^{th} receiver is likely to encounter more interference links, leading to a degradation in ASER performance. This can be observed in Figure 4.5, specifically around the interference-limited region. An increase in the $HPBW$ results in a more omnidirectional antenna pattern (360^o). This increases the likelihood of capturing the desired signals. However, it also increases the potential for interference. This trade-off is critical in dense networks where the directional antenna provided by a narrower $HPBW$ can significantly mitigate interference, thus enhancing ASER performance. However, this comes at the cost of higher directivity gains for interference when aligned. In addition, this introduces the possibility of beam misalignment errors in the desired link.

Figure 4.6 illustrates ASER versus γ, under settings that include $r = 100$m, $HPBW = 10.9^o$, $m_L = 2$, $m_N = 3$, $\beta = 1/141.4$, and $SIR = 10dB$, to examine the impact of different QAM constellation points and λ values. In scenarios without interference (i.e., $\lambda = 0$), ASER diminishes as γ increases. At lower γ values, interference has a negligible impact, as the system is primarily noise-limited, and performance is solely determined by the SNR. However, as the interference density increased, ASER degraded naturally, as demonstrated in Figure 4.6. Additionally, shifting to smaller QAM constellation sizes, such as from $16QAM$ to $4QAM$, causes

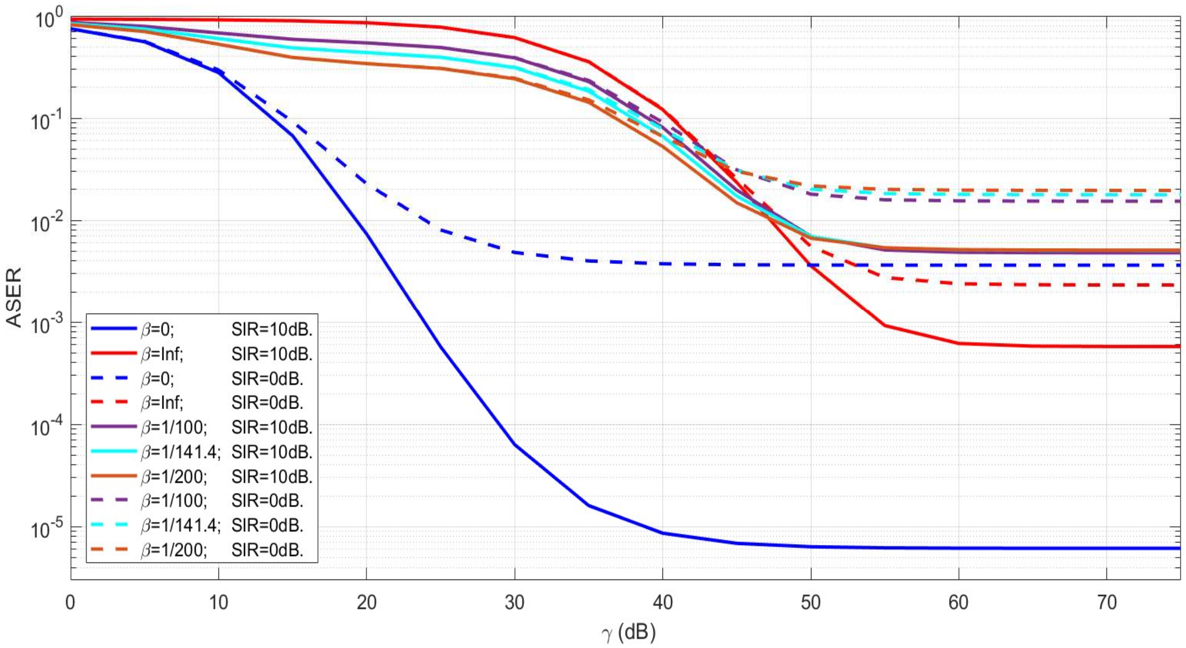


Figure 4.4: Average symbol error rate $ASER$ versus γ with different values of β and SIR.

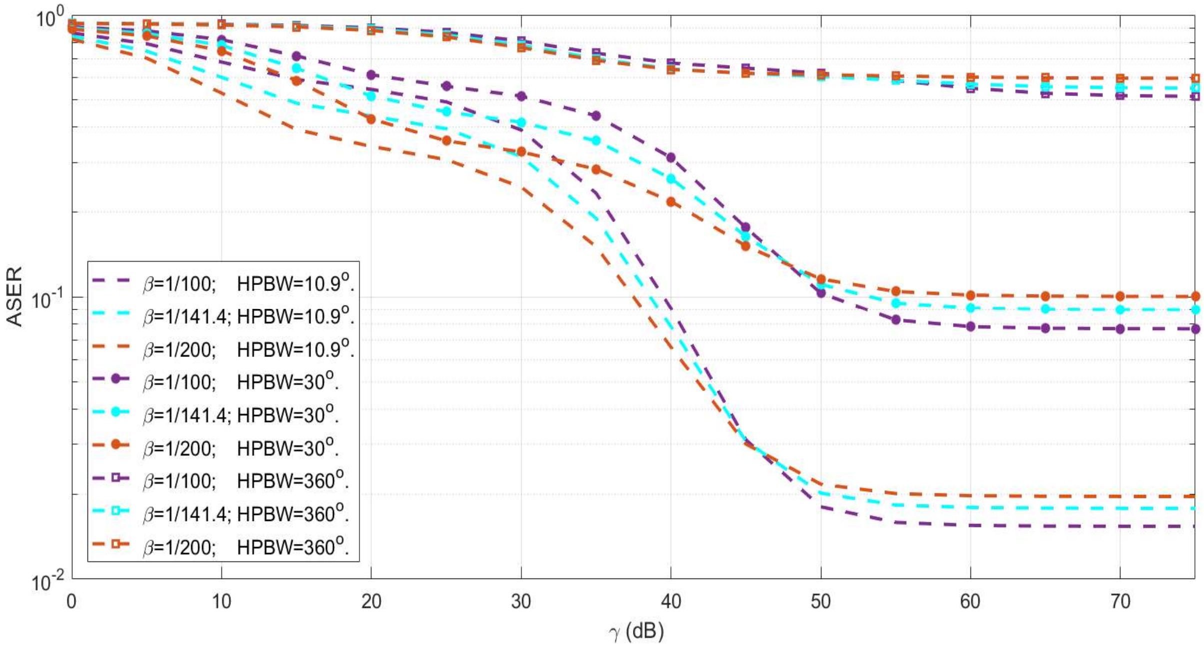


Figure 4.5: Average symbol error rate $ASER$ versus γ with different values of β and $HPBW$.

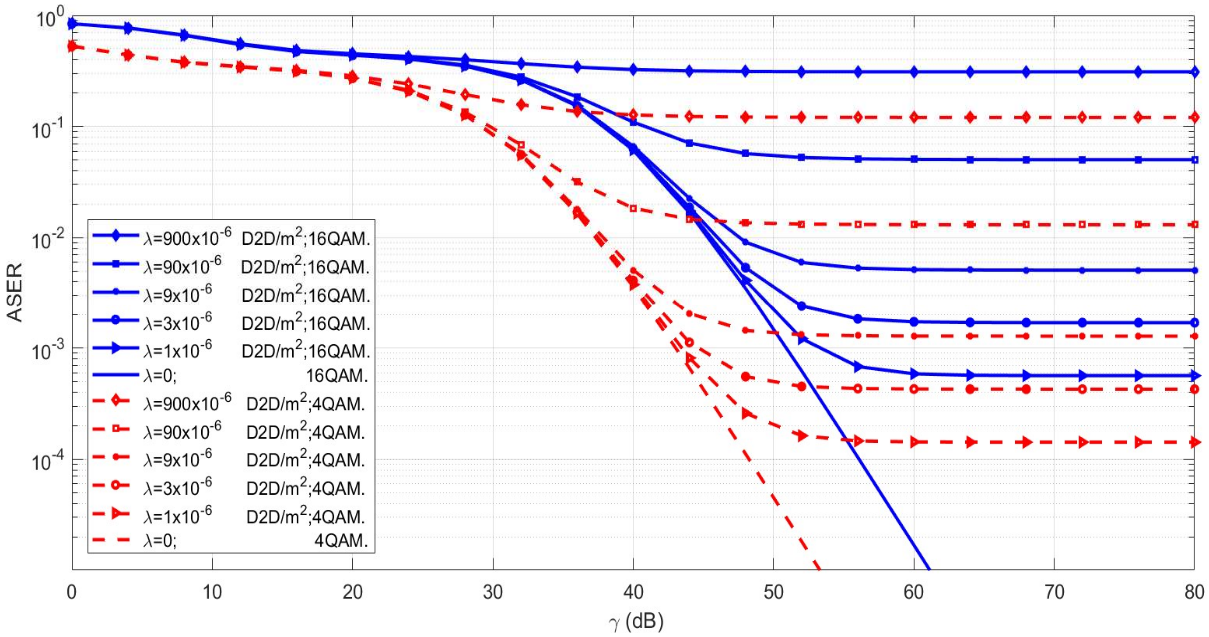


Figure 4.6: Average symbol error rate $ASER$ versus γ with different values of QAM and λ.

ASER curves to shift leftward, indicating improved performance. This is because the smaller constellations perform better under the same conditions.

4.5 Summary

In this chapter, from our analysis shows that an increase in either QAM constellation size or interference density, as well as a decrease in either blockage, $HPBW$, fading severity parameter, or SIR, leads to an increased ASER. Using a stochastic geometry approach provides mathematical flexibility in the analysis of error performance in mmWave D2D networks.

4.6 Acknowledgements:

The text of this chapter is, in part, a reprint of the paper, T. Y. Alkhamees and L. B. Milstein, " Error Analysis for Multicarrier Transmission of Device-to-Device in Millimeter-Wave

Communication," to be submitted to *IEEE Transactions on Vehicular Technology*. The dissertation author is the primary researcher and author of the paper.

Chapter 5:

Conclusion and Future Work

In the first part of our investigation, the optimal disruption of the sensing link in a CRN was derived, with a given of power constraint on the adversary. The disruption strategy was established by maximizing the average number of missed detections. In particular, for CRNs where SUs implemented ED-ENP, and the strategy was equal-power, partial-band flipping. The analysis indicated that increasing the flipping power enabled the adversary to flip more bands, ultimately leading to contamination across all ENP bands.

Future work in the first part includes extending the problem to formulate a joint attack between flipping and spoofing on CRNs. This involves addressing uncertainty about the state of the band for the adversary. In addition, future work will involve examining the performances of various fading channels.

In the second part, we showed the optimal disruption of the sharing link in MC CR-NOMA, subject to a power constraint on the adversary. The strategy for optimal sensing link disruption was formulated by maximizing the average number of DoS bands. Specifically, for MC CR-NOMA launching the pilot jamming attacks by the adversary, we derived and compared the optimal strategy against equal-power allocation approaches.

Future work in the second part involves extending the problem of sharing disruption in a CR-NOMA, where the SU and PU locations are distributed randomly, with the assumption that the adversary is aware of users’ locations probabilistically. Also, combining a jamming attack for both data and channel phases to minimize total throughput. Furthermore, providing a detection scheme and mitigation technique to counter this type of attack.

In the final part, we derived the average error probability of mmWave communications within D2D networks, specifically in environments with dense interference. Our analysis included different orders of $M-QAM$ modulation, blockage parameter, and severity parameters of Nakagami$-m$ fading channels. This study shows the interaction between noise-limited and interference-limited scenarios.

Future work involves extending the problem under high mobility with the possibility of beam misalignment errors in the desired link. In addition, future work can shift to analysis of the performance into a higher frequency band that is around the terahertz (THz) bands.

APPENDIX A: DERIVATIONS SUPPORTING OF CHAPTER 2

A.1 Flipping Attacks Optimization

We can rewrite Equation (2.14) as

$$\min_{P_{1,A},\ldots,P_{U,A}} \quad f_0\left(P_{1,A},\ldots,P_{U,A}\right) = -\sum_{k=1}^{U} \Phi\left(\frac{a\left(P_{k,A}+\rho\sigma_n^2/\alpha\right)}{(1+\gamma)\sigma_n^2/\alpha} + b\right) \tag{A-1}$$

$$s.t \quad f_k\left(P_{1,A},\ldots,P_{U,A}\right) = P_{k,A} \geq 0, \qquad \forall k \in \{1,\ldots,U\},$$

$$h\left(P_{1,A},\ldots,P_{U,A}\right) = \sum_{k=1}^{U} f_k\left(P_{1,A},\ldots,P_{U,A}\right) - P_A = 0$$

The Lagrangian associated with (A-1), is given by

$$L\left(\vec{P}_A, \vec{\lambda}, v\right) = f_0\left(\vec{P}_A\right) - \sum_{k=1}^{U} \lambda_k f_k\left(\vec{P}_A\right) + v\left(\sum_{k=1}^{U} f_k\left(\vec{P}_A\right) - P_A\right) \tag{A-2}$$

where $\vec{\lambda} = [\lambda_1 \;\; \lambda_2 \;\; \ldots \;\; \lambda_U] \in \mathbb{R}^U$ and $v \in \mathbb{R}$ are the Lagrangian multipliers, and $\vec{P}_A = \left[P_{1,A},\ldots,P_{U,A}\right] \in \mathbb{R}^U$. Suppose $\vec{P}_A^*$, $\overrightarrow{\lambda^*}$ and v^* are the optimal set of points. Then, the necessary KKT conditions are stated as follows [42]:

$$\sum_{k=1}^{U} f_k\left(\vec{P}_A^*\right) - P_A = 0, \text{ and } \vec{P}_A^* \succcurlyeq 0 \tag{A-3}$$

$$\lambda_k^* \geq 0, \forall k \in \{1,\ldots,U\} \tag{A-4}$$

$$\lambda_k^* P_{k,A}^* = 0, \forall k \in \{1,\ldots,U\} \tag{A-5}$$

$$\frac{-a}{\sqrt{2\pi}\;\; \sigma_n^2/\alpha(1+\gamma)} e^{-\frac{1}{2}\left(\frac{\left(P_{k,A}^*+\rho\sigma_n^2/\alpha\right)a}{(1+\gamma)\sigma_n^2/\alpha}+b\right)^2} - \lambda_k^* + v^* = 0, \forall k \in \{1,\ldots,U\} \tag{A-6}$$

To fulfil the complementary slackness condition (A-5), we have either the case where $P_{k,A}^* > 0$ and $\lambda_k^* = 0$, for some value of k, and in this case, from (A-6) we have that,

$$v^* = \frac{-a\; e^{-\frac{1}{2}\left(\frac{\left(P_{k,A}^*+\rho\sigma_n^2/\alpha\right)a}{(1+\gamma)\sigma_n^2/\alpha}+b\right)^2}}{\sqrt{2\pi}\;\; \sigma_n^2/\alpha(1+\gamma)} \tag{A-7}$$

Let the set φ_{A} be defined as $\varphi_{\mathrm{A}} = \{k \mid \lambda_k^* = 0, P_{k,A}^* > 0\}$, and let the cardinality of φ_{A} to be u $(0 < u \leq U)$. From (A-7), we can see that, v^* is the same for each $k \in \varphi_{\mathrm{A}}$; thus $P_{k,A}^*$ need to be uniform distributed over all the flipping bands, that means $P_{k,A}^* = P_A/u$.

Another case where $P_{k,A}^* = 0$, and $\lambda_k^* > 0$. For those values of k in this case, from (A-6), we can see that λ_k^* is independent of k. Let the set $\varphi_{\lambda} \triangleq \{k \mid \lambda_k^* > 0, P_{k,A}^* = 0\}$, by definition the cardinality of φ_{λ} is $U - u$. This means that λ_k^* is the same $\forall k \in \varphi_{\lambda}$.

Clearly, in (A-1) objective function is a strict convex because the Hessian matrix is positive definite. Therefore, the KKT conditions became both necessary and sufficient [42]. To conclude, $P_{k,A}^*$ is equal to either $P_{k,A}^* = P_A/u$, for $k \in \varphi_{\mathrm{A}}$, or $P_{k,A}^* = 0$, for $k \in \varphi_{\lambda}$.

A.2 Analysis of u^* :

From (2.17), it is difficult to obtain the solution of $f'(x^*) = 0$, since it is a nonlinear expression. As a consequence, we will evaluate the $f'(x)$ at it is boundaries. Since $x \in (0, \infty)$, then,

$$f'(x)|_{x=0} = \Phi(\infty) - p_{MD} - \lim_{x \longrightarrow 0^+} \frac{a\, P_A}{(1+\gamma)\, x\sigma_n^2/\alpha\, \sqrt{2\pi}}\; e^{-\frac{1}{2}\left(\frac{a(P_A + x\rho\sigma_n^2/\alpha)}{(1+\gamma)\, x\, \sigma_n^2/\alpha} + b\right)^2} \tag{A-8}$$

We define $\varepsilon \triangleq \frac{a\, P_A}{(1+\gamma)\sigma_n^2/\alpha}$, and let $\eta(x) = \frac{\varepsilon}{x\,\sqrt{2\pi}}$, $\theta(x) = e^{\frac{1}{2}\left(\frac{\varepsilon}{x} + \frac{a\,\rho}{(1+\gamma)} + b\right)^2}$, then $\lim_{x \longrightarrow 0^+} \frac{\eta(x)}{\theta(x)} = \frac{\infty}{\infty}$, and thus, we can apply L'Hospital's rule:

$$\lim_{x \longrightarrow 0^+} \frac{\eta'(x)}{\theta'(x)} = \lim_{x \longrightarrow 0^+} \frac{\frac{1}{\sqrt{2\pi}}}{e^{\frac{1}{2}\left(\frac{\varepsilon}{x} + \frac{a\,\rho}{(1+\gamma)} + b\right)^2} \left(\frac{\varepsilon}{x} + \frac{a\,\rho}{(1+\gamma)} + b\right)} = \frac{\frac{1}{\sqrt{2\pi}}}{\infty} = 0 \tag{A-9}$$

Substituting (A-9) into (A-8), we have

$$f'(x)|_{x=0} = 1 - \Phi\left(\frac{a}{\frac{1}{\rho}(1+\gamma)} + b\right) = Q\left(\frac{a}{\frac{1}{\rho}(1+\gamma)} + b\right) \tag{A-10}$$

$\because$ Q(·) is a monotonically decreasing function, thus $Q\left(\frac{a}{\frac{1}{\rho}(1+\gamma)} + b\right) > 0$. Additionally,

$$\lim_{x \to \infty} f'(x) \; = \Phi\left(\frac{a\rho}{1+\gamma} + b\right) - \Phi\left(\frac{a}{\frac{1}{\rho}(1+\gamma)} + b\right) = 0 \qquad \text{(A-11)}$$

Therefore, from (A-10) and (A-11), $f'(x)$ has a positive value at $x = 0$ and approaches 0 as x goes to infinity. To examine $f'(x)$, as x increases throughout the range of $(0, \infty)$, we need to derive $f''(x)$. The second derivative is given by

$$f''(x) = \frac{\partial}{\partial x}\left(\Phi\left(\frac{a\,P_A}{\sigma_n^2/\alpha(1+\gamma)\,x} + \frac{a\rho}{(1+\gamma)} + b\right) - p_{MD} - \frac{aP_A(\alpha/\sigma_n^2)}{(1+\gamma)\,x\,\sqrt{2\pi}}\, e^{-\frac{1}{2}\left(\frac{a\,P_A}{\sigma_n^2/\alpha(1+\gamma)\,x} + \frac{a\rho}{(1+\gamma)} + b\right)^2}\right) \text{(A-12)}$$

Let $y(x) \triangleq \Phi\left(\frac{a\,P_A}{\sigma_n^2/\alpha(1+\gamma)\,x} + \frac{a\rho}{(1+\gamma)} + b\right) - p_{MD}$, and $q(x) \triangleq -\frac{a\,P_A(\alpha/\sigma_n^2)}{(1+\gamma)\,x\,\sqrt{2\pi}}\, e^{-\frac{1}{2}\left(\frac{a(P_A + \rho x \sigma_n^2/\alpha)}{\sigma_n^2/\alpha(1+\gamma)\,x} + b\right)^2}$.

Then, we can express (A-12) as

$$f''(x) = \frac{\partial}{\partial x}\big(y(x) + q(x)\big) = y'(x) + q'(x) \qquad \text{(A-13)}$$

From (2.17), we have that $y'(x) = \frac{1}{\sqrt{2\pi}}\, e^{-\frac{1}{2}\left(\frac{a(P_A + \rho x \sigma_n^2/\alpha)}{\sigma_n^2/\alpha(1+\gamma)\,x} + b\right)^2} \left(\frac{a\,P_A(\alpha/\sigma_n^2)}{(1+\gamma)\,x^2}\right)$, and thus $q(x) = x\,y'(x)$.

The derivate of $q(x)$ is shown to be, $q'(x) = \; y'(x) + xy''(x)$. Therefore, after some algebraic manipulation, $f''(x)$ is expressed as,

$$f''(x) = \frac{(aP_A)^2}{\sqrt{2\pi}}\, e^{-\frac{1}{2}\left(\frac{a\,P_A}{\sigma_n^2/\alpha(1+\gamma)\,x} + \frac{a\rho}{(1+\gamma)} + b\right)^2} \left(-\frac{\left(aP_A + \left(a\rho\,\sigma_n^2/\alpha + b(1+\gamma)\sigma_n^2/\alpha\right)x\right)}{\left(\sigma_n^2/\alpha\right)^3 (1+\gamma)^3\, x^4}\right) \qquad \text{(A-14)}$$

From (A-14) $f''(x)$ is dependent upon a linear function, that is, $f_0(x) \triangleq a\,P_A + (a\rho\,\sigma_n^2/\alpha + b(1+\gamma)\sigma_n^2/\alpha)\,x$, since $\gamma > 0$, $\alpha > 0$, $\sigma_n^2 > 0$, $b > 0$, $a > 0$, $P_A > 0$, $\rho > 0$, and $e^{-\frac{1}{2}\left(\frac{a\,P_A}{\sigma_n^2/\alpha(1+\gamma)\,x} + \frac{a\rho}{(1+\gamma)} + b\right)^2} > 0$, then $f_0(x)$ is a first-order polynomial function, and thus, the slope of $f_0(x)$ is $(\rho\,\sigma_n^2/\alpha + b(1+\gamma)\sigma_n^2/\alpha) > 0$, and $f_0(x)|_{x=0} = a\,P_A > 0$. It is then straightforward to say that $f'(x) > 0$, for any $x \geq 0$. From the above analysis, we conclude that, $f(x)$ continuously increases as x increase for $x \geq 0$.

A.3 Acknowledgements:

This appendix is, in part, a reprint of material published as T. Y. Alkhamees and L. B. Milstein, "A Different Approach for Sensing Disruption," in *IEEE Access*, vol. 11, pp. 86431-86443, 2023, doi: 10.1109/ACCESS.2023.3304244. The dissertation author is the primary researcher and author of this paper.

APPENDIX B: DERIVATIONS SUPPORTING OF CHAPTER 3

B.1 Average Probability of DoS:

In this subsection, we evaluated the average probability of the DoS at the SU. From (3.14), we obtain

$$\overline{P_k} = \mathbb{E}_{\underline{Y_k}}\left\{\mathbb{P}_{DoS}^{(k)}\right\}$$

$$= \int_0^{\infty} Pr\left\{\underline{Y_k} < \theta_{PU}\eta_k \;\middle|\; \underline{Y_k} = z_k\right\} f_{\underline{Y_k}}(z_k)\; dz_k$$

$$= \int_0^{\infty} Pr\left\{\underline{Y} < \frac{\theta_{PU}\eta_k}{1-\sigma_{p,k}^2} \;\middle|\; \underline{Y_k} = z_k\right\} f_{\underline{Y_k}}(z_k)\, dz_k \,, \qquad \text{(B-1)}$$

where $\underline{Y} \sim \text{Exp}(1)$, as $\left|\underline{\hat{h}}_{k,p}\right|^2 \sim \text{Exp}\left(\frac{1}{1-\sigma_{p,k}^2}\right)$. From (3.6) if we substitute $\sigma_{p,k}^2 = \frac{\left(\sigma_{wBS}^2+P_{k,A}\beta_{k,A}z_k\right)}{\beta_{k,p}+\left(\sigma_{wBS}^2+P_{k,A}\beta_{k,A}z_k\right)}$, then the term $\frac{\eta_k}{\left(1-\sigma_{p,k}^2\right)}$ can be simplified as follows:

$$\frac{z_k\overbrace{\left(P_{k,A}\rho_k+P_{k,A}\beta_{k,p}\right)}^{A_1}+\overbrace{\beta_{k,p}\rho_k+\sigma_{wBS}^2\left(\beta_{k,p}+\rho_k\right)}^{A_2}}{\beta_{k,p}^2}. \qquad \text{(B-2)}$$

Now substitute (B-2) into (B-1), we have,

$$\overline{P_k} = \int_0^{\infty} Pr\left\{\underline{Y} < \frac{\theta_{PU}}{\beta_{k,p}^2}\left[z_kA_1 + A_2\right] \middle| \underline{Y_k} = z_k\right\} f_{\underline{Y_k}}(z_k)\, dz_k$$

$$= \int_0^{\infty}\left[1 - e^{-\left(\frac{\theta_{PU}}{\beta_{k,p}^2}\left[A_2+z_kA_1\right]\right)}\right]\frac{1}{\beta_{k,A}}\; e^{-\frac{z_k}{\beta_{k,A}}}\, dz_k$$

$$= 1 - \frac{e^{-\left(\frac{\theta_{PU}}{\beta_{k,p}^2} A_2\right)}}{\beta_{k,A}} \int_0^{\infty} e^{-z_k\left(\frac{\theta_{PU} A_1}{\beta_{k,p}^2} + \frac{1}{\beta_{k,A}}\right)} \, dz_k$$

$$= 1 - \frac{\beta_{k,p}^2}{\theta_{PU} P_{k,A} \, \beta_{k,A} \left[\beta_{k,p} + \rho_k\right] + \beta_{k,p}^2} \, e^{-\left(\frac{\theta_{PU} A_2}{\beta_{k,p}^2}\right)}. \quad \text{(B-3)}$$

B.2 Spectrum Sharing Disruption Attacks Optimization:

Let $\vec{P}_A \triangleq \left[P_{1,A}, \dots, P_{U,A}\right]$ (i.e., the power in each of the U bands), and define the objective function to be, $f_0\left(\vec{P}_A\right) \triangleq \sum_{k=1}^{U} \frac{e^{-(\tilde{a}_k \sigma_{WBS}^2 + \tilde{b}_k)}}{(\tilde{a}_k \, \beta_{k,A} \, f_k(\vec{P}_A) + 1)} - 1$, where $f_k\left(\vec{P}_A\right) \triangleq P_{k,A}$. Finally, let the constraint to be, $h\left(\vec{P}_A\right) \triangleq \sum_{k=1}^{U} f_k\left(\vec{P}_A\right) - P_A$. Then, we can rewrite the optimization problem of (3.17) as,

$$\min_{P_{1,A}, \dots, P_{U,A}} \quad f_0\left(\vec{P}_A\right), \quad \text{(B-4)}$$

$$s.t \quad - f_k\left(\vec{P}_A\right) \leq 0, \quad \forall k \in \{1, \dots, U\},$$

$$h\left(\vec{P}_A\right) = \sum_{k=1}^{U} P_{k,A} - P_A = 0.$$

The Lagrangian associated with (B-4) is given by

$$L\left(\vec{P}_A \ , \vec{\lambda} \, , v\right) = f_0\left(\vec{P}_A\right) - \sum_{k=1}^{U} \lambda_k \, f_k\left(\vec{P}_A\right) + v \, h\left(\vec{P}_A\right), \quad \text{(B-5)}$$

where $\vec{\lambda} = [\lambda_1 \ \ \lambda_2 \ \ \dots \ \ \lambda_U] \in \mathbb{R}^U$and $v \in \mathbb{R}$ are Lagrangian multipliers. Let $\vec{P}_A^*$, $\overrightarrow{\lambda^*}$ and v^*be the optimal sets of points. The KKT conditions are as follows [42].

$$\vec{P}_A^* \succcurlyeq 0 \quad \text{and} \quad \sum_{k=1}^{U} P_{k,A}^* = P_A, \quad \text{(B-6)}$$

$$\lambda_k^* \geq 0, \quad \forall k \in \{1, \dots, U\}, \quad \text{(B-7)}$$

$$\lambda_k^* P_{k,A}^* = 0, \quad \forall k \in \{1, \dots, U\}, \quad \text{(B-8)}$$

$$\frac{-\tilde{a}_k\,\beta_{k,A}\,e^{-(\tilde{a}_k\sigma_{wBS}^2+\,\tilde{b}_k)}}{\left(\,\tilde{a}_k\,\beta_{k,A}\,P_{k,A}^*+1\right)^2}-\lambda_k^*+v^*=0,\forall k\in\{1,\ldots,U\}. \tag{B-9}$$

From (B-9), we see that if $v^*-\frac{(\tilde{a}_k\,\beta_{k,A}\,)\,e^{-(\tilde{a}_k\sigma_{wBS}^2+\,\tilde{b}_k)}}{\left(\,\tilde{a}_k\,\beta_{k,A}\,P_{k,A}^*+1\right)^2}$, then $\lambda_k^*=0$. Thus, relations (B-7) and (B-8) are as follows:

$$v^*\geq\frac{\tilde{a}_k\,\beta_{k,A}\;\,e^{-(\sigma_{wBS}^2\,\tilde{a}_k+\tilde{b}_k\,)}}{\left(\tilde{a}_k\,\beta_{k,A}\,P_{k,A}^*+1\right)^2}, \tag{B-10}$$

$$\left(v^*-\frac{\tilde{a}_k\,\beta_{k,A}\;\,e^{-(\tilde{a}_k\sigma_{wBS}^2+\,\tilde{b}_k)}}{\left(\tilde{a}_k\,\beta_{k,A}\,P_{k,A}^*+1\right)^2}\quad\right)P_{k,A}^*=0, \tag{B-11}$$

where $k\in\{1,\ldots,U\}$. For some values of k, from (B-11), we can state that $P_{k,A}^*$ has a positive root if and only if $v^*<\tilde{a}_k\,\beta_{k,A}\;\,e^{-(\tilde{a}_k\sigma_{wBS}^2+\,\tilde{b}_k)}$. This implies that when $v^*\geq\tilde{a}_k\,\beta_{k,A}\;\,e^{-(\tilde{a}_k\sigma_{wBS}^2+\,\tilde{b}_k)}$, then $P_{k,A}^*\,=0$. Combining these arguments, we need to fulfill the complementary slackness condition of (B-9). Hence, we have:

$$P_{k,A}^*=\begin{cases}\frac{e^{-\frac{1}{2}(\sigma_{wBS}^2\,\tilde{a}_k+\tilde{b}_k\,)}}{\sqrt{\tilde{a}_k\,\beta_{k,A}v^*}}-\frac{1}{a_k\,\beta_{k,A}},if\;\frac{v^*}{\tilde{a}_k\,\beta_{k,A}}<e^{-(\tilde{a}_k\sigma_{wBS}^2+\,\tilde{b}_k)}\\0,\qquad\qquad\qquad\qquad\quad if\;\frac{v^*}{\tilde{a}_k\,\beta_{k,A}}\geq e^{-(\tilde{a}_k\sigma_{wBS}^2+\,\tilde{b}_k)}\end{cases}. \tag{B-12}$$

The term v^* is determined from (B-6), and is given by $\sum_{k=1}^{U}\max\left(0,\left(\frac{e^{-\frac{1}{2}(\sigma_{wBS}^2\,\tilde{a}_k+\tilde{b}_k\,)}}{\sqrt{\tilde{a}_k\,\beta_{k,A}v^*}}-\frac{1}{\tilde{a}_k\,\beta_{k,A}}\right)\right)=P_A$. From (3.16), we can say that$e^{-(\tilde{a}_k\sigma_{wBS}^2+\,\tilde{b}_k)}=1-\mathbb{P}_{DoS}^{(k)}(0)$, from which we can rewrite (B-12) as follows:

$$P_{k,A}^*=\begin{cases}\sqrt{\frac{1-\mathbb{P}_{DoS}^{(k)}(0)}{\tilde{a}_k\,\beta_{k,A}v^*}}-\frac{1}{\tilde{a}_k\,\beta_{k,A}},\mathbb{P}_{DoS}^{(k)}(0)<1-\frac{v^*}{\tilde{a}_k\,\beta_{k,A}}\\0,\qquad\qquad\qquad\qquad\quad\mathbb{P}_{DoS}^{(k)}(0)\geq1-\frac{v^*}{\tilde{a}_k\,\beta_{k,A}}\end{cases}. \tag{B-13}$$

B.3 Acknowledgement:

This appendix is, in part, a reprint of material published as T. Y. Alkhamees and L. B. Milstein, "Impact of Sharing Disruption in MC CR-NOMA," in *IEEE Access*, vol. 11, pp. 82871-82881, 2023, doi: 10.1109/ACCESS.2023.3300659. The dissertation author is the primary researcher and author of this paper.

Bibliography

[1] S. Atapattu, C. Tellambura and H. Jiang, *Energy Detection for Spectrum Sensing in Cognitive Radio*, New York, NY, USA:Springer-Verlag, 2014.

[2] S. K. Sharma, *et al.*, "Cognitive Radio Techniques Under Practical Imperfections: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 1858-1884, Fourthquarter 2015, doi: 10.1109/COMST.2015.2452414.

[3] Y. Zeng *et al.*, "A review on spectrum sensing for cognitive radio: Challenges and solutions," EURASIP J. Adv. Signal Process., vol. 2010, p. 381465, Dec. 2010.

[4] R. Umar *et al.*, "Unveiling the Hidden Assumptions of Energy Detector Based Spectrum Sensing for Cognitive Radios," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 713-728, Second Quarter 2014, doi: 10.1109/SURV.2013.081313.00054.

[5] R. Tandra, "Fundamental limits on detection in low snr," Master's thesis, University of California, Berkeley, 2005.

[6] A. Mariani, A. Giorgetti, and M. Chiani, "Effects of Noise Power Estimation on Energy Detection for Cognitive Radio Applications," in *IEEE Transactions on Communications*, vol. 59, no. 12, pp. 3410-3420, December 2011, doi: 10.1109/TCOMM.2011.102011.100708

[7] Y. Ma, S. Dehnie, and V. D. Chakravarthy, "On the Near-Optimality of Training-Based GLRT Spectrum Sensing," in *IEEE Transactions on Wireless Communications*, vol. 14, no. 9, pp. 4894-4906, Sept. 2015, doi: 10.1109/TWC.2015.2429136.

[8] V. Rakovic *et al.*, "Capacity-Aware Cooperative Spectrum Sensing Based on Noise Power Estimation," in *IEEE Transactions on Communications*, vol. 63, no. 7, pp. 2428-2441, July 2015, doi: 10.1109/TCOMM.2015.2433297.

[9] L. Zhang *et al.*, "Byzantine Attack and Defense in Cognitive Radio Networks: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1342-1363, thirdquarter 2015, doi: 10.1109/COMST.2015.2422735.

[10] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks," in *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 428-445, First Quarter 2013, doi: 10.1109/SURV.2011.122211.00162.

[11] R. K. Sharma and D. B. Rawat, "Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1023-1043, Secondquarter 2015, doi: 10.1109/COMST.2014.2380998.

[12] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan and V. K. Bhargava, "A Survey on Non-Orthogonal Multiple Access for 5G Networks: Research Challenges and Future Trends," in IEEE Journal on Selected Areas in Communications, vol. 35, no. 10, pp. 2181-2195, Oct. 2017, doi: 10.1109/JSAC.2017.2725519.

[13] Y. Liu, Z. Qin, M. Elkashlan, Z. Ding, A. Nallanathan and L. Hanzo, "Nonorthogonal Multiple Access for 5G and Beyond," in *Proceedings of the IEEE*, vol. 105, no. 12, pp. 2347-2381, Dec. 2017, doi: 10.1109/JPROC.2017.2768666.

[14] M. Vaezi, G. A. Aruma Baduge, Y. Liu, A. Arafa, F. Fang and Z. Ding, "Interplay Between NOMA and Other Emerging Technologies: A Survey," in *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 4, pp. 900-919, Dec. 2019, doi: 10.1109/TCCN.2019.2933835.

[15] L. Lv, J. Chen, Q. Ni, Z. Ding and H. Jiang, "Cognitive Non-Orthogonal Multiple Access with Cooperative Relaying: A New Wireless Frontier for 5G Spectrum Sharing," in *IEEE Communications Magazine*, vol. 56, no. 4, pp. 188-195, April 2018, doi: 10.1109/MCOM.2018.1700687.

[16] F. Zhou, Y. Wu, Y. -C. Liang, Z. Li, Y. Wang and K. -K. Wong, "State of the Art, Taxonomy, and Open Issues on Cognitive Radio Networks with NOMA," in *IEEE Wireless Communications*, vol. 25, no. 2, pp. 100-108, April 2018, doi: 10.1109/MWC.2018.1700113.

[17] Z. Ding, P. Fan and H. V. Poor, "Impact of User Pairing on 5G Nonorthogonal Multiple-Access Downlink Transmissions," in *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6010-6023, Aug. 2016, doi: 10.1109/TVT.2015.2480766.

[18] Z. Ding, R. Schober and H. V. Poor, "A General MIMO Framework for NOMA Downlink and Uplink Transmission Based on Signal Alignment," in *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 4438-4454, June 2016, doi: 10.1109/TWC.2016.2542066.

[19] J. Zhu, J. Wang, Y. Huang, S. He, X. You and L. Yang, "On Optimal Power Allocation for Downlink Non-Orthogonal Multiple Access Systems," in *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 12, pp. 2744-2757, Dec. 2017, doi: 10.1109/JSAC.2017.2725618.

[20] Z. Yang, Z. Ding, P. Fan and G. K. Karagiannidis, "On the Performance of Non-orthogonal Multiple Access Systems with Partial Channel Information," in *IEEE Transactions on Communications*, vol. 64, no. 2, pp. 654-667, Feb. 2016, doi: 10.1109/TCOMM.2015.2511078.

[21] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao and K. Zeng, "Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities," in *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8169-8181, Oct. 2019, doi: 10.1109/JIOT.2019.2927379.

[21] W. Hong *et al.*, "The Role of Millimeter-Wave Technologies in 5G/6G Wireless Communications," in *IEEE Journal of Microwaves*, vol. 1, no. 1, pp. 101-122, Jan. 2021, doi: 10.1109/JMW.2020.3035541.

[22] T. S. Rappaport *et al.*, "Millimeter Wave Mobile Communications for 5G Cellular: It Will Work!," in *IEEE Access*, vol. 1, pp. 335-349, 2013, doi: 10.1109/ACCESS.2013.2260813.

[23] T. S. Rappaport, F. Gutierrez, E. Ben-Dor, J. N. Murdock, Y. Qiao and J. I. Tamir, "Broadband Millimeter-Wave Propagation Measurements and Models Using Adaptive-Beam Antennas for Outdoor Urban Cellular Communications," in *IEEE Transactions on Antennas and Propagation*, vol. 61, no. 4, pp. 1850-1859, April 2013, doi: 10.1109/TAP.2012.2235056.

[24] T. S. Rappaport, G. R. MacCartney, M. K. Samimi and S. Sun, "Wideband Millimeter-Wave Propagation Measurements and Channel Models for Future Wireless Communication System Design," in *IEEE Transactions on Communications*, vol. 63, no. 9, pp. 3029-3056, Sept. 2015, doi: 10.1109/TCOMM.2015.2434384.

[26] H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," in *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 767-809, Secondquarter 2022, doi: 10.1109/COMST.2022.3159185.

[27] G. Ding *et al.*, "Robust Spectrum Sensing With Crowd Sensors," in *IEEE Transactions on Communications*, vol. 62, no. 9, pp. 3129-3143, Sept. 2014, doi: 10.1109/TCOMM.2014.2346775.

[28] S. Anand, Z. Jin and K. P. Subbalakshmi, "An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks," *2008 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Chicago, IL, USA, 2008, pp. 1-6, doi: 10.1109/DYSPAN.2008.16.

[29] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Impact of Primary User Emulation Attacks on Dynamic Spectrum Access Networks," in *IEEE Transactions on Communications*, vol. 60, no. 9, pp. 2635-2643, September 2012, doi: 10.1109/TCOMM.2012.071812.100729.

[30] Q. Peng, P. C. Cosman and L. B. Milstein, "Optimal Sensing Disruption for a Cognitive Radio Adversary," in *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1801-1810, May 2010, doi: 10.1109/TVT.2010.2043966.

[31] M. Soysa, P. C. Cosman and L. B. Milstein, "Optimized Spoofing and Jamming a Cognitive Radio," in *IEEE Transactions on Communications*, vol. 62, no. 8, pp. 2681-2695, Aug. 2014, doi: 10.1109/TCOMM.2014.2331964.

[32] Q. Peng, P. C. Cosman and L. B. Milstein, "Optimal Sensing Disruption: A Generalized Framework for a Power-Limited Adversary," in IEEE Transactions on Communications, vol. 67, no. 2, pp. 1341-1355, Feb. 2019, doi: 10.1109/TCOMM.2018.2874888.

[33] H. Li and Z. Han, "Dogfight in Spectrum: Combating Primary User Emulation Attacks in Cognitive Radio Systems, Part I: Known Channel Statistics," in *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3566-3577, November 2010, doi: 10.1109/TWC.2010.091510.100629.

[34] C. Cordeiro, K. Challapali, D. Birru, and S. Shankar N "IEEE 802.22: an introduction to the first wireless standard based on cognitive radios," J. Commun., vol. 1, no. 1, pp. 38–47, Apr. 2006.

[35] Ecma 392: MAC and PHY for Operation in TV White Spaces, Ecma International Std., Dec. 2012. Available: http://www.ecma-international. org/publications/standards/Ecma-392.htm.

[36] H. Urkowitz, "Energy detection of unknown deterministic signals," in *Proceedings of the IEEE*, vol. 55, no. 4, pp. 523-531, April 1967, doi: 10.1109/PROC.1967.5573.

[37] S. M. Kay, *Fundamentals of Statistical Processing: Estimation Theory*. Prentice-Hall, 1993, vol. 1.

[38] D. A. Shnidman, "Radar detection probabilities and their calculation," in *IEEE Transactions on Aerospace and Electronic Systems*, vol. 31, no. 3, pp. 928-950, July 1995, doi: 10.1109/7.395246.

[39] J. J. Lehtomaki, M. Juntti and H. Saarnisaari, "CFAR strategies for channelized radiometer," in *IEEE Signal Processing Letters*, vol. 12, no. 1, pp. 13-16, Jan. 2005, doi: 10.1109/LSP.2004.839701.

[40] M. Abramowitz and I. A. Stegun, editors, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*., National Bureau of Standards Applied Mathematics Series 55, Washington, D.C.: U. S. Government Printing Office, 1964.

[41] M. Soysa, P. C. Cosman and L. B. Milstein, "Disruptive Attacks on Video Tactical Cognitive Radio Downlinks," in *IEEE Transactions on Communications*, vol. 64, no. 4, pp. 1411-1422, April 2016, doi: 10.1109/TCOMM.2016.2535257.

[42] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[43] H. Hancock, *Theory of Maxima and Minima*. New York: Dover, 1960.

[44] C. Shahriar *et al.*, "PHY-Layer Resiliency in OFDM Communications: A Tutorial," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 292-314, First quarter 2015, doi: 10.1109/COMST.2014.2349883.

[45] R. Miller and W. Trappe, "On the Vulnerabilities of CSI in MIMO Wireless Communication Systems," in *IEEE Transactions on Mobile Computing*, vol. 11, no. 8, pp. 1386-1398, Aug. 2012, doi: 10.1109/TMC.2011.156.

[46] X. Zhou, B. Maham and A. Hjorungnes, "Pilot Contamination for Active Eavesdropping," in *IEEE Transactions on Wireless Communications*, vol. 11, no. 3, pp. 903-907, March 2012, doi: 10.1109/TWC.2012.020712.111298.

[47] B. Akgun, M. Krunz and O. Ozan Koyluoglu, "Vulnerabilities of Massive MIMO Systems to Pilot Contamination Attacks," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 5, pp. 1251-1263, May 2019, doi: 10.1109/TIFS.2018.2876750.

[48] K. -W. Huang, H. -M. Wang, Y. Wu and R. Schober, "Pilot Spoofing Attack by Multiple Eavesdroppers," in *IEEE Transactions on Wireless Communications*, vol. 17, no. 10, pp. 6433-6447, Oct. 2018, doi: 10.1109/TWC.2018.2859949.

[49] H. -M. Wang and S. -D. Wang, "Cooperative Pilot Spoofing in MU-MIMO Systems," in IEEE Wireless Communications Letters, vol. 9, no. 11, pp. 1956-1960, Nov. 2020, doi: 10.1109/LWC.2020.3009370.

[50] T. C. Clancy and N. Goergen, "Security in Cognitive Radio Networks: Threats and Mitigation," *2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*, Singapore, 2008, pp. 1-8, doi: 10.1109/CROWNCOM.2008.4562534.

[51] T. C. Clancy, "Efficient OFDM Denial: Pilot Jamming and Pilot Nulling," *2011 IEEE International Conference on Communications (ICC)*, Kyoto, Japan, 2011, pp. 1-5, doi: 10.1109/icc.2011.5962467.

[52] X. Zhou, D. Niyato and A. Hjorungnes, "Optimizing Training-Based Transmission Against Smart Jamming," in *IEEE Transactions on Vehicular Technology*, vol. 60, no. 6, pp. 2644-2655, July 2011, doi: 10.1109/TVT.2011.2151890.

[53] H. Pirzadeh, S. M. Razavizadeh and E. Björnson, "Subverting Massive MIMO by Smart Jamming," in *IEEE Wireless Communications Letters*, vol. 5, no. 1, pp. 20-23, Feb. 2016, doi: 10.1109/LWC.2015.2487960.

[54] N. Wang, L. Jiao, A. Alipour-Fanid, M. Dabaghchian and K. Zeng, "Pilot Contamination Attack Detection for NOMA in 5G mm-Wave Massive MIMO Networks," in *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1363-1378, 2020, doi: 10.1109/TIFS.2019.2939742.

[55] N. Nandan, S. Majhi and H. -C. Wu, "Beamforming and Power Optimization for Physical Layer Security of MIMO-NOMA Based CRN Over Imperfect CSI," in *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 5990-6001, June 2021, doi: 10.1109/TVT.2021.3079136.

[56] S. N. Diggavi and T. M. Cover, "The worst additive noise under a covariance constraint," in *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 3072-3081, Nov. 2001, doi: 10.1109/18.959289.

[57] Z. Ding, F. Adachi and H. V. Poor, "The Application of MIMO to Non-Orthogonal Multiple Access," in *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 537-552, Jan. 2016, doi: 10.1109/TWC.2015.2475746

[58] J. G. Andrews, T. Bai, M. N. Kulkarni, A. Alkhateeb, A. K. Gupta and R. W. Heath, "Modeling and Analyzing Millimeter Wave Cellular Systems," in *IEEE Transactions on Communications*, vol. 65, no. 1, pp. 403-430, Jan. 2017, doi: 10.1109/TCOMM.2016.2618794.

[59] T. Bai, R. Vaze and R. W. Heath, "Analysis of Blockage Effects on Urban Cellular Networks," in *IEEE Transactions on Wireless Communications*, vol. 13, no. 9, pp. 5070-5083, Sept. 2014, doi: 10.1109/TWC.2014.2331971.

[60] T. Bai and R. W. Heath, "Coverage and Rate Analysis for Millimeter-Wave Cellular Networks," in *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 1100-1114, Feb. 2015, doi: 10.1109/TWC.2014.2364267.

[61] M. Cheng, J. -B. Wang, Y. Wu, X. -G. Xia, K. -K. Wong and M. Lin, "Coverage Analysis for Millimeter Wave Cellular Networks With Imperfect Beam Alignment," in *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8302-8314, Sept. 2018, doi: 10.1109/TVT.2018.2842213.

[62] K. Venugopal, M. C. Valenti and R. W. Heath, "Device-to-Device Millimeter Wave Communications: Interference, Coverage, Rate, and Finite Topologies," in *IEEE Transactions on Wireless Communications*, vol. 15, no. 9, pp. 6175-6188, Sept. 2016, doi: 10.1109/TWC.2016.2580510.

[63] S. Kusaladharma, Z. Zhang and C. Tellambura, "Interference and Outage Analysis of Random D2D Networks Underlaying Millimeter-Wave Cellular Networks," in *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 778-790, Jan. 2019, doi: 10.1109/TCOMM.2018.2870378.

[64] L. Tlebaldiyeva, B. Maham and T. A. Tsiftsis, "Device-to-Device mmWave Communication in the Presence of Interference and Hardware Distortion Noises," in *IEEE Communications Letters*, vol. 23, no. 9, pp. 1607-1610, Sept. 2019, doi: 10.1109/LCOMM.2019.2922905.

[65] K. Belbase, C. Tellambura and H. Jiang, "Coverage, Capacity, and Error Rate Analysis of Multi-Hop Millimeter-Wave Decode and Forward Relaying," in *IEEE Access*, vol. 7, pp. 69638-69656, 2019, doi: 10.1109/ACCESS.2019.2919099.

[66] A. Aboutaleb, W. Fatnassi, Z. Rezki and A. Chaaban, "Optimal Diversity and Coding Gains for Millimeter-Wave Communication," in *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4601-4614, May 2021, doi: 10.1109/TVT.2021.3071330.

[67] E. Turgut and M. C. Gursoy, "Average Error Probability Analysis in mmWave Cellular Networks," *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, Boston, MA, USA, 2015, pp. 1-5, doi: 10.1109/VTCFall.2015.7390851.

[68] M. Haenggi, *Stochastic Geometry for Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

[69] H. ElSawy, A. Sultan-Salem, M. -S. Alouini and M. Z. Win, "Modeling and Analysis of Cellular Networks Using Stochastic Geometry: A Tutorial," in *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 167-203, Firstquarter 2017, doi: 10.1109/COMST.2016.2624939.

[70] Y. Hmamouche, M. Benjillali, S. Saoudi, H. Yanikomeroglu and M. D. Renzo, "New Trends in Stochastic Geometry for Wireless Networks: A Tutorial and Survey," in *Proceedings of the IEEE*, vol. 109, no. 7, pp. 1200-1252, July 2021, doi: 10.1109/JPROC.2021.3061778.

[71] M. Z. Win, P. C. Pinto and L. A. Shepp, "A Mathematical Theory of Network Interference and Its Applications," in *Proceedings of the IEEE*, vol. 97, no. 2, pp. 205-230, Feb. 2009, doi: 10.1109/JPROC.2008.2008764.

[72] Y. Cai, Z. Qin, F. Cui, G. Y. Li and J. A. McCann, "Modulation and Multiple Access for 5G Networks," in *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 629-646, Firstquarter 2018, doi: 10.1109/COMST.2017.2766698.

[73] R. Nissel, S. Schwarz and M. Rupp, "Filter Bank Multicarrier Modulation Schemes for Future Mobile Communications," in *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 8, pp. 1768-1782, Aug. 2017, doi: 10.1109/JSAC.2017.2710022.

[74] N. C. Beaulieu and Julian Cheng, "Precise error-rate analysis of bandwidth-efficient BPSK in Nakagami fading and cochannel interference," in *IEEE Transactions on Communications*, vol. 52, no. 1, pp. 149-158, Jan. 2004, doi: 10.1109/TCOMM.2003.822187.

[75] P. Wu, P. C. Cosman and L. B. Milstein, "Resource Allocation for Multicarrier Device-to-Device Video Transmission: Symbol Error Rate Analysis and Algorithm Design," in *IEEE Transactions on Communications*, vol. 65, no. 10, pp. 4446-4462, Oct. 2017, doi: 10.1109/TCOMM.2016.2623313.

[76] X. Liu and L. Hanzo, "Exact BER of Rectangular-Constellation Quadrature Amplitude Modulation Subjected to Asynchronous Co-Channel Interference and Nakagami-m Fading," *2007 IEEE Wireless Communications and Networking Conference*, Hong Kong, China, 2007, pp. 2216-2220, doi: 10.1109/WCNC.2007.414.

[77] M. D. Renzo and W. Lu, "The Equivalent-in-Distribution (EiD)-Based Approach: On the Analysis of Cellular Networks Using Stochastic Geometry," in *IEEE Communications Letters*, vol. 18, no. 5, pp. 761-764, May 2014, doi: 10.1109/LCOMM.2014.030714.132865.

[78] Y. M. Shobowale and K. A. Hamdi, "A unified model for interference analysis in unlicensed frequency bands," in *IEEE Transactions on Wireless Communications*, vol. 8, no. 8, pp. 4004-4013, August 2009, doi: 10.1109/TWC.2009.070276.

[79] P. C. Pinto and M. Z. Win, "Communication in a Poisson Field of Interferers--Part I: Interference Distribution and Error Probability," in *IEEE Transactions on Wireless Communications*, vol. 9, no. 7, pp. 2176-2186, July 2010, doi: 10.1109/TWC.2010.07.060438.

[80] A. AlAmmouri, H. ElSawy, O. Amin and M. -S. Alouini, "In-Band α -Duplex Scheme for Cellular Networks: A Stochastic Geometry Approach," in *IEEE Transactions on Wireless Communications*, vol. 15, no. 10, pp. 6797-6812, Oct. 2016, doi: 10.1109/TWC.2016.2591005.

[81] L. H. Afify, H. ElSawy, T. Y. Al-Naffouri and M. -S. Alouini, "The Influence of Gaussian Signaling Approximation on Error Performance in Cellular Networks," in *IEEE Communications Letters*, vol. 19, no. 12, pp. 2202-2205, Dec. 2015, doi: 10.1109/LCOMM.2015.2469686.

[82] A. Giorgetti and M. Chiani, "Influence of fading on the Gaussian approximation for BPSK and QPSK with asynchronous cochannel interference," in *IEEE Transactions on Wireless Communications*, vol. 4, no. 2, pp. 384-389, March 2005, doi: 10.1109/TWC.2004.843036.

[83] N. C. Beaulieu, "A useful integral for wireless communication theory and its application to rectangular signaling constellation error rates," in *IEEE Transactions on Communications*, vol. 54, no. 5, pp. 802-805, May 2006, doi: 10.1109/TCOMM.2006.874003.

[84] M. K. Simon and M.-S. Alouini, *Digital Communication Over Fading Channels*. New York, NY, USA: Wiley, 2004

[85] K. A. Hamdi, "A Useful Technique for Interference Analysis in Nakagami Fading," in *IEEE Transactions on Communications*, vol. 55, no. 6, pp. 1120-1124, June 2007, doi: 10.1109/TCOMM.2007.898823.