UNIVERSITY OF CALIFORNIA, SAN DIEGO

Video Transmission in Tactical Cognitive Radio Networks Under Disruptive Attacks

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

in

Electrical Engineering
(Communication Theory and Systems)

by

Madushanka Soysa

Committee in charge:

Professor Pamela C. Cosman, Chair
Professor Laurence B. Milstein, Co-Chair
Professor Patrick J. Fitzsimmons
Professor William S. Hodgkiss
Professor Paul H. Siegel

2015

The dissertation of Madushanka Soysa is approved, and it is acceptable in quality and form for publication on microfilm and electronically:

Co-Chair

Chair

University of California, San Diego

2015

DEDICATION

To Moomoo

EPIGRAPH

The search for truth is more precious than its possession.

— Gotthold Ephraim Lessing

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGEMENTS

I would like to thank everyone who supported me during my Ph.D at UCSD.

First, I would like to extend my sincerest gratitude to my advisors, Professor Pamela Cosman and Professor Laurence Milstein. Their advice and guidance have been inestimable and critical in the completion of my research. Their approach to tackling research problems, with the combination of close attention to detail and broad view analysis, is a valuable learning outcome that I am grateful for. They encouraged independent pursuit of research ideas, closely followed the progress, and provided useful direct feedback, which guided the work. The interest they showed in my research directions boosted my confidence in my ability to tackle the research problems, and I am very thankful for that.

I would like to thank my dissertation committee members, Professor Patrick Fitzsimmons, Professor William Hodgkiss, and Professor Paul Siegel, for their time and useful feedback on my PhD qualifying and defense exams. I am thankful to Professor Siegel also for his feedback during my preliminary exam, and for allowing me to attend the presentations by his research group.

I would also like to express my gratefulness to my parents, sister and Damitha, for all their encouragement and support. I am very grateful for Wimsey, for being an excellent travel companion and for being greatly supportive throughout my PhD. I want to thank Anand for his company and conversations, which were not only immensely enjoyable but also helpful academically. I also want to thank Damith for all his help and for being very accommodating.

I am also grateful for my colleagues Laura, Tu, Brian, Arash, Qing, Huiling, Patrick, Kanke, Jerry, and the rest of my lab-mates, for their technical help, and for being great company. I would like to thank the staff of the ECE department, and all my friends in the US, Finland and Sri Lanka, for all their help.

Chapter 2, in part, is a reprint of material as it appears in M. Soysa, P. Cosman, and L. Milstein, “Optimized spoofing and jamming a cognitive radio,” *IEEE Transactions on Communications*, vol. 62, no. 8, pp. 2681–2695, Aug 2014. The dissertation author was the primary author of this paper.

Chapter 3, in part, is a reprint of material as it appears in M. Soysa, P. Cosman, and L. Milstein, “Spoofing optimization over Nakagami-m fading channels of a cognitive radio adversary,” in *IEEE Global Conference on Signal and Information Processing (GlobalSIP), 2013*, Dec 2013, pp. 1190–1193. The dissertation author was the primary author of this paper.

Chapter 4, in part, is a reprint of material as it may appear in M. Soysa, P. Cosman, and L. Milstein, “Disruptive attacks on video tactical cognitive radio downlinks,” submitted to *IEEE Transactions on Communications.* The dissertation author was the primary author of this paper.

Chapter 5, in part, is a reprint of material as it may appear in M. Soysa, P. Cosman, and L. Milstein, “Video cognitive radio networks under disruptive attack,” manuscript under preparation. The dissertation author was the primary author of this paper.

VITA

2009	B. Sc. in Engineering with Honors, University of Moratuwa, Sri Lanka.
2011	M. Sc. in Electrical and Computer Engineering, University of Alberta, Canada.
2015	Ph. D. in Electrical Engineering, University of California, San Diego.

PUBLICATIONS

M. Soysa, P. Cosman, and L. Milstein, “Disruptive attacks on video tactical cognitive radio downlinks,” submitted to *IEEE Transactions on Communications*, Aug. 2015.

M. Soysa, P. Cosman, and L. Milstein, “Optimized spoofing and jamming a cognitive radio,” *IEEE Transactions on Communications*, vol.62, no.8, pp.2681-2695, Aug. 2014

M. Soysa, N. Rajatheva, and M. Latva-aho, “Linear and non-linear transceiver processing for MIMO-FBMC systems,” *IEEE International Conference on Communications*, pp.4607-4612, Jun. 2014

M. Soysa, P. Cosman, and L. Milstein, “Spoofing optimization over Nakagami-m fading channels of a cognitive radio adversary,” *IEEE Global Conference on Signal and Information Processing*, pp.1190-1193, Dec. 2013

M. Soysa, H.A. Suraweera, C. Tellambura, and H.K. Garg, “Partial and opportunistic relay selection with outdated channel estimates,” *IEEE Transactions on Communications*, vol. 60, no. 3, pp.840-850, Mar. 2012

C. Tellambura, M. Soysa, and D. Senaratne, “Performance analysis of wireless systems from the MGF of the reciprocal of the signal-to-noise ratio,” *IEEE Communication Letters*, vol.15, no.1, pp.55-57, Jan. 2011

H.A. Suraweera, M. Soysa, C. Tellambura, and H.K. Garg, “Performance analysis of partial relay selection with feedback delay,” *IEEE Signal Processing Letters*, vol.17, no.6, pp.531-534, Jun. 2010

ABSTRACT OF THE DISSERTATION

Video Transmission in Tactical Cognitive Radio Networks Under Disruptive Attacks

by

Madushanka Soysa

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

University of California, San Diego, 2015

Professor Pamela C. Cosman, Chair
Professor Laurence B. Milstein, Co-Chair

In this dissertation, I examine the performance of a cognitive radio (CR) system in a hostile environment where an intelligent adversary tries to disrupt communications with a Gaussian noise signal. I analyze a cluster-based network of secondary users (SUs). The adversary can limit access for SUs by either transmitting a spoofing signal in the sensing interval, or a desynchronizing signal in the code acquisition interval. By jamming the network during the transmission interval, the adversary can reduce the rate of successful transmission.

In the first part (Chapters 2 and 3), I investigate the optimal strategy for spoofing and jamming to minimize the SU throughput in a generic communication system. I investigate the system performance under attack over slow and fast Rayleigh fading channels. I present how the adversary can optimally allocate power across subcarriers during sensing and transmission intervals with knowledge of the system, using a simple optimization approach. I determine a worst-case optimal-energy allocation for spoofing and jamming, which gives a lower bound to the overall information throughput of SUs under attack. I then extend the analysis to optimal spoofing power allocation for a CR network operating in Nakagami-m fading. The optimized adversary reduces the throughput by a factor of 4 to 5, relative to an adversary who divides power equally across all bands, around 25 dB jamming-to-signal-power ratio (JSR), under slow fading. Under fast fading, the optimized adversary can disrupt the communication at a JSR 10 dB lower than an unoptimized adversary.

In the second part (Chapters 4 and 5), I consider the disruptive attacks on a video-transmitting CR network. I investigate the optimal strategy for spoofing, desynchronizing and jamming a cluster based CR network with a Gaussian noise signal. I generalize the optimization approach from Chapter 1 to show how the adversary can optimally allocate its energy across subcarriers during sensing, code acquisition and transmission intervals. I determine a worst-case optimal-energy allocation for spoofing, desynchronizing and jamming, which gives an upper bound to the received video distortion of SUs. I also propose cross-layer resource allocation algorithms and evaluate their performance under disruptive attacks. The optimized adversary can reduce the received video peak-signal-to-noise-ratio up to 5 dB lower than an equal-power adversary, at low JSR.

Chapter 1

Introduction

Robust and efficient video transmission over wireless networks has become an important challenge, as mobile video traffic rose to 55% of the total mobile data traffic by the end of 2014 [1]. This is becoming increasingly important, as 72% of mobile data traffic is forecasted to be video traffic by 2019. In the last few years, mobile devices have become increasingly powerful processing units and are being equipped with larger screens, which drive the demand for increasingly higher quality video delivery over wireless channels. With the spread of social media, video sharing from mobile devices has become commonplace. Video communication is important not only for personal use, but also for professional purposes. Videoconferencing is more often used with the global spread of organizations and increase of remote workers, which also increases the video traffic on wireless networks. In addition, video over wireless is attractive in tactical settings, such as surveillance applications [2]. Further, for applications such as search-and-rescue operations, video communication over wireless channels is better suited, as it is easier to send cameras to remote locations without wired network infrastructure.

Increased numbers of users, data communication and increased video communication, have caused the demand for wireless spectrum to grow rapidly. Even though the demand for spectrum has grown, a large portion of the assigned spectrum is used only sporadically. The limited available spectrum and the inefficiency in spectrum usage necessitate a new communication paradigm to exploit the existing wireless spectrum opportunistically. Cognitive radio has been proposed as a solution.

In addition to the constraints in spectrum availability, in tactical networks, a key challenge is the presence of adversarial units that may attempt to disrupt communications. Incidents of radar jamming to disrupt guided enemy missiles or aircrafts, and jamming enemy radio broadcasts, have occurred throughout history since World War II [3]. Attacking consumer broadcasting networks has been used by some governments as a tool of censorship [3]. Further, incidents of jamming mobile devices to disrupt civilian protests and stop the flow of information, such as video broadcasts by protesters, have been reported [3]. There are also several reported incidents of hijacking a radio or TV broadcasts in order to change the broadcasting content, which are called broadcast signal intrusions [4]. With the widening use of unmanned aerial vehicles (UAVs) and video surveillance, the tactical value of video transmission over wireless channels is becoming even more significant now. Therefore, methods of attacks on video transmission over wireless networks, and robustness of communication systems against such potential attacks, are of interest. In this work we investigate video over a tactical cognitive radio network, under a disruptive attack.

1.1 System introduction

1.1.1 Cognitive Radio

Cognitive radio (CR) [5], which allows dynamic spectrum access, has been widely investigated as a solution to improve the spectrum usage efficiency. In CR systems, users are defined as primary users (PUs) if they have priority of access over the spectrum, and secondary users (SUs) otherwise. SUs will sense the wireless channels (or bands) licensed by PUs before transmission, to detect if a PU is already communicating in those bands. Any time an unlicensed SU senses that a licensed band is unused by PUs, it can dynamically access the band, as shown in Figure 1.1, where we denote the sensing intervals which detect PUs by red and the sensing intervals which detect the bands as vacant by green.

1.1.2 Network model

We investigate the impact of an adversary on a cluster-based SU network, as shown in Figure 1.2. We denote the cluster head serving the SUs by the CH, and A is

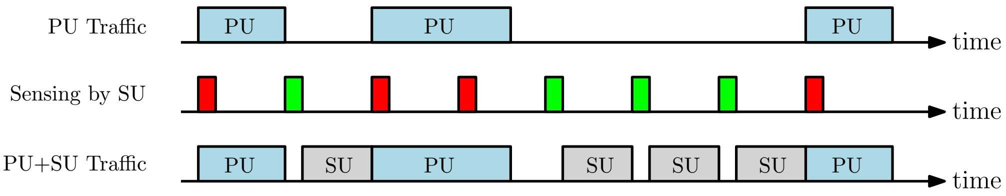


Figure 1.1: Dynamic spectrum access by secondary users

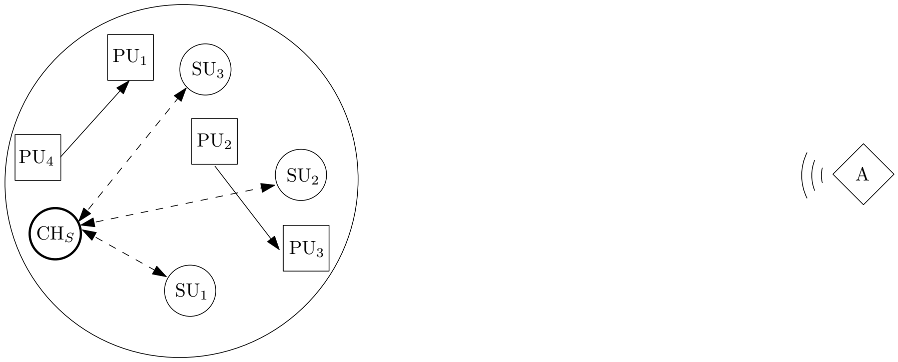


Figure 1.2: The system network model

the adversary. A cluster is an organizational structure in an ad hoc network deployment, and the cluster head acts as a replaceable base station for the cluster. In our system, the CH performs the sensing decision and resource allocation. All SU communication goes through the CH. SUs and the CH transmit video over wireless channels, and we look at both downlink communication from the CH to SUs, and uplink communication from SUs to the CH. The adversary attempts to disrupt the communication by transmitting Gaussian interference signals.

1.1.3 Video source

A video source outputs a sequence of images, where each image can be described by a matrix of pixels. Pixels can be parameterized by either three color values or a luminance and two chrominance values. An uncompressed video described as above contains a large amount of data, which can be prohibitively expensive to transmit over wireless channels, due to limited bandwidth resources. However, because there is significant spatial and temporal correlation among the pixels of a video, it is possible to compress the video data to a fraction of its size without noticeable reductions in quality.

In this work we consider a video source encoded with the H.264/AVC standard [6].

H.264/AVC, first released in 2003, is a block-oriented motion-compensation-based lossy compression standard, which has a wide set of applications from Blu-ray discs to video streaming sources, such as YouTube and Vimeo [7].

H.264 frame types

There are three frame types in H.264; ‘I’, ‘P’ and ‘B’. I-frames are intra-coded frames; i.e. they do not use any information from other frames in encoding or decoding. Therefore, I frames are largest in size, and generally have the highest quality. Further, I frames can stop decoding errors from previous frames propagating further. P frames, or ’predicted’ frames, are encoded using previous I or P frames as a reference. B frames can use bi-directional prediction; i.e., they are encoded using both forward and backward I, P or B frames as references, Therefore, B frames have the most efficient compression out of the three frame types. In encoding, frames are divided in to smaller macroblocks, which are regions of 16 pixels × 16 pixels or smaller [8]. A consecutive group of macroblocks is called a slice, and each slice is encoded independently from other slices [9].

Group of pictures (GOP)

A group of pictures (GOP) is a parameter which defines the order of I, P and B frames. A GOP starts with an I frame, which is followed by several P and B frames. This pattern repeats throughout the video. A short GOP has better protection against error propagation, and using long GOPs improves the compression rate.

In this work we use an IPP GOP structure, with GOP length 15.

Quantization Parameter (QP)

The frame data residual, after prediction from reference frames, is transformed into the spatial frequency domain by an integer transform [8]. The quantization parameter (QP) determines the step size for quantizing the transformed coefficients. Smaller values of QP result in smaller quantization step sizes, and result in a more accurate representation of the spatial frequency spectrum. This relates to a higher quality of video, as the loss of data due to compression is smaller. However, this is at the cost of higher encoded bit rate. Therefore, by varying QP, we can change the compressed video source rate and the quality of the video. The source rate can also be changed by altering the frame rate (temporal scalability), or modifying the video resolution (spatial scalability). In this work, we vary QP to change the source rate and video quality.

Error concealment

Due to channel conditions, noise or interference, there can be packet losses. A packet loss will result in one or more slices not being decoded. Error concealment is a post-processing technique used at the decoder to reconstruct the areas corresponding to the lost slices [10]. A widely used error concealment method is ‘frame-copying’, where a lost slice replaced by the corresponding slice in the nearest reference frame that is already decoded [9]. This is best suited for frames with less motion relative to the reference. Frame-copying is a method of temporal error concealment. Another category of error concealment methods is called spatial error concealment. Here, the lost slices are interpolated using the neighboring macroblocks [10]. Further, the relative motion of the neighboring macroblocks in its frame or reference frames can also be used to recover lost slices, which is called ‘motion-copying’. In this work, we use frame-copying as the method for error concealment.

1.1.4 Multicarrier direct sequence code division multiple access (MC-DS-CDMA)

Direct sequence spread spectrum code division multiple access (DS-CDMA) offers resistance against jamming and is widely used in tactical communication networks. In DS-CDMA, the data is multiplied by a spreading sequence before transmission. At the receiver, the received signal is multiplied by the same sequence to retrieve the original data. The multiplication by the spreading sequence spreads the signal in the frequency domain, and the despreading operation at the receiver spreads the interference in frequency, and retrieves the original symbols, which makes it more robust against jamming signals [11]. In our system, SUs and the CH communicate over a multicarrier direct sequence code division multiple access (MC-DS-CDMA) system. In MC-DS-CDMA, we have several substreams, each of which is a DS-CDMA signal, modulated in different orthogonal frequency bands (subcarriers) [12,13].

1.1.5 Channel fading

Channel fading is the random variations of the signal attenuation in a wireless communication channel. Channel fading changes with time, signal frequency and physical location. Fading can be due to diffractions around large obstacles, or due to reflections and scattering from objects causing multiple versions of the transmitted signal to arrive at the receiver [14].

Slow and Fast fading

Fading is characterized as slow and fast fading, based on the rate of fluctuations in the channel, with reference to the symbol time. The coherence time of a wireless channel is the time period during which the channel remains constant or highly correlated. Slow fading is when the coherence time is larger than the symbol time of the system, and fast fading is when the coherence time is smaller than the symbol time [15].

Flat and frequency selective fading

A channel experiences flat fading if the signal bandwidth is smaller than the coherence bandwidth of the channel. The coherence bandwidth is the range of frequencies over which the channel fading remains constant. In flat fading, all frequency components of the signal undergo the same channel fade. Frequency selective fading is when the coherence bandwidth is smaller than the signal bandwidth, causing different frequency components in the signal to experience different channel fades [15].

Statistical channel models

Due to the rapid fluctuations in wireless channels, statistical models are used to characterize channel fading. One popular statistical model used is Rayleigh fading, which is applicable when there is no line-of-sight (LOS) signal component from the transmitter to the receiver, and the received signal is a combination of reflected paths from a large number of scatterers. The probability distribution function (pdf) of a Rayleigh random variable (r.v.) with scale parameter σ is [14]

$$f(x) = \frac{x}{\sigma^2} e^{-\frac{x^2}{2\sigma^2}}, \quad x \geq 0. \tag{1.1}$$

A more general Nakagami-m fading distribution was developed to fit a range of empirical measurements. The pdf of a Nakagami random variable is

$$f(x) = \frac{2m^m}{\Gamma(m)\Omega^m} x^{2m-1} e^{-\frac{mx^2}{\Omega}}, \quad x \geq 0 \tag{1.2}$$

where $m > \frac{1}{2}$ is the scaling parameter and $\Omega > 0$ is the spreading parameter [14].

In this work, we focus mainly on slow, flat, Rayleigh fading channels, but an extension to Nakagami-m fading is considered in Chapter 3.

1.2 Performance metrics

We use two performance metrics to evaluate the performance of the CR system.

1.2.1 Throughput

The throughput of a wireless system is the number of packets or bits successfully transmitted in a given time interval. This depends on the transmission rate and the error rate, and is applicable to general data communication networks.

1.2.2 Video peak-signal-to-noise-ratio (PSNR)

Video distortion can be defined to be the mean square error (MSE) of the received video, with reference to the source video. Peak-signal-to-noise-ratio (PSNR) is calculated as follows:

$$\text{PSNR} \triangleq 10 \log_{10} \frac{255^2}{\text{MSE}} \quad \text{(dB)}. \tag{1.3}$$

The distortion and the PSNR depend on the video properties, source encoding rate, and frame errors. While throughput is a good performance metric for general data communication systems, it is not suited for video communication networks. For example, consider the two cases where (1) a single transmitted packet is lost due to error and (2) the number of transmitted packets is decreased by one through reduced source rate. In both cases, the throughput is the same. However, in case 1, a packet loss due to error will make one or more slices of a frame undecodable. Therefore, the undecoded area of the frame needs to be reconstructed using neighboring (spatially or temporally) blocks. Further, if the undecodable slices belong to a reference frame, the errors due to imperfect slice recovery can propagate to other frames. In case 2, the encoder can decide on how to allocate bits to macroblocks in order to reduce the source rate as required, while controlling the increase in the overall source distortion. Therefore, the source distortion in case 2 is generally smaller than the concealment distortion in case 1. The distortion in case 1 is further increased by error propagation. Consequently, the distortion increase in case 1 can be significantly higher than that of case 2. Therefore, video distortion and PSNR are better performance metrics than throughput, for video communication networks.

1.3 Methods of disruptive attacks

In this section, we look at the system vulnerabilities and methods of possible disruptive attacks.

1.3.1 Spoofing attack

As discussed in Subsection 1.1.1, spectrum sensing is a key concept for CR, but it is also a vulnerable aspect. An adversary intending to disrupt the communication in a CR network can transmit a spoofing signal during the sensing interval [16]. Here the spoofing signal may cause SUs to mistakenly conclude that the channel is occupied by a PU and therefore, not available for transmission. We call this a spoofing attack. In this way, an intelligent attacker reduces the bandwidth available for the SU. Such exploitations and their impact are discussed in [17–24].

1.3.2 Desynchronizing attack

In MC-DS-CDMA receivers, the received signal is multiplied by the despreading sequence to retrieve the source signal. For this, the receiver must be synchronized with the incoming waveform. This synchronization is achieved through code acquisition, which is an initial detection of the correct phase of the spreading sequence needed to retrieve the source signal. Another method of attack to disrupt the communication is to transmit an interference signal to degrade the performance of the code acquisition process. We call this a desynchronizing attack.

1.3.3 Jamming attack

Further, the adversary can disrupt communications using jamming techniques during data transmission [11]. Here the adversary is transmitting a jamming signal that interferes with the symbol detection at the receiver, which increases the probability of detection error.

1.4 Problem description

In this work, we are investigating the worst-case performance of video cognitive radio systems under a disruptive attack. We aim to study how the adversary can optimally allocate energy across MC-DS-CDMA subcarriers during the sensing period, desynchronizing period and data transmission period. That is, we look at optimal energy allocation for each individual method of attack, spoofing, desynchronizing and jamming. Then we examine the optimal energy allocation among these three methods of attack, in order to minimize the system throughput or maximize the video distortion.

1.5 Dissertation outline

In Chapter 2, we investigate the optimal strategy for an adversary trying to disrupt communications by minimizing the CR network throughput, via spoofing and jamming with a Gaussian noise signal over a Rayleigh fading channel. We present how the adversary can optimally allocate power across subcarriers during sensing and transmission intervals with knowledge of the system parameters, using a simple optimization approach specific to this problem. We determine a worst-case optimal energy allocation for spoofing and jamming, which gives a lower bound to the overall information throughput of SUs under attack. Appendix A presents the optimization approach, and Appendix B provide supporting proof for the analysis in Chapter 2.

In Chapter 3, we extend the analysis to Nakagami-m fading for spoofing optimization by the adversary. We use the optimization approach described in Chapter 2 to determine the power allocation that minimizes the number of accessible bands under Nakagami-m fading.

In Chapter 4, we investigate the optimal strategy for spoofing, desynchronizing and jamming a cluster-based video CR network downlink with a Gaussian noise signal. The adversary can limit access for SUs by either transmitting a spoofing signal in the sensing interval, or a desynchronizing signal in the code acquisition interval. By jamming the network during the transmission interval, the adversary can reduce the rate of successful transmission. We show how the adversary can optimally allocate its energy across subcarriers during sensing, code acquisition and transmission intervals. We determine a worst-case optimal-energy allocation for spoofing, desynchronizing and jamming, which gives an upper bound to the received video distortion of SUs. We also propose cross-layer resource allocation algorithms for the downlink and evaluate their performance under disruptive attacks. Appendix C presents the generalized optimization approach used in this Chapter.

In Chapter 5, we study disruptive attacks in a video CR network uplink. We look at the optimal strategy for desynchronizing and jamming attacks on the uplink. Using results for optimal spoofing and downlink desynchronizing attack from Chapter 4, we determine the optimal energy allocation among spoofing, downlink desynchronizing, uplink desynchronizing and jamming. We also propose uplink resource allocation algorithms and evaluate their performance under disruptive attack.

In Chapter 6, we summarize the contributions of this dissertation and discuss possible future work.

Chapter 2

Spoofing and jamming optimization over Rayleigh fading channels of a cognitive radio adversary

2.1 Introduction

In this chapter, I examine the performance of a cognitive radio system in a hostile environment where an intelligent adversary tries to disrupt communications by minimizing the system throughput. I analyze two modes of attack, spoofing and jamming, under slow and fast fading Rayleigh channels. Spoofing, i.e. attacking the sensing subsystem, reduces the bandwidth available for SUs, and hence reduces the system throughput. Such exploitations and their impact are discussed in [16–24]. Jamming increases the error rate and also reduces the throughput [11].

I analyze the worst-case impact of an intelligent adversary on a tactical, spread spectrum, CR system. In [17], the presence of such an intelligent adversary disrupting the sensing by spoofing with a noise signal in an additive white Gaussian noise (AWGN) channel was discussed. This work was extended in [18], to obtain spoofing performance bounds under Rayleigh fading, when the adversary is aware of instantaneous channel state information (CSI). In [19], the design of an adversary with optimal power allocation for spoofing and jamming under an AWGN channel was investigated. In this chapter, I extend the analysis to a Rayleigh fading channel, and include forward error correction (FEC) coding, which reduces the effectiveness of jamming. Assuming knowledge of the SU system at the adversary, I determine a worst-case optimal energy allocation for spoofing and jamming. I further propose an optimization method specific to this problem, to find the optimal power allocation over subcarriers to minimize throughput. This enables us to perform the optimization when a closed form expression for the objective function is not available. In [25] and [26], jamming attacks are analyzed as a dynamic game, where the users and the adversary use the probability of successful jamming as a predetermined parameter. In the jamming section of this work, I analyze the probability of successful jamming by the adversary, and optimize the adversary power allocation to maximize the average probability of successful jamming.

In Section 2.2, I present the system model, and derive the performance metrics as functions of spoofing or jamming powers under fast and slow Rayleigh fading. Sections 2.3 and 2.4 discuss the spoofing and jamming optimization, respectively, where I prove that the performance metric functions derived in Section 2.2 have the required properties that enable the optimization method in Appendix A to be used, in almost all cases. In Section 2.5, I discuss the optimal energy allocation between spoofing and jamming. Section 2.6 contains system simulation results and Section 2.7 presents the conclusions. In Appendix A, I present the optimization approach, and Appendix B provide proofs supporting the jamming optimization.

2.2 System model

I investigate the impact of an adversary on a cluster based SU network, as shown in Figure 2.1. The cluster head serving the SUs is denoted by CH, and A is the adversary. I consider the downlinks from the cluster head to the users of an MC-DS-CDMA system with N_T bands (or subcarriers). The N_T bands are shared among PUs and SUs. *Vacant bands* are ones unoccupied by PUs. *Busy bands* are bands that the SU network cannot use due to PU activity. A vacant band may appear busy due to background noise and

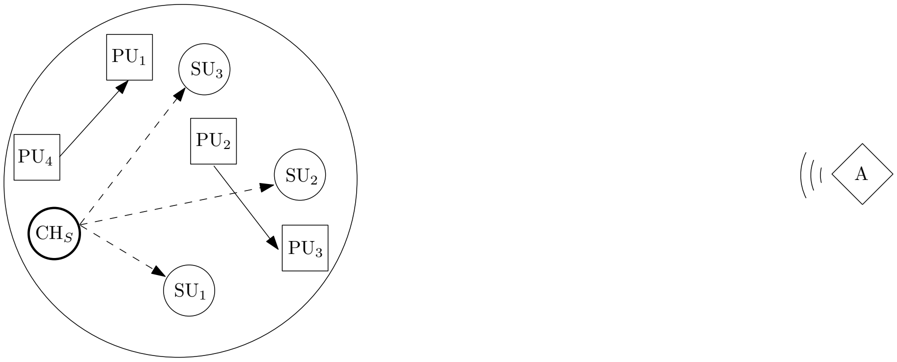


Figure 2.1: The downlink network model

spoofing. This is called a *false detection.* The bands detected as vacant are called *allowed bands.* I ignore the effects of missed detections in this analysis, as the adversary cannot do anything to increase the probability of missed detections. The CH periodically performs spectrum sensing, and uses a subset of allowed bands to transmit data to the SUs. The cluster head uses power control to maintain constant average link signal-to-noise ratio (SNR) for all SUs. I denote the length of the sensing interval by T_0 and the length of the data transmission interval by T_1.

Let $B = \{1, 2, \ldots, N_T\}$ be the set of bands, and $B_{su} \subseteq B$ be the subset of bands used by the SU network for communication in one transmission interval. The throughput (Γ) of the SU network during the data transmission interval is given by

$$\Gamma = \sum_{i \in B_{su}} \sum_{u=1}^{\Omega_i} L_P(1 - p_e^{(i,u)}) \log_2 M_{i,u} \tag{2.1}$$

where Ω_i is the number of SUs in the i-th band, L_P is the packet length in symbols, $p_e^{(i,u)}$ is the probability of packet error of the u-th user in the i-th band, and $\log_2 M_{i,u}$ is the number of bits per symbol in the alphabet used by the u-th user in the i-th band. The SUs use a single 4-QAM alphabet for fast fading, and may use either a single alphabet or adaptive modulation for slow fading. The adversary uses a Gaussian noise signal to attack by spoofing or jamming. Spoofing reduces $|B_{su}|$, and jamming increases $p_e^{(i,u)}$ in (2.1), thus reducing Γ.

In Subsection 2.2.1, I discuss the portion of the system involved in sensing, and derive expressions for the probability of false detection. The transmission and receiver

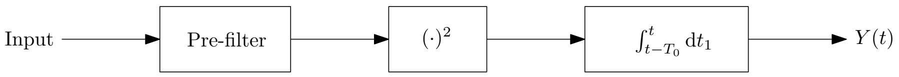


Figure 2.2: Energy detector block diagram

structures of SUs, i.e. the portion of the system involved in the transmission interval, is presented in Subsection 2.2.2, with the derivations of the expressions for the packet error rate. The assumptions regarding the knowledge available for the adversary are detailed in Subsection 2.2.3.

2.2.1 Sensing subsystem

The CH uses an energy detector for sensing (Fig. 2.2). Let W be the bandwidth of one subcarrier. The energy detector output, $Y(t)$, when there is no PU signal present, is given by $Y(t) = \int_{t-T_0}^{t}(\sqrt{\alpha_J(t_1)}n_s(t_1) + n_0(t_1))^2 \mathrm{d}t_1$, where $\alpha_J(t)$ is the gain of the channel from the adversary to the CH, $n_s(t)$ is the spoofing signal, and $n_0(t)$ is the noise after passing through the bandpass filter. The signal $n_s(t)$ is Gaussian with double sided power spectral density (PSD) $\frac{\eta_s}{2}$ in the band, $n_0(t)$ is Gaussian with PSD $\frac{N_0}{2}$ in the band, and $\alpha_J(t)$ is exponentially distributed with mean $\bar{\alpha}_J$. The integrand can be expressed as

$$\sqrt{\alpha_J(t)}n_s(t) + n_0(t) = (\sqrt{\alpha_J(t)}n_{s,i}(t)+n_{0,i}(t))\cos\omega_c t-(\sqrt{\alpha_J(t)}n_{s,q}(t)+n_{0,q}(t))\sin\omega_c t$$

where ω_c is the subcarrier frequency, $n_{s,i}(t), n_{s,q}(t)$ are Gaussian with PSD η_s in the frequency range $(-\frac{W}{2}, \frac{W}{2})$, and $n_{0,i}(t), n_{0,q}(t)$ are Gaussian with PSD N_0 in the frequency range $(-\frac{W}{2}, \frac{W}{2})$.

From [27],

$$Y(t) = \frac{1}{2W}\sum_{k=1}^{T_0 W}(a_{i,k}^2 + a_{q,k}^2) \tag{2.2}$$

where $a_{i,k} = \sqrt{\alpha_J\left(t - T_0 + \frac{k}{W}\right)}n_{s,i}\left(t - T_0 + \frac{k}{W}\right) + n_{0,i}\left(t - T_0 + \frac{k}{W}\right)$ and $a_{q,k} = \sqrt{\alpha_J\left(t - T_0 + \frac{k}{W}\right)}n_{s,q}\left(t - T_0 + \frac{k}{W}\right) + n_{0,q}\left(t - T_0 + \frac{k}{W}\right)$.

Fast fading

Under fast fading, I assume the channel coherence time is much smaller than the sensing duration T_0, and the channel varies significantly during the sensing interval so that the channel samples in time are mutually independent. Then, $E[a_{i,k}^2] = \bar{\alpha}_J\eta_s W + N_0 W$, $E[a_{i,k}^4] = 6\bar{\alpha}_J^2\eta_s^2 W^2 + 6\bar{\alpha}_J\eta_s N_0 W^2 + 3N_0^2 W^2$ and $\mathrm{Var}(a_{i,k}^2) = E[a_{i,k}^4] - E[a_{i,k}^2]^2 = 5\bar{\alpha}_J^2\eta_s^2 W^2 + 4\bar{\alpha}_J\eta_s N_0 W^2 + 2N_0^2 W^2$. Following the same approach, I can show $E[a_{i,k}^2 + a_{q,k}^2] = 2(\bar{\alpha}_J\eta_s W + N_0 W)$ and $\mathrm{Var}(a_{i,k}^2 + a_{q,k}^2) = 2(5\bar{\alpha}_J^2\eta_s^2 W^2 + 4\bar{\alpha}_J\eta_s N_0 W^2 + 2N_0^2 W^2)$. Since $\mathrm{Var}(a_{i,k}^2 + a_{q,k}^2)$ is finite, I can use the Lindeberg-Lévy central limit theorem to approximate $Y(t)$ in (2.2). Therefore, for large $T_0 W$, $Y(t) \sim \mathcal{N}(T_0 W(\bar{\alpha}_J\eta_s + N_0), T_0 W(5\bar{\alpha}_J^2\eta_s^2 + 4\bar{\alpha}_J\eta_s N_0 + 2N_0^2)/2)$. A band is detected as occupied by PUs if the energy detector output is greater than the threshold $K\sqrt{T_0 W}$. Let $p_{fd,f}(P_{S,i})$ be the probability of false detection under fast fading, as a function of the spoofing power in that band $P_{S,i}$. Then,

$$\begin{aligned} p_{fd,f}(P_{S,i}) &= \Pr(Y(t) > K\sqrt{T_0 W}) \\ &= Q\left(\frac{K\sqrt{T_0 W} - T_0 W(\bar{\alpha}_J(P_{S,i}/W) + N_0)}{\sqrt{T_0 W(5\bar{\alpha}_J^2(P_{S,i}/W)^2 + 4\bar{\alpha}_J(P_{S,i}/W)N_0 + 2N_0^2)/2}}\right) \end{aligned} \tag{2.3}$$

Slow fading

Under slow fading, I assume the channel coherence time is larger than the sensing duration T_0. Therefore, the channel gain remains constant during the sensing interval and I denote it by α_J. When conditioned on α_J, $a_{i,k} = \sqrt{\alpha_J} n_{s,i}\left(t - T_0 + \frac{k}{W}\right) + n_{0,i}\left(t - T_0 + \frac{k}{W}\right) \sim \mathcal{N}(0, \alpha_J\eta_s W + \eta_0 W)$, and similarly, $a_{q,k} \sim \mathcal{N}(0, \alpha_J\eta_s W + \eta_0 W)$. Therefore, $E[a_{i,k}^2 + a_{q,k}^2|\alpha_J] = 2(\alpha_J\eta_s W + \eta_0 W)$ and $\mathrm{Var}(a_{i,k}^2 + a_{q,k}^2|\alpha_J) = 4(\alpha_J\eta_s W + \eta_0 W)$. Using these results in (2.2), for large $T_0 W$, I conclude, when conditioned on α_J, $Y(t) \sim \mathcal{N}(T_0 W(\alpha_J\eta_s + \eta_0), T_0 W(\alpha_J\eta_s + \eta_0)^2)$.

The average probability of false detection under slow fading ($p_{fd,s}$), when the spoofing signal PSD is $\eta_{S,i}$, is given by

$$\begin{aligned} &\Pr(Y(t) > K\sqrt{T_0 W} | \eta_{S,i}) \\ &= \int_0^\infty \Pr(Y(t) > K\sqrt{T_0 W} | \alpha_J = y, \eta_{S,i}) f_{\alpha_J}(y) \mathrm{d}y \end{aligned} \tag{2.4}$$

where $f_{\alpha_J}(y)$ is the probability density function of the channel gain α_J. Since the channel has Rayleigh fading, $f_{\alpha_J}(y) = \frac{1}{\bar{\alpha}_J} e^{-\frac{y}{\bar{\alpha}_J}}$. Substituting this in (2.4) yields

$$\begin{aligned} &\Pr(Y(t) > K\sqrt{T_0 W} | \eta_{S,i}) \\ &= \frac{1}{\bar{\alpha}_J} \int_0^\infty Q\left(\frac{K}{\eta_{S,i} y + \eta_0} - \sqrt{T_0 W} \right) e^{-\frac{y}{\bar{\alpha}_J}} \mathrm{d}y \end{aligned} \tag{2.5}$$

Note that $P_{S,i} = \eta_{S,i} W$. Hence, the probability of false detection in a band, as a function of the spoofing power allocated for that band under slow fading, is given by

$$p_{fd,s}(P_{S,i}) = \Pr\left(Y(t) > K\sqrt{T_0 W} | \frac{P_{S,i}}{W} \right) \tag{2.6}$$

2.2.2 Transceiver subsystem

The transmitter model is adapted from [19]. A block diagram of the transmitter for a single user is given in Figure 2.3. Low density parity check (LDPC) codes are used for FEC. The output bit sequence of the FEC block of the u-th user is denoted by $d_m^{(u)}$. This binary sequence is mapped to a symbol sequence $s_k^{(u)}$ from an alphabet a_i, based on the predicted instantaneous CSI. Note that $s_k^{(l)}$ is generally complex valued, and normalized to have unit average energy, i.e. $E[|s_k|^2] = 1$. The $\{c_n^{(u)}\}$ are the chips of a pseudo-random spreading sequence, and there are N_c chips per symbol. The sequence $s_k^{(u)} c_n^{(u)}$ modulates an impulse train. After passing through both the chip-wave shaping filter $g(t)$ and modulator, the transmitted signal takes the form $x(t) = \Re\left\{ \sum_{u=1}^{\Omega_u} \sqrt{2E_c^{(u)}} \sum_{n=-\infty}^{\infty} s_k^{(u)} c_n^{(u)} g(t - nT_c) e^{j\omega_c t + \phi_u} \right\}$, where $E_c^{(u)}$ is the energy per chip, T_c is the chip duration, Ω_u is the number of users sharing the band, ϕ_u is the carrier phase of the u-th user, $k = \lfloor n/N_c \rfloor$ and $g(t)$ is a root raised cosine chip-wave shaping

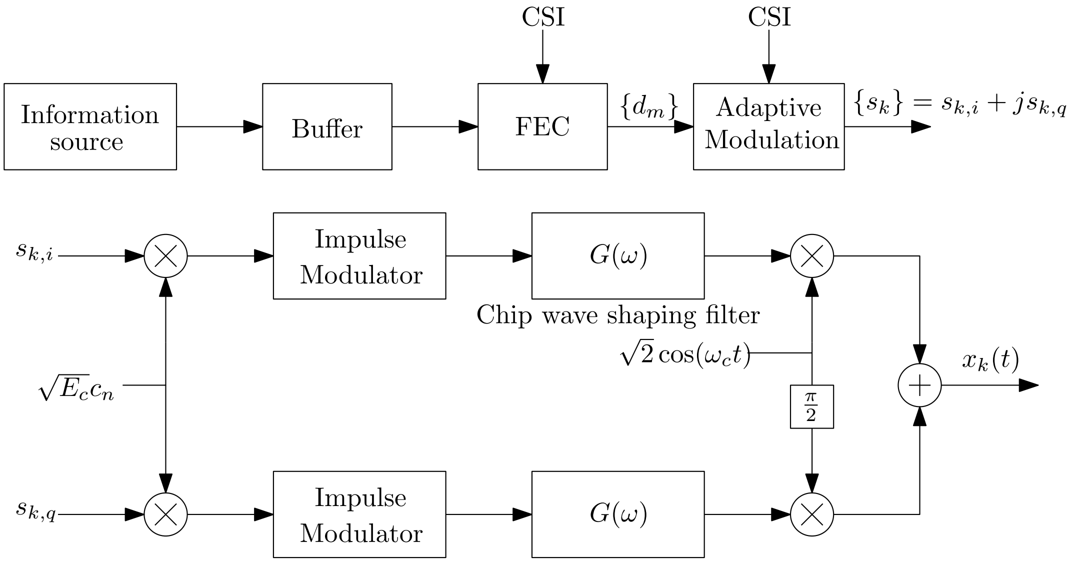


Figure 2.3: Transmitter block diagram of a single subcarrier of MC-DS CDMA

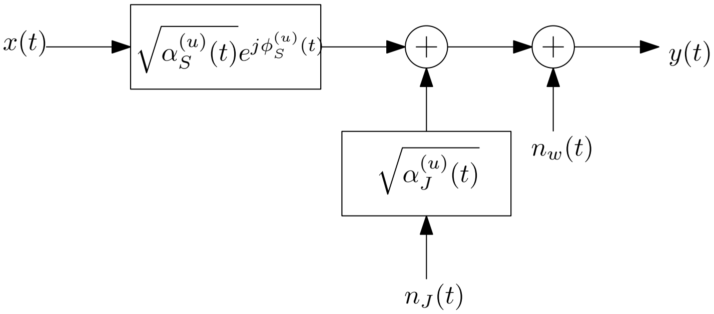

$x(t)$
$\sqrt{\alpha_S^{(u)}(t)}e^{j\phi_S^{(u)}(t)}$
$y(t)$
$n_w(t)$
$\sqrt{\alpha_J^{(u)}(t)}$
$n_J(t)$

Figure 2.4: Channel response and jamming

filter, such that

$$G(\omega)G^*(\omega) = \begin{cases} T_c, & \text{if } |\omega| \leq \frac{1-\beta}{2T_c} \\ \frac{T_c}{2}\left(1+\cos\left(\frac{\pi T_c}{\beta}\left(|\omega|-\frac{1-\beta}{2T_c}\right)\right)\right), & \text{if } \frac{1-\beta}{2T_c} < |\omega| \leq \frac{1+\beta}{2T_c} \\ 0, & \text{elsewhere} \end{cases} \tag{2.7}$$

where $G(\omega)$ is the Fourier transform of $g(t)$ and β is the roll-off factor.

Figure 2.4 shows the channel fading and jamming experienced by the l-th user in one subcarrier. The transmitted signal $x(t)$ is attenuated by Rayleigh fading, and corrupted by AWGN and jamming. The jamming signal undergoes Rayleigh fading, independent of the source-user channel.

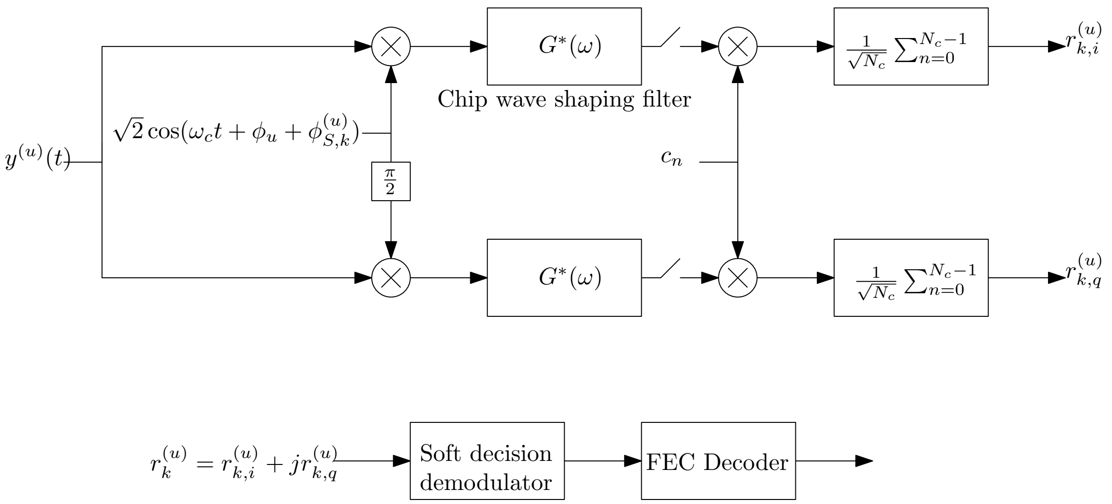

$y^{(u)}(t)$
$\sqrt{2}\cos(\omega_c t + \phi_u + \phi_{S,k}^{(u)})$
$\frac{\pi}{2}$
$G^*(\omega)$
Chip wave shaping filter
$G^*(\omega)$
c_n
$\frac{1}{\sqrt{N_c}}\sum_{n=0}^{N_c-1}$
$\frac{1}{\sqrt{N_c}}\sum_{n=0}^{N_c-1}$
$r_{k,i}^{(u)}$
$r_{k,q}^{(u)}$
$r_k^{(u)} = r_{k,i}^{(u)} + jr_{k,q}^{(u)}$
Soft decision demodulator
FEC Decoder

Figure 2.5: u-th user receiver block diagram

The received signal of the u-th user ($y^{(u)}(t)$) is given by

$$y^{(u)}(t) = \Re\left\{\sqrt{2E_c^{(u)}\alpha_S^{(u)}(t)}e^{j\phi_S^{(u)}(t)}\sum_{u=1}^{\Omega_u}\sum_{n=-\infty}^{\infty} s_k^{(u)}c_n^{(u)}g(t-nT_c)e^{j\omega_c t+\phi_u} \right.$$
$$\left. + \, n_w(t) + \sqrt{\alpha_J^{(u)}(t)}n_J(t)\right\},$$

where $\alpha_S^{(u)}(t)$ and $\phi_S^{(u)}(t)$ are the power gain and phase components of the response of the channel from the source to the u-th user. The power gain of the jammer-to-user channel is $\alpha_J^{(u)}(t)$. I assume the channel gains $\alpha_S^{(u)}(t)$ and $\alpha_J^{(u)}(t)$ are mutually independent. The background noise $n_w(t)$ is AWGN with a double-sided PSD $\frac{N_0}{2}$ and $\sqrt{\alpha_J^{(u)}(t)}n_J(t)$ is the received jamming signal. The receiver block diagram is given in Figure 2.5. I assume the gains and phases of fading channels remain constant during a symbol detection. I denote the gain and phase components of the response of the channel from the source to the u-th user during the k-th symbol detection by $\alpha_{S,k}^{(u)}$ and $\phi_{S,k}^{(u)}$, respectively. The gain of the jammer-to-user channel is denoted by $\alpha_{J,k}^{(u)}$. The complex output samples are given by

$$r_k^{(u)} \triangleq r_{k,i}^{(u)} + r_{k,q}^{(u)} = \sqrt{E_S^{(u)}\alpha_{S,k}^{(u)}}s_k^{(u)} + \sqrt{\alpha_{J,k}^{(u)}}n_{J,k} + n_{w,k} + I_k \qquad (2.8)$$

where $E_S^{(u)} = E_c^{(u)}N_c$, is the symbol energy, $n_{J,k}$ is the jamming signal, $n_{w,k}$ is the background noise and I_k is the interference from other users occupying the same band. Further, $n_{J,k} \sim \mathcal{CN}(0, \eta_J)$ and $n_{w,k} \sim \mathcal{CN}(0, N_0)$, where k is the time index and $\frac{\eta_J}{2}$ is the double sided PSD of the jamming signal. I assume the users in the downlink are synchronized at the transmitter, and hence the interference can be removed by using mutually orthogonal spreading codes (e.g., Walsh-Hadamard codes). The received instantaneous signal-to-interference-plus-noise ratio (SINR) at the k-th symbol detection can be written as

$$\gamma_k = \frac{E_S^{(u)} \alpha_{S,k}^{(u)}}{\eta_J \alpha_{J,k}^{(u)} + N_0} = \frac{\alpha_{S,k}^{(u)} \frac{E_S^{(u)}}{N_0}}{\alpha_{J,k}^{(u)} \frac{\eta_J}{N_0} + 1} = \frac{\frac{\alpha_{S,k}^{(u)}}{\bar{\alpha}_S^{(u)}} \bar{\gamma}_S}{\frac{\alpha_{J,k}^{(u)}}{\bar{\alpha}_J} \bar{\gamma}_J + 1} \tag{2.9}$$

where $\gamma_{S,k}^{(u)} \triangleq \alpha_{S,k}^{(u)} \frac{E_S^{(u)}}{N_0}$ and $\gamma_{J,k}^{(u)} \triangleq \alpha_{J,k}^{(u)} \frac{\eta_J}{N_0}$. $\bar{\gamma}_S = \mathrm{E}[\gamma_{S,k}] = \frac{\bar{\alpha}_S^{(u)} E_S^{(u)}}{N_0}$ and $\bar{\gamma}_J = \frac{\bar{\alpha}_J \eta_J}{N_0}$, where $\bar{\alpha}_S^{(u)} = \mathrm{E}[\alpha_{S,k}^{(u)}]$ and $\bar{\alpha}_J = \mathrm{E}[\alpha_{J,k}^{(u)}]$. I define $\tilde{\alpha}_{S,k} \triangleq \frac{\alpha_{S,k}^{(u)}}{\bar{\alpha}_S^{(u)}}$ and $\tilde{\alpha}_{J,k} \triangleq \frac{\alpha_{J,k}^{(u)}}{\bar{\alpha}_J}$ to simplify the analysis, so that

$$\gamma_k = \frac{\tilde{\alpha}_{S,k} \bar{\gamma}_S}{\tilde{\alpha}_{J,k} \bar{\gamma}_J + 1} \tag{2.10}$$

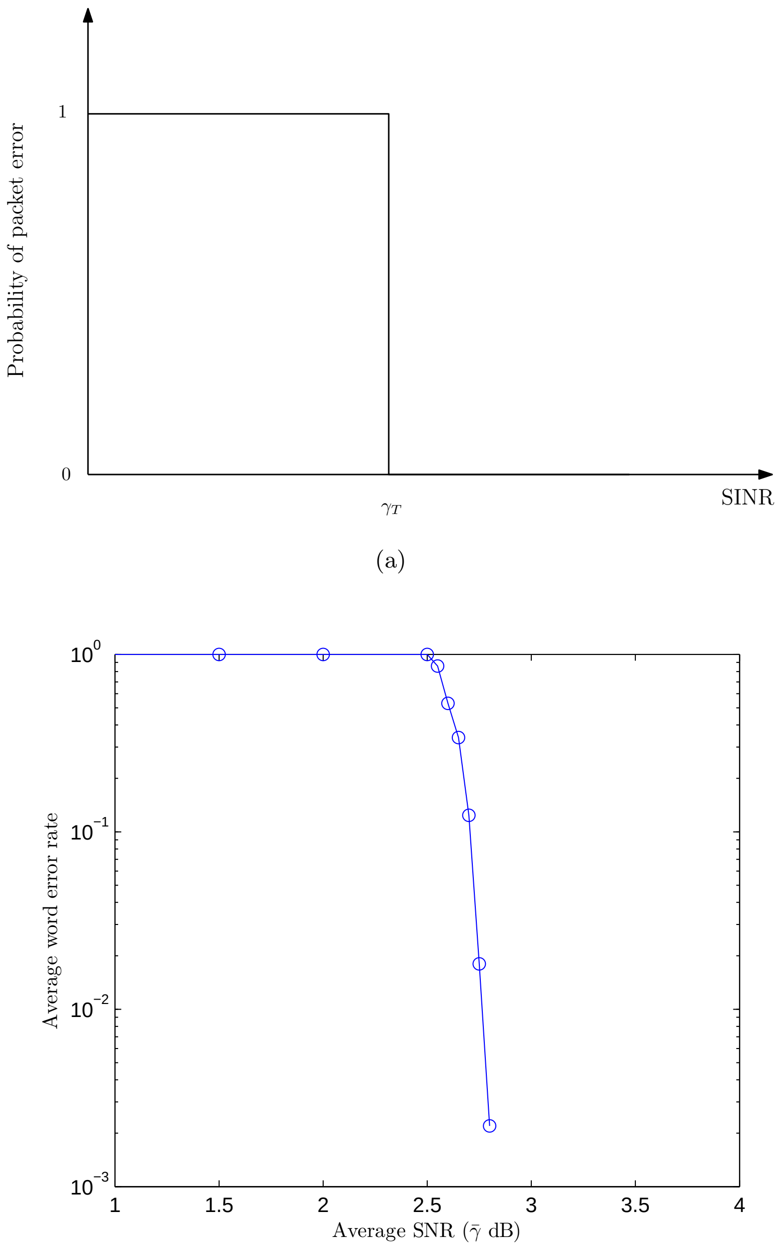
and $\tilde{\alpha}_{S,k}, \tilde{\alpha}_{J,k} \sim \mathrm{Exp}(1)$. Since $P_{J,i}$ is the jamming power allocated for the subcarrier, I know $P_{J,i} = \eta_J W$, so that

$$\bar{\gamma}_J = \frac{\bar{\alpha}_J P_{J,i}}{N_0 W} \tag{2.11}$$

Fast fading

Under fast fading, I assume the channel coherence time is significantly lower than the transmission duration of one codeword, T_1. The adversary models the probability of packet error as a step function of the received average SINR over a word, as shown in Fig 2.6(a). Therefore,

$$\Pr(\text{packet error}) = \begin{cases} 0, & \text{if } \tilde{\gamma} > \gamma_T \\ 1, & \text{if } \tilde{\gamma} \leq \gamma_T \end{cases} \tag{2.12}$$



(a)

(b)

Figure 2.6: (a) Step function approximation for the probability of packet error r_e. (b) Average probability of word error of DVB-S2 LDPC code of rate $\frac{1}{2}$ using 4-QAM vs. average SNR.

where $\tilde{\gamma}$ is the SINR at the receiver averaged over the duration of the word, and γ_T is a threshold parameter dependent on the alphabet and the FEC used. Note that γ_T is determined through simulations, and in Fig 2.6(b), the simulation results of the word error rate of the DVB-S2 rate $\frac{1}{2}$ LDPC code with 4-QAM modulation under Rayleigh fading are presented.

In fast fading, as the channel coherence time is significantly smaller than the duration of a codeword, I approximate the average SINR over a codeword with the ensemble average over the channel gains $\tilde{\alpha}_{S,k}$ and $\tilde{\alpha}_{J,k}$. The average SINR over a word in this case can be calculated as follows:

$$\tilde{\gamma}(\bar{\gamma}_{J,i}) = \int_0^\infty \int_0^\infty \frac{x\bar{\gamma}_S}{y\bar{\gamma}_{J,i}+1} e^{-x} e^{-y} \, \mathrm{d}x\mathrm{d}y \tag{2.13}$$

$$= -\frac{\bar{\gamma}_S e^{\frac{1}{\bar{\gamma}_{J,i}}}}{\bar{\gamma}_{J,i}} \mathrm{Ei}\left(-\frac{1}{\bar{\gamma}_{J,i}}\right) \quad [28, \text{Eq. } 4.2.6] \tag{2.14}$$

where $\mathrm{Ei}(x) = -\int_{-x}^{\infty} \frac{e^{-t}}{t} \, \mathrm{d}t$ is the exponential integral function [29, Eq. 5.1.2].

Lemma 1: $\tilde{\gamma}(\bar{\gamma}_{J,i})$ is a monotonically decreasing function of $\bar{\gamma}_{J,i}$, and the range of $\tilde{\gamma}$ is $(0, \bar{\gamma}_S]$.

Proof:

From (2.13), it can be seen that $\tilde{\gamma}(\bar{\gamma}_{J,i})$ is monotonically decreasing in $\bar{\gamma}_{J,i}$. From (2.13), I further have $\tilde{\gamma}(0) = \int_0^\infty \int_0^\infty \frac{x\bar{\gamma}_S}{y.0+1} e^{-x} e^{-y} \, \mathrm{d}x\mathrm{d}y = \bar{\gamma}_S$. and from (2.14),

$$\lim_{\bar{\gamma}_{J,i}\to\infty} \tilde{\gamma}(\bar{\gamma}_{J,i}) = \lim_{\bar{\gamma}_{J,i}\to\infty} -\frac{\bar{\gamma}_S e^{\frac{1}{\bar{\gamma}_{J,i}}}}{\bar{\gamma}_{J,i}} \mathrm{Ei}\left(-\frac{1}{\bar{\gamma}_{J,i}}\right)$$

$$\propto \lim_{\bar{\gamma}_{J,i}\to\infty} -\frac{1}{\bar{\gamma}_{J,i}} \log\left(\frac{-1}{\bar{\gamma}_{J,i}}\right) \tag{2.15}$$

$$= 0 \tag{2.16}$$

Note that $\lim_{x\to 0} \mathrm{Ei}(x) \propto \log x$ [29]. Hence, I have shown $\tilde{\gamma}(\bar{\gamma}_{J,i})$ is a monotonically decreasing function in $\mathbb{R}^+$, and the range of $\tilde{\gamma}(\bar{\gamma}_{J,i})$ is $(0, \bar{\gamma}_S]$.

From lemma 1, it is known a unique $\bar{\gamma}_J^*$ exists $\forall\ \gamma_T \in (0, \bar{\gamma}_S]$, such that $\tilde{\gamma}(\bar{\gamma}_J^*) = \gamma_T$, and $\bar{\gamma}_{J,i} < \bar{\gamma}_J^* \Leftrightarrow \tilde{\gamma} > \gamma_T$. Using (2.11), I define $P_J^* \triangleq \frac{N_0 W \bar{\gamma}_J^*}{\bar{\alpha}_J}$. Since the jamming power in the band $P_{J,i} \propto \bar{\gamma}_{J,i}$, $P_{J,i} < P_J^* \Leftrightarrow \bar{\gamma}_{J,i} < \bar{\gamma}_J^* \Leftrightarrow \tilde{\gamma} > \gamma_T$. Using this result and (2.12), I can write the packet error rate as a function of jamming power under fast fading, $r_{e,f}(P_{J,i})$, as

$$r_{e,f}(P_{J,i}) = \begin{cases} 0, & \text{if } P_{J,i} < P_J^* \\ \log_2 M, & \text{if } P_{J,i} \geq P_J^* \end{cases} \tag{2.17}$$

where $\log_2 M$ is the number of bits per symbol.

Slow fading

In slow fading, I assume the coherence time is larger than T_1. Therefore, the channel gains $\tilde{\alpha}_{S,k}$ and $\tilde{\alpha}_{J,k}$, and instantaneous SINR, γ_k, remain constant over a word. The adversary again models the probability of word error with a step function of the SINR.

$$\Pr(\text{packet error}) = \begin{cases} 0, & \text{if } \gamma_k > \gamma_T \\ 1, & \text{if } \gamma_k \leq \gamma_T \end{cases} \tag{2.18}$$

where γ_k is the instantaneous SINR at the receiver, and γ_T is a threshold parameter dependent on the alphabet and the FEC used. Through simulations of word error rates of an ensemble of LDPC rate $\frac{1}{2}$ codes of code length L_p, γ_T is estimated. Therefore, from (2.12), the probability of packet error in a band jammed with power $P_{J,i}$, as a function of $\bar{\gamma}_{J,i} = \frac{\bar{\alpha}_J P_{J,i}}{N_0 W}$ is given by

$$\begin{aligned} &\Pr(\text{packet error}|\bar{\gamma}_{J,i}) = \Pr\left(\frac{\tilde{\alpha}_{S,i}\bar{\gamma}_S}{\tilde{\alpha}_{J,i}\bar{\gamma}_{J,i}+1} < \gamma_T\right) \\ &= \int_0^\infty \int_0^{\frac{(y\bar{\gamma}_{J,i}+1)\gamma_T}{\bar{\gamma}_S}} f_{\tilde{\alpha}_{S,k}}(x) f_{\tilde{\alpha}_{J,k}}(y) \mathrm{d}x\mathrm{d}y \\ &= \int_0^\infty \int_0^{\frac{(y\bar{\gamma}_{J,i}+1)\gamma_T}{\bar{\gamma}_S}} e^{-x}e^{-y} \mathrm{d}x\mathrm{d}y \\ &= 1 - \frac{e^{-\frac{\gamma_T}{\bar{\gamma}_S}}}{\left(\frac{\bar{\gamma}_{J,i}\gamma_T}{\bar{\gamma}_S}+1\right)} \end{aligned} \tag{2.19}$$

The packet error rate per user per band, $r_{e,s,1}(P_{J,i})$ under slow fading for a single alphabet size, as a function of the jamming power allocated to the band $P_{J,i}$ is given by

$$r_{e,s,1}(P_{J,i}) = \Pr\left(\text{packet error}|\frac{\bar{\alpha}_J P_{J,i}}{N_0 W}\right)\log_2 M. \tag{2.20}$$

Slow fading with adaptive modulation

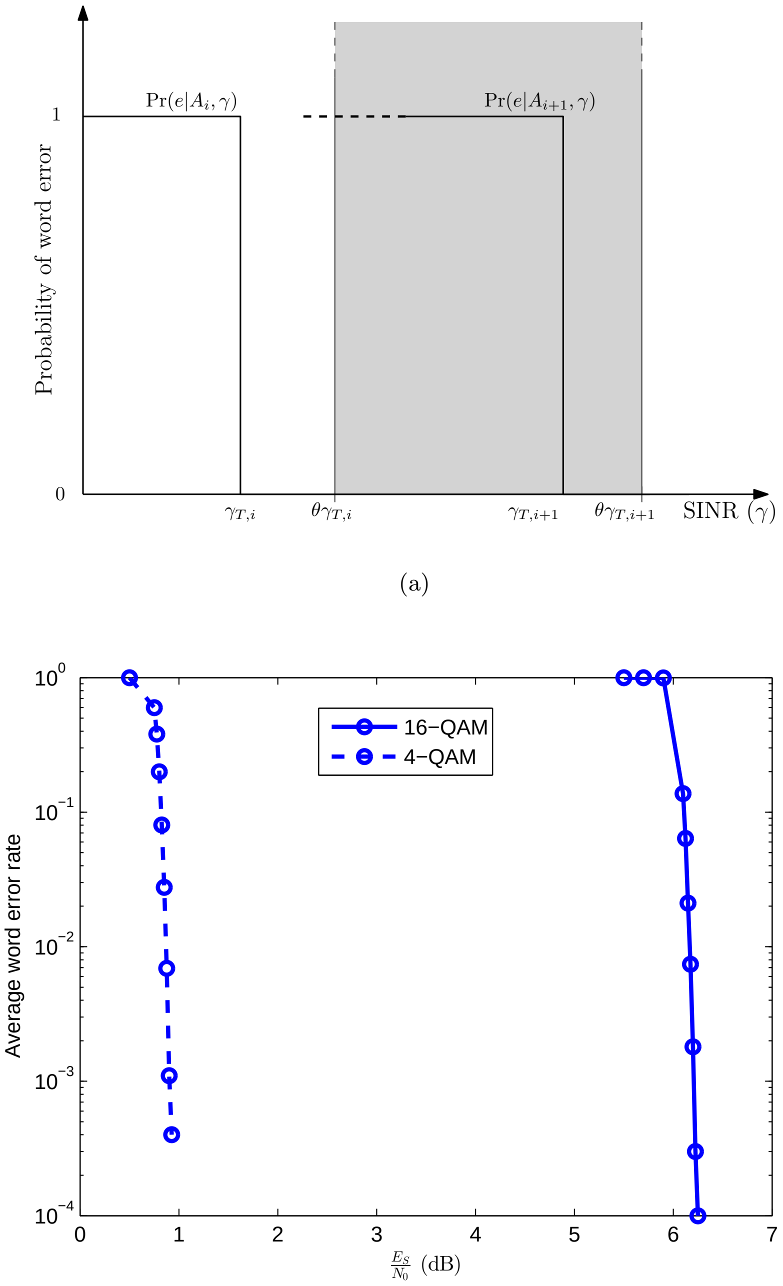
If the SU network is experiencing slow fading due to low mobility, the system may use an adaptive modulation scheme to improve the system throughput. Here, I analyze the jamming optimization in an adaptive modulation system under slow fading. I assume the SU network has a choice of N_A alphabets, which are known to the adversary.

Let a_i denote the i-th alphabet and A_i denote the event that a_i is used for transmission. The probability of a received word being in error for a given alphabet a_i (Pr $(e|A_i)$), is a step function of the instantaneous SINR (γ_k, Eq. (2.10)).

$$\Pr(e|A_i, \gamma_k) = \begin{cases} 0, & \text{if } \gamma_k > \gamma_{T,i} \\ 1, & \text{if } \gamma_k \leq \gamma_{T,i} \end{cases} \tag{2.21}$$

As shown in Fig 2.7(a), the alphabet a_i is used if the SNR $(\gamma_{S,k}) \in \ (\theta\gamma_{T,i}, \theta\gamma_{T,i+1})$. Fig 2.7(b) shows the word error rate of the DVB-S2 rate $\frac{1}{2}$ LDPC code for alphabets 4-QAM and 16-QAM in an AWGN channel. Consider the probability a word is received in error, when the alphabet a_i is selected $(\Pr(e \cap A_i))$. Since alphabet a_i is selected when $\tilde{\alpha}_{S,k} \in \left(\frac{\theta\gamma_{T,i}}{\bar{\gamma}_S}, \frac{\theta\gamma_{T,i+1}}{\bar{\gamma}_S}\right)$,

$$\Pr(A_i|\tilde{\alpha}_{S,k}) = \begin{cases} 1, & \text{if } \tilde{\alpha}_{S,k} \in \left(\frac{\theta\gamma_{T,i}}{\bar{\gamma}_S}, \frac{\theta\gamma_{T,i+1}}{\bar{\gamma}_S}\right) \\ 0, & \text{otherwise} \end{cases} \tag{2.22}$$



(a)

(b)

Figure 2.7: (a) The probability of word error given an alphabet a_i ($\Pr(e|A_i)$). The shaded area represents the region of SNR in which the alphabet a_i is used. (b) Average word error rate of DVB-S2 LDPC code of rate $\frac{1}{2}$ for alphabets 4-QAM and 16-QAM vs. SNR.

A word is received in error when $\frac{\tilde{\alpha}_{S,k}\bar{\gamma}_S}{\tilde{\alpha}_{J,k}\bar{\gamma}_J+1} < \gamma_{T,i}$, so that

$$
\begin{aligned}
\Pr(e \cap A_i) &= \int_0^\infty \int_0^\infty \Pr(e \cap A_i | \tilde{\alpha}_{S,k} = x, \tilde{\alpha}_{J,k} = y) f_{\tilde{\alpha}_{S,k}}(x) f_{\tilde{\alpha}_{J,k}}(y) \mathrm{d}x\mathrm{d}y \\
&= \int_0^{\frac{\theta-1}{\bar{\gamma}_J}} \int_{\frac{\theta\gamma_{T,i}}{\bar{\gamma}_S}}^{\frac{\theta\gamma_{T,i+1}}{\bar{\gamma}_S}} \Pr\left(\frac{x\bar{\gamma}_S}{y\bar{\gamma}_J+1} < \gamma_{T,i} | \tilde{\alpha}_{S,k} = x, \tilde{\alpha}_{J,k} = y\right) f_{\tilde{\alpha}_{S,k}}(x) f_{\tilde{\alpha}_{J,k}}(y) \mathrm{d}x\mathrm{d}y \\
&+ \int_{\frac{\theta-1}{\bar{\gamma}_J}}^{\left(\frac{\theta\gamma_{T,i+i}}{\gamma_{T,i}\bar{\gamma}_J} - \frac{1}{\bar{\gamma}_J}\right)} \int_{\frac{\theta\gamma_{T,i}}{\bar{\gamma}_S}}^{\frac{\theta\gamma_{T,i+1}}{\bar{\gamma}_S}} \Pr\left(\frac{x\bar{\gamma}_S}{y\bar{\gamma}_J+1} < \gamma_{T,i} | \tilde{\alpha}_{S,k} = x, \tilde{\alpha}_{J,k} = y\right) f_{\tilde{\alpha}_{S,k}}(x) f_{\tilde{\alpha}_{J,k}}(y) \mathrm{d}x\mathrm{d}y \\
&+ \int_{\left(\frac{\theta\gamma_{T,i+i}}{\gamma_{T,i}\bar{\gamma}_J} - \frac{1}{\bar{\gamma}_J}\right)}^{\infty} \int_{\frac{\theta\gamma_{T,i}}{\bar{\gamma}_S}}^{\frac{\theta\gamma_{T,i+1}}{\bar{\gamma}_S}} \Pr\left(\frac{x\bar{\gamma}_S}{y\bar{\gamma}_J+1} < \gamma_{T,i} | \tilde{\alpha}_{S,k} = x, \tilde{\alpha}_{J,k} = y\right) f_{\tilde{\alpha}_{S,k}}(x) f_{\tilde{\alpha}_{J,k}}(y) \mathrm{d}x\mathrm{d}y \\
&= \frac{\bar{\gamma}_J\gamma_{T,i}}{(\bar{\gamma}_J\gamma_{T,i} + \bar{\gamma}_S)} \left(e^{-\left(\frac{\theta\gamma_{T,i}}{\bar{\gamma}_S} + \frac{\theta-1}{\bar{\gamma}_J}\right)} - e^{-\left(\frac{\theta\gamma_{T,i+1}}{\bar{\gamma}_S} + \frac{\theta\gamma_{T,i+i}}{\gamma_{T,i}\bar{\gamma}_J} - \frac{1}{\bar{\gamma}_J}\right)} \right) \qquad (2.23)
\end{aligned}
$$

The average packet error rate per user per band, $r_{e,s,2}(P_{J,i})$ under slow fading with adaptive modulation, as a function of $P_{J,i}$ is given by

$$
r_{e,s,2}(P_{J,i}) = \sum_{j=1}^{N_A} \Pr(e \cap A_j) \log_2 M_j \qquad (2.24)
$$

where $\log_2 M_i$ is the number of bits per symbol when using the alphabet a_i.

2.2.3 Adversary

The adversary uses Gaussian noise signals when it spoofs or jams. The objective of the adversary is to disrupt the communication, and I use the average throughput as the performance metric. In this work I assume that the system design parameters and statistical averages of system parameters are known by the adversary, but that knowledge of instantaneous system parameters is not available for the adversary, in accordance with previous work [17–19]. Because a practical adversary does not have all the assumed knowledge, the work done here is a worst-case analysis, which gives a lower bound to the throughput with jamming and spoofing.

System design parameters

I assume that the adversary is aware of the bandwidth of the waveform, sensing, code acquisition and transmission times, receiver structure and system false alarm probability i.e., the probability of false detection caused only due to background noise with no spoofing. The SNR of SUs maintained constant by the CH through power control is assumed to be known by the adversary. I further assume that the adversary is aware of the type and rate of FEC, alphabet sizes and thresholds used.

Statistical averages of system parameters

I assume that the adversary knows the PSD of the background noise, and that all links undergo Rayleigh fading. I also assume that the adversary knows the average number of SUs and the average number of bands occupied by PUs.

Instantaneous system parameters

I do not assume the adversary knows which channels are occupied by PUs at the start of the sensing interval, which channels each user is assigned to, or other instantaneous values of time varying system parameters (e.g. channel gains). The adversary senses and detects the bands used for transmission before jamming, and hence knows $B_{su} \cup B_{pu}$, where $B_{pu} \subseteq \{1, 2, \ldots, N_T\}$ is the set of bands occupied by PUs.

2.3 Spoofing power optimization

During the sensing interval, the adversary attacks the system by spoofing to reduce the bandwidth available to the SUs. Let $B_{al} \subseteq B$ be the set of vacant bands in the current sensing interval. Spoofing directly affects the number of allowed bands. Further, reducing the number of allowed bands via spoofing will make jamming more effective, as it reduces the number of occupied bands in the transmission interval. As both these effects are determined by the number of allowed bands, the objective of the adversary when spoofing is to minimize the number of allowed bands. Following the same approach as in [17, Eq. 1], I can show that the expected number of allowed bands is $\sum_{i\in B_{al}}(1-p_{fd}^{(i)})$, where $p_{fd}^{(i)}$ is the probability of false detection of the i-th band, given that the i-th band is vacant.

At the start of the sensing interval the adversary does not know which bands are allowed for SUs. Therefore, from the adversary's perspective, every band has an equal probability of being vacant. Hence, the objective of the adversary is to accomplish:

$$\max \sum_{i=1}^{N_T} p_{fd}^{(i)}, \quad \text{s.t.} \sum_{i=1}^{N_T} P_{S,i} \leq P_S \tag{2.25}$$

where $P_{S,i}$ is the spoofing power allocated for the i-th band and P_S is the total spoofing power available.

2.3.1 Fast fading

For fast fading, from (2.3),

$$p_{fd}^{(i)} = p_{fd,f}(P_{S,i}) = Q\left(\frac{K\sqrt{T_0W} - T_0W(\bar{\alpha}_J(P_{S,i}/W) + N_0)}{\sqrt{T_0W(5\bar{\alpha}_J^2(P_{S,i}/W)^2 + 4\bar{\alpha}_J(P_{S,i}/W)N_0 + 2N_0^2)/2}}\right) \tag{2.26}$$

Therefore, the objective of the optimization in (2.25) is to maximize $\sum_{i=1}^{N_T} p_{fd,f}(P_{S,i})$, under the constraint $\sum_{i=1}^{N_T} P_{S,i} \leq P_S$.

Proposition 1: $p_{fd,f}$ has properties **P0**, **P1** and **P2** stated in Theorem 1 in Appendix A.

Proof:

Define

$$\begin{aligned} g_f(y) \triangleq\; & p_{fd,f}\left(\frac{WN_0y}{\bar{\alpha}_J}\right) \\ =& Q\left(\frac{K\sqrt{2}/N_0 - \sqrt{2T_0W} - \sqrt{2T_0W}y}{\sqrt{(5y^2+4y+2)}}\right) \\ =& Q\left(\frac{b-ay}{\sqrt{5y^2+4y+2}}\right) \end{aligned} \tag{2.27}$$

where $b = \frac{K\sqrt{2}}{N_0} - \sqrt{2T_0W}$ and $a = \sqrt{2T_0W}$. As long as the detector threshold is selected so that the false alarm probability (false detection without spoofing) is less than 0.5, then $p_{fd,f}(0) < 0.5 \Leftrightarrow g(0) < 0.5 \Leftrightarrow b > 0$. I now show that the conditions of Theorem 1 are satisfied.

1) From the definition of $p_{fd,f}(P_{S,i})$, condition **P0** is obviously satisfied by $p_{fd,f}(P_{S,i})$.

2) From the definition of $g_f(y)$, I have

$$p_{fd,f}(P_{S,i}) = g\left(\frac{\bar{\alpha}_J P_{S,i}}{WN_0}\right) \tag{2.28}$$

and from (2.27),

$$\begin{aligned} g_f'(y) &= \frac{\mathrm{d}}{\mathrm{d}y} Q\left(\frac{b-ay}{\sqrt{5y^2+4y+2}}\right) \\ &= \frac{\big((2a+5b)y+2a+2b\big)}{(5y^2+4y+2)^{\frac{3}{2}}\sqrt{2\pi}} e^{-\frac{(ay-b)^2}{2(5y^2+4y+2)}} \end{aligned} \tag{2.29}$$

From (2.29), $g_f'(y) > 0 \ \forall y > 0$, because $a, b > 0$. From (2.28), $\frac{\mathrm{d}}{\mathrm{d}P_{S,i}} p_{fd,f}(P_{S,i}) = \frac{\bar{\alpha}_J}{WN_0} g_f'\left(\frac{\bar{\alpha}_J P_{S,i}}{WN_0}\right) > 0 \ \forall P_{S,i} > 0$. Therefore, condition **P1** is satisfied.

3) From (2.29),

$$g_f''(y) = \frac{\mathrm{d}}{\mathrm{d}y} g_f'(y) = \frac{p(y)}{(5y^2+4y+2)^{\frac{7}{2}}\sqrt{2\pi}} e^{-\frac{(ay-b)^2}{2(5y^2+4y+2)}} \tag{2.30}$$

where $p(y) = c_4y^4 + c_3y^3 + c_2y^2 + c_1y + c_0$, $c_0 = -16a - 4b + 4a^2b + 8ab^2 + 4b^3$, $c_3 = -250a - 400b - a(2a+5b)^2 < 0$, $c_4 = -50(2a+5b) < 0$ and

$$\begin{aligned} c_1 &= -100a - 88b - 4a^3 + 24ab^2 + 20b^3 \\ &= 5c_0 - 20a - 68b - 4a^3 - 20a^2b - 16ab^2, \end{aligned} \tag{2.31}$$

$$\begin{aligned} c_2 &= -216a - 270b - 8a^3 - 24a^2b + 25b^3 \\ &= \frac{5}{4}c_1 - 91a - 160b - 3a^3 - 24a^2b - 30ab^2. \end{aligned} \tag{2.32}$$

According to Descartes' rule of signs, the number of real positive roots of the polynomial $p(y) = 0$ equals the number of sign changes between nonzero c_is (ordered from c_4 to c_0), or is less than the number of sign changes by a multiple of 2. Note that

$c_4, c_3 < 0$. From (2.31), I see that $c_0 \leq 0 \Rightarrow c_1 < 0$, and from (2.32), $c_1 \leq 0 \Rightarrow c_2 < 0$. Therefore, if $c_0 \leq 0$, all non-zero coefficients are negative and there are no sign changes, i.e., there are no positive roots.

Let us consider the case $c_0 > 0$. If $c_1 \leq 0$, then $c_2 < 0$, and there is only one sign change in the coefficients ($\because c_0 > 0, c_1, c_2, c_3, c_4 \leq 0$). If otherwise, i.e., $c_1 > 0$, there will be only one sign change irrespective of the sign of c_2 ($\because c_0, c_1 > 0, c_3, c_4 < 0$). Therefore, I can see that the number of sign changes between coefficients is either 0 or 1. Hence, there will be at most one positive root for $p(y) = 0$. Further, since $c_4 < 0$, $\lim_{y \to \infty} p(y) \to -\infty$. I conclude that $p(y) < 0 \; \forall y > 0$ or $\exists y_0 > 0$, s.t. $q(y) < 0 \; \forall y > y_0$ and $p(y) \geq 0 \; \forall y \leq y_0$. From (2.30), I know $g_f''(y)$ has the same sign as $p(y)$. Therefore, I conclude that $g_f(y)$ satisfies the condition **P2**. From (2.28), $\frac{\mathrm{d}^2}{\mathrm{d}P_{S,i}^2} p_{fd,f}(P_{S,i}) = \frac{\bar{\alpha}_J^2}{W^2 N_0^2} g_f'' \left(\frac{\bar{\alpha}_J P_{S,i}}{W N_0} \right)$. Therefore, $p_{fd,f}(P_{S,i})$ satisfies the condition **P2**.

Therefore, I can use Theorem 1 from Appendix A to solve this optimization problem.

2.3.2 Slow fading

For slow fading, $p_{fd}^{(i)} = p_{fd,s}(P_{S,i})$, from (2.6).

Proposition 2: $\Pr(Y(t) > K\sqrt{T_0 W} | \eta_{S,i})$ has properties **P0**, **P1** and **P2** defined in Theorem 1 in Appendix A.

Proof : Consider $\Pr(Y(t) > K\sqrt{T_0 W} | \eta_{S,i})$.

1) Condition **P0** is obviously satisfied from (2.5).

2) I have,

$$\begin{aligned} \frac{\mathrm{d}}{\mathrm{d}\eta_{S,i}} \Pr(Y(t) > K\sqrt{T_0 W} | \eta_{S,i}) &= \frac{K}{\bar{\alpha}_J \sqrt{2\pi}} \int_0^\infty \frac{y}{(y\eta_{S,i} + N_0)^2} e^{-\frac{1}{2}\left(\frac{K}{y\eta_{S,i}+N_0} - \sqrt{T_0 W}\right)^2} e^{-\frac{y}{\bar{\alpha}_J}} \, \mathrm{d}y \\ &> 0. \end{aligned} \tag{2.33}$$

Therefore, condition **P1** is satisfied.

$$
\begin{aligned}
&\mathit{3)}\ \frac{\mathrm{d}^2}{\mathrm{d}\eta_{S,i}^2}\Pr(Y(t) > K\sqrt{T_0W}|\eta_{S,i}) \\
&= \frac{K}{\bar{\alpha}_J\sqrt{2\pi}}\int_0^\infty \frac{y^2\left\{K(K-(y\eta_{S,i}+N_0)\sqrt{T_0W})-2(y\eta_{S,i}+N_0)^2\right\}}{(y\eta_{S,i}+N_0)^5}e^{-\frac{y}{\bar{\alpha}_J}} \\
&\times e^{-\frac{1}{2}\left(\frac{K}{y\eta_{S,i}+N_0}-\sqrt{T_0W}\right)^2}\,\mathrm{d}y \\
&=\int_0^\infty \frac{Ky^2(K^2-K\sqrt{T_0W}(y+N_0)-2(y+N_0)^2)}{\bar{\alpha}_J\sqrt{2\pi}\eta_{S,i}^3(y+N_0)^5}e^{-\frac{y}{\bar{\alpha}_J\eta_{S,i}}}e^{-\frac{1}{2}\left(\frac{K}{y+N_0}-\sqrt{T_0W}\right)^2}\mathrm{d}y \\
&=\frac{I(\eta_{S,i})}{\eta_{S,i}^3} \qquad (2.34)
\end{aligned}
$$

where $I(\eta_{S,i}) \triangleq \int_0^\infty \iota(y)e^{-\frac{y}{\bar{\alpha}_J\eta_{S,i}}}\,\mathrm{d}y$ and

$$
\iota(y) \triangleq \frac{Ky^2\ (K^2\ -\ K\sqrt{T_0W}\ (y\ +\ N_0)-2(y\ +\ N_0)^2)}{\bar{\alpha}_J\sqrt{2\pi}(y\ +\ N_0)^5}e^{-\frac{1}{2}\left(\frac{K}{y+N_0}-\sqrt{T_0W}\right)^2}. \qquad (2.35)
$$

Note that the sign of $\iota(y)$ depends only on the sign of the quadratic polynomial $K^2 - K\sqrt{T_0W}(y + N_0) - 2(y+N_0)^2$. Further, $\iota(y) > 0 \Leftrightarrow K^2 - K\sqrt{T_0W}(y + N_0) - 2(y+N_0)^2 > 0 \Leftrightarrow y + N_0 \in \left(-\frac{K(\sqrt{T_0W+8}+\sqrt{T_0W})}{4}, \frac{K(\sqrt{T_0W+8}-\sqrt{T_0W})}{4}\right)$. Define $y_0 \triangleq \max\left(\frac{K(\sqrt{T_0W+8}-\sqrt{T_0W})}{4} - N_0, 0\right)$. From the definition of y_0, $y > y_0 \Rightarrow \iota(y) < 0$ and $0 < y < y_0 \Rightarrow \iota(y) > 0$. Also,

$$
\begin{aligned}
I'(\eta_{S,i}) &\triangleq \frac{\mathrm{d}}{\mathrm{d}\eta_{S,i}}I(\eta_{S,i}) = \frac{1}{\bar{\alpha}_J\eta_{S,i}^2}\int_0^\infty y\iota(y)e^{-\frac{y}{\eta_{S,i}\bar{\alpha}_J}}\mathrm{d}y \\
&< \frac{1}{\bar{\alpha}_J\eta_{S,i}^2}\left(\int_0^{y_0} y_0\iota(y)e^{-\frac{y}{\eta_{S,i}\bar{\alpha}_J}}\mathrm{d}y + \int_{y_0}^\infty y_0\iota(y)e^{-\frac{y}{\eta_{S,i}\bar{\alpha}_J}}\mathrm{d}y\right) \\
&= \frac{y_0}{\bar{\alpha}_J\eta_{S,i}^2}\int_0^\infty \iota(y)e^{-\frac{y}{\eta_{S,i}\bar{\alpha}_J}}\mathrm{d}y \\
I'(\eta_{S,i}) &< \frac{y_0 I(\eta_{S,i})}{\bar{\alpha}_J\eta_{S,i}^2} \qquad (2.36)
\end{aligned}
$$

From (2.36), I have $I(\eta_{S,i}) \leq 0 \Rightarrow I'(\tilde{\eta}_{S,i}) < 0$. Therefore, if $\exists\tilde{\eta}_{S,i} \geq 0$ s.t. $I(\tilde{\eta}_{S,i}) \leq 0$, then $I(\eta_{S,i}) < 0\ \forall\ \eta_{S,i} > \tilde{\eta}_{S,i}$. Further, from (2.34), $\frac{\mathrm{d}^2}{\mathrm{d}\eta_{S,i}^2}\Pr(Y(t) > K\sqrt{T_0W}|\eta_{S,i}) \leq 0 \Leftrightarrow$

$I(\eta_{S,i}) \leq 0$.

$$\therefore \frac{\mathrm{d}^2}{\mathrm{d}\eta_{S,i}^2} \Pr(Y(t) > K\sqrt{T_0 W} | \eta_{S,i})(\tilde{\eta}_{S,i}) \leq 0$$

$$\Rightarrow I(\tilde{\eta}_{S,i}) \leq 0 \Rightarrow I(\eta_{S,i}) < 0 \; \forall \; \eta_{S,i} > \tilde{\eta}_{S,i}$$

$$\Rightarrow \frac{\mathrm{d}^2}{\mathrm{d}\eta_{S,i}^2} \Pr(Y(t) > K\sqrt{T_0 W} | \eta_{S,i}) < 0 \; \forall \; \eta_{S,i} > \tilde{\eta}_{S,i}.$$

Therefore, $\Pr(Y(t) > K\sqrt{T_0 W}|\eta_{S,i})$ satisfies condition **P2**.

Note that $p_{fd,s}(P_{S,i}) = \Pr\left(Y(t) > K\sqrt{T_0 W}|\frac{P_{S,i}}{W}\right) = \Pr\left(Y(t) > K\sqrt{T_0 W}|\eta_{S,i}\right)$. Since $\Pr\big(Y(t) > K\sqrt{T_0 W}|\eta_{S,i}\big)$ satisfies the conditions **P0**, **P1** and **P2**, $p_{fd,s}(P_{S,i})$ also satisfies the conditions **P0**, **P1** and **P2**.

Therefore, I can use Theorem 1 to solve this optimization problem.

2.4 Jamming power optimization

In Section 2.3, I analyzed the interference from the adversary during the sensing period, and discussed optimizing the adversary power allocation during the sensing period. In this section, I look at the interference from the adversary during the data transmission period, and the jamming power optimization of the adversary.

From (2.1), to minimize the throughput of the network by jamming, the adversary ideally aims to maximize $\sum_{i \in B_{su}} \sum_{u=1}^{\Omega_i} L_P p_e^{(i,u)} \log_2 M_{i,u}$. However, the adversary is not aware of instantaneous system parameters, such as the instantaneous CSI, the instantaneous numbers of secondary users in the i-th band (Ω_i), and which alphabet each user is using. Further, the adversary cannot differentiate between the bands occupied by PUs and SUs through observations during the transmission interval. Therefore, to minimize the average throughput without this information, the objective function to maximize is changed to be $\max \sum_{i \in B_{su} \cup B_{pu}} r_e(P_{J,i})$, under the constraint $\sum_{i \in B_{su} \cup B_{pu}} P_{J,i} \leq P_J$, where P_J is the total power available for jamming, $P_{J,i}$ is the jamming power allocated for the i-th band, $r_e(P_{J,i})$ is the expected value of $p_e^{(i,u)} \log_2 M_{i,u}$ and the expectation is taken over the fading gains of the links from the CH to the SUs, and from the adversary to the SUs.

2.4.1 Fast fading

Under fast fading, the objective is to maximize $\sum_{i \in B_{su} \cup B_{pu}} r_{e,f}(P_{J,i})$, under the constraint $\sum_{i \in B_{su} \cup B_{pu}} P_{J,i} \leq P_J$. From (2.17),

$$r_{e,f}(P_{J,i}) = \begin{cases} 0, & \text{if } P_{J,i} < P_J^* \\ \log_2 M, & \text{if } P_{J,i} \geq P_J^* \end{cases} \tag{2.37}$$

If the adversary has a total power P_J for jamming, to maximize $\sum_{i \in B_{su} \cup B_{pu}} r_{e,f}(P_{J,i})$, according to (2.37), the adversary aims to maximize the number of bands with $P_{J,i} \geq P_J^*$. Therefore, the optimal number of bands to jam is $n_J^* = \min\left(\left\lfloor \frac{P_J}{P_J^*} \right\rfloor, N_T\right)$.

Since the first and second derivatives of $r_{e,f}(P_{J,i})$ do not exist, I cannot use Theorem 1 here. Fortunately, I do not need Theorem 1, since the packet error rate as a function of jamming power ($r_{e,f}(P_{J,i})$) is a step function, as shown in (2.37), so the optimal jamming strategy is trivial.

2.4.2 Slow fading

Under slow fading with a single alphabet, the objective is to maximize $\sum_{i \in B_{su} \cup B_{pu}} r_{e,s,1}(P_{J,i})$, under the constraint $\sum_{i \in B_{su} \cup B_{pu}} P_{J,i} \leq P_J$.

Proposition 3: Pr(packet error$|\bar{\gamma}_{J,i}$) satisfies the conditions **P0**, **P1** and **P2** of Theorem 1.

Proof:

1) **P0** is satisfied by definition.

2) $\frac{\mathrm{d}}{\mathrm{d}\bar{\gamma}_{J,i}} \Pr(\text{packet error}|\bar{\gamma}_{J,i}) = \frac{\mathrm{d}}{\mathrm{d}\bar{\gamma}_{J,i}} \left(1 - \frac{e^{-\frac{\gamma_T}{\bar{\gamma}_S}}}{\left(\frac{\bar{\gamma}_{J,i}\gamma_T}{\bar{\gamma}_S}+1\right)}\right) = \frac{\frac{\gamma_T}{\bar{\gamma}_S} e^{-\frac{\gamma_T}{\bar{\gamma}_S}}}{\left(\frac{\bar{\gamma}_{J,i}\gamma_T}{\bar{\gamma}_S}+1\right)^2} > 0$. $\therefore$ **P1** is satisfied.

3) $\frac{\mathrm{d}^2}{\mathrm{d}\bar{\gamma}_{J,i}^2} \Pr(\text{packet error}|\bar{\gamma}_{J,i}) = \frac{\mathrm{d}}{\mathrm{d}\bar{\gamma}_{J,i}} \frac{\frac{\gamma_T}{\bar{\gamma}_S} e^{-\frac{\gamma_T}{\bar{\gamma}_S}}}{\left(\frac{\bar{\gamma}_{J,i}\gamma_T}{\bar{\gamma}_S}+1\right)^2} = \frac{\frac{\gamma_T}{\bar{\gamma}_S} e^{-\frac{\gamma_T}{\bar{\gamma}_S}}}{\left(\frac{\bar{\gamma}_{J,i}\gamma_T}{\bar{\gamma}_S}+1\right)^3}(-2)\frac{\gamma_T}{\bar{\gamma}_S} < 0$. $\therefore$ **P2** is satisfied.

From (2.20), $r_{e,s,1}(P_{J,i}) = \Pr\left(\text{packet error}|\frac{\bar{\alpha}_J P_{J,i}}{N_0 W}\right)\log_2 M$. Since $\Pr\left(\text{packet error}|\frac{\bar{\alpha}_J P_{J,i}}{N_0 W}\right)$ satisfies **P0**, **P1** and **P2**, $r_{e,s,1}(P_{J,i})$ also satisfies **P0**, **P1** and **P2**. Therefore, I can use Theorem 1 to solve this optimization problem.

2.4.3 Slow fading with adaptive modulation

Under slow fading with adaptive modulation, the objective is to maximize $\sum_{i \in B_{su} \cup B_{pu}} r_{e,s,2}(P_{J,i})$, under the constraint $\sum_{i \in B_{su} \cup B_{pu}} P_{J,i} \leq P_J$.

Proposition 4: $r_{e,s,2}(P_{J,i})$ satisfies the conditions **P0**, **P1** and **P2** of Theorem 1.

Proof:

1) By definition, I have $r_{e,s,2}(P_{J,i}) \leq \sum_{i=1}^{N_A} \log_2 M_i$. Hence, **P0** is satisfied.

2) Define $t_i \triangleq \frac{\gamma_{T,i}}{\bar{\gamma}_S}$. Note that $\theta > 1$ and $t_{i+1} > t_i > 0$ ($\because \gamma_{T,i} < \gamma_{T,i+1}$ by design). From (2.23),

$$r_{e,s,2}\left(P_{J,i}\right) = \sum_{i=1}^{N_A} h_i \left(\frac{\bar{\alpha}_J P_{J,i}}{N_0 W} \right)$$

where $h_i(x) \triangleq \frac{t_i x \log_2 M_i}{1+t_i x} \left(e^{-\left(\theta t_i + \frac{\theta - 1}{x}\right)} - e^{-\left(\theta t_{i+1} + \frac{\frac{t_{i+1}\theta}{t_i} - 1}{x}\right)} \right)$. From Appendix B, Eq. (B.2), I show that $h_i'(x) \geq 0$. As a consequence, $\frac{\mathrm{d}}{\mathrm{d}P_{J,i}} r_{e,s,2}(P_{J,i}) = \frac{\bar{\alpha}_J}{N_0 W} \sum_{i=1}^{N_A} h_i' \left(\frac{\bar{\alpha}_J P_{J,i}}{N_0 W} \right) \geq 0$. Therefore, **P1** is satisfied.

3) From Appendix B, Eq. (B.14), $\sum_{i=1}^{N_A} h_i''(x) < 0 \Leftrightarrow x > x^*$. It follows that

$$\frac{\mathrm{d}^2}{\mathrm{d}P_{J,i}^2} r_{e,s,2}(P_{J,i}) = \left(\frac{\bar{\alpha}_J}{N_0 W} \right)^2 \sum_{i=1}^{N_A} h_i'' \left(\frac{\bar{\alpha}_J P_{J,i}}{N_0 W} \right) < 0 \Leftrightarrow \frac{\bar{\alpha}_J P_{J,i}}{N_0 W} > x^* \tag{2.38}$$

Therefore, **P2** is satisfied.

Hence, I can use Theorem 1 to solve this optimization problem.

2.5 Joint spoofing and jamming optimization

Suppose the adversary has an energy budget E for a single sensing-plus-transmission duration $T_0 + T_1$. It can be shown that the average throughput of the SUs is proportional to $\sum_{i=1}^{\min(\bar{N}_r, \bar{N}_a - N_{fd})} (\Gamma_1 - r_e(P_{J,i}))$, where Γ_1 is the average number of packets per user per band per transmission interval, $\bar{N}_r$ is the average number of bands required by SUs, $\bar{N}_a$ is the average number of vacant bands, and N_{fd} is the average number of false detections per sensing interval. The average number of bands occupied by PUs is $N_T - \bar{N}_a$. The objective of the adversary is to minimize

$\sum_{i=1}^{\min(\bar{N}_r, \bar{N}_a - N_{fd})}(\Gamma_1 - r_e(P_{J,i}))$, under the constraint $T_0 P_S + T_1 P_J = E$. Let ξE be the amount of energy allocated for spoofing, where $\xi \in [0,1]$. Therefore, $P_S = \frac{\xi E}{T_0}$ and $P_J = \frac{(1-\xi)E}{T_1}$. The optimal energy allocation for spoofing (ξ^*) is given by

$$\xi^* = \underset{\xi \in [0,1]}{\arg\min} \; N_{su}(\xi)\Gamma_1 - \frac{N_{su}(\xi)}{N_{su}(\xi) + N_T - \bar{N}_a} F\big(r_e, \frac{(1-\xi)E}{T_1}, N_{su}(\xi) + N_T - \bar{N}_a\big) \tag{2.39}$$

where $N_{su}(\xi) = \min\Big(\bar{N}_r, \bar{N}_a - \frac{\bar{N}_a}{N_T} F\big(p_{fd}, \frac{\xi E}{T_0}, N_T\big)\Big)$.

The adversary can estimate $\bar{N}_r$ and $\bar{N}_a$ by detecting the average number of occupied bands in the T_0 and T_1 intervals, using an energy detector before it starts spoofing or jamming. From (A.1), I know that the threshold x^* in $F(f, X_T, N)$ does not depend on X_T or N. Therefore, the thresholds in $F\big(r_e, \frac{(1-\xi)E}{T_1}, N_{su}(\xi) + N_T - \bar{N}_a\big)$ and $F\big(p_{fd}, \frac{\xi E}{T_0}, N_T\big)$ do not depend on ξ. Hence, (2.39) only involves direct evaluations of $r_e(P_{J,i})$ and $p_{fd}(P_{S,i})$. Therefore, the optimal fraction of energy allocation for spoofing, ξ^*, can be found from (2.39) using a single parameter search [30].

2.6 Simulation results

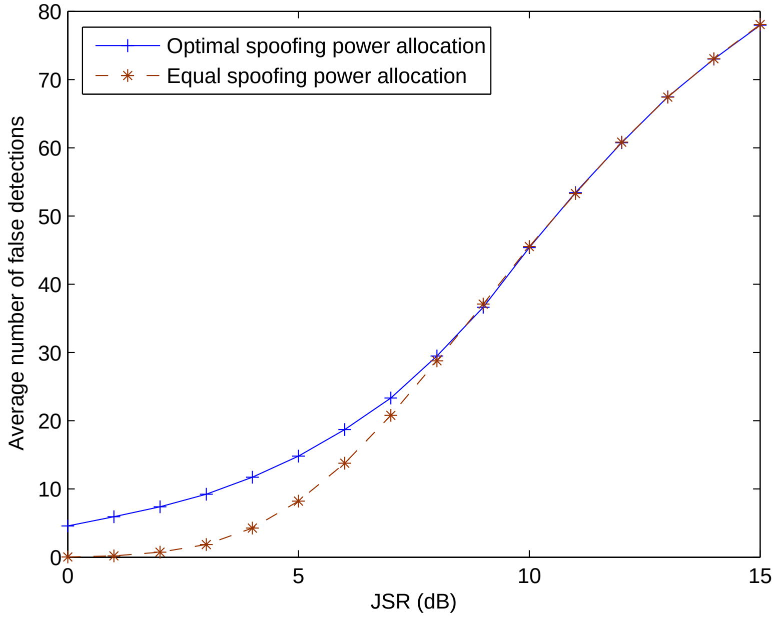
I consider a cluster-based SU system, sharing N_T DS-CDMA subcarriers with PUs. In the simulations, in each transmission and sensing interval, the PUs occupy $|B_{pu}| = \min(N_{pu}, N_T)$ bands at random, where N_{pu} is a Poisson random variable with mean parameter $\bar{N}_{pu}$. The number of SUs (Ω_{su}) in each transmission interval is modeled as a Poisson random variable with mean parameter $\bar{\Omega}_{su}$. The number of bands used by SUs in each transmission interval is $|B_{su}| = \min\Big(\lceil \frac{\Omega_{su}}{\Omega_M} \rceil, |B - B_{pu}|\Big)$, where Ω_M is the maximum number of SUs that can share a single band. I select $\bar{\alpha}_J = 1$, $\beta = 0.2$, $N_c = 256$, $\Omega_M = 8$, $T_0 = 128T_s$ and $T_1 = 1024T_s$, where T_s is the symbol time. For FEC, I use rate $\frac{1}{2}$ LDPC codes with block lengths varying from 1024 bits to 6144 bits. I assume the CH uses power control to maintain $\bar{\gamma}_S = 10$ dB at each SU. I define the jamming-to-signal power ratio (JSR) as the ratio of adversary-power-to-signal-power per user. That is, the adversary power J is taken to be the sum of the jamming and the spoofing power available in all bands, and the signal power S is taken to be the transmission power available for a single SU. When there is no knowledge of the system other than its operating frequency range, the adversary can perform equal power spoofing or jamming across the total bandwidth. I use this equal power spoofing and jamming strategy as a reference, to which the performance of the optimized strategy is compared.

2.6.1 Spoofing

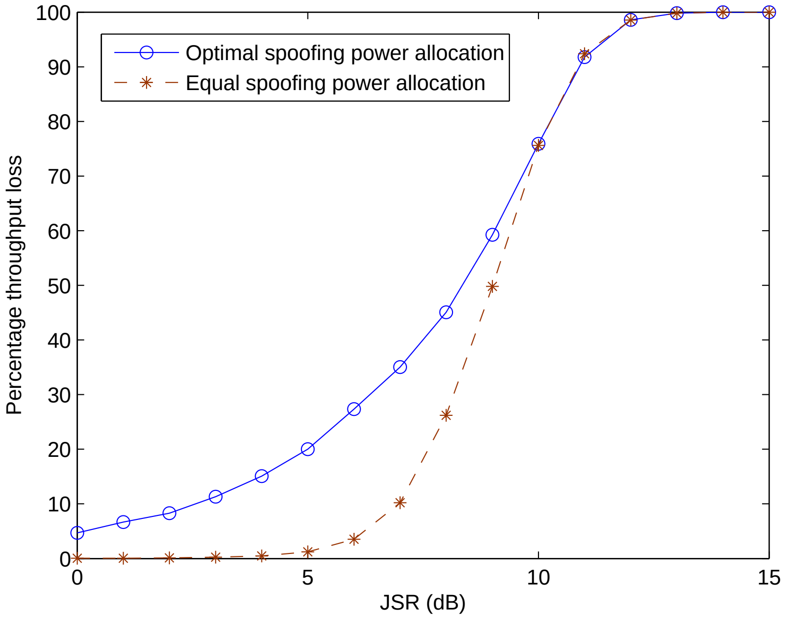
Figure 2.8(a) shows the average number of false detections per sensing interval versus the JSR under slow fading, when the adversary employs the optimal jamming and spoofing strategy (solid curve). For comparison, the average number of false detections if the adversary spoofed all bands at equal power is also presented (dashed curve). The optimal spoofing power allocation increases the average number of false detections by more than 5 for JSR $\in (0, 6)$ dB, compared to equal spoofing power allocation across bands without optimization. As JSR is further increased, the optimal spoofing power allocation strategy shifts from partial band spoofing to full band spoofing, and hence the curves overlap at high JSR. Figure 2.8(b) shows the average throughput loss in the SU network due to spoofing, under fast fading. At a JSR of 7 dB, the optimal spoofing power allocation reduces the throughput by 35.1%, while the equal power allocation reduces the throughput only by 10.2%. For JSR $>$ 10dB, the optimal spoofing strategy is equal power allocation across all bands.

2.6.2 Jamming

In the simulations of the slow fading system, I use the alphabets BPSK, 4-QAM, 16-QAM and 64-QAM for adaptive modulation. Figure 2.9 shows the comparison of the average PER versus JSR per band, calculated using the step-function approximation and the simulations. I note that the values of the PER calculated using the approximation are notably different from the simulation results. The two vertical dotted lines show the threshold JSR, on which the decision for partial band jamming or full band jamming is made. I note that using the approximation, the adversary would decide to move to full jamming at a lower JSR than the optimal value given by the simulations. The gray shaded region represents the reduction in the average PER, i.e., the performance loss of the adversary due to the use of the step function approximation when calculating



(a)



(b)

Figure 2.8: ($p_{fd,f}(0) = 10^{-4}$, $N_c = 256$, $T_0 = 128T_s$, $N_T = 100$, $\frac{\bar{\Omega}_{su}}{\Omega_M} = 50$, $\bar{N}_{pu} = 50$): (a) Average number of false detections under slow fading (b) Percentage loss of throughput under fast fading.

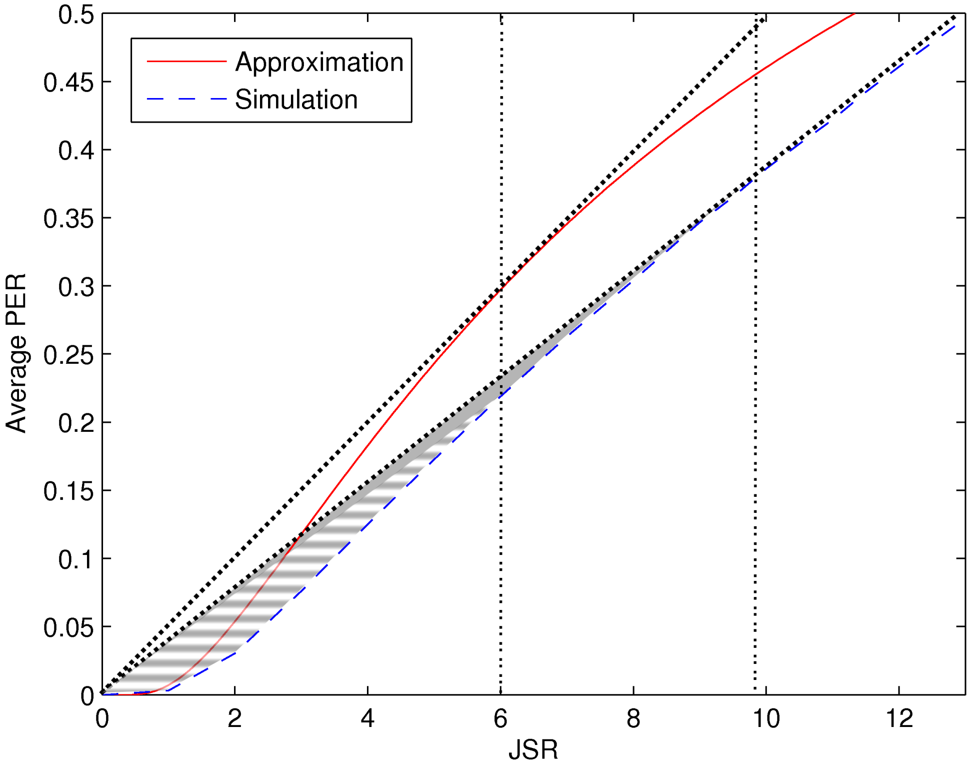


Figure 2.9: Average packet error rate vs. JSR per band. The shaded region shows the PER difference due to the approximation, and the vertical lines are the thresholds at which the jamming strategy switches from partial-band to full-band. ($N_c = 64$, $\bar{\gamma}_S = 12$ dB, $\theta = 2$ dB)

the PER, to decide on the optimal jamming strategy. The horizontal-striped region represents the increase in the average BER using optimization based on the step function approximation, over jamming all bands at every JSR. Therefore, I note that, even though the average PER value given by the approximation is different from the simulations, the optimization based on the approximation yields results comparable to the optimal achievable with perfect information of the FEC performance by the adversary.

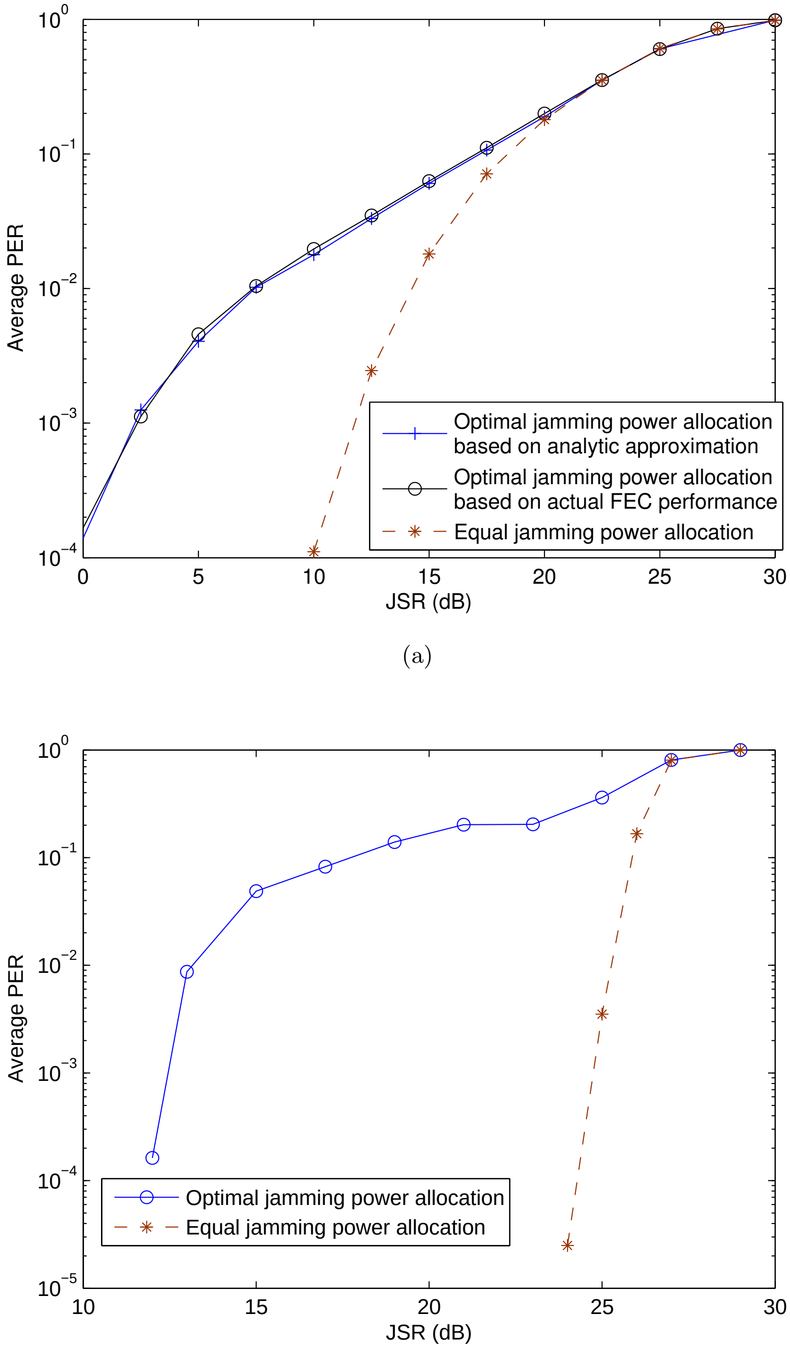
Figure 2.10(a) shows the average PER versus JSR, with total power put into jamming by the adversary, under slow fading. I note that the optimal jamming power allocation based on the step function approximation performs very close to the optimal power allocation with perfect FEC information. The average PER of the system when all transmitting bands are jammed at equal power without any attempt at optimizing is also presented for comparison. The optimization significantly increases the average PER at low JSR. Figure 2.10(b) shows the average PER due to jamming under fast fading. The optimal jamming power allocation achieves a 10^{-2} average PER at a JSR more than 10 dB below the JSR required for the same average PER with equal jamming power allocation.

2.6.3 Joint optimization of spoofing and jamming

Figure 2.11(a) shows the SU throughput-per-transmission interval versus JSR when the adversary jointly optimizes the jamming and spoofing power allocation under slow fading. It is compared with the throughput if the adversary spoofed and jammed bands at equal power. Notice that for JSR in the vicinity of 25dB, the use of the optimization technique by the adversary reduces the CR throughput by a factor of 4 to 5, relative to an adversary who divides power equally across all bands. At low JSR, below about 18dB under simulated system parameters, spoofing is ineffective, as the system is lightly loaded. However, the optimized adversary is able to reduce the throughput slightly through increased packet error rate by jamming. Beyond 18dB, the system throughput is significantly reduced, predominantly due to successful spoofing. Figure 2.11(b) shows the SU throughput-per-transmission interval versus JSR under fast fading. It can be seen that the optimal power allocation can significantly reduce the throughput of SUs at a JSR 10.5 dB lower than constant power allocation, under simulated system parameters.

2.7 Conclusion

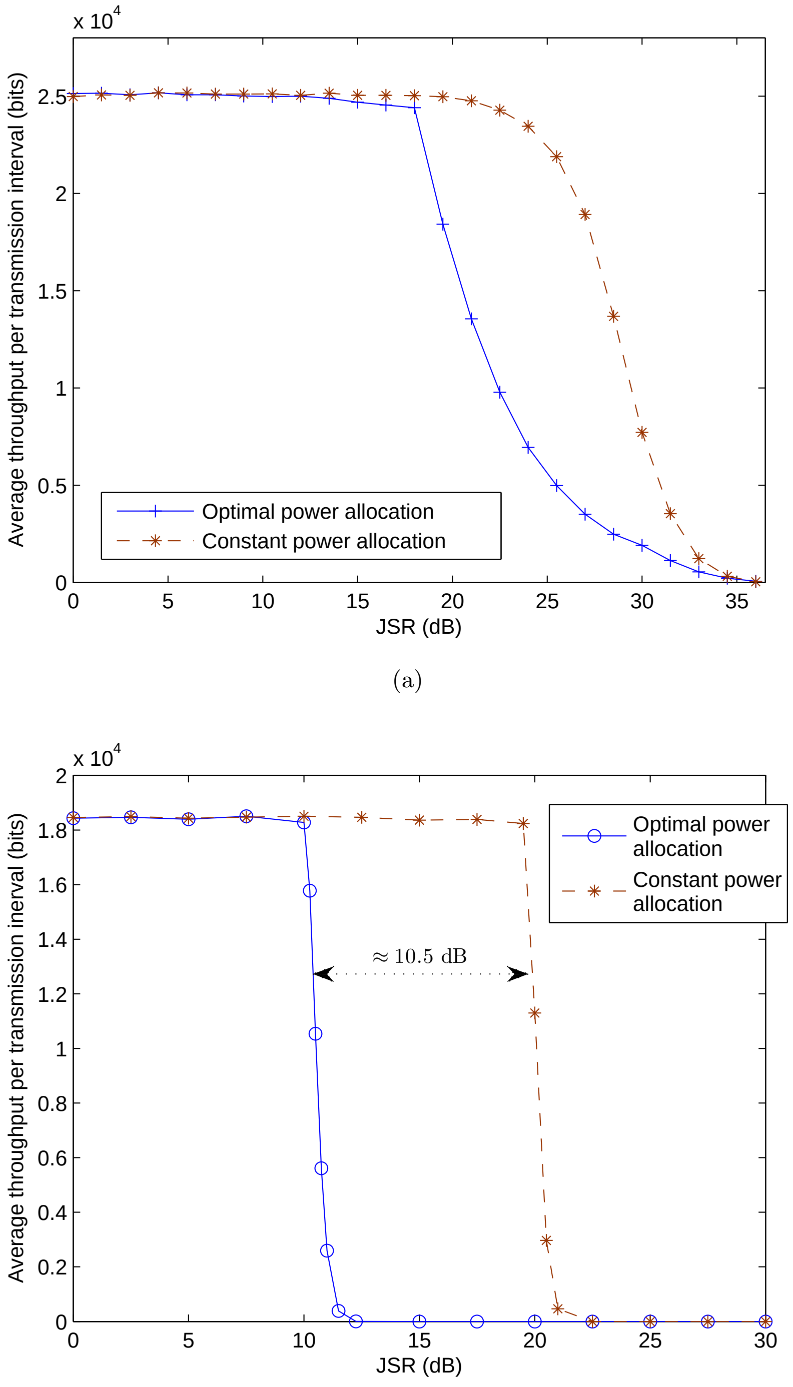
In this chapter, I analyze the optimal spoofing and jamming power allocations across subcarriers, in a Rayleigh fading channel, with an optimization approach which enables simplified calculation of threshold JSRs, below which partial-band attacks are optimal. I derive the optimal jamming power allocation based on a simplified step-function approximation of the word error rate of LDPC codes. Through comparisons of the throughput with optimal spoofing and jamming power allocation with the throughput for equal power spoofing and jamming, I observe that the optimization has notable gains



(a)

(b)

Figure 2.10: Average packet error rate vs. JSR ($\bar{\gamma}_S = 12$ dB, $N_c = 64$, $\frac{\bar{\Omega}_{su}}{\Omega_M} = 10$, $\bar{N}_{pu} = 10$, $N_T = 20$): (a) under slow fading (b) under fast fading.



(a)

(b)

Figure 2.11: Throughput vs. JSR ($T_0 = 128T_s$, $T_1 = 1024T_s$, $\frac{\bar{\Omega}_{su}}{\Omega_M} = 10$, $\bar{N}_{pu} = 10$, $N_T = 100$, $N_c = 256$): (a) under slow fading (b) under fast fading.

in the low and medium JSR regions.

I learn that it is generally optimal to attack with both spoofing and jamming, whereby the optimal energy allocation between the two methods of attack is dependent on system parameters and JSR. While successful spoofing has the most noticeable impact on SU throughput, I observe that when the system is not heavily loaded, spoofing is not effective at low JSR, and the optimal method of attack is jamming. An increase in the average number of subcarriers required by SUs, or a decrease in the sensing duration relative to the transmission duration, would lower the JSR, at which point the optimal strategy shifts from jamming to spoofing.

Chapter 2, in part, is a reprint of material as it appears in M. Soysa, P. Cosman, and L. Milstein, “Optimized spoofing and jamming a cognitive radio,” *IEEE Transactions on Communications*, vol. 62, no. 8, pp. 2681–2695, Aug 2014. The dissertation author was the primary author of this paper.

Chapter 3

Spoofing optimization over Nakagami-m fading channels of a cognitive radio adversary

3.1 Introduction

In this chapter, I analyze the impact of an intelligent adversary using spoofing attacks on a tactical CR system, under Nakagami-m fading. In Chapter 2, I discussed spoofing attacks under Rayleigh fading. In this chapter, I extend the analysis to slow and fast Nakagami-m fading channels.

In Section 3.2, I present the system model. Sections 3.3 and 3.4 discuss the spoofing strategy for fast and slow fading, respectively. Section 3.5 contains numerical results and Section 3.6 presents the conclusions.

3.2 System model

The system model is the same as the one in Chapter 2, given in Fig.2.1. The channels from adversary to the CH in each subcarrier are assumed to undergo i.i.d. Nakagami-m fading with $m \geq \frac{1}{2}$. The objective of the adversary is to maximize the average number of false detections.

The CH uses an energy detector for sensing (Fig.2.2). Let W be the bandwidth of one subcarrier, and T_0 be the duration of the sensing interval. The energy detector output, $Y(t)$, when there is no PU signal present, is given by $Y(t) = \int_{t-T_0}^{t}(\sqrt{\alpha_J(t_1)}n_s(t_1) + n_0(t_1))^2 \mathrm{d}t_1$, where $\alpha_J(t)$ is the gain of the channel from adversary to the CH, $n_s(t)$ is the spoofing signal, and $n_0(t)$ is the noise after passing through the bandpass filter. The signal $n_s(t)$ is Gaussian with double sided PSD $\frac{\eta_s}{2}$ in the band, $n_0(t)$ is Gaussian with PSD $\frac{N_0}{2}$ in the band. The pdf of $\alpha_J(t)$, $f_{\alpha_J(t)}(x) = \frac{m^m x^{m-1} e^{-\frac{mx}{\Omega}}}{\Gamma(m)\Omega^m}$ with fading parameters m, Ω [31, Eq. 2.21]. From [27], I have

$$Y(t) = \frac{1}{2W}\sum_{k=1}^{T_0 W}(a_{i,k}^2 + a_{q,k}^2) \tag{3.1}$$

where

$$a_{i,k} = \sqrt{\alpha_J\left(t - T_0 + \frac{k}{W}\right)} n_{s,i}\left(t - T_0 + \frac{k}{W}\right) + n_{0,i}\left(t - T_0 + \frac{k}{W}\right), \tag{3.2}$$

$$a_{q,k} = \sqrt{\alpha_J\left(t - T_0 + \frac{k}{W}\right)} n_{s,q}\left(t - T_0 + \frac{k}{W}\right) + n_{0,q}\left(t - T_0 + \frac{k}{W}\right), \tag{3.3}$$

$n_{s,i}(t), n_{s,q}(t)$ are Gaussian with PSD η_s in the frequency range $(-\frac{W}{2}, \frac{W}{2})$, and $n_{0,i}(t), n_{0,q}(t)$ are Gaussian with PSD N_0 in the frequency range $(-\frac{W}{2}, \frac{W}{2})$. A band is detected as occupied by PUs if the energy detector output is greater than the threshold $K\sqrt{T_0 W}$. Hence, the probability of false detection is equal to $\Pr(Y(t) > K\sqrt{T_0 W})$.

Following the same approach as in [17, Eq. 1], I can show that the expected number of allowed bands accessible to SUs is $\sum_{i \in B_{al}}(1 - p_{fd}^{(i)})$, where B_{al} is the set of allowed bands and $p_{fd}^{(i)}$ is the probability of false detection of the i-th band, given that the i-th band is allowed. At the start of the sensing interval the adversary does not know which bands are allowed for SUs. Therefore, from the adversary's perspective, every band has an equal probability of being vacant. Hence, the objective of the adversary is to maximize $\sum_{i=1}^{N_T} p_{fd}^{(i)}$, under the constraint $\sum_{i=1}^{N_T} P_{S,i} = P_S$, where $P_{S,i}$ is the spoofing power allocated for the i-th band and P_S is the total spoofing power available.

3.3 Fast fading

Here I assume the channel coherence time is much smaller than the sensing duration T_0, and the channel varies significantly during the sensing interval so that the channel samples in time are mutually independent. I can show that $E[a_{i,k}^2 + a_{q,k}^2] = 2(\Omega\eta_s W + N_0 W)$, and $\mathrm{Var}(a_{i,k}^2 + a_{q,k}^2) = 2(\tilde{m}\Omega^2\eta_s^2 W^2 + 4\Omega\eta_s N_0 W^2 + 2N_0^2 W^2)$, where $\tilde{m} = \frac{2m+3}{m}$. Since $\mathrm{Var}(a_{i,k}^2 + a_{q,k}^2)$ is finite, I can use the Lindeberg-Lévy CLT to approximate $Y(t)$ in (3.1). Therefore, for large T_0W, $Y(t) \sim \mathcal{N}(T_0W(\Omega\eta_s + N_0), T_0W(\tilde{m}\Omega^2\eta_s^2 + 4\Omega\eta_s N_0 + 2N_0^2)/2)$. Let $p_{fd,f}(P_{S,i})$ be the probability of false detection under fast fading, as a function of the spoofing power in that band $P_{S,i}$. Then,

$$\begin{aligned} p_{fd,f}(P_{S,i}) &= \Pr(Y(t) > K\sqrt{T_0W}) \\ &= Q\left(\frac{K\sqrt{T_0W} - T_0W\left(\Omega\left(\frac{P_{S,i}}{W}\right) + N_0\right)}{\sqrt{\frac{T_0W}{2}\left(\tilde{m}\Omega^2\left(\frac{P_{S,i}}{W}\right)^2 + 4\Omega\left(\frac{P_{S,i}}{W}\right)N_0 + 2N_0^2\right)}}\right) \end{aligned} \tag{3.4}$$

Define

$$g(y) \triangleq p_{fd,f}\left(\frac{WN_0y}{\Omega}\right) = Q\left(\frac{b - ay}{\sqrt{\tilde{m}y^2 + 4y + 2}}\right) \tag{3.5}$$

where $b = \frac{K\sqrt{2}}{N_0} - \sqrt{2T_0W}$ and $a = \sqrt{2T_0W}$. As long as the detector threshold is selected so that the false alarm probability (false detection without spoofing) is less than 0.5, then $p_{fd,f}(0) < 0.5 \Leftrightarrow g(0) < 0.5 \Leftrightarrow b > 0$. I now show that the conditions of Theorem 1 in Appendix A are satisfied.

1) From the definition of $p_{fd,f}(P_{S,i})$, condition **P0** is obviously satisfied by $p_{fd,f}(P_{S,i})$.

2) From the definition of $g(y)$, I have

$$p_{fd,f}(P_{S,i}) = g\left(\frac{\Omega P_{S,i}}{WN_0}\right) \tag{3.6}$$

and from (3.5),

$$g'(y) = \frac{\mathrm{d}g(y)}{\mathrm{d}y} = \frac{(2a + \tilde{m}b)y + 2a + 2b}{(\tilde{m}y^2 + 4y + 2)^{\frac{3}{2}}\sqrt{2\pi}} e^{-\frac{(ay-b)^2}{2(\tilde{m}y^2+4y+2)}} \tag{3.7}$$

From (3.7), $g'(y) > 0 \ \forall y > 0$, because $a, b > 0$. From (3.6), $\frac{\mathrm{d}}{\mathrm{d}P_{S,i}} p_{fd,f}(P_{S,i}) = \frac{\Omega}{WN_0} g'\left(\frac{\Omega P_{S,i}}{WN_0}\right) > 0 \ \forall P_{S,i} > 0$. Therefore, condition **P1** is satisfied.

3) From (3.7),

$$g''(y) = \frac{\mathrm{d}}{\mathrm{d}y} g'(y) = \frac{p(y)}{(\tilde{m}y^2 + 4y + 2)^{\frac{7}{2}} \sqrt{2\pi}} e^{-\frac{(ay-b)^2}{2(\tilde{m}y^2+4y+2)}} \tag{3.8}$$

where $p(y) = c_4 y^4 + c_3 y^3 + c_2 y^2 + c_1 y + c_0$, $c_0 = -16a - 4(6 - \tilde{m})b + 4a^2 b + 8ab^2 + 4b^3$, $c_3 = -2\tilde{m}(10 + 3\tilde{m})a - 16\tilde{m}^2 b - a(2a + \tilde{m}b)^2 < 0$, $c_4 = -2\tilde{m}^2(2a + \tilde{m}b) < 0$,

$$\begin{aligned} c_1 &= \tilde{m}c_0 - 4(10 - \tilde{m})a - 4((\tilde{m} - 2)^2 + 8)b - 4a^3 \qquad (3.9) \\ &\quad - 4\tilde{m}a^2 b - 4(\tilde{m} - 1)ab^2, \text{ and} \\ c_2 &= \frac{\tilde{m}}{4} c_1 - (16 + 3\tilde{m}(10 - \tilde{m}))a - 32\tilde{m}b - (8 - \tilde{m})a^3 \\ &\quad - 4(\tilde{m} + 1)a^2 b - \tilde{m}(\tilde{m} + 1)ab^2. \qquad (3.10) \end{aligned}$$

According to Descartes' rule of signs, the number of real positive roots of the polynomial $p(y) = 0$ equals the number of sign changes between nonzero c_is (ordered from c_4 to c_0), or is less than the number of sign changes by a multiple of 2. Note that $c_4, c_3 < 0$ and $\tilde{m} \in (2, 8]$ because $m \geq \frac{1}{2}$. From (3.9), I see that $c_0 \leq 0 \Rightarrow c_1 < 0$, and from (3.10), $c_1 \leq 0 \Rightarrow c_2 < 0$. Therefore, if $c_0 \leq 0$, all non-zero coefficients are negative and there are no sign changes, i.e., there are no positive roots.

Let us consider the case $c_0 > 0$. If $c_1 \leq 0$, then $c_2 < 0$, and there is only one sign change in the coefficients. If otherwise, i.e., $c_1 > 0$, there will be only one sign change irrespective of the sign of c_2. Therefore, I can see that the number of sign changes between coefficients is either 0 or 1. Hence, there will be at most one positive root for $p(y) = 0$. Further, since $c_4 < 0$, $\lim_{y \to \infty} p(y) \to -\infty$. I conclude that $p(y) < 0 \ \forall y > 0$ or $\exists y_0 > 0$, s.t. $q(y) < 0 \ \forall y > y_0$ and $p(y) \geq 0 \ \forall y \leq y_0$. From (3.8), I know $g''(y)$ has the same sign as $p(y)$. Therefore, I conclude that $g(y)$ satisfies condition **P2**. From (3.6), $\frac{\mathrm{d}^2}{\mathrm{d}P_{S,i}^2} p_{fd,f}(P_{S,i}) = \frac{\Omega^2}{W^2 N_0^2} g''\left(\frac{\Omega P_{S,i}}{WN_0}\right)$. Therefore, $p_{fd,f}(P_{S,i})$ satisfies condition **P2**.

3.4 Slow fading

Here I assume the channel coherence time is larger than the sensing duration T_0. Therefore, the channel gain remains constant during the sensing interval and I denote it by α_J. When conditioned on α_J, $a_{i,k} = \sqrt{\alpha_J} n_{s,i}\left(t - T_0 + \frac{k}{W}\right) + n_{0,i}\left(t - T_0 + \frac{k}{W}\right) \sim \mathcal{N}(0, \alpha_J \eta_s W + N_0 W)$, and similarly, $a_{q,k} \sim \mathcal{N}(0, \alpha_J \eta_s W + N_0 W)$. Therefore, $E[a_{i,k}^2 + a_{q,k}^2 | \alpha_J] = 2(\alpha_J \eta_s W + N_0 W)$ and $\mathrm{Var}(a_{i,k}^2 + a_{q,k}^2 | \alpha_J) = 4(\alpha_J \eta_s W + N_0 W)$. Using these results in (3.1), for large $T_0 W$, I conclude, when conditioned on α_J, $Y(t) \sim \mathcal{N}(T_0 W(\alpha_J \eta_s + N_0), T_0 W(\alpha_J \eta_s + N_0)^2)$.

The average probability of false detection under slow fading, when the spoofing signal PSD is $\eta_{S,i}$, is given by

$$\begin{aligned}
&\Pr(Y(t) > K\sqrt{T_0 W} | \eta_{S,i}) \\
&= \int_0^\infty \Pr(Y(t) > K\sqrt{T_0 W} | \alpha_J = y, \eta_{S,i}) f_{\alpha_J}(y) \mathrm{d}y \qquad (3.11)
\end{aligned}$$

where $f_{\alpha_J}(y) = \frac{m^m y^{m-1}}{\Gamma(m)\Omega^m} e^{-\frac{my}{\Omega}}$ is the probability density function of the channel gain α_J. Substituting this in (3.11) yields

$$\begin{aligned}
&\Pr(Y(t) > K\sqrt{T_0 W} | \eta_{S,i}) \\
&= \frac{m^m}{\Gamma(m)\Omega^m} \int_0^\infty Q\left(\frac{K}{\eta_{S,i} y + N_0} - \sqrt{T_0 W}\right) y^{m-1} e^{-\frac{my}{\Omega}} \mathrm{d}y \qquad (3.12)
\end{aligned}$$

As for the fast fading case, I now show that the three conditions of Theorem 1 in Appendix A are satisfied.

1) Condition **P0** is obviously satisfied from (3.12).

2) I have

$$\begin{aligned}
&\frac{\mathrm{d}}{\mathrm{d}\eta_{S,i}} \Pr(Y(t) > K\sqrt{T_0 W} | \eta_{S,i}) = \frac{m^m K}{\Gamma(m)\Omega^m \sqrt{2\pi}} \\
&\times \int_0^\infty \frac{y^m}{(y\eta_{S,i} + N_0)^2} e^{-\frac{1}{2}\left(\frac{K}{y\eta_{S,i} + N_0} - \sqrt{T_0 W}\right)^2} e^{-\frac{my}{\Omega}} \mathrm{d}y > 0
\end{aligned}$$

Therefore, condition **P1** is satisfied.

3) I can show that

$$\begin{aligned}\frac{\mathrm{d}^2}{\mathrm{d}\eta_{S,i}^2}\Pr(Y(t)>K\sqrt{T_0W}|\eta_{S,i}) &= \frac{m^m K}{\Gamma(m)\Omega\sqrt{2\pi}}\int_0^\infty e^{-\frac{my}{\Omega\eta_{S,i}}}e^{-\frac{1}{2}\left(\frac{K}{y+N_0}-\sqrt{T_0W}\right)^2}y^{m+1}\\ &\quad\times\frac{K^2-K\sqrt{T_0W}(y+N_0)-2(y+N_0)^2}{\eta_{S,i}^{m+2}(y+N_0)^5}\mathrm{d}y\\ &= \frac{I(\eta_{S,i})}{\eta_{S,i}^{m+2}}\end{aligned}\tag{3.13}$$

where $I(\eta_{S,i}) \triangleq \int_0^\infty \iota(y)e^{-\frac{my}{\Omega\eta_{S,i}}}\,\mathrm{d}y$ and

$$\iota(y)\triangleq\frac{m^m K y^{m+1}(K^2-K\sqrt{T_0W}(y+N_0)-2(y+N_0)^2)}{\Gamma(m)\Omega\sqrt{2\pi}(y+N_0)^5}e^{-\frac{1}{2}\left(\frac{K}{y+N_0}-\sqrt{T_0W}\right)^2}.\tag{3.14}$$

Note that the sign of $\iota(y)$ depends only on the sign of the quadratic polynomial $K^2 - K\sqrt{T_0W}(y+N_0)-2(y+N_0)^2$. Further,

$$\begin{aligned}\iota(y)>0 &\Leftrightarrow K^2-K\sqrt{T_0W}(y+N_0)-2(y+N_0)^2>0\\ &\Leftrightarrow y+N_0\in\left(-\frac{K(\sqrt{T_0W+8}+\sqrt{T_0W})}{4},\frac{K(\sqrt{T_0W+8}-\sqrt{T_0W})}{4}\right).\end{aligned}\tag{3.15}$$

Define $y_0 \triangleq \max\left(\frac{K(\sqrt{T_0W+8}-\sqrt{T_0W})}{4}-N_0,0\right)$. From the definition of y_0, $y>y_0 \Rightarrow \iota(y)<0$ and $0<y<y_0\Rightarrow\iota(y)>0$. Also,

$$\begin{aligned}I'(\eta_{S,i})\triangleq\frac{\mathrm{d}}{\mathrm{d}\eta_{S,i}}I(\eta_{S,i}) &= \frac{m}{\Omega\eta_{S,i}^2}\int_0^\infty y\iota(y)e^{-\frac{my}{\Omega\eta_{S,i}}}\mathrm{d}y\\ &< \frac{m}{\Omega\eta_{S,i}^2}\left(\int_0^{y_0}y_0\iota(y)e^{-\frac{my}{\Omega\eta_{S,i}}}\mathrm{d}y+\int_{y_0}^\infty y_0\iota(y)e^{-\frac{my}{\Omega\eta_{S,i}}}\mathrm{d}y\right)\\ &= \frac{my_0}{\Omega\eta_{S,i}^2}\int_0^\infty\iota(y)e^{-\frac{my}{\Omega\eta_{S,i}}}\mathrm{d}y\\ &= \frac{my_0I(\eta_{S,i})}{\Omega\eta_{S,i}^2}\end{aligned}\tag{3.16}$$

From (3.16), I have $I(\eta_{S,i})\le 0\Rightarrow I'(\tilde{\eta}_{S,i})<0$. Therefore, if $\exists\tilde{\eta}_{S,i}\ge 0$ s.t. $I(\tilde{\eta}_{S,i})\le 0$, then $I(\eta_{S,i})<0\ \forall\ \eta_{S,i}>\tilde{\eta}_{S,i}$. Further, from (3.13), $\frac{\mathrm{d}^2}{\mathrm{d}\eta_{S,i}^2}\Pr(Y(t)>K\sqrt{T_0W}|\eta_{S,i})\le 0\Leftrightarrow$

$I(\eta_{S,i}) \leq 0$.

$$\therefore \frac{\mathrm{d}^2}{\mathrm{d}\eta_{S,i}^2}\Pr(Y(t) > K\sqrt{T_0W}|\eta_{S,i})(\tilde{\eta}_{S,i}) \leq 0$$
$$\Rightarrow I(\tilde{\eta}_{S,i}) \leq 0 \Rightarrow I(\eta_{S,i}) < 0 \;\forall\; \eta_{S,i} > \tilde{\eta}_{S,i}$$
$$\Rightarrow \frac{\mathrm{d}^2}{\mathrm{d}\eta_{S,i}^2}\Pr(Y(t) > K\sqrt{T_0W}|\eta_{S,i}) < 0 \;\forall\; \eta_{S,i} > \tilde{\eta}_{S,i}.$$

Therefore, $\Pr(Y(t) > K\sqrt{T_0W}|\eta_{S,i})$ satisfies condition **P2**.

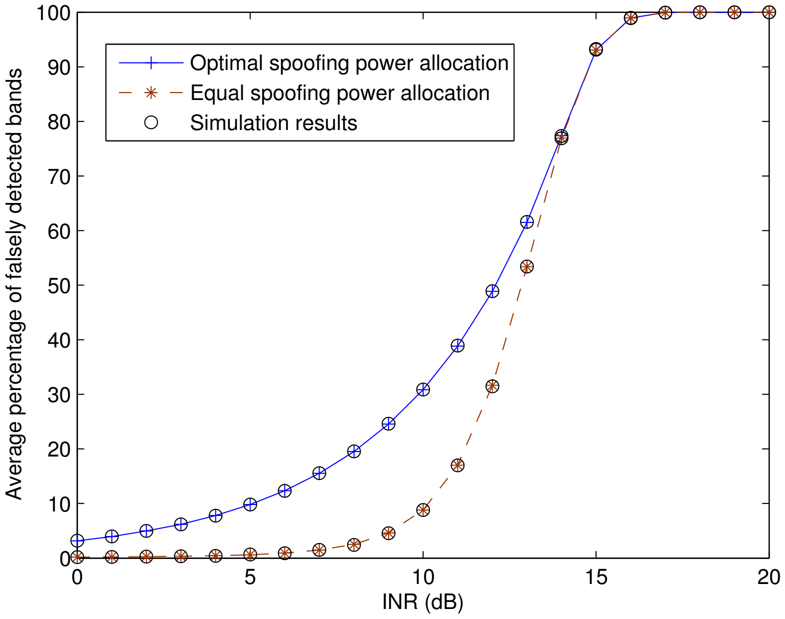
Since $P_{S,i} = \eta_{S,i}W$, the probability of false detection in a band, as a function of the spoofing power allocated for that band under slow fading, is given by $p_{fd,s}(P_{S,i}) = \Pr\left(Y(t) > K\sqrt{T_0W}|\frac{P_{S,i}}{W}\right)$. Since $\Pr\left(Y(t) > K\sqrt{T_0W}|\eta_{S,i}\right)$ satisfies the conditions **P0**, **P1** and **P2**, $p_{fd,s}(P_{S,i})$ also satisfies **P0**, **P1** and **P2**.

3.5 Results

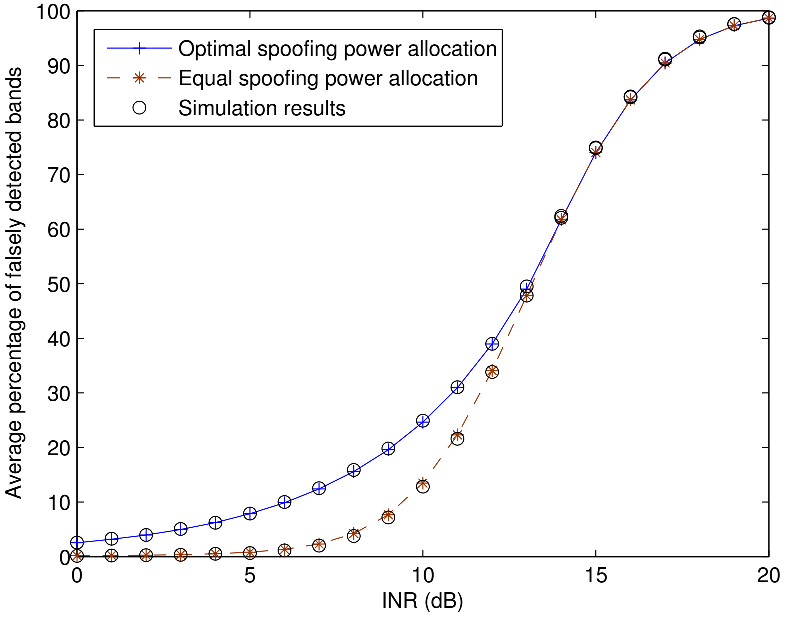
I consider a multi-carrier system with $N_T = 100$ bands, $m = 4$, $\Omega = 1$, $T_0W = 256$, and the false alarm probability $p_{fd,f}(0) = 0.001$. I derive the optimal spoofing power allocation using Theorem 1 in Appendix A. The average number of falsely detected bands as a percentage of the number of allowed bands under the optimal spoofing power allocation is evaluated using (3.4) and (3.11), and verified through Monte Carlo simulations. The performance under equal power allocation without optimization is also presented for comparison. I define the interference-to-noise power ratio (INR) as the ratio of adversary-spoofing-power to background-noise-power-per-band.

Figure 3.1(a) shows the average percentage of falsely detected bands per sensing interval versus the INR under fast fading. The optimal spoofing power allocation increases the average percentage of false detections by more than 11 for INR $\in [6, 12]$ dB, compared to equal spoofing power allocation across bands without optimization. As INR is further increased, the optimal spoofing power allocation strategy shifts from partial band spoofing to full band spoofing, and hence the curves overlap at high INR.

Figure 3.1(b) shows the average percentage of false detections due to spoofing, under slow fading. At an INR of 8 dB, the optimal spoofing power allocation causes 15.88% false detections on average, while the equal power allocation produces only 3.77%.



(a)



(b)

Figure 3.1: Average number of false detections ($p_{fd,f}(0) = 0.001$, $T_0W = 256$, $N_T = 100$, $m = 4$, $\Omega = 1$): (a) under fast fading (b) under slow fading.

For INR $>$ 14dB, the optimal spoofing strategy is equal power allocation across all bands, as can be seen from Figure 3.1(b).

3.6 Conclusion

In this chapter, I analyze the optimal spoofing power allocations across subcarriers, in a Nakagami-m fading channel, with an optimization approach which enables simplified calculation of threshold adversary power, below which partial-band attacks are optimal. Through comparisons of the average number of false detections with optimal spoofing power allocation with that of equal power spoofing, I observe that the optimization has notable gains in the low and medium INR regions.

Chapter 3, in part, is a reprint of material as it appears in M. Soysa, P. Cosman, and L. Milstein, "Spoofing optimization over Nakagami-m fading channels of a cognitive radio adversary," in *IEEE Global Conference on Signal and Information Processing (GlobalSIP), 2013*, Dec 2013, pp. 1190–1193. The dissertation author was the primary author of this paper.

Chapter 4

Disruptive Attacks on Video Tactical Cognitive Radio Downlinks

4.1 Introduction

In this chapter, I analyze the impact of an intelligent adversary on a tactical, spread spectrum, CR system transmitting video in H.264/AVC format. In Chapter 2, the optimal power allocation for spoofing and jamming for a generic communication network was studied, and the adversary was optimized to minimize the network throughput. In this chapter, I investigate H.264 video communication, and use the received video distortion as the performance metric. The main contributions of the current chapter are: (i) worst-case analysis of three modes of attack: spoofing, desynchronizing and jamming, (ii) investigating video performance under hostile conditions, (iii) evaluating various resource allocation algorithms and (iv) proving the optimality of an attacking strategy based on a set of sufficient conditions. The set of sufficient conditions of the performance metrics (e.g., probability of false detection, probability of packet error) enables us to prove that the optimal strategy of an adversary is to use equal-power, partial-band interference at low interference power, and as interference power increases, transition to equal-power, full-band interference, and then, while retaining full-band interference, transition multiple times from equal-power, to unequal-power, to equal-power, and so on. These transitions are due to the performance metric function transitioning between convex and concave regions.

In Section 4.2, I present the system model, and derive performance metrics as functions of spoofing, desynchronizing or jamming power. Sections 4.3, 4.4 and 4.5 discuss the optimization of spoofing, desynchronizing and jamming, respectively. In Section 4.6, I discuss the optimal energy allocation among the different modes of attack. Section 4.7 contains system simulations and Section 4.8 presents the conclusions. The optimization approach used in this chapter is presented in Appendix C.

4.2 System model

I analyze four main subcomponents of the system; sensing, code acquisition, resource allocation and data transmission. In Subsection 4.2.1, I present the sensing subsystem, and in Subsection 4.2.2 the code acquisition subsystem is discussed. In Subsection 4.2.3, I describe the resource allocation algorithms. The transmission and receiver blocks are discussed in Subsection 5.2.3.

The CH serving SUs transmits video to the SUs over a MC-DS-CDMA system with N_T bands. The system has periodic sensing intervals (T_0), each followed by a code acquisition interval (T_1) and a transmission interval (T_2). In the earlier chapters, I considered sensing only by CH. In contrast, I now consider distributed sensing, where all SUs perform spectrum sensing, and detect which bands are occupied during the sensing interval. This information is sent to the CH and the bands detected as vacant by all SUs is the set of *allowed bands*. Then, the CH broadcasts a known spreading sequence in all allowed bands during the code acquisition interval, which is used by the SUs for code acquisition and channel estimation. The estimated CSI and the rate-distortion curve of each SU is sent to the CH via a secure feedback channel. This information is used by the CH for channel allocation among SUs. The SUs then communicate during the transmission interval.

In Chapter 2, I assumed that the average channel gain is the same for all SUs. In this chapter, the average gain of the channel from the adversary to user u_j in the i-th band is assumed to have the form $\bar{\alpha}_J^{(u_j)} = 10^{-\upsilon_{u_j}}\bar{\alpha}_J$, where $\upsilon_{u_j} \sim \mathcal{N}(0, \sigma_\upsilon^2)$. I assume all channels experience slow Rayleigh fading and are mutually independent. The distortion of the received video of user u_j is a function of the source rate (r_{u_j}) and the probability of packet error (e_{u_j}) during the transmission interval. Let $f_D^{(u_j)}(r_{u_j}, e_{u_j})$ denote the average distortion of u_j. The function $f_D^{(u_j)}$ is dependent on the temporal and spatial correlation of the video.

Unlike the previous chapters, I use the average distortion (or MSE) of the received video as the performance metric. The objective of the adversary is to maximize $\sum_{\forall u_j} f_D^{(u_j)}(r_{u_j}, e_{u_j})$. I assume the adversary has the same knowledge of the system as in the previous chapters.

4.2.1 Sensing system model

SUs use energy detectors for sensing (Fig.2.2). From Chapter 2, the energy detector output $Y_i^{(u_j)}(t) \sim \mathcal{N}\big(T_0W(\alpha_{J,i}^{(u_j)}\eta_{s,i} + N_0), T_0W(\alpha_{J,i}^{(u_j)}\eta_{s,i} + N_0)^2\big)$, where $\alpha_{J,i}^{(u_j)}$ is the gain of the channel from the adversary to u_j in the i-th band, and $\alpha_{J,i}^{(u_j)}$ is exponentially distributed with mean $\bar{\alpha}_J^{(u_j)}$. This output is compared to the threshold $K\sqrt{T_0W}$ by u_j to determine if the i-th band is vacant, and this information is communicated to the CH. The i-th band is determined to be vacant if all SUs detect it as vacant. Therefore, a band will be falsely detected as occupied if $Y_i^{(u_j)}(t) > K\sqrt{T_0W}$ for any $u_j \in U_{al}$, where U_{al} is the set of secondary users. The average probability of such a *false detection* is

$$\Pr\left(\bigcup_{u_j \in U_{al}} \left(Y_i^{(u_j)}(t) > K\sqrt{T_0W}\right)\right) = 1 - \prod_{u_j \in U_{al}} \Pr\left(Y_i^{(u_j)}(t) < K\sqrt{T_0W}\right) \tag{4.1}$$

From (2.5),

$$\Pr\Big(Y_i^{(u_j)}(t) < K\sqrt{T_0W}\Big) = 1 - \frac{1}{\bar{\alpha}_J^{(u_j)}} \int_0^\infty Q\left(\frac{K}{\eta_{s,i}y + N_0} - \sqrt{T_0W}\right) e^{\frac{-y}{\bar{\alpha}_J^{(u_j)}}}\, \mathrm{d}y. \tag{4.2}$$

Substituting this in (4.1), and using $\eta_{s,i} = \frac{P_{S,i}}{W}$, I can express the average probability of false detection in the i-th band ($p_{fd}(P_{S,i})$), where the spoofing signal power is $P_{S,i}$, as

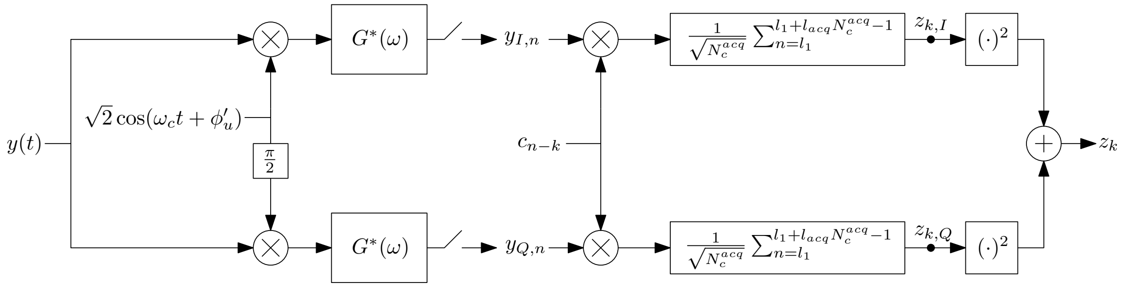

$y(t)$
$\sqrt{2}\cos(\omega_c t + \phi'_u)$
$\frac{\pi}{2}$
$G^*(\omega)$
$G^*(\omega)$
$y_{I,n}$
$y_{Q,n}$
c_{n-k}
$\frac{1}{\sqrt{N_c^{acq}}}\sum_{n=l_1}^{l_1+l_{acq}N_c^{acq}-1}$
$\frac{1}{\sqrt{N_c^{acq}}}\sum_{n=l_1}^{l_1+l_{acq}N_c^{acq}-1}$
$z_{k,I}$
$z_{k,Q}$
$(\cdot)^2$
$(\cdot)^2$
z_k

Figure 4.1: Code acquisition block

follows:

$$p_{fd}(P_{S,i}) = 1 - \prod_{u_j \in U_{al}} \left(1 - \frac{1}{\bar{\alpha}_J^{(u_j)}} \int_0^\infty Q\left(\frac{K}{\frac{P_{S,i}}{W}y + N_0} - \sqrt{T_0 W}\right) e^{-\frac{y}{\bar{\alpha}_J^{(u_j)}}} \mathrm{d}y\right) \tag{4.3}$$

4.2.2 Code acquisition block analysis

Following the sensing interval, the CH broadcasts a known sequence of chips in all allowed bands. SUs use this broadcasted sequence for coarse acquisition. For code acquisition, the CH transmits the signal $x_i(t) = \left\{\sqrt{2E_c}\sum_{n=0}^{k_{acq}N_c^{acq}-1} c_n g(t - nT_c)\cos(\omega_c t)\right\}$ in the i-th band, where $\{c_n\}$ is the binary spreading sequence with chip duration T_c, and $k_{acq}N_c^{acq}T_c$ is the code acquisition period. The received signal at user u_j in the i-th band is:

$$y(t) = \sqrt{2\alpha_{S,i}^{(u_j)}E_c} \sum_{n=0}^{k_{acq}N_c^{acq}-1} c_n g(t - t_d - nT_c)\cos\bigl(\omega_c(t - t_d) - \phi_{S,i}^{(u_j)}\bigr) + \sqrt{\alpha_{J,i}^{(u_j)}} n_{J,i}(t) + n_{w,i}(t) \tag{4.4}$$

where $\alpha_{S,i}^{(u_j)}$ and $\phi_{S,i}^{(u_j)}$ are the gain and phase components of the channel from the CH-to-u_j in the i-th band. The gain of the jammer-to-u_j channel is $\alpha_{J,i}^{(u_j)}$. The channel gains $\alpha_{S,i}^{(u_j)}$ and $\alpha_{J,i}^{(u_j)}$ are exponential random variables (r.v.) with means $\bar{\alpha}_S^{(u_j)}$ and $\bar{\alpha}_J^{(u_j)}$, respectively. The background noise $n_{w,i}(t)$ is AWGN with a double-sided PSD $\frac{N_0}{2}$ and $\sqrt{\alpha_{J,i}^{(u_j)}} n_{J,i}(t)$ is the received jamming signal, where $n_{J,i}(t)$ is Gaussian with PSD $\frac{\eta_{J,i}}{2}$ in the i-th band. The propagation delay is t_d.

I use the receiver block shown in Figure 4.1 for code acquisition. The CH broadcasts a known chip sequence c_n, and the received signal at an SU is $y(t)$. The received signal is sent through two down-converters (multiplied by $\cos(\omega_c t+\phi'_u)$ and $\sin(\omega_c t+\phi'_u)$), and root-raised-cosine matched filters. The output sequences from the matched filters ($y_{I,n}$ and $y_{Q,n}$) are sampled at a frequency of $\frac{1}{T_c}$, and stored for processing in the next step. The matched filter output sequences are despread using shifted versions of the c_n sequence (c_{n-k}). The despread samples ($z_{k,I}$ and $z_{k,Q}$) from the two signal paths are squared and summed to obtain the output sample z_k.

For despreading, I use the samples with indices from l_1 to $l_1 + l_{acq}N_c^{acq} - 1$. Here I use $l_{acq}(\geq 1)$ repetitions of the spreading sequence in the summation to improve the probability of successful code acquisition. Here I select l_1 and l_{acq}, such that the broadcast signal is present throughout the despreading interval. Because the SU knows T_0, an approximate estimate for the maximum distance to the CH and an estimate for the maximum delay spread for the channel, the SU can pick l_1 and l_{acq} that satisfy the above constraint for a sufficiently large T_1.

The signal at the output of the despreader in the I-path ($z_{k,I}$) can be written as follows:

$$\begin{aligned} z_{k,I} &= \frac{1}{\sqrt{N_c^{acq}}} \sum_{n=l_1}^{l_1+l_{acq}N_c^{acq}-1} c_n^{(k)} \int_{-\infty}^{\infty} g(\tau - nT_c)\sqrt{2}\cos(\omega_c\tau + \phi'_u)y(\tau)\,\mathrm{d}\tau \\ &= s_{k,I} + n_{w,k,I} + n_{J,k,I} \end{aligned} \tag{4.5}$$

where $s_{k,I}$, $n_{w,k,I}$ and $n_{J,k,I}$ are the signal, background noise, and jamming components. Here, ϕ'_u is a random phase at the start of acquisition, uniformly distributed in $[-\pi, \pi)$.

$$
\begin{aligned}
s_{k,I} &= \frac{1}{\sqrt{N_c^{acq}}} \sum_{n=l_1}^{l_1+l_{acq}N_c^{acq}-1} c_{n-k} \int_{-\infty}^{\infty} g(\tau - nT_c)\sqrt{2}\cos(\omega_c\tau + \phi'_u)\sqrt{2\alpha_{S,i}^{(u_j)} E_c} \\
&\times \sum_{m=0}^{k_{acq}N_c^{acq}-1} c_m g(\tau - t_d - mT_c)\cos\big(\omega_c(\tau - t_d) - \phi_{S,i}^{(u_j)}\big)\ \mathrm{d}\tau \\
&\approx \sqrt{\frac{\alpha_{S,i}^{(u_j)} E_c}{N_c^{acq}}} \int_{-\infty}^{\infty} \cos\big(\omega_c t_d + \phi_{S,i}^{(u_j)} + \phi'_u\big) \sum_{n=l_1}^{l_1+l_{acq}N_c^{acq}-1} \sum_{m=0}^{k_{acq}N_c^{acq}-1} c_{n-k} c_m g(\tau - nT_c) \\
&\times g(\tau - t_d - mT_c)\ \mathrm{d}\tau \\
&= \sqrt{\frac{\alpha_{S,i}^{(u_j)} E_c}{N_c^{acq}}} \cos\big(\omega_c t_d + \phi_{S,i}^{(u_j)} + \phi'_u\big) R_c(k, t_d)
\end{aligned}
\tag{4.6}
$$

where $R_c(k,t_d) \triangleq \sum_{n=l_1}^{l_1+l_{acq}N_c^{acq}-1} \sum_{m=0}^{k_{acq}N_c^{acq}-1} c_{n-k} c_m \int_{-\infty}^{\infty} g(\tau - nT_c) g(\tau - t_d - mT_c)\ \mathrm{d}\tau$.

$$
\begin{aligned}
n_{J,k,I} &= \frac{1}{\sqrt{N_c^{acq}}} \sum_{n=l_1}^{l_1+l_{acq}N_c^{acq}-1} c_{n-k} \int_{-\infty}^{\infty} g(\tau - nT_c)\sqrt{2}\cos(\omega_c\tau + \phi'_u)\sqrt{\alpha_{J,i}^{(u_j)}} n_J(\tau)\ \mathrm{d}\tau \\
&= \frac{1}{\sqrt{N_c^{acq}}} \sum_{n=l_1}^{l_1+l_{acq}N_c^{acq}-1} c_{n-k} \tilde{n}_{J,n}
\end{aligned}
\tag{4.7}
$$

where $\tilde{n}_{J,n}$ are i.i.d. zero mean Gaussian with variance $\frac{\alpha_{J,i}^{(u_j)}\eta_{J,i}}{2}$. Similarly, I can show that

$$
n_{w,k,I} = \frac{1}{\sqrt{N_c^{acq}}} \sum_{n=l_1}^{l_1+l_{acq}N_c^{acq}-1} c_{n-k} \tilde{n}_{w,n} \tag{4.8}
$$

where $\tilde{n}_{w,n} \sim \mathcal{N}(0, \frac{N_0}{2})$, and i.i.d. I make the simplifying assumption that the signal components ($s_{k,I}$ and $s_{k,Q}$) are non-zero only when $|kT_c - t_d| < \frac{T_c}{2}$ [32]. For this, it is necessary to have a spreading sequence that is orthogonal to its time-shifted versions.

Under this assumption, I can show that the noise components $n_{w,k_1,I}, n_{w,k_2,I}$ are uncorrelated by calculating $E\Big[n_{w,k_1,I} n_{w,k_2,I}\Big]$. In the same way, I can show $n_{J,k_1,I}, n_{J,k_2,I}, n_{J,k_1,Q}$ and $n_{J,k_2,Q}$ are uncorrelated if c_n is orthogonal to its time-shifted versions. Therefore, I conclude that $z_{k_1,I}$ and $z_{k_2,I}$ are uncorrelated, and because they are Gaussian, they are independent. In the same way, $z_{k_1,Q}$, and $z_{k_2,Q}$ are independent.

Therefore, I conclude that the outputs z_k are mutually independent.

Probability of code acquisition

Note that $z_k = z_{k,I}^2 + z_{k,Q}^2$. From (4.7) and (4.8), I know that $n_{w,k,I} \sim \mathcal{N}(0, \frac{l_{acq}N_0}{2})$ and $n_{J,k,I} \sim \mathcal{N}(0, \frac{l_{acq}\alpha_{J,i}^{(u_j)}\eta_J}{2})$, when conditioned on $\alpha_{J,i}^{(u_j)}$. Let k^* be the correct phase of the code. According to our simplifying assumption, $s_{k,I} = 0$ for $k \neq k^*$. From (4.6),

$$
\begin{aligned}
s_{k^*,I} &= \sqrt{\frac{\alpha_{S,i}^{(u_j)} E_c}{N_c^{acq}}} \cos\big(\omega_c t_d + \phi_{S,i}^{(u_j)} + \phi_u'\big) R_c(k^*, t_d) \\
&= \sqrt{\frac{\alpha_{S,i}^{(u_j)} E_c}{N_c^{acq}}} \cos\big(\omega_c t_d + \phi_{S,i}^{(u_j)} + \phi_u'\big) \times \zeta_d l_{acq} N_c^{acq} \\
&= \zeta_d l_{acq} \sqrt{\alpha_{S,i}^{(u_j)} E_c N_c^{acq}} \cos\big(\omega_c t_d + \phi_{S,i}^{(u_j)} + \phi_u'\big) \qquad (4.9)
\end{aligned}
$$

Here, ζ_d depends on t_d mod T_c and the pulse-shaping filter. From numerical evaluation of the autocorrelation of the root-raised cosine pulse, it can be shown that $\zeta_d \in [0.63, 1]$.

Under Rayleigh fading, $\sqrt{\alpha_{S,i}^{(u_j)}} \cos\big(\omega_c t_d + \phi_{S,i}^{(u_j)} + \phi_u'\big)$ is a zero-mean Gaussian r.v. with variance $\frac{\bar{\alpha}_S^{(u_j)}}{2}$. Therefore, $s_{k^*,I} \sim \mathcal{N}(0, \frac{l_{acq}^2 E_c N_c^{acq} \bar{\alpha}_S^{(u_j)}}{2})$. It follows that $z_{k^*,I} = s_{k^*,I} + n_{w,k^*,I} + n_{J,k^*,I} \sim \mathcal{N}\big(0, \frac{l_{acq}}{2}(\zeta_d^2 l_{acq} E_c N_c^{acq} \bar{\alpha}_S^{(u_j)} + \alpha_{J,i}^{(u_j)} \eta_{J,i} + N_0)\big)$, when conditioned on $\alpha_{J,i}^{(u_j)}$. Similarly, $z_{k^*,Q} \sim \mathcal{N}\big(0, \frac{l_{acq}}{2}(\zeta_d^2 l_{acq} E_c N_c^{acq} \bar{\alpha}_S^{(u_j)} + \alpha_{J,i}^{(u_j)} \eta_{J,i} + N_0)\big)$. Further $z_{k^*,I}$ and $z_{k^*,Q}$ are independent. Therefore, $z_{k^*} = z_{k^*,I}^2 + z_{k^*,Q}^2$ is an exponential r.v. with mean $l_{acq}(\zeta_d^2 l_{acq} E_c N_c^{acq} \bar{\alpha}_S^{(u_j)} + \alpha_{J,i}^{(u_j)} \eta_{J,i} + N_0)$. For $k \neq k^*$, $s_{k_I} \approx 0$ and $s_{k,Q} \approx 0$. Following the same approach as before, I can show that z_k is an exponential r.v. with mean $l_{acq}(\alpha_{J,i}^{(u_j)} \eta_{J,i} + N_0)$, for $k \neq k^*$.

The probability of code acquisition conditioned on $\alpha_{J,i}^{(u_j)}$ is $\Pr(z_{k^*} > z_k | \alpha_{J,i}^{(u_j)}), \quad \forall\ k \neq k^*, k \in \{0, 1, \ldots, N_c^{acq} - 1\}$. Therefore, the probability of a code acquisition failure is

$$
\begin{aligned}
\Pr\Bigg(\bigcup_{k \in \{0,\ldots,N_c^{acq}-1\} - k^*} z_{k^*} < z_k | \alpha_{J,i}^{(u_j)}\Bigg) &\geq \Pr\Big(z_{k^*} < z_k | \alpha_{J,i}^{(u_j)}\Big) \\
&= \int_0^\infty \Pr\Big(z_{k^*} < x | \alpha_{J,i}^{(u_j)}\Big) f_{z_k | \alpha_{J,i}^{(u_j)}}(x)\, \mathrm{d}x \qquad (4.10)
\end{aligned}
$$

where $f_{z_k|\alpha_{J,i}^{(u_j)}}(x)$ is the pdf of z_k conditioned on $\alpha_{J,i}^{(u_j)}$,

$$f_{z_k|\alpha_{J,i}^{(u_j)}}(x) = \frac{1}{l_{acq}(\alpha_{J,i}^{(u_j)}\eta_{J,i}+N_0)} e^{\overline{\frac{-x}{l_{acq}(\alpha_{J,i}^{(u_j)}\eta_{J,i}+N_0)}}}, \tag{4.11}$$

and

$$\Pr\left(z_{k^*} < x|\alpha_{J,i}^{(u_j)}\right) = 1 - e^{-\overline{\frac{x}{l_{acq}(\zeta_d^2 l_{acq}E_cN_c^{acq}\bar{\alpha}_S^{(u_j)}+\alpha_{J,i}^{(u_j)}\eta_{J,i}+N_0)}}}. \tag{4.12}$$

Substituting (4.11) and (4.12), in (4.10), I obtain

$$\begin{aligned}\Pr\left(\bigcup_{k\in\{0,\ldots,N_c^{acq}-1\}-k^*} z_{k^*} < z_k|\alpha_{J,i}^{(u_j)}\right) &\geq \int_0^\infty \left(1 - e^{-\frac{x}{l_{acq}(\zeta_d^2 l_{acq}E_cN_c^{acq}\bar{\alpha}_S+\alpha_J\eta_J+N_0)}}\right) \\ &\times \frac{e^{-\frac{x}{l_{acq}(\alpha_J\eta_J+N_0)}}}{l_{acq}(\alpha_J\eta_J+N_0)}\,\mathrm{d}x \\ &= \frac{1}{\left(\frac{l_{acq}\zeta_d^2E_cN_c^{acq}\bar{\alpha}_S^{(u_j)}}{(\alpha_{J,i}^{(u_j)}\eta_{J,i}+N_0)}+2\right)} \end{aligned} \tag{4.13}$$

Let $p_{cqf}(P_{ds,i})$ be the average probability of code acquisition failure, averaged over $\alpha_{J,i}^{(u_j)}$, where $P_{ds,i}$ is the desynchronizing power in the i-th band. Note that $\eta_{J,i} = \frac{P_{ds,i}}{W}$.

$$p_{cqf}(P_{ds,i}) = \int_0^\infty \Pr\left(\bigcup_{k\in\{0,1,\ldots,N_c^{acq}-1\}-k^*} z_{k^*} < z_k|\alpha_{J,i}^{(u_j)}\right)\frac{e^{-\frac{\alpha_{J,i}^{(u_j)}}{\bar{\alpha}_J^{(u_j)}}}}{\bar{\alpha}_J}\,\mathrm{d}\alpha_{J,i}^{(u_j)}$$

$$\geq \int_0^\infty \frac{1}{\left(\frac{\zeta_d^2 l_{acq}E_cN_c^{acq}\bar{\alpha}_S^{(u_j)}}{\alpha_{J,i}^{(u_j)}\frac{P_{ds,i}}{W}+N_0}+2\right)} \times \frac{e^{-\frac{\alpha_{J,i}^{(u_j)}}{\bar{\alpha}_J^{(u_j)}}}}{\bar{\alpha}_J^{(u_j)}}\,\mathrm{d}\alpha_{J,i}^{(u_j)} \tag{4.14}$$

$$= \frac{1}{2}\left(1+\frac{\zeta_d^2 l_{acq}E_cN_c^{acq}\bar{\alpha}_SW}{2\bar{\alpha}_JP_{ds,i}}e^{\frac{2N_0W+\zeta_d^2 l_{acq}E_cN_c^{acq}\bar{\alpha}_S^{(u_j)}W}{2\bar{\alpha}_J^{(u_j)}P_{ds,i}}}\mathrm{Ei}\left(-\frac{2N_0W+\zeta_d^2 l_{acq}E_cN_c^{acq}\bar{\alpha}_S^{(u_j)}W}{2\bar{\alpha}_J^{(u_j)}P_{ds,i}}\right)\right) \tag{4.15}$$

$$\triangleq p_{cqf,lb}(P_{ds,i})$$

where $\mathrm{Ei}(\cdot)$ is the exponential integral function and $p_{cqf,lb}(P_{ds,i})$ is a lower bound to $p_{cqf}(P_{ds,i})$.

4.2.3 User allocation methods

Let $B_{al} \subseteq B$ be the set of allowed bands in the current sensing interval, and let α be the $|B_{al}| \times |U_{al}|$ matrix, where $\alpha[i][j]$ is the channel gain of the j-th user in the i-th band. The maximum transmit power in a subcarrier is $P_{Tx,max}$ and P_{Rx} is the target received power per stream. The number of spreading sequences available in each band is N_{ss} and the maximum number of spreading sequences needed for user j ($N_{sc,\max}[j]$) is determined by the video properties.

One user allocation method is simple multi-user diversity, where each band is assigned to the user with the best channel gain in that band. The algorithm is given in Fig.4.2. I use P_{sc} to keep track of the transmit power in each subcarrier, and C_{al}, a $|B| \times |U_{al}|$ matrix, to keep track of the user-subcarrier assignment. A second algorithm, named MXD, iteratively assigns additional subcarriers to the set of users with the maximum distortion, and is given in Fig.4.3. After the initial assignment from either of the above algorithms, the swapping algorithm in Fig.4.4 can be used to check if changing a channel assignment from one user to another will decrease the sum distortion of all users.

4.2.4 Transmission system model

The transmitter and receiver models are adapted from Chapter 2. LDPC codes are used for FEC. I assume the users in the downlink are synchronized at the transmitter, and hence the interference can be removed by using mutually orthogonal spreading codes (e.g., Walsh-Hadamard codes). I consider a slow fading environment, where the channel remains constant over one transmission interval. I assume the transmitter has perfect CSI at the beginning of the transmission interval. The transmitter selects the average symbol energy (E_s) so that the received SNR is maintained at a constant γ_S for all users. If the required transmit power exceeds a predetermined threshold, I do not transmit to that user in that channel, in accordance with the resource allocation algorithms discussed in Subsection 4.2.3.

From Chapter 2, the received instantaneous SINR of user u_j at the k-th symbol

```
procedure MUD_ALLOC $(\alpha, U_{al}, B_{al}, C_{al}, P_{sc}, P_{Rx}, P_{Tx,\max}, N_{sc,\max}, N_{ss})$
    $U'_{al} \leftarrow U_{al}$
    $B'_{al} \leftarrow B_{al}$
    while $|U'_{al}| > 0$ do    ▷ While set of users to be assigned a channel is non-empty
        if $\sum_{k \in U_{al}} C_{al}[i][k] \geq N_{ss}$ then
            $B'_{al} \leftarrow B'_{al} - \{i\}$    ▷ Remove band if all spreading sequences are assigned
        end if
        $(i, j) \leftarrow \underset{j \in U'_{al}, i \in B'_{al}}{\arg\max} \left\{\alpha[i][j] \mid P_{sc}[i] + \frac{P_{Rx}}{\alpha[i][j]} \leq P_{Tx,\max}\right\}$ ▷ Select best channel & user
        $C_{al}[i][j] \leftarrow C_{al}[i][j] + 1$    ▷ Update channel assignment matrix
        $P_{sc}[i] \leftarrow P_{sc}[i] + \frac{P_{Rx}}{\alpha[i][j]}$    ▷ Update transmit power in selected ($i$-th) band
        if $\sum_{k \in B_{al}} C_{al}[k][j] \geq N_{sc,\max}[j]$ then
            $U'_{al} \leftarrow U'_{al} - \{j\}$    ▷ Remove user if max. no. of channel allocations is met
        end if
        $U'_{al} \leftarrow \left\{j \mid \max_{i \in B_{al}} \left(P_{sc}[i] + \frac{P_{Rx}}{\alpha[i][j]}\right) \leq P_{Tx,\max},\ j \in U'_{al}\right\}$    ▷ Update set of users
    end while
    return $\{C_{al}, P_{sc}\}$
end procedure
```

Figure 4.2: MUD algorithm for user allocation

```
procedure MXD_ALLOC $(\alpha, U_{al}, B_{al}, P_{Rx}, P_{Tx,\max}, N_{ss}, \vartheta)$
    $U''_{al} \leftarrow U_{al}$
    $C_{al} \leftarrow \mathbf{0}_{|U_{al}| \times |B|}$
    $P_{sc} \leftarrow \mathbf{0}_{|B| \times 1}$
    while $|U''_{al}| > 0$ do
        $\{C_{al}, P_{sc}\} \leftarrow$ MUD_ALLOC $(\alpha, U''_{al}, B_{al}, C_{al}, P_{sc}, P_{Rx}, P_{Tx,\max}, 1, N_{ss})$
        Calculate $D_{su}$; the video distortion of users with current channel allocation $C_{al}$.
        $U'_{al} \leftarrow \left\{j \mid \max_{i \in B_{al}} \left(P_{sc}[i] + \frac{P_{Rx}}{\alpha[i][j]}\right) \leq P_{Tx,\max},\ j \in U_{al}\right\}$
        Select $U''_{al} \subseteq U'_{al}$; up to $\vartheta|U_{al}|$ users with largest video distortion ( $D_{su}$)
    end while
    return $C_{al}$
end procedure
```

Figure 4.3: Algorithm ‘MXD’ for user allocation

```
procedure SWAP_ALLOC $(\alpha, U_{al}, B_{al}, C_{al}, P_{sc}, P_{Rx}, P_{Tx,\max}, \max\_it)$
    $iter \leftarrow 0$
    while $iter < \max\_it$ do
        Calculate $D_{su}^{(0)}[j]$; video distortion of $j$ with current channel allocation, $\forall j \in U_{al}$.
        Calculate $D_{su}^{(1)}[j]$; Distortion of $j$ with one additional channel allocation, $\forall j \in U_{al}$.
        for $i \in B_{al}$ do
            for $j \in U_{al}$ do
                $p_{sc} \leftarrow P_{sc}[i] + \frac{P_{Rx}}{\alpha[i][j]} - P_{Tx,max}$
                for $k \in\ U_{al} - \{j\}$ do
                    $c_{sc,l} \leftarrow \left\lceil \frac{p_{sc}\alpha[i][k]}{P_{Rx}} \right\rceil$
                    if $c_{sc,l} \leq C_{al}[i][k]$ then
                        $c_{sc}[k] \leftarrow \sum_{i \in B_{al}} C_{al}[i][k] - c_{sc,l}$
                        Calculate $D_{su}^{(-1)}[k]$; distortion of $k$ with $c_{sc}[k]$ channel allocations.
                        $\Delta D_{su}[i][k][j] \leftarrow (D_{su}^{(1)}[j] + D_{su}^{(-1)}[k]) - (D_{su}^{(0)}[j] + D_{su}^{(0)}[k])$
                    else
                        $\Delta D_{su}[i][k][j] \leftarrow 0$
                    end if
                end for
            end for
        end for
        if $\min \Delta D_{su}[i][j][k] < 0$ then
            $(i', j', k') \leftarrow \underset{j,k \in U_{al}; i \in B_{al}}{\arg\max} \ \Delta D_{su}[i][k][j]$
            $C_{al}[i'][j'] \leftarrow C_{al}[i'][j'] + 1$
            $C_{al}[i'][k'] \leftarrow C_{al}[i'][k'] - \left\lceil \left( \frac{P_{sc}[i]}{P_{Rx}} + \frac{1}{\alpha[i'][j']} - \frac{P_{Tx,max}}{P_{Rx}} \right) \alpha[i'][k'] \right\rceil$
            $P_{sc}[i] \leftarrow P_{sc}[i] + \frac{P_{Rx}}{\alpha[i'][j']} - \left\lceil \left( \frac{P_{sc}[i]}{P_{Rx}} + \frac{1}{\alpha[i'][j']} - \frac{P_{Tx,max}}{P_{Rx}} \right) \alpha[i'][k'] \right\rceil \frac{P_{Rx}}{\alpha[i'][k']}$
        else
            return $C_{al}$
        end if
        $iter \leftarrow iter + 1$
    end while
    return $C_{al}$
end procedure
```

Figure 4.4: Algorithm to swap subcarriers between users to decrease sum distortion

detection in the i-th band is $\gamma_{i,k}^{(u_j)} = \frac{\gamma_S}{\alpha_{J,i,k}^{(u_j)}\bar{\gamma}_{J,i}+1}$, where $\alpha_{J,i,k}^{(u_j)}$ is the gain of the adversary-to-u_j channel, $\bar{\gamma}_{J,i} = \frac{P_{J,i}}{N_0 W}$ and $P_{J,i}$ is the jamming power allocated for the i-th subcarrier. The channel gain $\alpha_{J,i,k}^{(u_j)}$ is exponentially distributed with average $\bar{\alpha}_J^{(u_j)}$. Similar to Chapter 2, to obtain an approximation for the packet error rate, the adversary models the probability of word error with a step function of the SINR:

$$\Pr(\text{packet error}) = \begin{cases} 0, & \text{if } \gamma_{i,k}^{(u_j)} > \gamma_T \\ 1, & \text{if } \gamma_{i,k}^{(u_j)} \leq \gamma_T \end{cases} \tag{4.16}$$

where $\gamma_{i,k}^{(u_j)}$ is the instantaneous SINR at the receiver, and γ_T is a threshold dependent on the alphabet and FEC used. I consider a system using a single alphabet size and LDPC coding rate. Through simulations of word error rates of an ensemble of LDPC rate $\frac{1}{2}$ codes of code length L_p, γ_T is estimated. Therefore, from (4.16), the probability of packet error is:

$$\begin{aligned}\Pr(\text{packet error}) &= \Pr\left(\frac{\gamma_S}{\alpha_{J,i.k}^{(u_j)}\bar{\gamma}_{J,i}+1} < \gamma_T\right) = \frac{1}{\bar{\alpha}_J^{(u_j)}}\int_{\frac{1}{\bar{\gamma}_{J,i}}\left(\frac{\gamma_S}{\gamma_T}-1\right)}^{\infty} e^{-\frac{x}{\bar{\alpha}_J^{(u_j)}}}\,\mathrm{d}x \\ &= e^{-\frac{1}{\bar{\alpha}_J^{(u_j)}\bar{\gamma}_{J,i}}\left(\frac{\gamma_S}{\gamma_T}-1\right)} \end{aligned} \tag{4.17}$$

The expected number of packet errors of user u_j in the i-th band $N_{e,u_j,i}(P_{J,i})$, is

$$N_{e,u_j,i}(P_{J,i}) = N_p \Pr\left(\text{packet error}\right) = N_p e^{-\frac{N_0 W}{\bar{\alpha}_J^{(u_j)} P_{J,i}}\left(\frac{\gamma_S}{\gamma_T}-1\right)} \tag{4.18}$$

where N_p is the number of packets of a single user in a single band per transmission interval.

4.3 Spoofing power optimization

During the sensing interval, the adversary attacks the system by spoofing to reduce the transmission rate available to SUs by reducing the bandwidth available to them. The adversary aims to maximize the following objective function:

$$\sum_{\forall u_j} f_D^{(u_j)}(r_{u_j}, e_{u_j}) = \sum_{\forall u_j} f_D^{(u_j)}\left(\sum_{i\in B(u_j)} r_{u_j,i}, e_{u_j}\right). \tag{4.19}$$

where $B(u_j)$ is the set of bands allocated for u_j and $r_{u_j,i}$ is the data rate of u_j in the i-th band.

The average distortion decreases monotonically with the source rate (r_{u_j}) and increases monotonically with the probability of packet error (e_{u_j}). Therefore, there are two ways to increase distortion by spoofing; by making the SUs decrease the source rate or increase the error rates.

Increasing distortion by decreasing the source rate: Successful spoofing can directly decrease the source rate by limiting SU access to vacant channels. To maximize the objective function in (4.19) by reducing the source rate, the adversary needs to minimize $\sum_{i\in B(u_j)} r_{u_j,i}$. Note that $B(u_j)$ and $r_{u_j,i}$ depend on the resource allocation algorithms, channel gains, video properties and the set of bands detected as vacant (B_{al}). Out of these parameters, the adversary can only influence B_{al}. Therefore, I use minimizing $|B_{al}|$ as the objective of the adversary.

Increasing distortion by increasing the probability of packet error: The probability of packet error e_{u_j} is not directly affected by spoofing, but is increased by jamming. But the effectiveness of jamming increases when the number of transmitting bands is decreased, so minimizing $|B_{al}|$ will also increase e_{u_j}, thus increasing the distortion.

Therefore, maximizing the distortion in (4.19) through spoofing is equivalent to minimizing $|B_{al}|$. Conditioned on $B - B_{pu}$, the average number of bands detected as allowed by the CH is $\sum_{i\in B-B_{pu}}(1 - p_{fd}(P_{S,i}))$, where $p_{fd}(P_{S,i})$ is the probability of false detection of the i-th band as a function of the spoofing power ($P_{S,i}$) in the i-th band, given that the i-th band is vacant [17]. Hence, the objective of the adversary is maximizing $\sum_{i\in B-B_{pu}} p_{fd}(P_{S,i})$.

At the start of the sensing interval, the adversary does not know which bands are vacant. From the adversary's perspective, every band has an equal probability of being vacant. Hence, the objective of the adversary is to maximize $\sum_{i=1}^{N_T} p_{fd}(P_{S,i})$, under the constraint $\sum_{i=1}^{N_T} P_{S,i} = P_S$, where $P_{S,i}$ is the spoofing power allocated for the i-th band and P_S is the total spoofing power available. This N_T variable optimization can be reduced to two dimensions, using the behavior of $p_{fd}(P_{S,i})$. I use the theorem in Appendix C, to simplify this optimization problem, using the properties **P0** (bounded above) and **P3** (non decreasing and twice differentiable). The adversary's estimate of $p_{fd}(P_{S,i})$ can be obtained from (4.3),

$$p_{fd}(P_{S,i}) = 1 - \left(1 - \frac{1}{\bar{\alpha}_J}\int_0^{\infty} Q\left(\frac{K}{\frac{P_{S,i}}{W}y + N_0} - \sqrt{T_0 W}\right) e^{-\frac{y}{\bar{\alpha}_J}}\,\mathrm{d}y\right)^{|U_{al}|} \tag{4.20}$$

where I use $\bar{\alpha}_J$ as an approximation for $\bar{\alpha}_J^{(u_j)}$. Because $p_{fd}(P_{S,i})$ is a probability, I know that $p_{fd}(P_{S,i}) \leq 1$, and hence bounded above. Therefore, condition **P0** is satisfied. Taking the derivative with respect to $P_{S,i}$:

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}P_{S,i}}\Big(p_{fd}(P_{S,i})\Big) &= -|U_{al}|\left(1 - \frac{1}{\bar{\alpha}_J}\int_0^{\infty} Q\left(\frac{K}{\frac{P_{S,i}}{W}y + N_0} - \sqrt{T_0 W}\right) e^{-\frac{y}{\bar{\alpha}_J}}\,\mathrm{d}y\right)^{|U_{al}|-1} \\ &\times\left(-\frac{1}{\bar{\alpha}_J}\int_0^{\infty} \frac{\mathrm{d}Q\left(\frac{K}{\frac{P_{S,i}}{W}y+N_0} - \sqrt{T_0 W}\right)}{\mathrm{d}\left(\frac{K}{\frac{P_{S,i}}{W}y+N_0} - \sqrt{T_0 W}\right)} \times \frac{\mathrm{d}}{\mathrm{d}P_{S,i}}\left(\frac{K}{\frac{P_{S,i}}{W}y + N_0} - \sqrt{T_0 W}\right) e^{-\frac{y}{\bar{\alpha}_J}}\,\mathrm{d}y\right) > 0\end{aligned} \tag{4.21}$$

From this, I see that $p_{fd}(P_{S,i})$ has the property **P3**. So, I use Theorem 2 in Appendix C to maximize $\sum_{i=1}^{N_T} p_{fd}(P_{S,i})$.

4.4 Desynchronizing power optimization

After the sensing interval, the CH determines which bands are allowed for SUs, and broadcasts a spreading sequence for code acquisition during the T_1 interval. The adversary can transmit an interference signal to disrupt the code acquisition process. If the code acquisition fails for an SU, that SU will not be able to estimate the channel gains and will not be assigned subcarriers. Therefore, the video distortion of user u_j is $f_D^{(u_j)}(r_{u_j}, e_{u_j})(1 - p_{cqf}^{(u_j)}) + f_D^{(u_j)}(0,0)p_{cqf}^{(u_j)} = f_D^{(u_j)}(r_{u_j}, e_{u_j}) + p_{cqf}^{(u_j)}(f_D^{(u_j)}(0,0) - f_D^{(u_j)}(r_{u_j}, e_{u_j}))$, where $p_{cqf}^{(u_j)}$ is the probability of code acquisition failure of user u_j. Because $f_D^{(u_j)}(r_{u_j}, e_{u_j}) < f_D^{(u_j)}(0,0)$, in order to maximize the distortion of user u_j through desynchronizing attacks, the adversary must maximize $p_{cqf}^{(u_j)}$.

Each SU tries to acquire the code in all the allowed bands, on which the CH is broadcasting. The acquisition in each band is followed by code tracking, and I assume that all incorrect phases will be rejected in the tracking mode. Hence, if the correct code phase is acquired in any band, the SU achieves code acquisition. Therefore, the probability of code acquisition failure is

$$p_{cqf}^{(u_j)} = \prod_{i \in B_{al}} p_{cqf}(P_{ds,i}) \tag{4.22}$$

where $p_{cqf}(P_{ds,i})$ is the probability of code acquisition failure as a function of desynchronizing power. The adversary aims to maximize $p_{cqf}^{(u_j)}$, which is equivalent to maximizing $\log\left(p_{cqf}^{(u_j)}\right) = \sum\limits_{i \in B_{al}} \log\big(p_{cqf}(P_{ds,i})\big)$. As the adversary is not aware of B_{al}, I modify the objective function to $\sum_{i=1}^{N_T} \log\big(p_{cqf}(P_{ds,i})\big)$. I use the lower bound $p_{cqf,lb}(P_{ds,i})$ derived in (4.15) in place of $p_{cqf}(P_{ds,i})$, and the objective function to maximize is $\sum_{i=1}^{N_T} \log\big(p_{cqf,lb}(P_{ds,i})\big)$. Taking the derivative of $p_{cqf,lb}(P_{ds,i})$ from (4.14), with respect to $P_{ds,i}$, I get

$$\frac{\mathrm{d}}{\mathrm{d}P_{ds,i}}\left(p_{cqf,lb}(P_{ds,i})\right) = \int_0^\infty \frac{\zeta_d^2 l_{acq} E_c N_c \bar{\alpha}_S^{(u_j)} \alpha_{J,i}^{(u_j)} e^{-\frac{\alpha_{J,i}^{(u_j)}}{\bar{\alpha}_J^{(u_j)}}}}{\left(\zeta_d^2 l_{acq} E_c N_c \bar{\alpha}_S^{(u_j)} + 2(\alpha_{J,i}^{(u_j)} \frac{P_{ds,i}}{W} + N_0)\right)^2 W \bar{\alpha}_J^{(u_j)}} \, \mathrm{d}\alpha_{J,i}^{(u_j)} > 0 \tag{4.23}$$

This shows that $p_{cqf,lb}(P_{ds,i})$ is monotonically increasing with $P_{ds,i}$, and property **P3** is satisfied. Therefore, I also know that

$$p_{cqf,lb}(P_{ds,i}) \leq \lim_{P_{ds,i} \to \infty} p_{cqf,lb}(P_{ds,i}) = \int_0^\infty \frac{1}{2} \times \frac{1}{\bar{\alpha}_J^{(u_j)}} e^{-\frac{\alpha_{J,i}^{(u_j)}}{\bar{\alpha}_J^{(u_j)}}} \, \mathrm{d}\alpha_{J,i}^{(u_j)} = \frac{1}{2} \tag{4.24}$$

This shows that the function is bounded above and has the property **P0**. Further, taking the derivative of (4.23) with respect to $P_{ds,i}$, I can also show that $\frac{\mathrm{d}^2}{\mathrm{d}P_{ds,i}^2}\left(p_{cqf,lb}(P_{ds,i})\right) < 0$. Because the log function is monotonically increasing, $\log\big(p_{cqf,lb}(P_{ds,i})\big)$ also has the properties **P0** and **P3**. Therefore, I can use the proposed optimization approach to maximize $\sum_{i=1}^{N_T} \log\big(p_{cqf,lb}(P_{ds,i})\big)$. Because $p_{cqf,lb}(P_{ds,i}) \geq 0$ and $\frac{\mathrm{d}^2}{\mathrm{d}P_{ds,i}^2}\Big(p_{cqf,lb}(P_{ds,i})\Big) < 0$, the second derivative $\frac{\mathrm{d}^2}{\mathrm{d}P_{ds,i}^2}\Big(\log\big(p_{cqf,lb}(P_{ds,i})\big)\Big) < 0$. Therefore, from (C.1), the optimal power allocation is equal power allocation at all desynchronizing power values.

4.5 Jamming power optimization

The objective of the adversary is to maximize $\sum_{\forall u_j} f_D^{(u_j)}(r_{u_j}, e_{u_j})$, by increasing the probability of packet error e_{u_j}. I know that $f_D^{(u_j)}(r_{u_j}, e_{u_j})$ is an increasing function of e_{u_j}, when r_{u_j} remains constant. Let $B(u_j)$ be the set of subcarriers allocated for user u_j. I assume that the adversary senses and detects the bands used for transmission before jamming, and hence knows $B_{al} \cup B_{pu}$. To simplify the notation, I number the bands such that $B_{al} \cup B_{pu} = \{1, 2, \ldots, N_{Tx}\}$.

4.5.1 Lightly loaded system

I first consider a lightly loaded system, in which each SU will generally be assigned many subcarriers; i.e. $|B(u_j)| \gg 1$. During one transmission interval, the expected number of packet errors of u_j, $N_{e,u_j} = \sum_{i \in B(u_j)} N_{e,u_j,i}(P_{J,i})$. However, without knowledge of $B(u_j)$, the adversary assumes that each band has an equal probability $\frac{|B(u_j)|}{N_{Tx}}$ of being assigned to u_j. Under this assumption, the expected number of packet errors of u_j during T_1, estimated by the adversary, is:

$$N_{e,u_j} = \sum_{i=1}^{N_{Tx}} \left\{ \begin{array}{l} \text{Probability} \\ \text{band} \quad i \quad \text{is} \\ \text{assigned to } u_j \end{array} \right\} \times \left\{ \begin{array}{l} \text{Expected number of packet} \\ \text{errors of } u_j \text{ in } i\text{-th band if} \\ \text{assigned} \end{array} \right\} = \sum_{i=1}^{N_{Tx}} \frac{|B(u_j)|}{N_{Tx}} N_{e,u_j,i}(P_{J,i}) \tag{4.25}$$

Using the result in (4.25), I can calculate the probability of packet error e_{u_j} as follows:

$$\begin{aligned} e_{u_j} &= \frac{\text{Expected number of packet errors}}{\text{Total transmitted packets}} = \frac{\sum_{i=1}^{N_{Tx}} \left(\frac{|B(u_j)|}{N_{Tx}}\right) N_{e,u_j,i}(P_{J,i})}{|B_{u_j}| N_p} \\ &= \frac{\sum_{i=1}^{N_{Tx}} N_{e,u_j,i}(P_{J,i})}{N_{Tx} N_p} \end{aligned} \tag{4.26}$$

I can write the objective function to be maximized from (4.19) as

$$\sum_{\forall u_j} f_D^{(u_j)}\left(r_{u_j}, \frac{\sum_{i=1}^{N_{Tx}} N_{e,u_j,i}(P_{J,i})}{N_{Tx}N_p}\right). \tag{4.27}$$

For any given source rate r_{u_j}, the distortion of a received video increases with the packet error rate. Further, r_{u_j} is affected only by spoofing power, and is unaffected by jamming. Therefore, to maximize $f_D\left(r_{u_j}, \frac{\sum_{i=1}^{N_{Tx}} N_{e,u_j,i}(P_{J,i})}{N_{Tx}N_p}\right)$, the adversary aims to maximize $\sum_{i=1}^{N_{Tx}} N_{e,u_j,i}(P_{J,i})$, under the constraints $\sum_{i=1}^{N_{Tx}} P_{J,i} = P_T$ and $P_{J,i} \geq 0$.

Using (4.18), I can write the approximation of the expected number of packet errors calculated by the adversary, $N_{e,i}(P_{J,i})$ as follows:

$$N_{e,i}(P_{J,i}) = N_p e^{-\frac{N_0 W}{\bar{\alpha}_J P_{J,i}}\left(\frac{\gamma_S}{\gamma_T}-1\right)} \tag{4.28}$$

where I use $\bar{\alpha}_J$ as an approximation for $\bar{\alpha}_J^{(u_j)}$. I use the optimization approach in Appendix C, as $N_{e,i}(P_{J,i})$ satisfies properties **P0** and **P3**.

4.5.2 Heavily loaded system

In this scenario, I assume that, due to heavy PU activity, SUs are often assigned only a single subcarrier; i.e. $|B(u_j)| = 1$. Suppose user u_j is assigned only the i-th band. Using (4.16), I write the video distortion as: $f_D^{(u_j)}(r_{u_j}, e_{u_j}) = \begin{cases} f_D^{(u_j)}(r_{u_j}, 0), & \text{if } \gamma_{i,k}^{(u_j)} > \gamma_T \\ f_D^{(u_j)}(r_{u_j}, 1), & \text{if } \gamma_{i,k}^{(u_j)} \leq \gamma_T \end{cases}.$

The expected video distortion for u_j is

$$\begin{aligned} \mathbb{E}\left[f_D^{(u_j)}(r_{u_j}, e_{u_j})\right] &= f_D^{(u_j)}(r_{u_j}, 0)\Pr(\gamma_{i,k}^{(u_j)} > \gamma_T) + f_D^{(u_j)}(r_{u_j}, 1)\Pr(\gamma_{i,k}^{(u_j)} \leq \gamma_T) \\ &\approx f_D^{(u_j)}(r_{u_j}, 0) + f_D^{(u_j)}(r_{u_j}, 1)\Pr(\gamma_{i,k}^{(u_j)} \leq \gamma_T) \\ &= f_D^{(u_j)}(r_{u_j}, 0) + f_D^{(u_j)}(r_{u_j}, 1) e^{-\frac{1}{\bar{\alpha}_J^{(u_j)}\bar{\gamma}_{J,i}}\left(\frac{\gamma_S}{\gamma_T}-1\right)} \qquad \text{(from (4.17))} \end{aligned} \tag{4.29}$$

Let $U(i)$ be the set of users in the i-th band. The objective function to maximize is

$$\sum_{\forall u_j} \mathbb{E}\left[f_D^{(u_j)}(r_{u_j}, e_{u_j})\right] = \sum_{i=1}^{N_{Tx}} \sum_{\forall u_j \in U(i)} \left(f_D^{(u_j)}(r_{u_j}, 0) + f_D^{(u_j)}(r_{u_j}, 1) e^{-\frac{1}{\bar{\alpha}_J^{(u_j)} \bar{\gamma}_{J,i}} \left(\frac{\gamma_S}{\gamma_T} - 1\right)} \right) \tag{4.30}$$

The terms $f_D^{(u_j)}(r_{u_j}, 1)$ and $f_D^{(u_j)}(r_{u_j}, 0)$ depend on the properties of the video of user u_j and the source rate r_{u_j}. Different jamming power allocations do not affect those terms, but do affect error rate. Hence, the objective to maximize is $\sum_{i=1}^{N_{Tx}} \sum_{\forall u_j \in U(i)} f_D^{(u_j)}(r_{u_j}, 1) e^{-\frac{1}{\bar{\alpha}_J^{(u_j)} \bar{\gamma}_{J,i}} \left(\frac{\gamma_S}{\gamma_T} - 1\right)}$.

The adversary does not know the instantaneous channel assignment, and assumes each user has a probability $\frac{1}{N_{Tx}}$ of being assigned the i-th band. Hence, taking the expectation over all channel assignments, the function to maximize can be rearranged as $\sum_{\forall u_j} \frac{f_D^{(u_j)}(r_{u_j},1)}{N_{Tx}} \sum_{i=1}^{N_{Tx}} e^{-\frac{1}{\bar{\alpha}_J^{(u_j)} \bar{\gamma}_{J,i}} \left(\frac{\gamma_S}{\gamma_T} - 1\right)}$. Now, since only $e^{-\frac{1}{\bar{\alpha}_J^{(u_j)} \bar{\gamma}_{J,i}} \left(\frac{\gamma_S}{\gamma_T} - 1\right)}$ can be changed by jamming, the function reduces to maximizing $\sum_{i=1}^{N_{Tx}} e^{-\frac{1}{\bar{\alpha}_J \bar{\gamma}_{J,i}} \left(\frac{\gamma_S}{\gamma_T} - 1\right)}$, where $\bar{\alpha}_J$ approximates $\bar{\alpha}_J^{(u_j)}$. Since the function satisfies the properties **P0** and **P3**, I use Appendix C to optimally allocate jamming power.

4.6 Energy optimization among modes of attack

Let E_{ad} be the total energy available for the adversary during a $T_0 + T_1 + T_2$ interval. Let θ_{sp} be the fraction of energy allocated for spoofing and let θ_{ds} be the fraction of energy allocated for desynchronizing attacks. I have $E_{sp} = \theta_{sp} E_{ad}$, $E_{ds} = \theta_{ds} E_{ad}$, and $E_{jm} = (1 - \theta_{sp} - \theta_{ds}) E_{ad}$.

The objective of the adversary is to find the parameters $(\theta_{sp}, \theta_{ds})$ that maximizes $\sum_{\forall u_j} f_D^{(u_j)}(r_{u_j}, e_{u_j})$. In the separate optimizations of spoofing, desynchronizing, and jamming attacks, I was able to derive objective functions to replace $f_D^{(u_j)}\left(r_{u_j}, e_{u_j}\right)$, using the knowledge that $f_D^{(u_j)}(r_{u_j}, e_{u_j})$ is a monotonically decreasing function of r_{u_j} and a monotonically increasing function of e_{u_j}, when the other parameters are kept constant. But I now need knowledge of $f_D^{(u_j)}$ to optimize energy allocation among the attacking methods. Because $f_D^{(u_j)}$ depends on video properties and encoding parameters that are not known by the adversary, I cannot calculate $f_D^{(u_j)}$ at the adversary. Therefore, I use throughput as an alternative target for this section.

The minimum throughput (worst case throughput) under spoofing, jamming and desynchronizing attacks, $\Gamma(\theta_{sp}, \theta_{ds})$, as a function of θ_{sp} and θ_{ds}, can be written as

$$\Gamma(\theta_{sp},\theta_{ds}) = L_p\left(N_p\tilde{B}_{su}(\theta_{sp}) - \tilde{N}_{er}\left(1-\theta_{sp}-\theta_{ds}, \tilde{B}_{su}(\theta_{sp}), \overline{|B_{pu}|}\right)\right)\left(1-\tilde{p}_{cqf}\left(\theta_{ds}, \tilde{B}_{su}(\theta_{sp})\right)\right) \tag{4.31}$$

where $\tilde{N}_{er}\left(\theta_{jm}, \tilde{B}_{su}(\theta_{sp}), \overline{|B_{pu}|}\right)$ is the expected number of packet errors under optimized jamming, $\tilde{p}_{cqf}\left(\theta_{ds}, \tilde{B}_{su}(\theta_{sp})\right)$ is the probability of code acquisition failure, and $\tilde{B}_{su}(\theta_{sp})$ is the expected number of allowed bands under optimized spoofing.

$$\tilde{B}_{su}(\theta_{sp}) \triangleq \min_{\sum_{i=1}^{N_T} P_{s,i} \leq \frac{\theta_{sp}E_{ad}}{T_0}} E\left[|B_{al}|\right] = \frac{(N_T - \overline{|B_{pu}|})}{N_T}\left(N_T - F\left(p_{fd}, \frac{\theta_{sp}E_{ad}}{T_0}, N_T\right)\right) \tag{4.32}$$

where F is defined in (C.15).

$$\begin{aligned} \tilde{N}_{er}\left(\theta_{jm}, \tilde{B}_{su}(\theta_{sp}), \overline{|B_{pu}|}\right) &\triangleq \max_{\sum_{i=1}^{\tilde{B}_{su}(\theta_{sp})+\overline{|B_{pu}|}} P_{J,i} \leq \frac{\theta_{jm}E_{ad}}{T_2}} E\left[\sum_{i\in B_{al}} N_{e,i}^{(u_j)}\right] \\ &= \frac{\tilde{B}_{su}(\theta_{sp})}{\tilde{B}_{su}(\theta_{sp}) + \overline{|B_{pu}|}} F\left(N_{e,i}, \frac{\theta_{jm}E_{ad}}{T_2}, \tilde{B}_{su}(\theta_{sp}) + \overline{|B_{pu}|}\right) \end{aligned} \tag{4.33}$$

where θ_{jm} is the fraction of energy allocated for jamming. Substituting the desynchronizing power $P_{ds,i} = \frac{\theta_{ds}E_{ad}}{T_1 N_T}$ in (4.22), I have

$$\tilde{p}_{cqf}\left(\theta_{ds}, \tilde{B}_{su}(\theta_{sp})\right) = \prod_{i=1}^{\tilde{B}_{su}(\theta_{sp})} p_{cqf,lb}^{(u_j)}\left(\frac{\theta_{ds}E_{ad}}{T_1 N_T}\right). \tag{4.34}$$

Using (4.31), I find the optimal energy allocation ratios $\left(\theta_{sp}^*, \theta_{ds}^*\right) = \underset{\theta_{sp},\theta_{ds}\in[0,1]}{\arg\min}\ \Gamma(\theta_{sp}, \theta_{ds})$ numerically, from a grid search.

4.7 Simulation results

I consider a cluster-based SU system, sharing N_T DS-CDMA subcarriers with PUs. In the simulations, in each sensing, acquisition and transmission interval, the PUs occupy $|B_{pu}| = \min(N_{B,pu}, N_T)$ bands at random, where $N_{B,pu}$ is a Poisson r.v. with mean parameter $\bar{N}_{pu}$. I select $\bar{\alpha}_S = \bar{\alpha}_J = 1, T_0 = 4T_s, T_1 = 16T_s$ and $T_2 = 2048T_s$, where T_s is the symbol time. The number of chips per symbol during a transmission interval (N_c) is 64, $N_c^{acq} = 256$ and $l_{acq} = 4$. I use Walsh-Hadamard codes as spreading sequences, a rate $\frac{1}{2}$ LDPC code with code block length 2048 bits, and QPSK modulation. The target received SNR maintained (γ_S) is 5 dB.

Each user transmits the 'soccer' video sequence of 300 frames with 4CIF resolution (704×576) at 30 frames per second. The source video is compressed by the baseline profile of H.264/AVC reference software JM 11.0 [7]. The GOP structure is IPP with 15 frames per GOP. Each user starts at a random frame of the video, and the resource allocation decision is done at the start of each GOP. The video performance is evaluated using PSNR. $\triangleq 10 \log_{10} \frac{255^2}{\mathbb{E}[\text{MSE}]}$.

When there is no knowledge of the system other than its operating frequency range, the adversary can perform equal power attacks across the total bandwidth. I use this equal power spoofing and jamming strategy as a our baseline. For desynchronizing attacks, the optimal strategy is an equal power attack, as shown in Section 4.4.

Spoofing attacks

Figure 4.5 shows the video PSNR, averaged over users, against JSR, for the resource allocation algorithms of Subsection 4.2.3. I plot average PSNR under equal power spoofing (dashed curves) and optimized worst case spoofing (solid curves).

The MUD algorithm, which only uses physical layer information for channel allocation, has the worst performance, as it fails to account for differences in the video properties. MUD+swap has notable gains over MUD, as the swapping enables more subcarriers to be assigned to users with higher motion video. The MXD algorithms perform the best under the simulated parameters.

Switching from equal power spoofing to optimized spoofing reduces the average PSNR by 3-4 dB in the MUD algorithms when operating in the 0-6 dB JSR range.

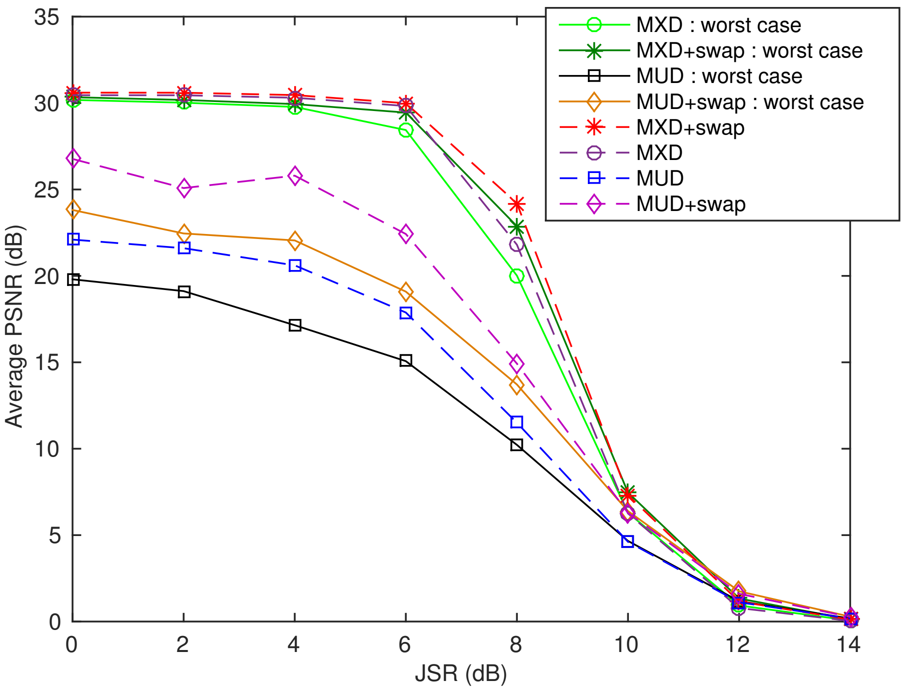


Figure 4.5: Average PSNR under spoofing attacks ($N_T = 64$, $\Omega_{su} = 4$, $\bar{N}_{pu} = 16$)

However, the MXD based algorithms are not notably affected by optimized spoofing in the same JSR range. It appears that MXD algorithms are more robust against a small bandwidth loss than are MUD algorithms. In MXD, as subcarriers are allocated to the users with maximum distortion first, a subcarrier loss means rate loss for a lower distortion user. But, in MUD, subcarrier loss could hit a high distortion user. Thus, optimizing spoofing at low JSR has a higher impact on MUD.

Desynchronizing attacks

Figure 4.6(a) shows the performance under desynchronizing attacks. There is a steep reduction in PSNR in the JSR range 30-45 dB, due to successful desynchronizing.

Jamming attacks

Figure 4.6(b) shows the performance of the system under jamming. Solid curves correspond to optimized jamming and dashed curves represent equal power jamming. The system is unaffected by equal power jamming up to about 5 dB JSR. However, the reduction in PSNR in the solid curves in the -5 to 5 dB region shows that optimized jamming affects the system at a lower JSR compared to equal power jamming. At JSR = 5 dB, the average PSNR under MXD algorithms is about 7 dB lower under optimized jamming than under equal power jamming. The difference between MXD and MUD+swap diminishes as JSR increases. At high JSR, the performance depends less on source rate, which is a result of the resource allocation algorithm, and is influenced more by packet error rate, which affects all transmissions equally.

Optimal energy allocation among attacking methods

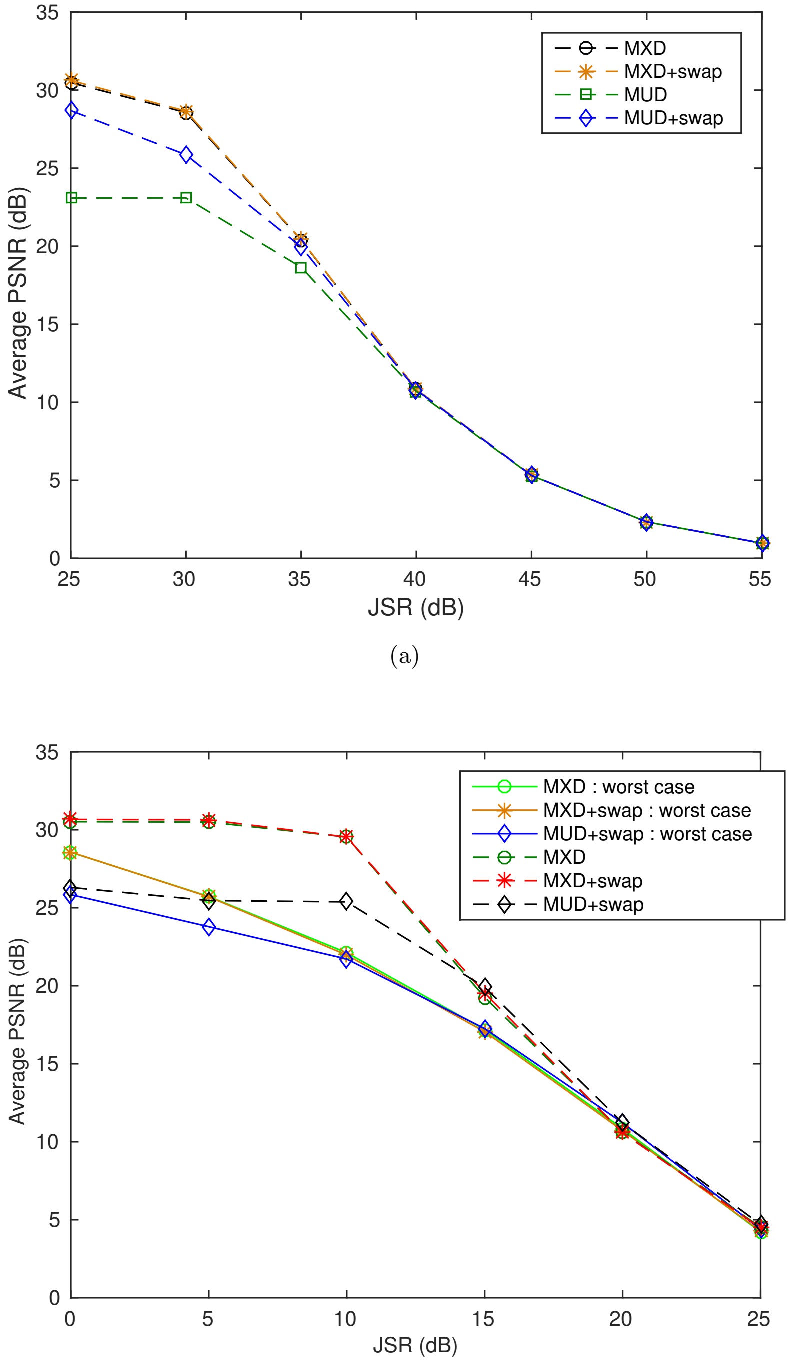
In Figure 4.7(a), I plot the optimal percentage of energy allocation among the three methods of attack. The spoofing only attack is optimal at low JSR. As I use a strong FEC code, at low JSR, jamming attacks have a low probability of success. As seen in Figure 4.6(a), successful desynchronizing attacks require JSR to be beyond 30 dB. Therefore, at low JSR, spoofing only is optimal.

As JSR increases, the optimal energy allocation involves both spoofing and jamming. At high JSR, limiting the available bandwidth by spoofing, and attacking the resulting smaller number of available subcarriers by jamming, appears to be the best strategy. Even at high JSR, desynchronizing is not used, because the other two methods of attack are more effective.

In Figure 4.7(b), I plot the optimal energy allocation for a lightly loaded system with $N_T = 256$, $\bar{N}_{pu} = 32$ and $\Omega_{su} = 4$. For this system, at low JSR, the optimal strategy is desynchronizing. If the system is lightly loaded, the small reduction of bandwidth due to spoofing at low JSR is unlikely to cause a notable performance degradation. Additionally, the probability of jamming success at low JSR is low. As the JSR increases, spoofing becomes more effective, and as the JSR increases beyond 20 dB, optimal energy allocation includes jamming.

4.8 Conclusion

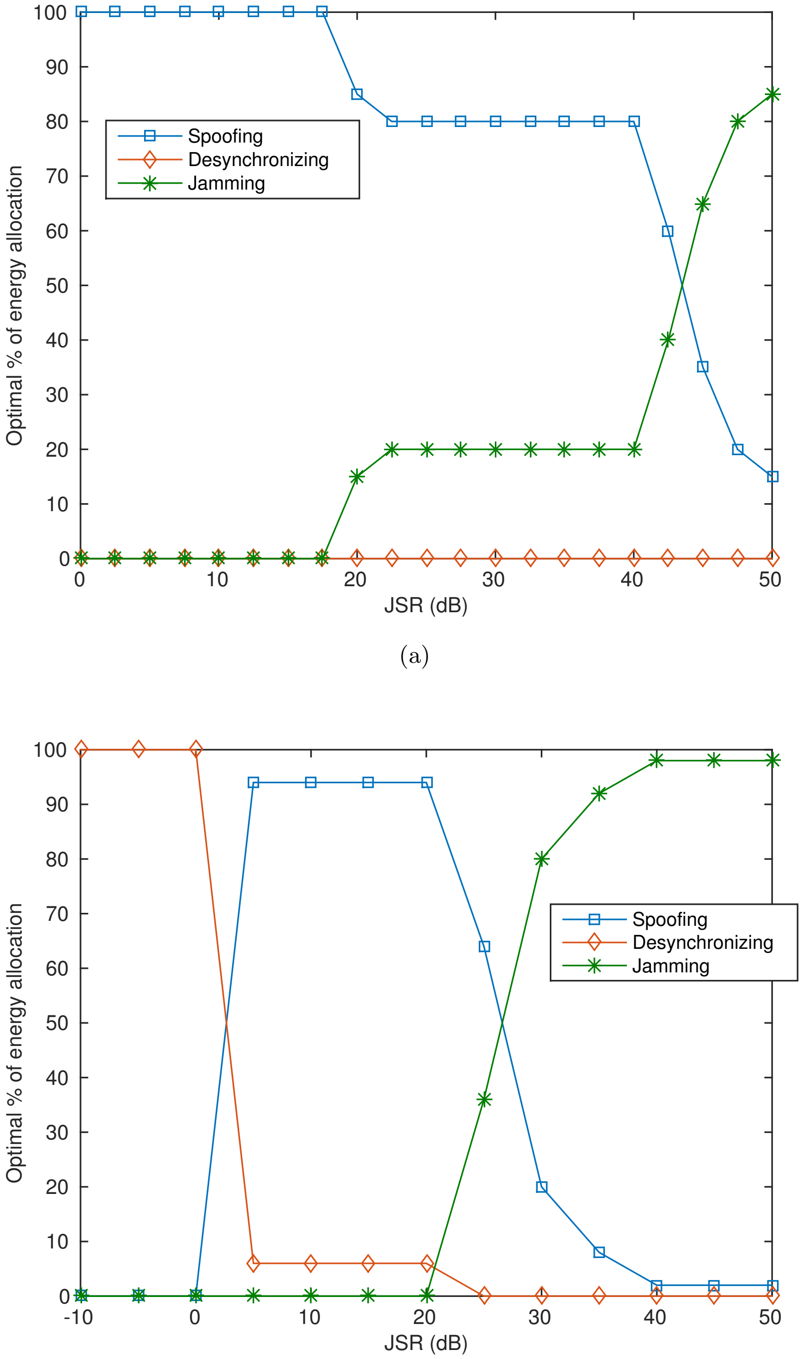
In this chapter, I analyzed the optimal spoofing, desynchronizing and jamming power allocations across subcarriers, in a Rayleigh fading channel, with an optimization



(a)

(b)

Figure 4.6: Average PSNR vs JSR ($N_T = 64$, $\Omega_{su} = 4$, $\bar{N}_{pu} = 16$): (a) under desynchronizing (b) under jamming.



(a)

(b)

Figure 4.7: Optimal energy allocation among the methods of attack: (a) Heavily loaded system ($N_T = 128$, $\Omega_{su} = 4$, $\bar{N}_{pu} = 64$). (b) Lightly loaded system ($N_T = 256$, $\Omega_{su} = 4$, $\bar{N}_{pu} = 32$).

approach which enables a simplified calculation of the threshold JSRs that determine the optimal power allocation. It is noted that at low JSRs, optimizing spoofing and jamming gives the adversary a notable advantage. I evaluated the performance of two types of resource allocation algorithms, and observed that the MXD algorithm offers superior performance. I learned that spoofing has the most noticeable impact on the received video distortion at low and medium JSR, with the exception of lightly loaded systems at low JSR, for which desynchronizing attacks cause the most increase in video distortion. Jamming is effective at high JSR.

Chapter 4, in part, is a reprint of material as it may appear in M. Soysa, P. Cosman, and L. Milstein, "Disruptive attacks on video tactical cognitive radio downlinks," submitted to *IEEE Transactions on Communications*. The dissertation author was the primary author of this paper.

Chapter 5

Disruptive Attacks on Video Tactical Cognitive Radio Uplinks

5.1 Introduction

In this chapter, I examine the performance of a cognitive radio system with users transmitting video on the uplink, and investigate spoofing, desynchronizing and jamming attacks. In the downlink analysis of Chapter 4, multiple access interference (MAI) was not an issue, because orthogonal spreading sequences were used. In this chapter, I propose cross-layer resource allocation algorithms that account for MAI on the uplink. I also investigate desynchronizing and jamming attacks on the uplink, accounting for MAI. I examine the worst-case desynchronizing attack on the uplink code acquisition, and calculate the optimal energy allocation among four modes of attack; spoofing, uplink and downlink desynchronizing, and jamming.

In Section 5.2, I present the system model, and derive performance metrics as functions of spoofing, desynchronizing or jamming power. Sections 5.3 and 5.4 discuss the optimization of desynchronizing and jamming, respectively. In Section 5.5, I discuss the optimal energy allocation among the different modes of attack. Section 5.6 contains system simulations, and Section 5.7 presents the conclusions.

5.2 System model

In this section I discuss the system model. There are four main subcomponents of the system; sensing, code acquisition, resource allocation and transmission, as described in Section 4.2. I use the sensing system model described in Subsection 4.2.1, and in Subsection 5.2.1 the code acquisition subsystem on the uplink is discussed. In Subsection 5.2.2, I describe the resource allocation methods. The transmission and receiver block are detailed in Subsection 5.2.3.

Similar to the system in Chapter 4, all SUs perform spectrum sensing, and detect which bands are occupied. This information is sent to the CH at the end of the sensing interval (T_0). In the system model of this chapter, we consider both downlink and uplink code acquisition, unlike in Chapter 4, where only the downlink code acquisition needed to be investigated. The CH broadcasts a known spreading sequence in all allowed bands during the first part of the code acquisition interval ($T_{1,d}$), which is used by the SUs for code acquisition and channel estimation. The SUs that performed code acquisition successfully transmit a pre-assigned sequence (different for each SU) in a subset of allowed bands, during the second part of the code acquisition interval ($T_{1,u}$). This is used for the CH to perform code acquisition. The estimated CSI and the rate-distortion curve of each SU is communicated to the CH following that. This information is used by the CH for channel allocation among the SUs. The SUs then communicate over a duration of T_2 in the allocated bands.

5.2.1 Code acquisition block analysis

The code acquisition at SUs was presented in Subsection 4.2.2. SUs that successfully perform code acquisition estimate the channel, and then start transmission to communicate the CSI. I now look at code acquisition by the CH. It uses the same receiver model from Chapter 4, shown in Fig.4.1, for code acquisition. The transmitted signal by u_j in the i-th band is

$$x_i^{(u_j)}(t) = \left\{ \sqrt{2E_c^{(u_j)}} \sum_{n=0}^{\frac{T_{1,u}}{T_c}-1} c_n^{(u_j)} g(t - nT_c) \cos(\omega_c t) \right\} \tag{5.1}$$

The received signal at the CH can be written as

$$y(t) = \sum_{u_j \in U(i)} \sqrt{2\alpha_{S,i}^{(u_j)} E_c^{(u_j)}} \sum_{n=0}^{\frac{T_{1,u}}{T_c}-1} c_n^{(u_j)} g(t - t_d^{(u_j)} - nT_c) \cos\big(\omega_c(t - t_d^{(u_j)}) - \phi_{S,i}^{(u_j)}\big)$$
$$+ \sqrt{\alpha_{J,i}^{(ch)}} n_{J,i}(t) + n_{w,i}(t) \tag{5.2}$$

where $U(i)$ is the set of users sharing the i-th band, and $\alpha_{S,i}^{(u_j)}$ and $\phi_{S,i}^{(u_j)}$ are the power gain and phase components of the response of the channel from user u_j-to-CH in the i-th band. The gain of the jammer-to-CH channel is $\alpha_{J,i}^{(ch)}$. I assume the channel gains $\alpha_{S,i}^{(u_j)}$ and $\alpha_{J,i}^{(ch)}$ are mutually independent. The time delay in user u_j is denoted by $t_d^{(u_j)}$. The background noise $n_{w,i}(t)$ is AWGN with PSD $\frac{N_0}{2}$ and $\sqrt{\alpha_{J,i}^{(ch)}} n_{J,i}(t)$ is the received jamming signal. The chip energy $E_c^{(u_j)}$ is chosen so that $\alpha_{S,i}^{(u_j)} E_c^{(u_j)} = \tilde{E}_{c,Rx}$, where $\tilde{E}_{c,Rx}$ is the target received chip energy at the CH.[1]

Following the same approach as in Subsection 4.2.2, I can write

$$z_{k,I} = \frac{1}{\sqrt{N_c^{acq}}} \sum_{n=l_1}^{l_1 + l_{acq} N_c^{acq} - 1} c_n^{(k)} \int_{-\infty}^{\infty} g(\tau - nT_c)\sqrt{2}\cos(\omega_c \tau + \phi_u') y(\tau)\, \mathrm{d}\tau$$
$$= s_{k,I} + n_{u,k,I} + n_{w,k,I} + n_{J,k,I} \tag{5.3}$$

where $s_{k,I}$, $n_{u,k,I}$, $n_{w,k,I}$ and $n_{J,k,I}$ are the signal, multiple access interference, background noise, and jamming components. In Subsection 4.2.2, it was shown that $n_{w,k,I} \sim \mathcal{N}(0, \frac{l_{acq} N_0}{2})$ and $n_{J,k,I} \sim \mathcal{N}(0, \frac{l_{acq} \alpha_{J,i}^{(ch)} \eta_{J,i}}{2})$, when conditioned on $\alpha_{J,i}^{(ch)}$. I assume the multiple access interference can be approximated by a Gaussian r.v., and I can show that $n_{u,k,I} \sim \mathcal{N}\left(0, \frac{l_{acq}\tilde{E}_{c,Rx}}{2}\left(1 - \frac{\beta}{4}\right)(|U(i)| - 1)\right)$, using the results from [33] and [34].

Let k^* denote the correct phase. From Subsection 4.2.2,

$$s_{k^*,I} = \zeta_d l_{acq} \sqrt{\tilde{E}_{c,Rx} N_c^{acq}} \cos\big(\omega_c t_d + \phi_{S,i}^{(u_j)} + \phi_u'\big). \tag{5.4}$$

Conditioned on $(\omega_c t_d + \phi_{S,i}^{(u_j)} + \phi_u')$ and α_J, $z_{k^*,I} \sim \mathcal{N}(\mu \cos\big(\omega_c t_d + \phi_{S,i}^{(u_j)} + \phi_u'\big), \sigma_k^2)$, where

[1] Note that if the gains $\alpha_{S,i}^{(u_j)}$ are too small $\forall i$, such that u_j cannot meet the target received chip energy $\tilde{E}_{c,Rx}$ due to power constraints, u_j will not transmit, as it will not be allocated any channels under the resource allocation algorithm.

$\mu = \zeta_d l_{acq}\sqrt{\tilde{E}_{c,Rx} N_c^{acq}}$, and $\sigma_k^2 = \frac{l_{acq}N_0}{2} + \frac{l_{acq}\alpha_{J,i}^{(ch)}\eta_{J,i}}{2} + \frac{l_{acq}\tilde{E}_{c,Rx}}{2}\left(1-\frac{\beta}{4}\right)(|U(i)|-1)$. Similarly, $z_{k^*,I} \sim \mathcal{N}(\mu\sin\left(\omega_c t_d + \phi_{S,i}^{(u_j)} + \phi'_u\right), \sigma_k^2)$. Therefore, $z_{k^*} = z_{k^*,I}^2 + z_{k^*,Q}^2$ is a square of a Rician r.v. when conditioned on $\alpha_{J,i}^{(ch)}$ and

$$f_{z_{k^*}|\alpha_{J,i}^{(ch)}}(x) = \frac{1}{2\sigma_k^2} e^{-\frac{x+\mu^2}{2\sigma_k^2}} I_0\left(\frac{\mu\sqrt{x}}{\sigma_k^2}\right). \tag{5.5}$$

Following the same approach as in Subsection 4.2.2, I can show that z_k is an exponential r.v. with mean $2\sigma_k^2$, for $k \neq k^*$.

The probability of code acquisition conditioned on $\alpha_{J,i}^{(ch)}$ is $\Pr\Big(z_{k^*} > z_k|\alpha_{J,i}^{(ch)}, \quad \forall\ k \neq k^*, k \in \{0, 1, \ldots, N_c^{acq}-1\}\Big)$. Therefore, the probability of a code acquisition failure conditioned on $\alpha_{J,i}^{(ch)}$ is

$$\begin{aligned}
\Pr\left(\bigcup_{k\in\{0,\ldots,N_c^{acq}-1\}-k^*} z_{k^*} < z_k|\alpha_{J,i}^{(ch)}\right) &\geq \Pr\left(z_{k^*} < z_k|\alpha_{J,i}^{(ch)}\right) \\
&= \int_0^\infty \Pr\left(z_k > x|\alpha_{J,i}^{(ch)}\right) f_{z_{k^*}|\alpha_{J,i}^{(ch)}}(x)\,\mathrm{d}x \\
&= \int_0^\infty e^{-\frac{x}{2\sigma_k^2}} \frac{1}{2\sigma_k^2} e^{-\frac{x+\mu^2}{2\sigma_k^2}} I_0\left(\frac{\mu\sqrt{x}}{\sigma_k^2}\right)\,\mathrm{d}x \\
&= \int_0^\infty e^{-\frac{x}{2\sigma_k^2}} \frac{1}{2\sigma_k^2} e^{-\frac{x+\mu^2}{2\sigma_k^2}} \sum_{n=0}^{\infty} \frac{1}{(n!)^2}\left(\frac{\mu\sqrt{x}}{2\sigma_k^2}\right)^{2n}\,\mathrm{d}x \\
&= \frac{1}{2\sigma_k^2} e^{-\frac{\mu^2}{2\sigma_k^2}} \sum_{n=0}^{\infty}\left(\frac{\mu}{2\sigma_k^2}\right)^{2n} \int_{x=0}^{\infty} \frac{x^n}{(n!)^2} e^{-\frac{x}{\sigma_k^2}}\,\mathrm{d}x \\
&= \frac{1}{2\sigma_k^2} e^{-\frac{\mu^2}{2\sigma_k^2}} \sum_{n=0}^{\infty}\left(\frac{\mu}{2\sigma_k^2}\right)^{2n} \frac{n!\sigma_k^{2(n+1)}}{(n!)^2} \\
&= \frac{1}{2} e^{-\frac{\mu^2}{4\sigma_k^2}} = \frac{1}{2} e^{-\frac{\mu^2}{2l_{acq}\left(N_0+\alpha_{J,i}^{(ch)}\eta_{J,i}+\tilde{E}_{c,Rx}\left(1-\frac{\beta}{4}\right)(|U(i)|-1)\right)}}
\end{aligned} \tag{5.6}$$

Let $p_{cqf,ul}(P_{ds,u,i})$ be the average probability of code acquisition failure by the CH, averaged over $\alpha_{J,i}^{(ch)}$, where $P_{ds,u,i}$ is the uplink desynchronizing power in the i-th band. Note that $\eta_{J,i} = \frac{P_{ds,u,i}}{W}$.

$$\begin{aligned} p_{cqf,ul}(P_{ds,u,i}) &= \int_0^\infty \Pr\left(\bigcup_{k\in\{0,1,\dots,N_c^{acq}-1\}-k^*} z_{k^*} < z_k|\alpha_{J,i}^{(ch)}\right) \frac{e^{-\frac{\alpha_{J,i}^{(ch)}}{\bar{\alpha}_J^{(u_j)}}}}{\bar{\alpha}_J}\,\mathrm{d}\alpha_{J,i}^{(ch)} \\ &\geq \int_0^\infty \frac{1}{2} e^{-\frac{\mu^2}{2l_{acq}\left(N_0+\alpha_{J,i}^{(ch)}\frac{P_{ds,u,i}}{W}+\tilde{E}_{c,Rx}\left(1-\frac{\beta}{4}\right)(|U(i)|-1)\right)}} \frac{e^{-\frac{\alpha_{J,i}^{(ch)}}{\bar{\alpha}_J^{(u_j)}}}}{\bar{\alpha}_J}\,\mathrm{d}\alpha_{J,i}^{(ch)} \\ &\triangleq p_{cqf,lb,ul}(P_{ds,u,i}) \end{aligned} \tag{5.7}$$

5.2.2 User allocation methods

Let $B_{al} \subseteq B$ be the set of allowed bands in the current sensing interval, let U_{al} be the set of SUs, and let G_{ch} be the $|B_{al}| \times |U_{al}|$ matrix, where $G_{ch}[i][j]$ is the channel gain of the j-th user in the i-th band. Let $U(i)$ be the set of users assigned to band i. The maximum transmit power for a user is $P_{Tx,\max}$, the maximum transmit power per user per subcarrier is $P_{Tx,sc,\max}$, $\gamma_{Rx}^{(i,j)}$ is the received signal-to-interference-plus-noise ratio (SINR) of user j in band i, and $\tilde{\gamma}_{Rx}$ is the target received SINR. The maximum number of spreading sequences needed for user j, which is determined by the video properties, is denoted by $N_{sc,\max}[j]$. I assume perfect CSI at the CH.

I use P_{sc}, a $|B| \times |U_{al}|$ matrix to keep track of the transmit power for each user in each band, and C_{al}, a $|B| \times |U_{al}|$ matrix to keep track of the user-subcarrier assignment. Using the Gaussian approximation for the multiple access interference [15], the received SINR per stream for user i in band j is calculated as follows:

$$\gamma_{Rx}^{(i,j)} = \frac{N_c G_{ch}[i][j] E_c^{(i,j)}}{\sum_{k\in U_{al}-\{j\}} C_{al}[i][k] G_{ch}[i][k] E_c^{(i,k)} \left(1-\frac{\beta}{4}\right) + N_0} \tag{5.8}$$

where N_0 is the PSD of the background noise in band i and $E_c^{(i,j)}$ is the chip energy of user j in band i. The transmit power per stream of user j in band i is $P_{Tx,i,j} \triangleq \frac{E_c^{(i,j)}}{T_c}$. Here, by power per stream, I refer to the transmit power for one spreading sequence. Since there are $C_{al}[i][j]$ spreading sequences used by user j in band i, the total transmit power for user j in band i would be $C_{al}[i][j]P_{Tx,i,j}$.

I assume the system has perfect power control and $G_{ch}[i][j]E_c^{(i,j)}$ is kept constant for all users in the i-th band. Let us define $\tilde{E}_{c,Rx,i} \triangleq G_{ch}[i][j]E_c^{(i,j)}$. Substituting this in (5.8), I have

$$\begin{aligned}\gamma_{Rx}^{(i,j)} &= \frac{N_c\tilde{E}_{c,Rx,i}}{\sum_{k\in U_{al}-\{j\}} C_{al}[i][k]\tilde{E}_{c,Rx,i}\left(1-\frac{\beta}{4}\right)+N_0} \\ &= \frac{N_c}{\sum_{k\in U_{al}-\{j\}} C_{al}[i][k]\left(1-\frac{\beta}{4}\right)+\frac{N_0}{\tilde{E}_{c,Rx,i}}}\end{aligned} \tag{5.9}$$

From the definition of $P_{Tx,i,j}$, I have

$$P_{Tx,i,j} = \frac{\tilde{E}_{c,Rx,i}}{G_{ch}[i][j]T_c}. \tag{5.10}$$

The user-allocation is done by the CH, and hence all the above calculations are done at the CH.

I look at several user-subcarrier allocation methods. The first one is similar to a simple multi-user diversity channel allocation method, where each band is assigned to the user which can transmit with the least power in that band. I name it MUDup. The MUDup algorithm is presented in Fig.5.1. Here, the user-subcarrier assignment which requires the least increase in total transmit power of all users, while not exceeding the power constraints $P_{Tx,\max}$ and $P_{Tx,sc,\max}$, is selected first. Then, the next user-subcarrier assignment which requires the least transmit power is made, and so on, until all users obtain the maximum required number of assignments $N_{sc,\max}$, or until no further assignments can be made for users without $N_{sc,\max}$ assignments due to the power constraints.

The second algorithm, named MXDup, is presented in Fig.5.3. Here, each user is initially assigned a single subcarrier, using the MUDup algorithm. Then, a subset of users with the highest distortion under the current channel allocation is selected, and each user is allocated an additional subcarrier using the MUDup algorithm. This process of assigning an additional subcarrier to the subset of users with highest distortion is done iteratively, until no further assignments can be made due to the power constraints.

After the initial assignment from either of the above algorithms, a swapping algorithm can be used to check if changing a channel assignment from one user to another will decrease the sum distortion of all users. A description of this swapping algorithm is presented in Fig.5.4. In Fig.5.2, the procedure for calculating the target received chip energy is presented, and in Fig.5.5, the steps for checking if the power constraints are satisfied is detailed.

5.2.3 Transmission system model for the uplink

In this subsection, I analyze the transmission subsystem on the uplink. I derive an expression for the average SINR, which can be used to derive an approximation for the packet error rate.

A block diagram of the transmitter of a single user and a single carrier is shown in Figure 2.3. LDPC codes are used for FEC. The output bit sequence of the FEC block of user u_j is denoted by $d_\ell^{(u_j)}$. This binary sequence is mapped to a symbol sequence $s_k^{(u_j,m)}$, where k is a time index and $m = 1, \ldots, \Omega_i^{(u_j)}$, where $\Omega_i^{(u_j)}$ is the number of spreading sequences assigned to u_j in the i-th band. Note that $s_k^{(u_j,m)}$ is generally complex valued, and normalized to have unit average energy, i.e. $E[|s_k^{(u_j,m)}|^2] = 1$. The $\{c_n^{(u_j,m)}\}$ are the chips of the m-th pseudo-random spreading sequence of u_j, and there are N_c chips per symbol. The sequence $s_k^{(u_j,m)}c_n^{(u_j,m)}$ modulates an impulse train. After passing through both the chip-wave shaping filter $g(t)$ and the modulator, the transmitted signal of u_j in the i-th band takes the form

$$x_i^{(u_j)}(t) = \Re\left\{\sqrt{2E_c^{(u_j)}}\sum_{m=1}^{\Omega_i^{(u_j)}}\sum_{n=-\infty}^{\infty} s_k^{(u_j,m)}c_n^{(u_j,m)}g(t-nT_c)e^{j(\omega_c t+\phi_{u_j})}\right\} \tag{5.11}$$

where $\Omega_i^{(u_j)}$ is the number of streams of u_j in band i, ϕ_{u_j} is the carrier phase of u_j, and $k = \lfloor n/N_c \rfloor$.

The transmitted signal $x_i^{(u_j)}(t)$ is attenuated by Rayleigh fading, and corrupted by AWGN and jamming, as shown in Figure 5.6. The jamming signal undergoes Rayleigh fading, independent of the source-user channel. The received signal $(y_i(t))$ at the CH in

```
procedure MUDUP($G_{ch}, U_{al}, B_{al}, C_{al}, P_{sc}, \tilde{\gamma}_{Rx}, P_{Tx,\max}, P_{Tx,sc,\max}, N_{sc,\max}, N_0, \beta$)
    $U'_{al} \leftarrow U_{al}$
    while $|U'_{al}| > 0$ do    ▷ While set of users to be assigned a channel is non-empty
        $\Delta P_{Tx} \leftarrow |U_{al}|P_{Tx,\max} \times \mathbf{1}_{|U_{al}|\times|B|}$    ▷ Initialize all elements with $|U_{al}|P_{Tx,\max}$
        $\tilde{E}_{c,Rx,i} \leftarrow$ CALC_ECRX $(C_{al}, U_{al}, i, \tilde{\gamma}_{Rx}, N_c, N_0, \beta)$
        for $i \in B_{al}$ do
            for $j \in U'_{al}$ do
                $P'_{sc} \leftarrow P_{sc}$
                $P_{Tx,i,j} \leftarrow \frac{\tilde{E}_{c,Rx,i}}{G_{ch}[i][j]T_c}$
                $P'_{sc}[i][j] \leftarrow P_{Tx,i,j} + P_{sc}[i][j]$
                if $P'_{sc}[i][j] \leq P_{Tx,sc,\max}$ AND $\sum_{l\in B_{al}} P'_{sc}[l][j] \leq P_{Tx,\max}$ then
                    $C'_{al} \leftarrow C_{al}$, $C'_{al}[i][j] \leftarrow C_{al}[i][j] + 1$
                    $\tilde{E}'_{c,Rx,i} \leftarrow$ CALC_ECRX $(C'_{al}, U_{al}, i, \tilde{\gamma}_{Rx}, N_c, N_0, \beta)$
                    $\forall k \in U_{al},\ P_{\Delta I,i,j,k} \leftarrow \frac{C'_{al}[i][k]}{G_{ch}[i][k]T_c}\left(\tilde{E}'_{c,Rx,i} - \tilde{E}_{c,Rx,i}\right)$
                    if $\forall k \in U_{al}, \Big(P'_{sc}[i][k] + P_{\Delta I,i,j,k} \leq P_{Tx,sc,\max}$ AND $\sum_{l\in B_{al}} P'_{sc}[l][k] \leq P_{Tx,\max} - P_{\Delta I,i,j,k}\Big)$ then    ▷ If power constraints are satisfied
                        $\Delta P_{Tx}[i][j] \leftarrow P_{Tx,i,j} + \sum_{k\in U_{al}} P_{\Delta I,i,j,k}$
                    end if
                end if
            end for
        end for
        $(i, j) \leftarrow \arg\min_{j\in U'_{al}, i\in B_{al}} \left\{\Delta P_{Tx}[i][j]\right\}$    ▷ Select band & user which require the lowest transmit power
        if $\Delta P_{Tx}[i][j] < |U_{al}|P_{Tx,\max}$ then
            $C_{al}[i][j] \leftarrow C_{al}[i][j] + 1$    ▷ Update channel assignment matrix
            $P_{sc}[i, j] \leftarrow P_{Tx,i,j} + P_{sc}[i][j]$
            $\forall k \in U_{al},\ P_{sc}[i, k] \leftarrow P_{\Delta I,i,j,k} + P_{sc}[i][k]$    ▷ Update transmit power in selected ($i$-th) band
            if $\sum_{k\in B_{al}} C_{al}[k][j] \geq N_{sc,\max}[j]$ then
                $U'_{al} \leftarrow U'_{al} - \{j\}$    ▷ Remove user if max. no. of allocations is met
            end if
        else
            return $\{C_{al}, P_{sc}\}$
        end if
    end while
    return $\{C_{al}, P_{sc}\}$
end procedure
```

Figure 5.1: MUDup algorithm for user allocation

```
procedure CALC_ECRX($(C_{al}, U_{al}, i, \tilde{\gamma}_{Rx}, N_c, N_0, \beta)$)
    if $\sum_{k\in U_{al}} C_{al}[i][k] == 0$ then    ▷ If there are no users in $i$
        $E_{c,Rx} \leftarrow \frac{\tilde{\gamma}_{Rx} N_0}{N_c}$
    else
        $\tilde{k} \leftarrow \underset{k\in U_{al}}{\arg\min} \Big\{ C_{al}[i][k] \mid C_{al}[i][k] > 0 \Big\}$    ▷ User with the smallest non-zero allocation in $i$
        $E_{c,Rx} \leftarrow \frac{N_0}{\frac{N_c}{\tilde{\gamma}_{Rx}} - \sum_{k\in U_{al}-\{\tilde{k}\}} C_{al}[i][k]\left(1-\frac{\beta}{4}\right)}$
    end if
    return $E_{c,Rx}$
end procedure
```

Figure 5.2: Calculation of the target received chip energy

```
procedure MXDUP $(G_{ch}, U_{al}, B_{al}, \tilde{\gamma}_{Rx}, P_{Tx,\max}, P_{Tx,sc,\max}, N_0, \beta, \vartheta)$
    $U'_{al} \leftarrow \{\}$
    $U''_{al} \leftarrow U_{al}$
    $C_{al} \leftarrow \mathbf{0}_{|U_{al}|\times|B|}$
    $P_{sc} \leftarrow \mathbf{0}_{|B|\times|U_{al}|}$
    while $|U''_{al}| > 0$ do
        $\{C'_{al}, P_{sc}\} \leftarrow$MUDUP$(G_{ch}, U''_{al}, B_{al}, C_{al}, P_{sc}, \tilde{\gamma}_{Rx}, P_{Tx,\max}, P_{Tx,sc,\max}, 1, N_0, \beta)$
        Calculate $D_{su}$; the video distortion of users with current channel allocation $C'_{al}$.
        $U'_{al} \leftarrow \Big\{ j \mid j \in U''_{al},\ \forall i \in B_{al}\ \ C'_{al}[i][j] == C_{al}[i][j] \Big\} \cup U'_{al}$
        Select $U''_{al} \subseteq U_{al} - U'_{al}$; up to $\vartheta|U_{al}|$ users with largest video distortion $(D_{su})$
    end while
    return $C_{al}$
end procedure
```

Figure 5.3: MXDup algorithm for user allocation

```
procedure SWAP_ALLOC $(\alpha, U_{al}, B_{al}, C_{al}, P_{Rx}, P_{Tx,\max}, \max\_it)$
    $iter \leftarrow 0$, $\Delta D_{su} \leftarrow \mathbf{0}_{|B_{al}|\times|U_{al}|\times|U_{al}|}$
    while $iter < \max\_it$ do
        for $j \in U_{al}$ do
            Calculate $D_{su}^{(0)}[j]$; video distortion of $j$ with current channel allocation.
            Calculate $D_{su}^{(1)}[j]$; distortion of $j$ with one additional channel alloc.
        end for
        for $i \in B_{al}$ do
            $C'_{al} \leftarrow C_{al}$.
            for $j \in U_{al}$ do
                $C'_{al}[i][j] \leftarrow C'_{al}[i][j] + 1$
                for $k \in U_{al} - \{j\}$ do
                    while !ISUNDPMAX$(G_{ch}, C'_{al}, U_{al}, B_{al}, P_{Tx,\max}, P_{Tx,sc,\max}, \tilde{\gamma}_{Rx}, N_c, N_0, \beta)$ AND $C'_{al}[i][k] > 0$ do
                        $C'_{al}[i][k] \leftarrow C'_{al}[i][k] - 1$    ▷ Decrement the no. of assignments of $k$ in $i$, until either the power constraints are met or $k$ is removed from $i$
                    end while
                    if $C'_{al}[i][k] \geq 0$ then
                        Calculate $D_{su}^{(-1)}[k]$; distortion of $k$ with $C'_{al}$ channel allocation.
                        $C''_{al}[i][j][k] \leftarrow C'_{al}[i][k]$
                        $\Delta D_{su}[i][j][k] \leftarrow (D_{su}^{(1)}[j] + D_{su}^{(-1)}[k]) - (D_{su}^{(0)}[j] + D_{su}^{(0)}[k])$
                    end if
                end for
            end for
        end for
        if $\min \Delta D_{su}[i][j][k] < 0$ then
            $(i', j', k') \leftarrow \underset{j,k \in U_{al}; i \in B_{al}}{\arg\max} \Delta D_{su}[i][j][k]$    ▷ Band and users corresponding to the largest reduction in distortion
            $C_{al}[i'][j'] \leftarrow C_{al}[i'][j'] + 1$
            $C_{al}[i'][k'] \leftarrow C''_{al}[i'][j'][k']$
        else    ▷ When swapping does not decreases the distortion
            return $C_{al}$
        end if
        $iter \leftarrow iter + 1$
    end while
    return $C_{al}$
end procedure
```

Figure 5.4: Algorithm to swap subcarriers between users to decrease sum distortion

```
procedure ISUNDPMAX($G_{ch}, C_{al}, U_{al}, B_{al}, P_{Tx,\max}, P_{Tx,sc,\max}, \tilde{\gamma}_{Rx}, N_c, N_0, \beta$)
    $P_{sc} \leftarrow \mathbf{0}_{|B_{al}|\times|U_{al}|}$
    for $i \in B_{al}$ do
        $E_{c,Rx,i} \leftarrow$ CALC_ECRX $(C_{al}, U_{al}, i, \tilde{\gamma}_{Rx}, N_c, N_0, \beta)$
        for $j \in U_{al}$ do
            $P_{sc}[i][j] \leftarrow \frac{C_{al}[i][j]E_{c,Rx,i}}{G_{ch}[i][j]T_c}$        ▷ Transmit power required for user $j$ in $i$-th band
            if $P_{sc}[i][j] > P_{Tx,sc,\max}$ then        ▷ Per subcarrier power constraint
                return FALSE
            end if
        end for
    end for
    for $j \in U_{al}$ do
        if $\sum_{i\in B_{al}} P_{sc}[i][j] > P_{Tx,\max}$ then        ▷ Total power constraint
            return FALSE
        end if
    end for
    return TRUE
end procedure
```

Figure 5.5: Procedure to test if the power constraints are satisfied

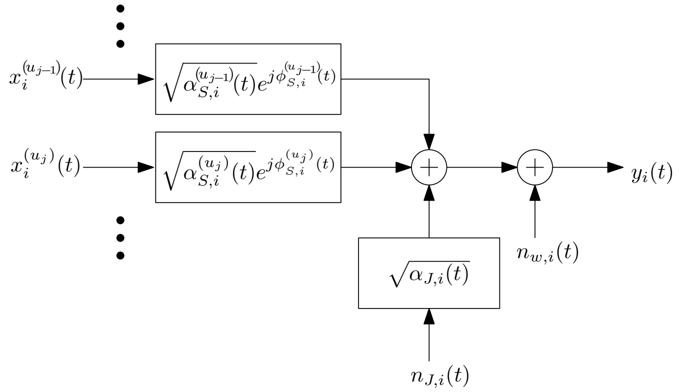

$x_i^{(u_{j-1})}(t)$
$\sqrt{\alpha_{S,i}^{(u_{j-1})}(t)}e^{j\phi_{S,i}^{(u_{j-1})}(t)}$
$x_i^{(u_j)}(t)$
$\sqrt{\alpha_{S,i}^{(u_j)}(t)}e^{j\phi_{S,i}^{(u_j)}(t)}$
$y_i(t)$
$n_{w,i}(t)$
$\sqrt{\alpha_{J,i}(t)}$
$n_{J,i}(t)$

Figure 5.6: Channel response and jamming in the i-th band for user u_j

the i-th band is given by

$$y_i(t) = \Re\Bigg\{ \sum_{u_j \in U(i)} \sqrt{2\alpha_{S,i}^{(u_j)}(t)} e^{j\phi_{S,i}^{(u_j)}(t)} \sqrt{E_c^{(u_j)}} \sum_{m=1}^{\Omega_i^{(u_j)}} \sum_{n=-\infty}^{\infty} s_k^{(u_j,m)} c_n^{(u_j,m)} g(t - nT_c - \tau^{(u_j)}) \\ \times e^{j(\omega_c t + \phi_{u_j})} \Bigg\} + n_{w,i}(t) + \sqrt{\alpha_{J,i}^{(ch)}(t)} n_{J,i}(t) \tag{5.12}$$

I assume the channel gains $\alpha_{S,i}^{(u_j)}(t)$ and $\alpha_{J,i}^{(ch)}(t)$ are mutually independent. The time delay in user u_j is denoted by $\tau^{(u_j)}$. The background noise $n_{w,i}(t)$ is AWGN with PSD $\frac{N_0}{2}$ in the i-th band and $\sqrt{\alpha_{J,i}^{(ch)}(t)} n_{J,i}(t)$ is the received jamming signal. The diagram of the block of the receiver that detects the symbols from the m-th stream of u_j is shown in Figure 2.5. I assume the channel remains constant during a symbol detection. I denote the gain and phase components of the response of the u_j-to-CH channel during the k-th symbol detection by $\alpha_{S,i,k}^{(u_j)} \triangleq \alpha_{S,i}^{(u_j)}(kN_cT_c)$ and $\phi_{S,i,k}^{(u_j)} \triangleq \phi_{S,i}^{(u_j)}(kN_cT_c)$, respectively. The gain of the jammer-to-CH channel is denoted by $\alpha_{J,i,k} \triangleq \alpha_{J,i}^{(ch)}(kN_cT_c)$. The complex output samples are given by

$$z_{k,i}^{(u_j,m)} \triangleq z_{k,i,1}^{(u_j,m)} + jz_{k,i,2}^{(u_j,m)} = \sqrt{E_S^{(u_j)} \alpha_{S,i,k}^{(u_j)}} s_k^{(u_j,m)} + \sqrt{\alpha_{J,i,k}} n_{J,i,k}^{(u_j,m)} + n_{w,i,k}^{(u_j,m)} + I_{i,k}^{(u_j,m)} \tag{5.13}$$

where $E_S^{(u_j)} = E_c^{(u_j)} N_c$, is the symbol energy, $n_{J,i,k}^{(u_j,m)}$ is the jamming signal, $n_{w,i,k}^{(u_j,m)}$ is the background noise and $I_{i,k}^{(u_j,m)}$ is the interference from other users occupying the i-th band. Further, $n_{J,i,k}^{(u_j,m)} \sim \mathcal{CN}(0, \eta_{J,i})$ and $n_{w,i,k}^{(u_j,m)} \sim \mathcal{CN}(0, N_0)$, where $\frac{\eta_{J,i}}{2}$ is the PSD of the jamming signal in the i-th band.

The interference from other users, $I_{i,k}^{(u_j,m)}$, is given by

$$I_{i,k}^{(u_j,m)} = \Re\Bigg\{ \sum_{u_l \in U(i)-\{u_j\}} \sqrt{\alpha_{S,i,k'}^{(u_l)} E_c^{(u_l)}} \sum_{n=k}^{k+N_c-1} \frac{c_n^{(u_j,m)}}{\sqrt{N_c}} \sum_{m=1}^{\Omega_i^{(u_l)}} \sum_{n'=-\infty}^{\infty} \\ \left(\frac{\cos(\psi)\Re\{s_{k'}^{(u_l,m)}\} - \sin(\psi)\Im\{s_{k'}^{(u_l,m)}\}}{2} + \frac{j\big(\sin(\psi)\Re\{s_{k'}^{(u_l,m)}\} + \cos(\psi)\Im\{s_{k'}^{(u_l,m)}\}\big)}{2} \right) \\ \times c_{n'}^{(u_l,m)} \int_{t=-\infty}^{\infty} g(t - n'T_c - \tau^{(u_l)}) g(t - nT_c - \tau^{(u_j)}) \mathrm{d}t \Bigg\} \tag{5.14}$$

where $\psi = \phi_{u_l} + \phi_{S,i,k}^{(u_l)} - \phi_{u_j} - \phi_{S,i,k}^{(u_j)}$ is the phase difference between users u_j and u_l. The analysis of the interference for similar systems was done in [33] and [34]. I approximate the above interference with a Gaussian r.v.. Using the results from [33] and [34], I can obtain the variance of $I_{i,k}^{(u_j,m)}$:

$$I_{i,k}^{(u_j,m)} \sim \mathcal{CN}\left(0, \tilde{E}_{c,Rx}\left(1-\frac{\beta}{4}\right)\sum_{u_l\in U(i)-\{u_j\}}\Omega_i^{(u_j)}\right) \tag{5.15}$$

Using (5.13), I can write the uplink SINR for user u_j for any stream in the i-th band as follows:

$$\begin{aligned}
\gamma_{i,k}^{(u_j)} &= \frac{N_c\tilde{E}_{c,Rx}}{\tilde{E}_{c,Rx}\left(1-\frac{\beta}{4}\right)\sum_{u_l\in U(i)-\{u_j\}}\Omega_i^{(u_j)} + \eta_{J,i}\alpha_{J,i,k} + N_0} \\
&= \frac{\left(\frac{N_c\tilde{E}_{c,Rx}}{\tilde{E}_{c,Rx}\left(1-\frac{\beta}{4}\right)\sum_{u_l\in U(i)-\{u_j\}}\Omega_i^{(u_j)}+N_0}\right)}{\left(\frac{\eta_{J,i}\alpha_{J,i,k}}{\tilde{E}_{c,Rx}\left(1-\frac{\beta}{4}\right)\sum_{u_l\in U(i)-\{u_j\}}\Omega_i^{(u_j)}+N_0}\right)+1} \\
&\approx \frac{\gamma_{S,ul}}{\alpha_{J,i,k}\bar{\gamma}_{J,i,ul}^{(u_j)}+1}
\end{aligned} \tag{5.16}$$

where $\bar{\gamma}_{J,i,ul}^{(u_j)} = \frac{\eta_{J,i}}{\tilde{E}_{c,Rx}\left(1-\frac{\beta}{4}\right)\sum_{u_l\in U(i)-\{u_j\}}\Omega_i^{(u_j)}+N_0}$.

Following the same approach as in Subsection , I can show that the expected number of packet errors of user u_j in the i-th band $N_{e,i}(P_{J,i})$, is

$$N_{e,i}(P_{J,i}) = N_p e^{-\frac{\left(\tilde{E}_{c,Rx}\left(1-\frac{\beta}{4}\right)\sum_{u_l\in U(i)-\{u_j\}}\Omega_i^{(u_j)}+N_0\right)W}{\bar{\alpha}_J^{(ch)}P_{J,i}}\left(\frac{\gamma_{S,ul}}{\gamma_T}-1\right)} \tag{5.17}$$

where N_p is the average number of packets of a single user in a single band per transmission interval, γ_T is the threshold parameter that depends on the FEC from (4.16) and $\bar{\alpha}_J^{(ch)}$ is the average gain of the adversary-to-CH channel.

5.3 Desynchronizing power optimization

In this subsection, I analyze the performance of the system under desynchronizing attacks. I derive an objective function for the adversary, in order to maximize the video distortion under desynchronizing attacks.

After the sensing interval, the CH determines which bands are allowed for SUs, and broadcasts a spreading sequence for code acquisition for SUs during the $T_{1,d}$ interval. If an SU performs successful code acquisition, it will estimate the CSI, and transmit a predetermined sequence in a randomly selected subset of allowed bands, for code acquisition at the CH during $T_{1,u}$. The adversary can transmit an interference signal to disrupt the code acquisition process. I call this a desynchronizing attack. If the code acquisition fails either on the downlink at an SU or on the uplink at the CH, that SU will not be able to estimate the channel gains and will not be assigned subcarriers during the resource allocation.

Define $X_{acq}^{(u_j)}$, $X_{acq,dl}^{(u_j)}$, and $X_{acq,ul}^{(u_j)}$ as follows:

$$X_{acq}^{(u_j)} \triangleq \begin{cases} 1 & \text{if code acquisition of } u_j \text{ is successful} \\ 0 & \text{if code acquisition of } u_j \text{ fails} \end{cases} \tag{5.18}$$

$$X_{acq,dl}^{(u_j)} \triangleq \begin{cases} 1 & \text{if code acquisition of } u_j \text{ is successful on the downlink} \\ 0 & \text{if code acquisition of } u_j \text{ fails on the downlink} \end{cases} \tag{5.19}$$

$$X_{acq,ul}^{(u_j)} \triangleq \begin{cases} 1 & \text{if code acquisition of } u_j \text{ is successful on the uplink} \\ 0 & \text{if code acquisition of } u_j \text{ fails on the uplink} \end{cases} \tag{5.20}$$

$$\begin{aligned}\text{Average video distortion of } u_j &= E[\text{Video distortion of } u_j | X_{acq}^{(u_j)} = 1] \Pr\left(X_{acq}^{(u_j)} = 1\right) \\ &\quad + E[\text{Video distortion of } u_j | X_{acq}^{(u_j)} = 0] \Pr\left(X_{acq}^{(u_j)} = 0\right) \\ &= \overline{f_{D,1}^{(u_j)}} \Pr\left(X_{acq}^{(u_j)} = 1\right) + \overline{f_{D,0}^{(u_j)}} \Pr\left(X_{acq}^{(u_j)} = 1\right) \qquad (5.21)\end{aligned}$$

where $\overline{f_{D,1}^{(u_j)}} \triangleq E[\text{Video distortion of } u_j | X_{acq}^{(u_j)} = 1]$ is the average video distortion of u_j if it achieves code acquisition, and $\overline{f_{D,0}^{(u_j)}} \triangleq E[\text{Video distortion of } u_j | X_{acq}^{(u_j)} = 0]$ is the average video distortion of u_j if it fails to achieve code acquisition.

Because the code acquisition failure of u_j can be due to either code acquisition failure on the downlink, or code acquisition failure on the uplink,

$$\begin{aligned}\Pr\left(X_{acq}^{(u_j)} = 0\right) &= \Pr\left(X_{acq,dl}^{(u_j)} = 0\right) + \Pr\left(X_{acq,dl}^{(u_j)} = 1 \cap X_{acq,ul}^{(u_j)} = 0\right) \\ &= \Pr\left(X_{acq,dl}^{(u_j)} = 0\right) + \Pr\left(X_{acq,dl}^{(u_j)} = 1\right) \Pr\left(X_{acq,ul}^{(u_j)} = 0 | X_{acq,dl}^{(u_j)} = 1\right) \\ &= \Pr\left(X_{acq,dl}^{(u_j)} = 0\right) + \left(1 - \Pr\left(X_{acq,dl}^{(u_j)} = 0\right)\right) \Pr\left(X_{acq,ul}^{(u_j)} = 0 | X_{acq,dl}^{(u_j)} = 1\right) \\ &= p_{cqf,dl}^{(u_j)} + \left(1 - p_{cqf,dl}^{(u_j)}\right) p_{cqf,ul}^{(u_j)} \qquad (5.22)\end{aligned}$$

where $p_{cqf,dl}^{(u_j)} \triangleq \Pr\left(X_{cqf,dl}^{(u_j)} = 0\right)$ is the probability of code acquisition failure on the downlink, and $p_{cqf,ul}^{(u_j)} \triangleq \Pr\left(X_{cqf,ul}^{(u_j)} = 0 | X_{cqf,dl}^{(u_j)} = 1\right)$ is the probability of code acquisition failure on the uplink, given that code acquisition was successful on the downlink. Using (5.22),

$$\begin{aligned}\Pr\left(X_{acq}^{(u_j)} = 1\right) &= 1 - \Pr\left(X_{acq}^{(u_j)} = 0\right) \\ &= 1 - \left(p_{cqf,dl}^{(u_j)} + \left(1 - p_{cqf,dl}^{(u_j)}\right) p_{cqf,ul}^{(u_j)}\right) \\ &= \left(1 - p_{cqf,dl}^{(u_j)}\right)\left(1 - p_{cqf,ul}^{(u_j)}\right) \qquad (5.23)\end{aligned}$$

Substituting (5.22) and (5.23), in (5.21):

$$\begin{aligned}
&\text{Average video distortion of } u_j \\
&= \overline{f_{D,1}^{(u_j)}}(1 - p_{cqf,dl}^{(u_j)})(1 - p_{cqf,ul}^{(u_j)}) + \overline{f_{D,0}^{(u_j)}}\left(p_{cqf,dl}^{(u_j)} + \left(1 - p_{cqf,dl}^{(u_j)}\right) p_{cqf,ul}^{(u_j)}\right) \\
&= \overline{f_{D,1}^{(u_j)}}(1 - p_{cqf,dl}^{(u_j)})(1 - p_{cqf,ul}^{(u_j)}) + \overline{f_{D,0}^{(u_j)}}\big(1 - (1 - p_{cqf,dl}^{(u_j)})(1 - p_{cqf,ul}^{(u_j)})\big) \\
&= \overline{f_{D,0}^{(u_j)}} - (1 - p_{cqf,dl}^{(u_j)})(1 - p_{cqf,ul}^{(u_j)})\big(\overline{f_{D,0}^{(u_j)}} - \overline{f_{D,1}^{(u_j)}}\big) \qquad (5.24)
\end{aligned}$$

Note that if u_j fails code acquisition, u_j will not transmit any data in the subsequent transmission interval, and if u_j performs code acquisition successfully, it is likely u_j will transmit data over the subsequent transmission interval, depending on the channel state and resource allocation methods. Therefore, $\overline{f_{D,1}^{(u_j)}} < \overline{f_{D,0}^{(u_j)}}$, and in order to maximize the distortion of user u_j through desynchronizing attacks, the adversary must minimize $(1 - p_{cqf,dl}^{(u_j)})(1 - p_{cqf,ul}^{(u_j)})$.

Let $P_{ds,dl}$ and $P_{ds,ul}$ be the total desynchronizing power at the adversary during $T_{1,dl}$ and $T_{1,ul}$, respectively. Note that $P_{ds,dl}$ will only affect $p_{cqf,dl}^{(u_j)}$ and $P_{ds,ul}$ will only affect $p_{cqf,ul}^{(u_j)}$. For a given pair of values $P_{ds,dl}$ and $P_{ds,ul}$, to minimize $(1 - p_{cqf,dl}^{(u_j)})(1 - p_{cqf,ul}^{(u_j)})$, the adversary aims to maximize $p_{cqf,dl}^{(u_j)}$ under the power constraint $P_{ds,dl}$ and maximize $p_{cqf,ul}^{(u_j)}$ under the power constraint $P_{ds,ul}$.[2]

In Chapter 4, I showed that the optimal strategy to maximize $p_{cqf,dl}^{(u_j)}$, under a total power constraint $P_{ds,dl}$, is to allocate equal power to all bands. I now look at the optimal power allocation to maximize $p_{cqf,ul}^{(u_j)}$. Let $N_{acq,ul}$ be the number of bands on which u_j transmits the spreading sequence for code acquisition. The CH tries to acquire the code in all $N_{acq,ul}$ bands. The acquisition in each band is followed by code tracking, and I assume that all incorrect phases will be rejected in the tracking mode. Hence, if the correct code phase is acquired in any band, the CH achieves code acquisition. Therefore,

[2] Note that in this section I am finding the optimal desynchronizing strategies on the downlink and the uplink, as functions of $P_{ds,dl}$ and $P_{ds,ul}$, respectively. I can find the optimal $P_{ds,dl}$ and $P_{ds,ul}$ values in the energy optimization among attacking methods in Section 5.5. When $P_{ds,dl}$ and $P_{ds,ul}$ are fixed, code acquisition failure/success on the downlink and uplink are mutually independent events, as all channels and noise samples are uncorrelated.

the probability of code acquisition failure is

$$p_{cqf,ul}^{(u_j)} = \prod_{i=1}^{N_{acq,ul}} p_{cqf,ul}(P_{ds,u,i}) \tag{5.25}$$

where $p_{cqf,ul}(P_{ds,u,i})$ is the probability of code acquisition failure on the uplink as a function of desynchronizing power, and I have denoted the indices of the bands on which u_j is transmitting from 1 to $N_{acq,ul}$. The objective of the adversary is to maximize $p_{cqf,ul}^{(u_j)}$, which is equivalent to maximizing $\log\left(p_{cqf,ul}^{(u_j)}\right) = \sum_{i=1}^{N_{acq,ul}} \log\bigl(p_{cqf,ul}(P_{ds,u,i})\bigr)$. As the adversary is not aware of the subset of bands on which u_j is transmitting, I modify the objective function as $\sum_{i=1}^{N_T} \log\bigl(p_{cqf,ul}(P_{ds,u,i})\bigr)$ I use the lower bound $p_{cqf,lb,ul}(P_{ds,u,i})$ derived in (5.7) in place of $p_{cqf,ul}(P_{ds,u,i})$, and the objective function to maximize is $\sum_{i=1}^{N_T} \log\bigl(p_{cqf,lb,ul}(P_{ds,u,i})\bigr)$.

From (5.7), I can see that $p_{cqf,lb,ul}(P_{ds,u,i})$ is an increasing function of $P_{ds,u,i}$ and **P3** from Appendix C is satisfied. Therefore, I also know that

$$p_{cqf,lb,ul}(P_{ds,u,i}) \leq \lim_{P_{ds,u,i}\to\infty} p_{cqf,lb,ul}(P_{ds,u,i}) = \int_0^\infty \frac{1}{2} \times \frac{e^{-\frac{\alpha_{J,i}^{(ch)}}{\bar{\alpha}_J^{(ch)}}}}{\bar{\alpha}_J^{(ch)}} \, \mathrm{d}\alpha_{J,i}^{(ch)} = \frac{1}{2} \tag{5.26}$$

The above result shows that the function is bounded above and has the property **P0** from Appendix C. Because the log function is monotonically increasing, $\log\bigl(p_{cqf,lb,ul}(P_{ds,u,i})\bigr)$ also has the properties **P0** and **P3**. Therefore, I can use the optimization approach proposed in Appendix C to maximize $\sum_{i=1}^{N_T} \log\bigl(p_{cqf,lb,ul}(P_{ds,u,i})\bigr)$, under the constraint $\sum_{i=1}^{N_T} P_{ds,u,i} \leq P_{ds,ul}$.

5.4 Jamming power optimization

Following the same approach as in Section 4.5, I can show that in order to maximize user distortion, the adversary must aim to maximize

$$\sum_{i=1}^{N_{Tx}} e^{-\frac{\left(\tilde{E}_{c,Rx}\left(1-\frac{\beta}{4}\right)\sum_{u_l\in U(i)-\{u_j\}} \Omega_i^{(u_j)}+N_0\right)W}{\bar{\alpha}_J P_{J,i}}\left(\frac{\gamma_{S,ul}}{\gamma_T}-1\right)} \tag{5.27}$$

where N_{Tx} is the number of bands occupied by PUs and SUs. Because the number of users assigned to each band is not known, the adversary assumes that equal numbers of users are assigned to each band, and estimates $\max\left(1, \left\lfloor \frac{|\bar{U_{al}}|}{N_{Tx}-|\bar{B_{pu}}|} \right\rfloor\right)$ users are assigned to each band, where $|\bar{B_{pu}}|$ is the average number of bands occupied by PUs. Hence, the interference component is $\tilde{E}_{c,Rx}\left(1-\frac{\beta}{4}\right)\max\left(\frac{|\bar{U_{al}}|}{N_{Tx}-|\bar{B_{pu}}|}-1, 0\right)$. The function to maximize is

$$\sum_{i=1}^{N_{Tx}} e^{-\frac{\left(\tilde{E}_{c,Rx}\left(1-\frac{\beta}{4}\right)\max\left(\frac{|U_{al}|}{N_{Tx}-|\bar{B}_{pu}|}-1,0\right)+N_0\right)W}{\bar{\alpha}_J P_{J,i}}\left(\frac{\gamma_{S,ul}}{\gamma_T}-1\right)}. \tag{5.28}$$

I can show that $e^{-\frac{\left(\tilde{E}_{c,Rx}\left(1-\frac{\beta}{4}\right)\max\left(\frac{|U_{al}|}{N_{Tx}-|\bar{B}_{pu}|}-1,0\right)+N_0\right)W}{\bar{\alpha}_J P_{J,i}}\left(\frac{\gamma_{S,ul}}{\gamma_T}-1\right)}$ satisfies properties **P0** and **P3**, and use optimization approach from Appendix C to maximize (5.28).

5.5 Energy optimization among modes of attack

In this section, I look at the optimal energy allocation among spoofing, desynchronizing and jamming attacks. Let E_{adv} be the total energy available for the adversary during a $T_0 + T_{1,d} + T_{1,u} + T_2$ interval. Let θ_{sp} be the fraction of energy allocated for spoofing, and let $\theta_{ds,d}$ and $\theta_{ds,u}$ be the fraction of energy allocated for desynchronizing attacks on the downlink and uplink, respectively. I have $E_{sp} = \theta_{sp}E_{adv}$, $E_{ds,d} = \theta_{ds,d}E_{adv}$, $E_{ds,u} = \theta_{ds,u}E_{adv}$, and $E_{jm} = (1 - \theta_{sp} - \theta_{ds,d} - \theta_{ds,u})E_{adv}$.

The objective of the adversary is to find the parameters $(\theta_{sp}, \theta_{ds})$ that maximizes $\sum_{\forall u_j} f_D^{(u_j)}(r_{u_j}, e_{u_j})$. In the separate optimizations of desynchronizing and jamming attacks in Sections 5.3 and 5.4, I was able to derive objective functions to replace $f_D^{(u_j)}\left(r_{u_j}, e_{u_j}\right)$, using the knowledge that $f_D^{(u_j)}(r_{u_j}, e_{u_j})$ is a monotonically decreasing function of r_{u_j} and a monotonically increasing function of e_{u_j}, when the other parameters are kept constant. But I now need knowledge of $f_D^{(u_j)}$ to optimize energy allocation among the attacking methods. Because $f_D^{(u_j)}$ depends on the video properties and encoding parameters that are not known by the adversary, $f_D^{(u_j)}$ cannot be calculated at the adversary. Therefore, I use throughput as an alternative target for this section.

Following the same approach as in Section 4.6, I can find an estimate for minimum throughput (worst case throughput) under spoofing, jamming and desynchronizing attacks, $\Gamma(\theta_{sp}, \theta_{ds,d}, \theta_{ds,u})$, which can be written as

$$\begin{aligned}\Gamma(\theta_{sp},\theta_{ds,d},\theta_{ds,u}) = L_p\Big(N_p\tilde{B}_{su}(\theta_{sp}) - \tilde{N}_{er}\Big(1-\theta_{sp}-\theta_{ds,d}-\theta_{ds,u}, \tilde{B}_{su}(\theta_{sp}), \overline{|B_{pu}|}\Big)\Big)\\ \times\Big(1-\tilde{p}_{cqf,d}\Big(\theta_{ds,d}, \tilde{B}_{su}(\theta_{sp})\Big)\Big)\Big(1-\tilde{p}_{cqf,u}\Big(\theta_{ds,u}, \tilde{B}_{su}(\theta_{sp})\Big)\Big) \qquad (5.29)\end{aligned}$$

where $\tilde{p}_{cqf,d}\Big(\theta_{ds,d}, \tilde{B}_{su}(\theta_{sp})\Big)$ is the probability of downlink code acquisition failure, $\tilde{p}_{cqf,u}\Big(\theta_{ds,u}, \tilde{B}_{su}(\theta_{sp})\Big)$ is the probability of uplink code acquisition failure, $\tilde{N}_{er}\left(\theta_{jm}, \tilde{B}_{su}(\theta_{sp}), \overline{|B_{pu}|}\right)$ is the expected number of packet errors under optimized jamming, and $\tilde{B}_{su}(\theta_{sp})$ is the expected number of allowed bands under optimized spoofing. Note that from (4.32)

$$\tilde{B}_{su}(\theta_{sp}) \triangleq \min_{\sum_{i=1}^{N_T} P_{s,i} \le \frac{\theta_{sp}E_{adv}}{T_0}} E\left[|B_{al}|\right] = \frac{(N_T - \overline{|B_{pu}|})}{N_T}\left(N_T - F\left(p_{fd}, \frac{\theta_{sp}E_{adv}}{T_0}, N_T\right)\right) \qquad (5.30)$$

where F is defined in (C.15), and from (4.33)

$$\begin{aligned}\tilde{N}_{er}\left(\theta_{jm}, \tilde{B}_{su}(\theta_{sp}), \overline{|B_{pu}|}\right) &\triangleq \max_{\sum_{i=1}^{\tilde{B}_{su}(\theta_{sp})+\overline{|B_{pu}|}} P_{J,i} \le \frac{\theta_{jm}E_{adv}}{T_2}} E\left[\sum_{i\in B_{al}} N_{e,i}^{(u_j)}\right]\\ &= \frac{\tilde{B}_{su}(\theta_{sp})}{\tilde{B}_{su}(\theta_{sp}) + \overline{|B_{pu}|}} F\left(N_{e,i}, \frac{\theta_{jm}E_{adv}}{T_2}, \tilde{B}_{su}(\theta_{sp}) + \overline{|B_{pu}|}\right) \qquad (5.31)\end{aligned}$$

where θ_{jm} is the fraction of energy allocated for jamming. For uplink desynchronization, I use equal power allocation, because the optimization does not yield noticeable gains. Therefore, substituting the uplink desynchronizing power $P_{ds,u,i} = \frac{\theta_{ds,u}E_{adv}}{T_{1,u}N_T}$ in (5.25), I have

$$\tilde{p}_{cqf,u}\Big(\theta_{ds}, \tilde{B}_{su}(\theta_{sp})\Big) = \prod_{i=1}^{\min(\tilde{B}_{su}(\theta_{sp}), N_{acq,ul})} p_{cqf,lb,ul}^{(u_j)}\left(\frac{\theta_{ds,u}E_{adv}}{T_{1,u}N_T}\right). \qquad (5.32)$$

and from (4.34),

$$\tilde{p}_{cqf,d}\Big(\theta_{ds,d},\tilde{B}_{su}(\theta_{sp})\Big)=\prod_{i=1}^{\tilde{B}_{su}(\theta_{sp})}p^{(u_j)}_{cqf,lb,dl}\left(\frac{\theta_{ds,d}E_{adv}}{T_{1,d}N_T}\right). \tag{5.33}$$

Using (5.29), I find the optimal energy allocation ratios

$$\big(\theta^*_{sp},\theta^*_{ds,d},\theta^*_{ds,u}\big)=\underset{\theta_{sp}\in[0,\theta_{sp,\max}],\theta_{ds,d}\in[0,\theta_{sp,\max}],\theta_{ds,u}\in[0,\theta_{ds,u,\max}]}{\arg\min}\Gamma(\theta_{sp},\theta_{ds,d},\theta_{ds,u}) \tag{5.34}$$

from a numerical grid search, where $\theta_{sp,\max}=\min\Big(\frac{E_{adv}\rho_{fac}T_0}{T_0+T_{1,d}+T_{1,u}+T_2},1\Big)$, $\theta_{ds,d,\max}=\min\Big(\frac{E_{adv}\rho_{fac}T_{1,d}}{T_0+T_{1,d}+T_{1,u}+T_2},1\Big)$, $\theta_{ds,u,\max}=\min\Big(\frac{E_{adv}\rho_{fac}T_{1,u}}{T_0+T_{1,d}+T_{1,u}+T_2},1\Big)$ and ρ_{fac} is the ratio of maximum adversary power to average adversary power.

5.6 Simulation results

I consider a cluster-based SU system, sharing N_T DS-CDMA subcarriers with PUs. In the simulations, in each sensing, acquisition and transmission interval, the PUs occupy $|B_{pu}|=\min(N_{B,pu},N_T)$ bands at random, where $N_{B,pu}$ is a Poisson random variable with mean parameter $\bar{N}_{pu}$. I select $\bar{\alpha}_S=\bar{\alpha}_J=1,\sigma_v=0.01,\beta=0.25,T_0=4T_s,T_{1,d}=T_{1,u}=8T_s$ and $T_2=2048T_s$. The number of chips per symbol during a transmission interval (N_c) is 64, $N_c^{acq}=64$, $l_{acq}=4$ and $N_{acq,ul}=2$. I use Gold codes as spreading sequences, a rate $\frac{1}{2}$ LDPC code with code-block-length 2048 bits, and QPSK modulation. The target received SNR maintained (γ_S) is 7 dB.

Each user transmits the 'soccer' video sequence of 300 frames with 4CIF resolution (704×576) at 30 frames per second. The source video is compressed by the baseline profile of H.264/AVC reference software JM 11.0 [7]. The GOP structure is IPP with 15 frames per GOP. Each user starts at a random frame of the video, and the resource allocation decision is done at the start of each GOP. The video performance is evaluated using PSNR. $\triangleq 10\log_{10}\frac{255^2}{\mathbb{E}[\mathrm{MSE}]}$.

When there is no knowledge of the system other than its operating frequency range, the adversary can perform equal power attacks across the total bandwidth. I use this equal power spoofing and jamming strategy as a reference, to which the performance

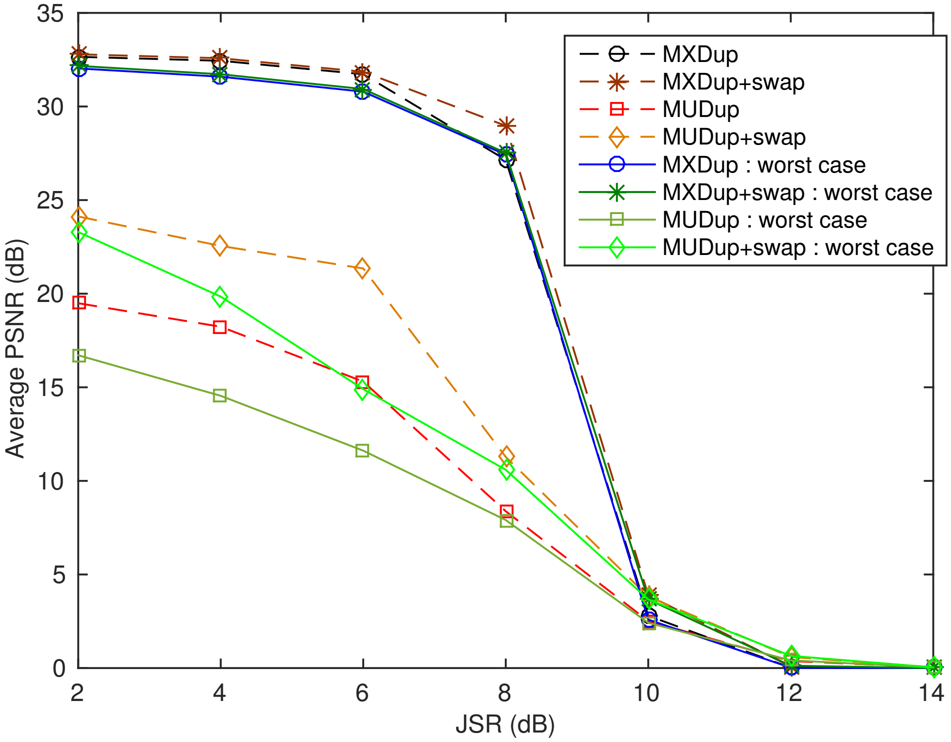


Figure 5.7: Average PSNR under spoofing attacks on the uplink ($N_T = 64$, $\Omega_{su} = 8$, $\bar{N}_{pu} = 16$)

of the optimized strategy is compared.

5.6.1 Spoofing attacks

Figure 5.7 shows the PSNR vs. JSR, for the resource allocation algorithms discussed in subsection 5.2.2. I plot the average PSNR under equal power spoofing (dashed curves) and optimized spoofing (solid curves). The optimal spoofing strategy, which I use here to evaluate the performance of the uplink resource algorithms under spoofing, was derived in Chapter 4.

The MXDup algorithms perform better than MUDup algorithms under the simulated parameters. While swapping improves the performance of MUDup, MXDup+swap does not have noticeable performance improvement over MXDup. Optimized spoofing only reduces the performance of MXDup algorithms by about 1 dB in the $2-6$ dB JSR range. In contrast, the performance of MUDup algorithms worsens by about 5 dB when

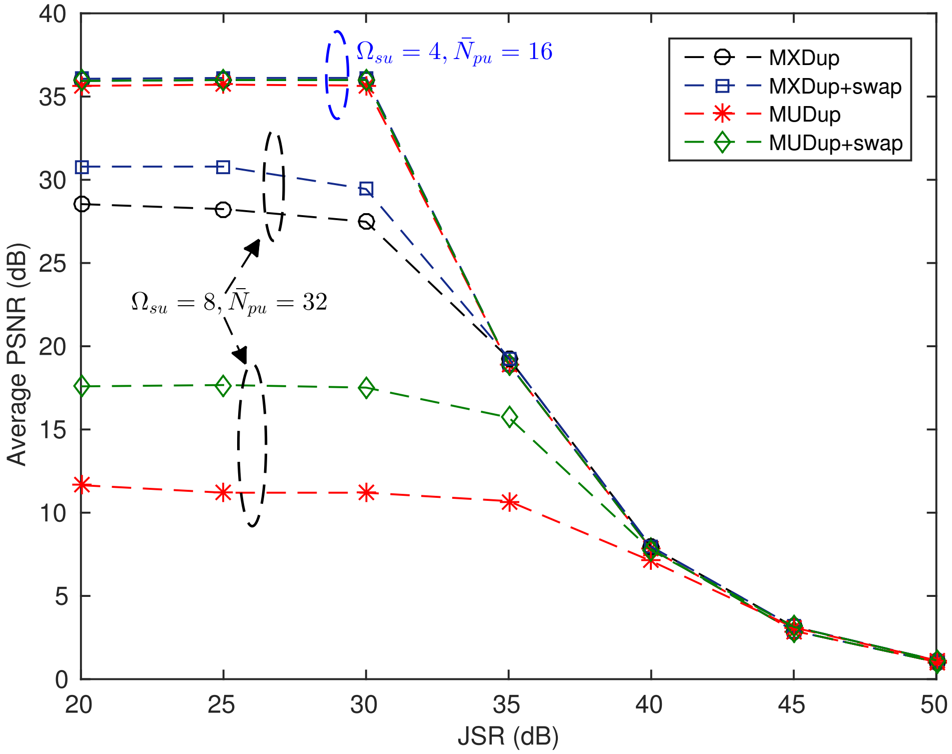


Figure 5.8: Average PSNR under desynchronizing attacks on the uplink ($N_T = 64$)

the spoofing attack is optimized around 6 dB JSR. The average PSNR under MXDup algorithms remains fairly constant up to about 6 dB JSR, and there is a steep drop in PSNR from 8-10 dB. I can conclude that the MXDup algorithms are able to reduce the performance degradation due to false detections at low JSRs, when compared to MUDup algorithms. The performance of the optimized spoofing attacks converges with equal power spoofing beyond 10 dB of JSR, as the optimal spoofing strategy becomes equal power spoofing, as concluded from the optimization approach.

5.6.2 Desynchronizing attacks

In Figure 5.8, I have the average PSNR under equal power desynchronizing attacks for both a lightly loaded system ($\Omega_{su} = 4$ and $\bar{N}_{pu} = 16$) and a heavily loaded system ($\Omega_{su} = 8$ and $\bar{N}_{pu} = 32$). The performances of the different resource allocation algorithms in the lightly loaded system are almost identical. In the heavily loaded sys-

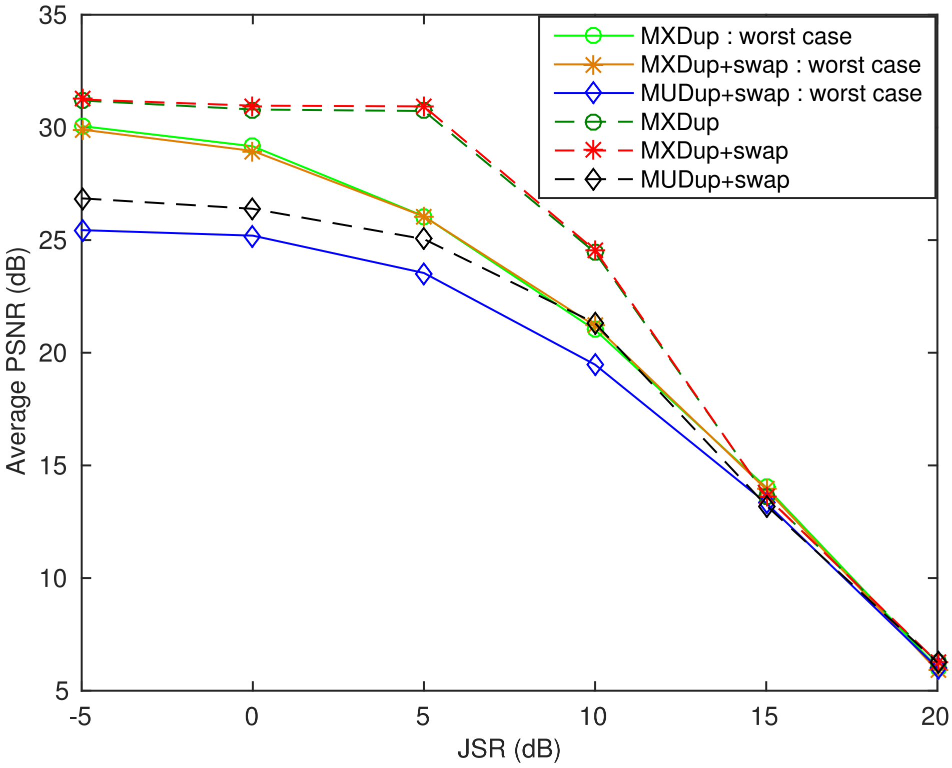


Figure 5.9: Average PSNR under jamming attacks ($N_T = 64$, $\Omega_{su} = 8$, $\bar{N}_{pu} = 16$, $\rho_{fac} = 100$)

tem, the MXDup algorithms perform significantly better with more than 10 dB higher average PSNR over MUDup algorithms in the JSR < 30 dB region.

5.6.3 Jamming attacks

Figure 5.9 shows the performance of the system under jamming attacks. The solid curves correspond to worst-case jamming and the dashed curves represent equal-power jamming. From the dashed curves I can see that the system is unaffected by equal-power jamming up to about 5 dB JSR. However, the reduction in PSNR in the solid curves in the -5 to 5 dB region shows that optimized jamming affects the system at a lower JSR compared to equal-power jamming. At JSR $= 5$ dB, the average PSNR for MXDup algorithms is about 5 dB lower under optimized jamming than under equal power jamming. The performance difference between MXDup and MUDup+swap diminishes as JSR increases. At high JSR, the performance is less dependent on the source rate, which is a result of the resource allocation algorithm, and influenced more by the packet error rate, which affects all transmissions equally.

5.6.4 Optimal energy allocation among attacking methods

In Figure 5.10, I plot the optimal percentage of energy allocation among the three methods of attack.

At low JSR ($<$ 15 dB), most of the energy is allocated for spoofing. As I use a strong FEC code, at low JSR, jamming attacks have a low probability of success. From Figure 5.8, I note that desynchronizing attacks are not effective at low JSR. From Figure 5.7, I can see that spoofing attacks successfully lower the PSNR even at low JSR. Therefore, at low JSR, spoofing is optimal. The fraction of energy allocated for spoofing is limited by ρ_{fac}, and the remaining energy is shared between jamming and uplink desynchronizing. I note that uplink desynchronizing appears to be more effective than downlink desynchronizing. For downlink code acquisition, the CH broadcasts a spreading sequence in all allowed bands, and for uplink code acquisition, each user broadcasts its spreading sequence in a subset of allowed bands. Increasing the number of transmitting bands can improve the code acquisition probability, by enabling the receiver to make a higher number of parallel detections. However, in the uplink, increasing the number of bands per user also increases the MAI, which degrades the code acquisition performance. Therefore, the number of bands over which the spreading sequence for code acquisition is transmitted by each user is generally higher on the downlink than on the uplink. Downlink code acquisition can be performed in parallel in more bands than the uplink code acquisition, and hence it is more difficult to successfully attack downlink code acquisition.

As JSR increases, the optimal energy allocation involves both spoofing and jamming. At high JSR, limiting the available bandwidth by spoofing, and attacking the resulting smaller number of available subcarriers by jamming, appears to be the best strategy. At high JSR, desynchronizing is not used, because the other two methods of attack are more effective.

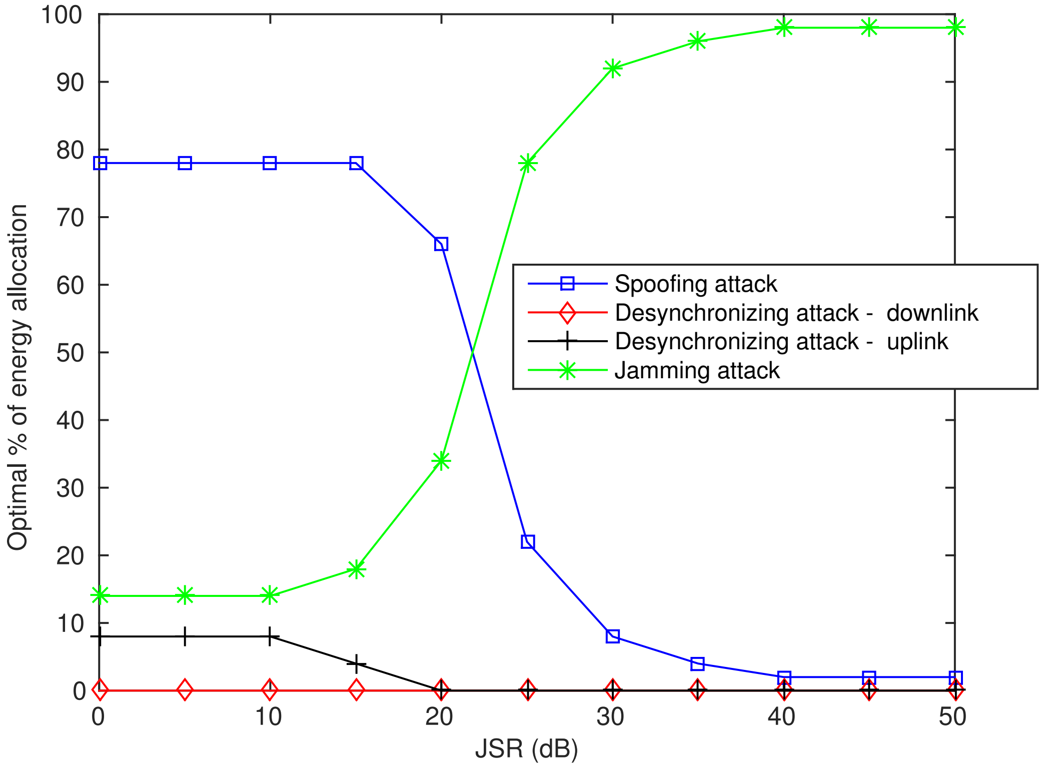


Figure 5.10: Optimal energy allocation among the methods of attack ($N_T = 64$, $\Omega_{su} = 8$, $\bar{N}_{pu} = 16$)

5.7 Conclusion

In this chapter, I evaluate an uplink CR video system under spoofing, desynchronizing and jamming attacks. I analyze the worst-case spoofing, desynchronizing and jamming power allocations across subcarriers, in a Rayleigh fading channel, with an optimization approach which enables a simplified calculation of the threshold JSRs that determine the optimal power allocation. I evaluated the performance of two types of resource allocation algorithms, and observed that the MXDup algorithm offers superior performance. I learned that it is optimal to allocate the largest portion of energy to spoofing in order to have the most noticeable impact on the received video distortion at low and medium JSR. Further, uplink desynchronizing attacks are more successful than downlink desynchronizing attacks at low JSR, and jamming is most effective at high JSR.

Chapter 5, in part, is a reprint of material as it may appear in M. Soysa, P. Cosman, and L. Milstein, “Video cognitive radio networks under disruptive attack,” manuscript under preparation. The dissertation author was the primary author of this paper.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

In this work, I investigated CR networks under disruptive attack. I looked at optimal energy allocations across subcarriers and among different modes of attack, that minimized SU throughput or maximized video distortion.

In Chapter 2, I analyzed the optimal spoofing and jamming power allocations across subcarriers, in a Rayleigh fading channel, with an optimization approach which enabled simplified calculation of threshold JSRs, below which partial-band attacks are optimal. I derived the optimal jamming power allocation based on a simplified step-function approximation of the word error rate of LDPC codes. Through comparisons of the throughput with optimal-spoofing and jamming power allocation with the throughput for equal-power spoofing and jamming, it can be observed that the optimization yields notable gains in the low and medium JSR regions. I learned that it is generally optimal to attack with both spoofing and jamming, whereby the optimal-energy allocation between the two methods of attack is dependent on system parameters and JSR. While successful spoofing has the most noticeable impact on SU throughput, it can be observed that when the system is not heavily loaded, spoofing is not effective at low JSR, and the optimal method of attack is jamming.

In Chapter 3, I analyzed the optimal spoofing power allocations across subcarriers in Nakagami-m fading channels, with the optimization approach proposed in Chapter 2. Through comparisons of the average number of false detections with optimal-spoofing power allocation, with that of equal-power spoofing, it can be observed that the optimization has notable gains in the low and medium INR regions. It can also be noted that optimal-spoofing power allocation has larger gains over equal-power spoofing for larger values of the fading parameter, m.

In Chapter 4, I analyzed the worst-case spoofing, desynchronizing and jamming power allocations across subcarriers which corresponded to the maximum video distortion, in a Rayleigh fading channel, with an optimization approach which enabled a simplified calculation of the threshold JSRs that determine the optimal power allocation. It can be noted that at low JSRs, optimizing spoofing and jamming gives the adversary a notable advantage. I evaluated the performance of two types of downlink resource allocation algorithms, and observed that the MXD algorithm offers superior performance. I learned that spoofing has the most noticeable impact on the received video distortion at low and medium JSR, with the exception of lightly loaded systems at low JSR, for which desynchronizing attacks cause the most increase in video distortion. Jamming is most effective at high JSR.

In Chapter 5, I examined the performance of a video cognitive radio system under disruptive attack, on the uplink. I analyzed the worst-case uplink desynchronizing attack and uplink jamming attack, accounting for MAI, using the optimization approach proposed in Appendix C. I evaluated the performance of two types of uplink resource allocation algorithms. I learned that it is optimal to allocate the largest portion of energy to spoofing in order to have the most noticeable impact on the received video distortion at low and medium JSR. Further, uplink desynchronizing attacks are more successful than downlink desynchronizing attacks at low JSR, and jamming is most effective at high JSR.

6.2 Future work

Based on the investigations in this dissertation, possible future work on disruptive attacks on video CR networks and system improvements in defense of such attacks is as follows:

- *Disruptive attacks on channel estimation process:* In this dissertation we did not consider the effects of the adversary on the channel estimation process, and how the adversary may optimally allocate power to disrupt the channel estimation. Channel estimation errors will reduce the benefits of the resource allocation, and also increase the symbol error rate. Therefore, investigating the effects of disruptive attacks on channel estimation, along with spoofing, desynchronizing and jamming attacks, will give more insights in to the performance of a CR network under attack.

- *Optimizing video encoder parameters to defend for spoofing and jamming attacks:* A smaller GOP size will increase the source rate, but will result in low error propagation. Under a jamming attack, a smaller GOP size could give better performance due to less error propagation. However, under spoofing attacks, the available bandwidth becomes the bottleneck, and higher compression efficiency becomes more important. Therefore, under spoofing attacks, a larger GOP size, which will result in a smaller source rate, will offer better performance. Optimizing video encoding parameters, such as the GOP size, in light of the adversary's strategy would be an interesting direction for future investigations. Further, studying the trade-off between source-coding rate and channel-coding rate, when under disruptive attacks, may yield useful insights.

- *SU system improvements to mitigate the impact of spoofing:* From the results of this work, it can be seen that SUs are most vulnerable to spoofing attacks, when compared with the other modes of attack. Therefore, strengthening the sensing subsystem, by investigating alternatives to energy detection for sensing, will be important for mitigating disruptive attacks on CR networks.

Appendix A: Optimization Approach

A.1 Theorem 1

Let $f : \mathbb{R}^+ \to \mathbb{R}^+$ be a function such that

P0: f is bounded above, i.e., $\exists M < \infty,$ s.t. $f(x) \leq M \; \forall x \in [0, \infty)$

P1: f is an increasing function, i.e., $f'(x) \geq 0$, where $f'(x)$ is the first derivative of $f(x)$,

P2: $f''(x) = 0$ has at most one root in $x > 0$, where $f''(x)$ is the second derivative of $f(x)$. Also, define $g : \mathbb{R}^+ \to \mathbb{R}$, as $g(x) \triangleq f(x) - f(0) - xf'(x)$. Then, if $\sum_{i=1}^{N} x_i \leq X_T$ and $x_i \geq 0$,

$$\sum_{i=1}^{N} f(x_i) \leq \begin{cases} Nf\left(\frac{X_T}{N}\right), & \text{if } \frac{X_T}{N} \geq x^* \\ (N - n^*) f(0) + n^* f(\frac{X_T}{n^*}), & \text{if } \frac{X_T}{N} < x^* \end{cases} \tag{A.1}$$

where $n^* = \frac{X_T}{x^*}$ and x^* is the largest root of $g(x) = 0$. Also, the set of arguments, S_x, that correspond to the equality when n^* is an integer, is given by

$$\begin{aligned} S_x &= \underset{\sum_{i=1}^{N} x_i = X_T,\, x_i \geq 0}{\arg\max} \left(\sum_{i=1}^{N} f(x_i) \right) \\ &= \begin{cases} \Big\{ \underbrace{\frac{X_T}{N}, \ldots, \frac{X_T}{N}}_{N \text{ elements}} \Big\}, & \text{if } \frac{X_T}{N} \geq x^* \\ \Big\{ \underbrace{\frac{X_T}{n^*}, \ldots, \frac{X_T}{n^*}}_{n^* \text{ elements}}, \underbrace{0, \ldots, 0}_{(N-n^*)} \Big\}, & \text{if } \frac{X_T}{N} < x^* \end{cases} \end{aligned} \tag{A.2}$$

When $\frac{X_T}{x^*}$ is not an integer, I use the approximation $n^* = \underset{n=\left\{\left\lfloor \frac{X_T}{x^*}\right\rfloor, \left\lceil \frac{X_T}{x^*}\right\rceil\right\}}{\arg\max} (N-n)\, f(0) + nf\left(\frac{X_T}{n}\right)$, to arrive at a suboptimal set S_x.

In optimizing power allocation for spoofing, $f(x)$ is the probability of false detection in one band as a function of the spoofing power allocated for that band. A false detection is mistakenly detecting a vacant band as being occupied by the PUs. In jamming, $f(x)$ is the packet error rate per user in a band, as a function of the jamming power allocated for that band. Geometrically, $g(x_t)$ is the difference between $f(0)$ and the y-intercept of the tangent to $f(x)$ at x_t.

A.2 Proof of Theorem 1

Case 1 : $\frac{X_T}{N} \geq x^*$

From Section A.3, Eq. (A.12), I know $f(x) \leq f\left(\frac{X_T}{N}\right) + (x - \frac{X_T}{N}) f'\left(\frac{X_T}{N}\right)$.

$$\begin{aligned} \therefore \sum_{i=1}^{N} f\left(\frac{X_T}{N}\right) &\leq \sum_{i=1}^{N}\left(f\left(\frac{X_T}{N}\right) + \left(x_i - \frac{X_T}{N}\right) f'\left(\frac{X_T}{N}\right)\right) \\ &= Nf\left(\frac{X_T}{N}\right) \end{aligned} \tag{A.3}$$

Case 2 : $0 \leq \frac{X_T}{N} < x^*$

From Section A.3, Eq. (A.13), I have $f(x) \leq f(0) + \frac{x_i}{x^*}(f(x^*) - f(0))$.

$$\therefore \sum_{i=1}^{N} f(x_i) \leq \sum_{i=1}^{N}\left(f(0) + \frac{x_i}{x^*}(f(x^*) - f(0))\right) = (N-n^*)f(0) + n^* f(x^*) \tag{A.4}$$

where $n^* = \frac{X^T}{x^*}$. From (A.3) and (A.4),

$$\sum_{i=1}^{N} f(x_i) \leq F(f, X_T, N) \triangleq \begin{cases} Nf\left(\frac{X_T}{N}\right), & \text{if } \bar{x} \geq x^* \\ (N-n^*)f(0) + n^* f(x^*), & \text{if } \bar{x} < x^* \end{cases} \tag{A.5}$$

Lemma 2: $g(x) = 0$ has at most one solution in $x > 0$

Proof of Lemma 2

Taking the derivative of $g(x) = f(x) - f(0) - xf'(x)$ with respect to x, I have $g'(x) = -xf''(x)$. From property **P2**, I know $f''(x) < 0\ \forall x > 0$ or $\exists x_0 > 0$ such that $f''(x) < 0$ for $x \in (x_0, \infty)$ and $f''(x) > 0$ for $x \in (0, x_0)$.

If $\forall x > 0\ f''(x) < 0$, then $g'(x) > 0$ and $g(x) > 0$ because $g(0) = 0$. Therefore, $g(x) = 0$ does not have any solutions in $x > 0$ and $x^* = 0$. If $f''(x) > 0$ for $0 < x < x_0$, then for $x \in (0, x_0)$, $g'(x) < 0$ and $g(x) < 0$. But, $\lim\limits_{x\to\infty} g(x) = \lim\limits_{x\to\infty} \big(f(x) - f(0) - xf'(x)\big) = \lim\limits_{x\to\infty} f(x) - f(0) - 0 > 0$, because $f(x)$ is an increasing function (**P1**) and $\lim\limits_{x\to\infty} xf'(x) = 0$ (see (A.7) below). Therefore, $g(x) = 0$ for some $x \in (x_0, \infty)$. Since $g'(x) > 0$ for $x \in (x_0, \infty)$, there is only one root.

Since I defined x^* is the largest root of $g(x) = 0$, from the above analysis I have

$$f''(x^*) < 0 \tag{A.6}$$

<u>Proof $\lim\limits_{x\to\infty} xf'(x) = 0$.</u>

I prove this by contradiction. Suppose $\lim\limits_{x\to\infty} xf'(x) \neq 0$. Because $xf'(x) \geq 0$, I have $\lim_{x\to\infty} xf'(x) > 0$. Since $f'(x)$ is decreasing in $x > x_0$, I know $xf'(x)$ does not have oscillations and $\exists L > 0, x_L > x_0$, s.t. $xf'(x) > L\ \forall\ x > x_L$.

$$\begin{aligned}
&\Rightarrow\ f'(x) > \frac{L}{x} \quad \forall x > x_L \\
&\Rightarrow\ \lim_{x_1\to\infty} \int_{x_L}^{x_1} f'(x)\mathrm{d}x > \lim_{x_1\to\infty} \int_{x_L}^{x_1} \frac{L}{x}\mathrm{d}x \\
&\Rightarrow\ \lim_{x_1\to\infty} (f(x_1) - f(x_L)) > \lim_{x_1\to\infty} L(\ln(x_1) - \ln(x_L)) \\
&\Rightarrow\ L < \frac{\lim_{x_1\to\infty}(f(x_1) - f(x_L))}{\lim_{x_1\to\infty}(\ln(x_1) - \ln(x_L))} = 0 \ \ (\because f(x) \text{ is finite, from property } \mathbf{P0}) \\
&\Rightarrow\ L < 0, \text{ but this is a contradiction.}
\end{aligned}$$

Therefore, I conclude that

$$\lim_{x\to\infty} xf'(x) = 0 \tag{A.7}$$

A.3 Proof of upper bounds to $f(x)$

Define $d_{x_0}(x) \triangleq f(x_0)+(x-x_0)f'(x_0)-f(x)$. Taking the derivative with respect to x, I obtain $d'_{x_0}(x) = f'(x_0) - f'(x)$ and

$$d''_{x_0}(x) = -f''(x) \tag{A.8}$$

From (A.6) and **P2**, I know $f''(x) < 0$ for $x \geq x^*$ and therefore, $d''_{x_0}(x) > 0$ for $x \geq x^*$.

Let $x_0 \geq x^*$. I have

$$d_{x_0}(x) \geq 0 \; \forall x > x_0 \quad (\because\; d_{x_0}(x_0) = 0,\; d'_{x_0}(x_0) = 0) \tag{A.9}$$

Further, from (A.8) and **P2**, I know $d''_{x_0}(x) = 0$ has at most one root in $(0, x_0]$. Therefore, $d'_{x_0}(x)$ has at most one root in $(0, x_0)$ because $d'_{x_0}(x_0) = 0$. Since $d''_{x_0}(x_0) > 0$, $\lim\limits_{x \to x_0^-} d'_{x_0}(x_0) = 0^-$. $\therefore$, $\exists\; x_1 \in [0, x_0)$ s.t. $d'_{x_0}(x) > 0 \; \forall x \in (0, x_1)$ and $d'_{x_0}(x) < 0 \; \forall x \in (x_1, x_0)$. From the definition of $d_{x0}(x)$, I have $d_{x_0}(0) = g(x_0)$ and from Appendix A, I know $g(x_0) > 0 \; \forall x_0 \geq x^*$.

$$\therefore\; d_{x_0}(x) \geq 0 \; \forall x \in [0, x_1] \tag{A.10}$$

Further,

$$d_{x_0}(x) \geq 0 \; \forall x \in (x_1, x_0] \tag{A.11}$$

because $d'_{x_0}(x) < 0 \; \forall x \in (x_1, x_0)$, $d_{x_0}(x_0) = 0$. From (A.9),(A.10) and (A.11), I know when $x_0 \geq x^*$, $d_{x_0}(x) \geq 0 \; \forall x \geq 0$. Therefore, when $\frac{X_T}{N_0} \geq x^*$, $d_{\frac{X_T}{N_0}}(x) \geq 0$, and

$$f(x) \leq f\left(\frac{X_T}{N}\right) + \left(x - \frac{X_T}{N}\right) f'\left(\frac{X_T}{N}\right) \tag{A.12}$$

Further, since $d_{x^*}(x) \geq 0$, $f(x) \leq f(x^*) + (x - x^*) f'(x^*)$. From the definition of x^*, $g(x^*) = f(x^*) - f(0) - x^* f'(x^*) = 0$, and $f'(x^*) = \frac{f(x^*)-f(0)}{x^*}$. Substituting this in (A.3), I have

$$\begin{aligned} f(x) &\leq f(x^*) + (x - x^*)\frac{(f(x^*) - f(0))}{x^*} \\ &= f(0) + \frac{x}{x^*}(f(x^*) - f(0)) \qquad \text{(A.13)} \end{aligned}$$

Appendix B: Derivations Supporting the Analysis in Subsection 2.4.3

B.1 Proof that $h_i'(x) \geq 0$

$$\begin{aligned} h_i'(x) = \frac{t_i e^{-t_i} \log_2 M_i}{(1+t_i x)^2} \Bigg\{ &\left((t_i\theta - t_i) \left(1 + \frac{1}{t_i x}\right) + 1 \right) e^{-\left((t_i\theta - t_i)\left(1+\frac{1}{t_i x}\right)\right)} \\ &- e^{-\left((t_{i+1}\theta - t_i)\left(1+\frac{1}{t_i x}\right)\right)} \left((t_{i+1}\theta - t_i) \left(1 + \frac{1}{t_i x}\right) + 1 \right) \Bigg\} \end{aligned} \tag{B.1}$$

Define $q_t(x) \triangleq (t_i\theta - t_i)\left(1 + \frac{1}{t_i x}\right)$ and $q_v(x) \triangleq (t_{i+1}\theta - t_i)\left(1 + \frac{1}{t_i x}\right)$. Note $q_v(x) > q_t(x) > 0$.

$$\begin{aligned} h_i'(x) &= \frac{t_i e^{-(t_i + q_v(x))}(q_t(x)+1)\log_2 M_i}{(1+t_i x)^2} \left(e^{(q_v(x) - q_t(x))} - \left(1 + \frac{q_v(x) - q_t(x)}{q_t(x)+1}\right)\right) \\ &> \frac{t_i e^{-(t_i + q_v(x))}(q_t(x)+1)\log_2 M_i}{(1+t_i x)^2} \left(e^{(q_v(x) - q_t(x))} - (1 + (q_v(x) - q_t(x)))\right) \\ &\geq 0 \end{aligned} \tag{B.2}$$

B.2 Proof that $\exists x^* \geq 0$ s.t. $\sum_{i=1}^{N_A} h_i''(x) < 0 \Leftrightarrow x > x^*$

$$h_i''(x) = \left(\frac{e^{-t_i}\log_2 M_i}{x^2(1+t_ix)^3}\right)\Big\{((t_i\theta - t_i)(1+t_ix)q_t(x) - 2t_i^2x^2(q_t(x)+1))e^{-q_t(x)} \tag{B.3}$$

$$- ((t_{i+1}\theta - t_i)(1+t_ix)q_v(x) - 2t_i^2x^2(q_v(x)+1))e^{-q_v(x)}\Big\}$$

$$\frac{t_ix^3e^{t_i}h_i''(x)}{\log_2 M_i} = \Big((t_i\theta - t_i)^2e^{-q_t(x)} - (t_{i+1}\theta - t_i)^2e^{-q_v(x)}\Big) \tag{B.4}$$

$$- \frac{2t_i^3x^3}{(1+t_ix)^3}\left\{\left(\frac{q_t^2(x)}{2} + q_t(x) + 1\right)e^{-q_t(x)} - \left(\frac{q_v^2(x)}{2} + q_v(x) + 1\right)e^{-q_v(x)}\right\}$$

Substituting $y = 1 + \frac{1}{t_ix}$, I can rewrite (B.4) as follows:

$$g_i(y) \triangleq \frac{t_ix^3e^{t_i}h_i''(x)}{\log_2 M_i} \tag{B.5}$$

$$= k_{t_i}^2e^{-k_{t_i}y} - k_{v_i}^2e^{-k_{v_i}y} - \frac{2}{y^3}\left[\left(\frac{k_{t_i}^2y^2}{2} + k_{t_i}y + 1\right)e^{-k_{t_i}y} - \left(\frac{k_{v_i}^2y^2}{2} + k_{v_i}y + 1\right)e^{-k_{v_i}y}\right]$$

where $k_{t_i} = t_i\theta - t_i$, $k_{v_i} = t_{i+1}\theta - t_i$ and $y = 1 + \frac{1}{t_ix} \in (1, \infty)$. I have $k_{v_i} - k_{t_i} = (t_{i+1} - t_i)\theta > 0$. Further $k_{t_i} = t_i(\theta - 1) > 0$. Therefore, I have $k_{v_i} > k_{t_i} > 0$. Further, $g_i'(y) = -k_{t_i}^3e^{-k_{t_i}y} + k_{v_i}^3e^{-k_{v_i}y} + \frac{6}{y^4}\left[\left(\frac{k_{t_i}^3y^3}{6} + \frac{k_{t_i}^2y^2}{2} + k_{t_i}y + 1\right)e^{-k_{t_i}y} - \left(\frac{k_{v_i}^3y^3}{6} + \frac{k_{v_i}^2y^2}{2} + k_{v_i}y + 1\right)e^{-k_{v_i}y}\right]$. I have

$$g_i'(y) = \frac{\mathrm{d}}{\mathrm{d}y}g_i(y)$$

$$= -k_{t_i}^3e^{-k_{t_i}y} + k_{v_i}^3e^{-k_{v_i}y} + \frac{6}{y^4} \tag{B.6}$$

$$\times\left[\left(\frac{k_{t_i}^3y^3}{6} + \frac{k_{t_i}^2y^2}{2} + k_{t_i}y + 1\right)e^{-k_{t_i}y} - \left(\frac{k_{v_i}^3y^3}{6} + \frac{k_{v_i}^2y^2}{2} + k_{v_i}y + 1\right)e^{-k_{v_i}y}\right]$$

because $k_{v_i} > k_{t_i} > 0$ and $y > 1$. Further,

$$\begin{aligned} g_i(1) &= -2[(k_{t_i}+1)e^{-k_{t_i}} - (k_{v_i}+1)e^{-k_{v_i}}] \\ &= -2(k_{t_i}+1)e^{-k_{v_i}} \left(e^{(k_{v_i}-k_{t_i})} - \left(1 + \frac{k_{v_i}-k_{t_i}}{1+k_{t_i}}\right)\right) \\ &< -2(k_{t_i}+1)e^{-k_{v_i}} \left(e^{(k_{v_i}-k_{t_i})} - (1 + (k_{v_i}-k_{t_i}))\right) \\ &< 0 \end{aligned} \tag{B.7}$$

because $k_{v_i} > k_{t_i} > 0$, and

$$\begin{aligned} \lim_{y\to\infty} g_i(y) &= \lim_{y\to\infty} k_{t_i}^2 e^{-k_{t_i}y} - k_{v_i}^2 e^{-k_{v_i}y} - \frac{2}{y^3} \\ &\quad \times \left[\left(\frac{k_{t_i}^2 y^2}{2} + k_{t_i}y + 1 \right) e^{-k_{t_i}y} - \left(\frac{k_{v_i}^2 y^2}{2} + k_{v_i}y + 1 \right) e^{-k_{v_i}y} \right] \\ &= \lim_{y\to\infty} k_{t_i}^2 e^{-k_{t_i}y} - k_{v_i}^2 e^{-k_{v_i}y} \\ &= 0^+ \end{aligned} \tag{B.8}$$

because $k_{t_i}^2 e^{-k_{t_i}y} - k_{v_i}^2 e^{-k_{v_i}y} > 0 \Leftrightarrow y > \frac{2\ln\left(\frac{k_{v_i}}{k_{t_i}}\right)}{k_{v_i}-k_{t_i}}$ from (B.15) in Subsection B.2.1.

I need to show that $\sum_{i=1}^{N_A} h_i''(x)$ has only one zero for $x \in (0,\infty)$ and goes from positive to negative with increasing x. From (B.5),

$$\begin{aligned} \sum_{i=1}^{N_A} h_i''(x) < 0 &\Leftrightarrow \sum_{i=1}^{N_A} \frac{\log_2 M_i g_i\left(1+\frac{1}{t_i x}\right)}{t_i x^3 e^{t_i}} < 0 \\ &\Leftrightarrow \sum_{i=1}^{N_A} \frac{g_i(y_i)\log_2 M_i}{t_i e^{t_i}} < 0, \end{aligned} \tag{B.9}$$

where $y_i = 1 + \frac{1}{t_i x}$. Define

$$G(y_1) \triangleq \sum_{i=1}^{N_A} \frac{g_i(y_i)\log_2 M_i}{t_i e^{t_i}} \tag{B.10}$$

where y_i= $1+\frac{1}{t_i x} = \frac{t_1}{t_i}y_1 + 1 - \frac{t_1}{t_i}$. Therefore, I have $\frac{\mathrm{d}}{\mathrm{d}y_1}y_i = \frac{t_1}{t_i}$ and $k_{t_i} = (\theta-1)t_i = \left(\frac{t_i}{t_1}\right)k_{t_1}$.

$$\begin{aligned}
G'(y_1) &= \frac{\mathrm{d}}{\mathrm{d}y_1}\sum_{i=1}^{N_A}\frac{g_i\left(y_i\right)\log_2 M_i}{t_i e^{t_i}} \\
&= \sum_{i=1}^{N_A}\frac{g_i'\left(y_i\right)\log_2 M_i}{t_i e^{t_i}}\frac{\mathrm{d}y_i}{\mathrm{d}y_1} \\
&= \sum_{i=1}^{N_A}\frac{g_i'\left(y_i\right)\log_2 M_i}{t_i e^{t_i}}\left(\frac{t_1}{t_i}\right) \\
&> \sum_{i=1}^{N_A}\frac{-k_{t_i}g_i\left(y_i\right)\log_2 M_i}{t_i e^{t_i}}\left(\frac{t_1}{t_i}\right) \\
&= -k_{t_1}\sum_{i=1}^{N_A}\frac{g_i\left(y_i\right)\log_2 M_i}{t_i e^{t_i}} \\
&= -k_{t_i}G(y_1) \qquad \text{(B.11)}
\end{aligned}$$

Further, because $y_1 = 1 \Rightarrow y_i = 1$ and $g_i(1) < 0$ from (B.7), I have

$$G(1) = \sum_{i=1}^{N_A}\frac{g_i\left(1\right)\log_2 M_i}{t_i e^{t_i}} < 0 \qquad \text{(B.12)}$$

and because $y_1 \to \infty \Rightarrow y_i \to \infty$ and $\lim_{y_i\to\infty} g_i\left(y_i\right) = 0^+$ from (B.8), I have

$$\begin{aligned}
\lim_{y_1\to\infty} G(y_1) &= \lim_{y_1\to\infty}\sum_{i=1}^{N_A}\frac{g_i\left(y_i\right)\log_2 M_i}{t_i e^{t_i}} \\
&= \sum_{i=1}^{N_A}\frac{\lim_{y_i\to\infty} g_i\left(y_i\right)\log_2 M_i}{t_i e^{t_i}} = 0^+ \qquad \text{(B.13)}
\end{aligned}$$

From (B.12) and (B.13), I know $G(y_1) = 0$ has at least one finite solution in $y_1 \in (1,\infty)$. From (B.11) I know at a root of $G(y_1) = 0$, $G'(y_1) > 0$, i.e., at the roots the function is increasing, and therefore, must go from negative to positive. Hence, there can be only one solution for $G(y_1) = 0$. Define y_1^*, s.t. $G(y_1^*) = 0$. From (B.12) it follows that, $G(y_1) < 0 \Leftrightarrow y_1 < y_1^*$. Define $x^* \triangleq \frac{1}{t_1(y_1^*-1)}$. Therefore, $y_1 < y_1^* \Leftrightarrow x > x^*$ and

$G(y_1) < 0 \Leftrightarrow \sum_{i=1}^{N_A} h_i''(x) < 0$ from (B.9).

$$\therefore \sum_{i=1}^{N_A} h_i''(x) < 0 \Leftrightarrow x > x^* \tag{B.14}$$

B.2.1 Proof that $\exists y^* > 0$ s.t. $k_{t_i}^n e^{-k_{t_i} y} - k_{v_i}^n e^{-k_{v_i} y} < 0 \Leftrightarrow y < y^*$

Define $Q_n^{(i)} : \Re^+ \to \Re$, $Q_n^{(i)}(y) \triangleq k_{t_i}^n e^{-k_{t_i} y} - k_{v_i}^n e^{-k_{v_i} y}$, where $0 < k_{t_i} < k_{v_i}$ are constants. Note that $Q_n^{(i)}(0) = k_{t_i}^n - k_{v_i}^n < 0$, because $k_{t_i} < k_{v_i}$. Further, $Q_n^{(i)}(y) = 0 \Leftrightarrow k_{t_i}^n e^{-k_{t_i} y} - k_{v_i}^n e^{-k_{v_i} y} = 0 \Leftrightarrow e^{(k_{v_i} - k_{t_i}) y} = \frac{k_{v_i}^n}{k_{t_i}^n} \Leftrightarrow y = \frac{n \ln\left(\frac{k_{v_i}}{k_{t_i}}\right)}{k_{v_i} - k_{t_i}}$, i.e., $Q_n^{(i)}(y) = 0$ has exactly one solution at $y = \frac{n \ln\left(\frac{k_{v_i}}{k_{t_i}}\right)}{k_{v_i} - k_{t_i}} \in (0, \infty)$. Therefore,

$$Q_n^{(i)}(y) < 0 \Leftrightarrow y < \frac{n \ln\left(\frac{k_{v_i}}{k_{t_i}}\right)}{k_{v_i} - k_{t_i}} \tag{B.15}$$

Appendix C: Generalized Optimization Approach

C.1 Theorem 2

Let $f : \mathbb{R}^+ \cup \{0\} \rightarrow \mathbb{R}^+ \cup \{0\}$ be a function such that

P0: f is bounded above, i.e., $\exists M < \infty,$ s.t. $f(x) \leq M \; \forall x \in [0, \infty)$.

P3: $f'(x) \geq 0$ and $f'(x)$ is differentiable over $x \in [0, \infty)$, where $f'(x)$ is the first derivative of $f(x)$.

Then, if $0 \leq \sum_{i=1}^{N} \tilde{x}_i \leq X_T$, $\tilde{x}_i \geq 0$ and $X_T > 0$,

$$\sum_{i=1}^{N} f(\tilde{x}_i) \leq \begin{cases} \left(N - \frac{X_T}{x_0}\right) f(0) + \frac{X_T}{x_0} f(x_0), & \text{if } \frac{X_T}{N} \leq x_0 \\ Nf\left(\frac{X_T}{N}\right), & \text{if } x_{j-1} < \frac{X_T}{N} < y_j, \; j = 1, 2, \ldots, N_r \\ \frac{X_T - Ny_j}{x_j - y_j} f(x_j) + \frac{Nx_j - X_T}{x_j - y_j} f(y_j), & \text{if } y_j \leq \frac{X_T}{N} \leq x_j, \; j = 1, 2, \ldots, N_r \\ Nf\left(\frac{X_T}{N}\right), & \text{if } x_{N_r} < \frac{X_T}{N} \end{cases} \tag{C.1}$$

I have defined x_js and y_js in the discussion below.

<u>Definition of x_0</u>

Let

$$g_0(x) \triangleq \begin{cases} \min\limits_{t \geq 0} \Big(f(0) + \frac{(f(x) - f(0))t}{x} - f(t) \Big) & x > 0 \\ \min\limits_{t \geq 0} \Big(f(0) + f'(0)t - f(t) \Big) & x = 0 \end{cases} \tag{C.2}$$

Define x_0 as the largest root of $g_0(x) = 0$. The existence of a root of g_0 is proved in Section C.7.

```
procedure OPTPARAM ($f,\ f',\ g,\ x_0$)
    $j \leftarrow 0$
    while $\{y|g(y) = 0, y > x_j\} \neq \{\}$ do
        $j \leftarrow j + 1$
        $y_j \leftarrow \min\{y|g(y) = 0, y > x_{j-1}\}$
        $x_j \leftarrow \max\{t|f(y_j) + (t - y_j)f'(y_j) - f(t) = 0\}$
    end while
    $N_r \leftarrow j$
    return $\{y_j|j = 1, 2, \ldots, N_r\},\ \{x_j|j = 0, 1, \ldots, N_r\},\ N_r$
end procedure
```

Figure 6.1: Algorithm to obtain x_js and y_js

Definition of y_js, and x_js for $j = 1, 2, \ldots, N_r$

Define the function $l_y(t)$ as follows:

$$l_y(t) \triangleq f(y) + (t - y)f'(y). \tag{C.3}$$

where $y \in [0, \infty)$ and $t \in [0, \infty)$. Define the function $g : \mathbb{R}^+ \cup \{0\} \to \mathbb{R}$ as follows:

$$g(y) \triangleq \min_{t>y}\Big(l_y(t) - f(t)\Big) \tag{C.4}$$

where $y \in [0, \infty)$ (according to the function domain) and $t \in (0, \infty)$. Define

$$y_j \triangleq \min\{y|g(y) = 0, y > x_{j-1}\} \tag{C.5}$$

and

$$x_j \triangleq \max\{t|l_{y_j}(t) - f(t) = 0\} \tag{C.6}$$

where $j = 1, 2, \ldots, N_r$, and N_r is the number of all pairs (y_j, x_j).

I can obtain x_js and y_js from the algorithm shown in Fig.6.1. Here I calculate (y_j, x_j) pairs iteratively, for $j = 1, 2, \ldots, N_r$. First I calculate x_0 from (C.2). Then, I use x_0 in (C.5) to calculate y_1. I use this y_1 to find x_1, using (C.6). Now I can use x_1 to calculate y_2, and so on.

From the definition of y_j in (C.5), $g(y_j) = \min_{t>y_j}\big(l_{y_j}(t) - f(t)\big) = 0$. From the definition in (C.6), x_j is the maximum t value at which $\big(l_{y_j}(t) - f(t)\big) = 0$. Because the range considered here in $g(y_j)$ is $t > y_j$, I see that $x_j > y_j$. In the definition of y_j in (C.5), I have restricted the range of y to $y > x_{j-1}$, hence $y_j > x_{j-1}$. Therefore, I have $x_{j-1} < y_j < x_j$, which is consistent with the interval ranges in (C.1).

As can be seen from the algorithm in Fig.6.1, $\{y|g(y) = 0, y > x_{N_r}\}$ will be the empty set; i.e., when I iteratively attempt finding (y_j, x_j)s, I will stop after (y_{N_r}, x_{N_r}), because $\{y|g(y) = 0, y > x_{N_r}\}$ does not yield any solutions.

$N_r \in \mathbb{Z}^+ \cup \{0\}$, and $N_r = 0$ implies that there are no (y_j, x_j) pairs. When $N_r = 0$, (C.1) reduces to

$$\sum_{i=1}^{N} f(\tilde{x}_i) \leq \begin{cases} \left(N - \frac{X_T}{x_0}\right) f(0) + \frac{X_T}{x_0} f(x_0), & \text{if } \frac{X_T}{N} \leq x_0 \\ Nf\left(\frac{X_T}{N}\right), & \text{if } x_0 < \frac{X_T}{N} \end{cases} \tag{C.7}$$

C.2 Proof of Theorem 2

I consider the different ranges of $\frac{X_T}{N}$ separately in 4 cases in the proof below.

Case 1

$\frac{X_T}{N} \leq x_0$

Since $X_T > 0$, and $\frac{X_T}{N} \leq x_0$, I have $x_0 > 0$. Therefore, from the definition of x_0, I have $g_0(x_0) = 0$. From (C.2),

$$g_0(x_0) = \min_{t \geq 0}\Big(f(0) + \frac{(f(x_0) - f(0))t}{x_0} - f(t)\Big) = 0 \tag{C.8}$$

Therefore, I know that, $\forall\, t \geq 0$,

$$f(0) + \frac{f(x_0) - f(0)}{x_0} t - f(t) \geq 0 \tag{C.9}$$

Hence,

$$\begin{aligned}
\sum_{i=0}^{N} f(\tilde{x}_i) &\leq \sum_{i=0}^{N} \left[f(0) + \frac{f(x_0) - f(0)}{x_0} \tilde{x}_i \right] \qquad \text{(from (C.9))} \\
&= Nf(0) + \frac{f(x_0) - f(0)}{x_0} \sum_{i=0}^{N} \tilde{x}_i \\
&\leq Nf(0) + \frac{f(x_0) - f(0)}{x_0} X_T \qquad (\text{ because } \sum_{i=1}^{N} \tilde{x}_j \leq X_T) \\
&= \left(N - \frac{X_T}{x_0} \right) f(0) + \frac{X_T}{x_0} f(x_0) \qquad \text{(C.10)}
\end{aligned}$$

Case 2

$x_{j-1} < \frac{X_T}{N} < y_j, \; j = 1, 2, \ldots, N_r$

From Eq. (C.55) in Section C.5, I know $l_{\frac{X_T}{N}}(t) \geq f(t), \; \forall \, t \geq 0$.

$$\begin{aligned}
\sum_{i=0}^{N} f(\tilde{x}_i) &\leq \sum_{i=0}^{N} l_{\frac{X_T}{N}}(\tilde{x}_i) \\
&= \sum_{i=0}^{N} \left[f\left(\frac{X_T}{N}\right) + \left(\tilde{x}_i - \frac{X_T}{N}\right) f'\left(\frac{X_T}{N}\right) \right] \\
&= Nf\left(\frac{X_T}{N}\right) + \left(\sum_{i=0}^{N} \tilde{x}_i - N \times \frac{X_T}{N} \right) f'\left(\frac{X_T}{N}\right) \\
&\leq Nf\left(\frac{X_T}{N}\right) + (X_T - X_T) f'\left(\frac{X_T}{N}\right) \qquad (\text{ because } \sum_{i=1}^{N} \tilde{x}_j \leq X_T) \\
&= Nf\left(\frac{X_T}{N}\right) \qquad \text{(C.11)}
\end{aligned}$$

Case 3

$y_j \leq \frac{X_T}{N} \leq x_j$.

Note that by definition in (C.6), I have

$$\begin{aligned}
l_{y_j}(x_j) - f(x_j) = f(y_j) + (x_j - y_j) f'(y_j) - f(x_j) = 0 \\
f'(y_j) = \frac{f(x_j) - f(y_j)}{x_j - y_j} \qquad \text{(C.12)}
\end{aligned}$$

From Eq. (C.55) in Section C.5, I know $\forall\, t \geq 0$, $l_{y_j}(t) \geq f(t)$.

$$\begin{aligned}
\sum_{i=1}^{N} f(\tilde{x}_i) &\leq \sum_{i=1}^{N} l_{y_j}(\tilde{x}_i) \\
&= \sum_{i=1}^{N} f(y_j) + (\tilde{x}_i - y_j) f'(y_j) \\
&= N f(y_j) + \left(\sum_{i=1}^{N} \tilde{x}_i - N y_j \right) f'(y_j) \\
&\leq N f(y_j) + (X_T - N y_j)\, f'(y_j) \quad (\text{ because } \sum_{i=1}^{N} \tilde{x}_j \leq X_T) \\
&= N f(y_j) + (X_T - N y_j) \frac{f(x_j) - f(y_j)}{x_j - y_j} \quad (\text{from (C.12)}) \\
&= \frac{N(x_j - y_j) - (X_T - N y_j)}{x_j - y_j} f(y_j) + \frac{X_T - N y_j}{x_j - y_j} f(x_j) \\
&= \frac{N x_j - X_T}{x_j - y_j} f(y_j) + \frac{X_T - N y_j}{x_j - y_j} f(x_j) \qquad \text{(C.13)}
\end{aligned}$$

Case 4

$x_{N_r} < \frac{X_T}{N}$

From Section C.6, I know $l_{\frac{X_T}{N}}(t) \geq f(t)$, $\forall\, t \geq 0$, for $x_{N_r} < \frac{X_T}{N}$.

$$\begin{aligned}
\sum_{i=0}^{N} f(\tilde{x}_i) &\leq \sum_{i=0}^{N} l_{\frac{X_T}{N}}(\tilde{x}_i) \\
&= \sum_{i=0}^{N} \left[f\left(\frac{X_T}{N}\right) + \left(\tilde{x}_i - \frac{X_T}{N}\right) f'\left(\frac{X_T}{N}\right) \right] \\
&= N f\left(\frac{X_T}{N}\right) + \left(\sum_{i=0}^{N} \tilde{x}_i - N \times \frac{X_T}{N} \right) f'\left(\frac{X_T}{N}\right) \\
&\leq N f\left(\frac{X_T}{N}\right) + (X_T - X_T)\, f'\left(\frac{X_T}{N}\right) \quad (\text{ because } \sum_{i=1}^{N} \tilde{x}_j \leq X_T) \\
&= N f\left(\frac{X_T}{N}\right) \qquad \text{(C.14)}
\end{aligned}$$

From (C.10), (C.11), (C.13) and (C.14), I have

$$\sum_{i=1}^{N} f(\tilde{x}_i) \leq F(f, X_T, N)$$

$$\triangleq \begin{cases} \left(N - \frac{X_T}{x_0}\right) f(0) + \frac{X_T}{x_0} f(x_0), & \text{if } \frac{X_T}{N} \leq x_0 \\ Nf\left(\frac{X_T}{N}\right), & \text{if } x_{j-1} < \frac{X_T}{N} < y_j,\ j = 1, 2, \ldots, N_r \\ \frac{X_T - Ny_j}{x_j - y_j} f(x_j) + \frac{Nx_j - X_T}{x_j - y_j} f(y_j), & \text{if } y_j \leq \frac{X_T}{N} \leq x_j,\ j = 1, 2, \ldots, N_r \\ Nf\left(\frac{X_T}{N}\right), & \text{if } x_{N_r} < \frac{X_T}{N} \end{cases} \tag{C.15}$$

C.3 Proof that $g(x_j) > 0,\ j = 0, 1, \ldots, N_r$

Proof that $g(x_0) > 0$, for $x_0 > 0$

From (C.9), I have

$$f(0) + \frac{f(x_0) - f(0)}{x_0} t - f(t) \geq 0,\ \forall t > 0 \tag{C.16}$$

Select $\delta > 0$, such that $x_0 - \delta > 0$ (*Note that* $x_0 > 0$). Substituting $t = x_0 \pm \delta$, I get

$$f(0) + \frac{f(x_0) - f(0)}{x_0}(x_0 \pm \delta) - f(x_0 \pm \delta) \geq 0$$

$$f(0) + \Big(f(x_0) - f(0)\Big)\left(1 \pm \frac{\delta}{x_0}\right) - f(x_0 \pm \delta) \geq 0 \tag{C.17}$$

Using Taylor's theorem in the Lagrange remainder form, I can write

$$f(x_0 + \delta) = f(x_0) + \delta f'(x_0) + \frac{\delta^2}{2} f''(x_1^*) \tag{C.18}$$

$$f(x_0 - \delta) = f(x_0) - \delta f'(x_0) + \frac{\delta^2}{2} f''(x_2^*) \tag{C.19}$$

where $x_1^* \in (x_0, x_0 + \delta)$ and $x_2^* \in (x_0 - \delta, x_0)$. Using (C.18) in (C.17), I have

$$\begin{aligned}
f(0) + \Big(f(x_0) - f(0)\Big)\left(1 + \frac{\delta}{x_0}\right) - \Big(f(x_0) + \delta f'(x_0) + \frac{\delta^2}{2} f''(x_1^*)\Big) &\geq 0 \\
\frac{\delta}{x_0}\Big(f(x_0) - f(0)\Big) - \delta f'(x_0) - \frac{\delta^2}{2} f''(x_1^*) &\geq 0 \\
\delta\Big(\frac{f(x_0) - f(0)}{x_0} - f'(x_0)\Big) - \frac{\delta^2}{2} f''(x_1^*) &\geq 0 \\
\Big(\frac{f(x_0) - f(0)}{x_0} - f'(x_0)\Big) - \frac{\delta}{2} f''(x_1^*) &\geq 0 \\
\Big(\frac{f(x_0) - f(0)}{x_0} - f'(x_0)\Big) &\geq \frac{\delta}{2} f''(x_1^*) \quad \text{(C.20)}
\end{aligned}$$

Using (C.19) in (C.17), I have

$$\begin{aligned}
f(0) + \Big(f(x_0) - f(0)\Big)\left(1 - \frac{\delta}{x_0}\right) - \Big(f(x_0) - \delta f'(x_0) + \frac{\delta^2}{2} f''(x_2^*)\Big) &\geq 0 \\
-\frac{\delta}{x_0}\Big(f(x_0) - f(0)\Big) + \delta f'(x_0) - \frac{\delta^2}{2} f''(x_2^*) &\geq 0 \\
-\delta\Big(\frac{f(x_0) - f(0)}{x_0} - f'(x_0)\Big) - \frac{\delta^2}{2} f''(x_2^*) &\geq 0 \\
-\Big(\frac{f(x_0) - f(0)}{x_0} - f'(x_0)\Big) - \frac{\delta}{2} f''(x_2^*) &\geq 0 \\
-\Big(\frac{f(x_0) - f(0)}{x_0} - f'(x_0)\Big) &\geq \frac{\delta}{2} f''(x_2^*) \quad \text{(C.21)}
\end{aligned}$$

For both the inequalities in (C.20) and (C.21) to hold for any small δ, $\frac{f(x_0)-f(0)}{x_0} - f'(x_0) = 0$. I prove this by contradiction.
Assume $\frac{f(x_0)-f(0)}{x_0} - f'(x_0) \neq 0$. Define $\mu \triangleq \frac{f(x_0)-f(0)}{x_0} - f'(x_0) \neq 0$. Define M as:

$$M \triangleq \max_{x \in (x_0 - \delta, x_0 + \delta)} |f''(x)|. \quad \text{(C.22)}$$

Because $f'(x)$ is differentiable in $x \in [0, \infty)$, M is finite.

From the definition of M, I have

$$f''(x_1^*) \geq -M \ \text{ and } f''(x_2^*) \geq -M \quad \text{(C.23)}$$

because $x_1^* \in (x_0, x_0 + \delta)$ and $x_2^* \in (x_0 - \delta, x_0)$ by definition in (C.18) and (C.19).
Case 1: $M = 0$

From (C.20) and (C.23), I have

$$\Big(\frac{f(x_0)-f(0)}{x_0}-f'(x_0)\Big)\geq\frac{\delta}{2}f''(x_1^*)\geq 0\ \ \text{(from (C.23))}\tag{C.24}$$

From (C.21) and (C.23), I have

$$-\Big(\frac{f(x_0)-f(0)}{x_0}-f'(x_0)\Big)\geq\frac{\delta}{2}f''(x_2^*)\geq 0\ \ \text{(from (C.23))}\tag{C.25}$$

This is in contradiction with (C.24). Therefore, our assumption that $\frac{f(x_0)-f(0)}{x_0}-f'(x_0)\neq 0$ is incorrect. Hence, $\frac{f(x_0)-f(0)}{x_0}-f'(x_0)=0$.

Case 2: $M\neq 0$

By definition in (C.22), $M>0$. Select a new $\tilde{\delta}\triangleq\min\Big(\frac{|\mu|}{M},\delta\Big)$.

Case 2a: $\tilde{\delta}=\delta$

That is, $\delta\leq\frac{|\mu|}{M}$.

$$\begin{aligned}\frac{\delta}{2}f''(x_1^*)&\geq-\frac{\delta}{2}M\ \ \text{(from (C.23))}\\&\geq-\frac{|\mu|}{2M}M\ \ (\text{because } 0<\delta\leq\frac{|\mu|}{M})\\&=-\frac{|\mu|}{2}\end{aligned}\tag{C.26}$$

From (C.20) and (C.26), I have

$$\begin{aligned}\Big(\frac{f(x_0)-f(0)}{x_0}-f'(x_0)\Big)\geq\frac{\delta}{2}f''(x_1^*)&\geq-\frac{|\mu|}{2}\\ \mu&\geq-\frac{|\mu|}{2}\ \ (\text{because }\frac{f(x_0)-f(0)}{x_0}-f'(x_0)=\mu\neq 0)\\ \Rightarrow\mu&>0\end{aligned}\tag{C.27}$$

From (C.23), I also have

$$\begin{aligned}\frac{\delta}{2}f''(x_2^*)&\geq-\frac{\delta}{2}M\\&\geq-\frac{|\mu|}{2M}M\ \ (\text{because } 0<\delta\leq\frac{|\mu|}{M})\\&=-\frac{|\mu|}{2}\end{aligned}\tag{C.28}$$

From (C.21) and (C.28), I have

$$\begin{aligned}
-\Big(\frac{f(x_0)-f(0)}{x_0} - f'(x_0)\Big) \geq \frac{\delta}{2} f''(x_2^*) \geq -\frac{|\mu|}{2} & \\
-\mu \geq -\frac{|\mu|}{2} \ \ \text{(because } \frac{f(x_0)-f(0)}{x_0} - f'(x_0) = \mu \neq 0) & \\
\Rightarrow \mu < 0 & \qquad \text{(C.29)}
\end{aligned}$$

This is in contradiction with (C.27). Therefore, our assumption that $\frac{f(x_0)-f(0)}{x_0} - f'(x_0) \neq 0$ is incorrect. Hence, $\frac{f(x_0)-f(0)}{x_0} - f'(x_0) = 0$.

Case 2b: $\tilde{\delta} = \frac{|\mu|}{M}$

That is, $\tilde{\delta} \leq \delta$. Rewriting (C.20) and (C.21) for $\tilde{\delta}$, I have

$$\Big(\frac{f(x_0)-f(0)}{x_0} - f'(x_0)\Big) \geq \frac{\tilde{\delta}}{2} f''(\tilde{x}_1^*) \qquad \text{(C.30)}$$

$$\Big(\frac{f(x_0)-f(0)}{x_0} - f'(x_0)\Big) \geq \frac{\tilde{\delta}}{2} f''(\tilde{x}_2^*) \qquad \text{(C.31)}$$

where $\tilde{x}_1^* \in (x_0, x_0+\tilde{\delta})$ and $\tilde{x}_2^* \in (x_0-\tilde{\delta}, x_0)$. Because $\tilde{\delta} \leq \delta$, $x_1^*, x_2^* \in (x_0-\delta, x_0+\delta)$, and from the definition of M in (C.22), I have

$$f''(\tilde{x}_1^*) \geq -M \ \ \text{and} \ \ f''(\tilde{x}_2^*) \geq -M \qquad \text{(C.32)}$$

Substituting $\frac{f(x_0)-f(0)}{x_0} - f'(x_0) = \mu$ and $\tilde{\delta} = \frac{|\mu|}{M}$ in (C.30), I have

$$\begin{aligned}
\mu &\geq \frac{|\mu|}{2M} f''(\tilde{x}_1^*) \\
&\geq \frac{|\mu|}{2M}(-M) \ \ \text{(from (C.32))} \\
&= -\frac{|\mu|}{2} \\
\Rightarrow \mu &> 0 \qquad \text{(C.33)}
\end{aligned}$$

Substituting $\frac{f(x_0)-f(0)}{x_0} - f'(x_0) = \mu$ and $\tilde{\delta} = \frac{|\mu|}{M}$ in (C.31), I have

$$\begin{aligned}
-\mu &\geq \frac{|\mu|}{2M} f''(\tilde{x}_2^*) \\
&\geq \frac{|\mu|}{2M}(-M) \;\; \text{(from (C.32))} \\
&= -\frac{|\mu|}{2} \\
\Rightarrow \mu &< 0
\end{aligned} \tag{C.34}$$

This is in contradiction with (C.33). Therefore, our assumption that $\frac{f(x_0)-f(0)}{x_0} - f'(x_0) \neq 0$ is incorrect. Hence,

$$\frac{f(x_0)-f(0)}{x_0} = f'(x_0). \tag{C.35}$$

Substituting the result of (C.35) in (C.20) and (C.21), I arrive at $f''(x_1^*) \leq 0$ and $f''(x_2^*) \leq 0$, where $x_1^* \in (x_0, x_0+\delta)$ and $x_2^* \in (x_0-\delta, x_0)$. I define x_0 as a root of g_0, hence (C.9) is satisfied. That is,

$$f(0) + \frac{f(x_0)-f(0)}{x_0} t - f(t) \geq 0, \; \forall t > 0. \tag{C.36}$$

From this, I can see that $f(t)$ has to be less than or equal to the linear function $l_{x_0}(t) = f(0) + \frac{f(x_0)-f(0)}{x_0} t$, while $l_{x_0}(x_0) = f(x_0)$. For the function $f(t)$ to equal a linear function at x_0, and be less than or equal to that linear function elsewhere, it is necessary that $f(t)$ is concave at x_0. That is, $f''(x_0) \leq 0$.

By the definition of x_0, for $t > x_0$,

$$\begin{aligned}
f(0) + \frac{f(x_0)-f(0)}{x_0} t - f(t) &> 0 \\
f(0) + (f(x_0) - f(0)) + \frac{f(x_0)-f(0)}{x_0}(t - x_0) - f(t) &> 0 \\
f(x_0) + \frac{f(x_0)-f(0)}{x_0}(t - x_0) - f(t) &> 0 \\
f(x_0) + f'(x_0)(t - x_0) - f(t) &> 0 \;\; \text{(from (C.35))} \\
l_{x_0}(t) - f(t) &> 0 \;\; \text{(from (C.3))} \\
g(x_0) &> 0 \;\; \text{(from (C.4))}
\end{aligned} \tag{C.37}$$

Proof that $g(x_0) > 0$, for $x_0 = 0$

From the definition in (C.2), I have

$$\begin{aligned} g_0(x_0) = \min_{t \geq 0}\Big(f(0) + f'(0)t - f(t)\Big) &= 0 \\ f(0) + f'(0)t - f(t) &> 0,\ \forall\, t > 0 \ \ (*) \\ f(x_0) + f'(x_0)(t - x_0) - f(t) &> 0,\ \forall\, t > x_0 \ \ (\because\ x_0 = 0) \\ l_{x_0}(t) - f(t) &> 0 \ \ \text{(from (C.3))} \\ g(x_0) &> 0 \ \ \text{(from (C.4))} \end{aligned} \tag{C.38}$$

$(*)$ - *Note that if* $\exists z > 0$, *s.t.* $f(0) + f'(0)z - f(z) = 0$, *then* $f'(0) = \frac{f(z)-f(0)}{z}$, *and* $f(0)+f'(0)t-f(t) = f(0)+\frac{(f(z)-f(0))t}{z}-f(t)$. *Therefore,* $g(z) = \min_{t\geq 0}\Big(f(0)+\frac{(f(z)-f(0))t}{z} - f(t)\Big) = \min_{t \geq 0}\Big(f(0) + f'(0)t - f(t)\Big) = g_0(0) = 0$, *which implies that* $z > 0$ *is also a root. This is a contradiction because* $x_0 = 0$ *is defined as the largest root.*

Proof that $g(x_j) > 0$, $j = 1, 2, \ldots, N_r$

From the definition of x_j in (C.6), I have

$$\begin{aligned} l_{y_j}(x_j) - f(x_j) &= 0 \\ f(y_j) + (x_j - y_j)f'(y_j) - f(x_j) &= 0 \end{aligned} \tag{C.39}$$

From the definition of y_j in (C.5), I know

$$g(y_j) = \min_{t > y_j}\Big(l_{y_j}(t) - f(t)\Big) = 0 \tag{C.40}$$

Therefore, $l_{y_j}(t) - f(t) \geq 0$ for $t > y_j$. Select a $\delta > 0$, s.t. $x_j - \delta > y_j$. Substituting

$t = x_j \pm \delta$ into $l_{y_j}(t) - f(t) \geq 0$, I have

$$\begin{aligned}
l_{y_j}(x_j \pm \delta) - f(x_j \pm \delta) &\geq 0 \\
f(y_j) + (x_j \pm \delta - y_j)f'(y_j) - f(x_j \pm \delta) &\geq 0 \\
f(y_j) + (x_j \pm \delta - y_j)f'(y_j) - \big(f(x_j) \pm \delta f'(x_j) + \delta^2 \epsilon\big) &\geq 0 \quad \text{(Taylor's theorem)} \\
f(y_j) + (x_j - y_j)f'(y_j) - f(x_j) \pm \delta f'(y_j) - \big(\pm \delta f'(x_j) + \delta^2 \epsilon\big) &\geq 0 \\
0 \pm \delta f'(y_j) - \big(\pm \delta f'(x_j) + \delta^2 \epsilon\big) &\geq 0 \quad \text{(from (C.39))} \\
\pm \delta (f'(y_j) - f'(x_j)) - \delta^2 \epsilon &\geq 0 \qquad \text{(C.41)}
\end{aligned}$$

For the above inequality to be satisfied for any small δ, $f'(y_j) - f'(x_j) = 0$. I prove this by contradiction. Suppose $f'(y_j) - f'(x_j) = \mu \neq 0$.

Case 1: $\epsilon = 0$

From (C.41), I have $\pm\delta\mu \geq 0$. This inequality cannot be satisfied since $\delta > 0$ and $\mu \neq 0$. This is a contradiction, and our assumption that $f'(y_j) - f'(x_j) \neq 0$ is wrong.

Case 2: $\epsilon \neq 0$

Select $\delta = \left|\frac{\mu}{2\epsilon}\right|$. From (C.41), I have

$$\begin{aligned}
\pm \left|\frac{\mu}{2\epsilon}\right| \mu - \left|\frac{\mu}{2\epsilon}\right|^2 \epsilon &\geq 0 \\
\pm \mu - \left|\frac{\mu}{2\epsilon}\right| \epsilon &\geq 0 \\
\mu \left(\pm 1 - \frac{|\mu|\epsilon}{2\mu|\epsilon|}\right) &\geq 0 \qquad \text{(C.42)}
\end{aligned}$$

Hence, I can see that irrespective of the sign of μ and ϵ, $\frac{|\mu|\epsilon}{2\mu|\epsilon|} = \pm\frac{1}{2}$, and the above inequality will not be satisfied. This is a contradiction. Therefore, our assumption that $f'(y_j) - f'(x_j) \neq 0$ is wrong. Hence,

$$f'(y_j) = f'(x_j) \qquad \text{(C.43)}$$

From (C.3), $\forall t \geq 0$

$$\begin{aligned}
l_{y_j}(t) &\equiv f(y_j) + (t - y_j)f'(y_j) \\
&\equiv f(y_j) + (x_j - y_j)f'(y_j) + (t - x_j)f'(y_j) \\
&\equiv f(x_j) + (t - x_j)f'(y_j) \ \ \text{(from (C.39))} \\
&\equiv f(x_j) + (t - x_j)f'(x_j) \ \ \text{(from (C.43))} \\
&\equiv l_{x_j}(t) \qquad \text{(C.44)}
\end{aligned}$$

For $t > x_j$, $l_{y_j}(t) - f(t) > 0$, because $l_{y_j}(t) - f(t) \geq 0$ and x_j is the largest root of $l_{y_j}(t) - f(t) = 0$ (from (C.5) and (C.6)). Therefore,

$$\begin{aligned}
&l_{y_j}(t) - f(t) > 0 \\
&l_{x_j}(t) - f(t) > 0 \ \ \text{(from (C.44))} \qquad \text{(C.45)}
\end{aligned}$$

Therefore, $g(x_j) > 0$ from the definition in (C.4).

C.4 Proof that $f''(x) \leq 0$ for $(x_{j-1} \leq x < y_j) \cup (x \geq x_{N_r})$

I prove this by contradiction. Suppose $\exists\, x_c \in [x_{j-1}, y_j)$, s.t. $f''(x_c) > 0$.

Select a $\delta > 0$.

$$\begin{aligned}
l_{x_c}(x_c + \delta) - f(x_c + \delta) &= f(x_c) + (x_c + \delta - x_c)f'(x_c) - f(x_c + \delta) \\
&= f(x_c) + \delta f'(x_c) - f(x_c + \delta) \\
&= f(x_c) + \delta f'(x_c) - (f(x_c) + \delta f'(x_c) + \delta^2 f''(x_c) + \delta^3 \epsilon) \\
&= -(\delta^2 f''(x_c) + \delta^3 \epsilon) \\
&= -\delta^2 (f''(x_c) + \delta \epsilon) \qquad \text{(C.46)}
\end{aligned}$$

I can find a δ small enough s.t. $-\delta^2(f''(x_c) + \delta\epsilon) < 0$ because $f''(x_c) > 0$. i.e. $\exists \delta$, s.t. $l_{x_c}(x_c + \delta) - f(x_c + \delta) < 0$. Therefore, from (C.4), $g(x_c) < 0$.

Note that $g(x_{j-1}) > 0$ (from Section A.3) and $g(x_c) < 0$ implies that $\exists x_d \in (x_{j-1}, x_c)$, s.t. $g(x_d) = 0$. This is a contradiction because by definition, y_j is the smallest root of $g(y) = 0$, larger than x_{j-1}. Therefore, the assumption that $f''(x_c) > 0$ is wrong. Hence, $f''(x) \leq 0$ for $x \in [x_{j-1}, y_j)$. In the same manner, I can show that $f''(x) \leq 0$ $\forall x \in [x_{N_r}, \infty)$, by selecting $x_c \in [x_{N_r}, \infty)$, and using the fact that $g(y) = 0$ does not have any roots for $y > x_{N_r}$.

C.5 Proof that $l_{y_j}(x)$ and $l_{x_j}(x)$ are upper bounds to $f(x)$

Select $\bar{x}$ such that $x_{j-1} < \bar{x} \leq y_j$. From Section C.3, I know $g(x_{j-1}) > 0$ and by definition of y_j in (C.5), $y_j \geq \bar{x}$ is the smallest root of $g(y) = 0$ greater than x_{j-1}. Hence, $g\left(\bar{x}\right) \geq 0$. Therefore, from (C.4)

$$l_{\bar{x}}(t) \geq f(t), \ \forall \ t > \bar{x}. \tag{C.47}$$

<u>For $x_{j-1} \leq t \leq \bar{x}$</u>

Define $d_1(t) \triangleq l_{\bar{x}}(t) - f(t) = f\left(\bar{x}\right) + \left(t - \bar{x}\right) f'\left(\bar{x}\right) - f(t)$.

$d_1'(t) = f'\left(\bar{x}\right) - f'(t) \leq 0$ because $f''(t) \leq 0$ for $t \in [x_{j-1}, \bar{x}]$ (from Section C.4). Further, $d_1\left(\bar{x}\right) = f\left(\bar{x}\right) + \left(\bar{x} - \bar{x}\right) f'\left(\bar{x}\right) - f(\bar{x}) = 0$. Therefore, $d_1(t) \geq 0$ $\forall x_{j-1} \leq t \leq \bar{x}$.

$$l_{\bar{x}}(t) \geq f(t), \ \forall \ x_{j-1} \leq t \leq \bar{x}. \tag{C.48}$$

<u>For $t \leq x_{j-1}$</u>

Define the function d_2,

$$\begin{aligned} d_2(t) &\triangleq l_{\bar{x}}(t) - l_{x_{j-1}}(t) = f\left(\bar{x}\right) + \left(t - \bar{x}\right) f'\left(\bar{x}\right) - \left(f\left(x_{j-1}\right) + \left(t - x_{j-1}\right) f'\left(x_{j-1}\right)\right) \\ d_2'(t) &= f'\left(\bar{x}\right) - f'(x_{j-1}) \leq 0 \end{aligned} \tag{C.49}$$

because $f''(t) \leq 0$ for $t \in [x_{j-1}, \bar{x}]$ (from Section C.4). Substituting $t = x_{j-1}$,

$$\begin{aligned} d_2(x_{j-1}) &= l_{\bar{x}}(x_{j-1}) - l_{x_{j-1}}(x_{j-1}) \\ &= f\left(\bar{x}\right) + \left(x_{j-1} - \bar{x}\right) f'\left(\bar{x}\right) - \left(f\left(x_{j-1}\right) + \left(x_{j-1} - x_{j-1}\right) f'\left(x_{j-1}\right)\right) \\ &= f\left(\bar{x}\right) + \left(x_{j-1} - \bar{x}\right) f'\left(\bar{x}\right) - f\left(x_{j-1}\right) \\ &= l_{\bar{x}}(x_{j-1}) - f(x_{j-1}) \geq 0 \ \text{ (from (C.48))} \end{aligned} \tag{C.50}$$

From (C.49) and (C.50), $d_2(t) \geq 0 \; \forall \; t \leq x_{j-1}$. Therefore,

$$l_{\bar{x}}(t) \geq l_{x_{j-1}}(t) \; \forall \; t \leq x_{j-1} \tag{C.51}$$

Our objective is to prove $l_{x_j}(t) \geq f(t), \; \forall t \geq 0$, for $j = 0, 1, \ldots, N_r - 1$. I do this by induction. I show that $l_{x_0}(t) \geq f(t), \; \forall t \geq 0$, and then assume $l_{x_{j-1}}(t) \geq f(t), \; \forall t \geq 0$ and show that $l_{x_j}(t) \geq f(t), \; \forall t \geq 0$.

Proof that $l_{x_0}(t) \geq f(t)$

From (C.9), I have

$$\begin{aligned} f(0) + \frac{f(x_0) - f(0)}{x_0} t - f(t) \geq 0, \; \forall t \geq 0 \\ f(0) + \big(f(x_0) - f(0)\big) + \frac{f(x_0) - f(0)}{x_0}(t - x_0) - f(t) \geq 0, \; \forall t \geq 0 \\ f(x_0) + \frac{f(x_0) - f(0)}{x_0}(t - x_0) - f(t) \geq 0, \; \forall t \geq 0 \\ f(x_0) + f'(x_0)(t - x_0) - f(t) \geq 0, \; \forall t \geq 0 \quad \text{(from (C.35))} \\ l_{x_0}(t) - f(t) \geq 0, \; \forall t \geq 0 \quad \text{(from (C.3))} \\ l_{x_0}(t) \geq 0, \; \forall t \geq 0 \end{aligned} \tag{C.52}$$

Assume $l_{x_{j-1}}(t) \geq f(t), \; \forall t \geq 0$

From (C.51), $l_{\bar{x}}(t) \geq l_{x_{j-1}}(t) \geq f(t), \; \forall t \leq x_{j-1}$.

$$l_{\bar{x}}(t) \geq f(t), \; \forall t \leq x_{j-1}. \tag{C.53}$$

From (C.47), (C.48) and (C.53),

$$l_{\bar{x}}(t) \geq f(t), \forall t \geq 0, \; \text{for } x_{j-1} < \bar{x} \leq y_j. \tag{C.54}$$

From (C.44), if $l_{y_j}(t) \geq f(t), \forall t \geq 0$, then $l_{x_j}(t) \geq f(t), \forall t \geq 0$.

Therefore, I have shown that $l_{x_j}(t) \geq f(t), \forall t \geq 0$, for $j = 0, 1, \ldots, N_r - 1$, using induction. From (C.54) I have

$$l_{\bar{x}}(t) \geq f(t), \forall \; t \geq 0, \text{for } x_{j-1} \leq \bar{x} \leq y_j, \; j = 1, 2, \ldots, N_r. \tag{C.55}$$

C.6 Proof that $l_{\bar{x}}(x)$ is an upper bound to $f(x)$ for $\bar{x} > x_{N_r}$

Select $\bar{x}$ such that $\bar{x} > x_{N_r}$. From Section C.1, I know $g(x_{N_r}) > 0$ and from the algorithm in Fig.6.1, I know that $\{y|g(y) = 0, y > x_{N_r}\}$ is the empty set; i.e. $y_{N_r+1} = \min\{y|g(y) = 0, y > x_{N_r}\}$ from (C.5) does not exist. Therefore, since $\bar{x} > x_{N_r}$, $g(\bar{x}) \geq 0$. Therefore, from (C.4)

$$l_{\bar{x}}(t) \geq f(t),\ \forall\, t > \bar{x}. \tag{C.56}$$

For $x_{N_r} \leq t \leq \bar{x}$

Define $d_1(t) \triangleq l_{\bar{x}}(t) - f(t) = f(\bar{x}) + (t - \bar{x}) f'(\bar{x}) - f(t)$.

$d_1'(t) = f'(\bar{x}) - f'(t) \leq 0$ because $f''(t) \leq 0$ for $t \in [x_{N_r}, \bar{x}]$ (from Section C.4). Further, $d_1(\bar{x}) = f(\bar{x}) + (\bar{x} - \bar{x}) f'(\bar{x}) - f(\bar{x}) = 0$. Therefore, $d(t) \geq 0\ \forall x_{N_r} \leq t \leq \bar{x}$.

$$l_{\bar{x}}(t) \geq f(t),\ \forall\, x_{N_r} \leq t \leq \bar{x}. \tag{C.57}$$

For $t \leq x_{N_r}$

Define the function d_2:

$$\begin{aligned} d_2(t) &\triangleq l_{\bar{x}}(t) - l_{x_{N_r}}(t) = f(\bar{x}) + (t - \bar{x}) f'(\bar{x}) - \left(f(x_{N_r}) + (t - x_{N_r}) f'(x_{N_r})\right) \\ d_2'(t) &= f'(\bar{x}) - f'(x_{N_r}) \leq 0 \end{aligned} \tag{C.58}$$

because $f''(t) \leq 0$ for $t \in [x_{N_r}, \bar{x}]$ (from Section C.4).

Substituting $t = x_{j-1}$:

$$\begin{aligned} d_2(x_{N_r}) &= l_{\bar{x}}(x_{N_r}) - l_{x_{N_r}}(x_{N_r}) \\ &= f(\bar{x}) + (x_{N_r} - \bar{x}) f'(\bar{x}) - \left(f(x_{N_r}) + (x_{N_r} - x_{N_r}) f'(x_{N_r})\right) \\ &= f(\bar{x}) + (x_{N_r} - \bar{x}) f'(\bar{x}) - f(x_{N_r}) \\ &= l_{\bar{x}}(x_{N_r}) - f(x_{N_r}) \geq 0 \ \text{ (from (C.57))} \end{aligned} \tag{C.59}$$

From (C.58) and (C.59), $d_2(t) \geq 0\ \forall\, t \leq x_{N_r}$. Therefore,

$$l_{\bar{x}}(t) \geq l_{x_{N_r}}(t)\ \forall\, t \leq x_{N_r}. \tag{C.60}$$

In Section C.5, I showed $l_{y_{N_r}}(t) \geq f(t)\ \forall t \geq 0$. From (C.44), it follows that $l_{x_{N_r}}(t) \geq f(t)\ \forall t \geq 0$. Therefore, from (C.60),

$$l_{\bar{x}}(t) \geq f(t),\ \forall t \leq x_{N_r}. \tag{C.61}$$

From (C.56), (C.57) and (C.61), $l_{\bar{x}}(t) \geq f(t)$, for $x_{N_r} < \bar{x}$.

C.7 On the existence of roots of $g_0(x)$

In (C.2), I defined $g_0(x)$ as follows:

$$g_0(x) \triangleq \begin{cases} \min\limits_{t\geq 0}\Big(f(0) + \frac{(f(x)-f(0))t}{x} - f(t)\Big) & x > 0 \\ \min\limits_{t\geq 0}\Big(f(0) + f'(0)t - f(t)\Big) & x = 0 \end{cases} \tag{C.62}$$

I can see that when I substitute $t = x$:

<u>For $x > 0$</u>

$$f(0) + \frac{(f(x)-f(0))t}{x} - f(t) = f(0) + \frac{(f(x)-f(0))x}{x} - f(x) = 0 \tag{C.63}$$

<u>For $x = 0$</u>

$$f(0) + f'(0)t - f(t) = f(0) + f'(0) \times 0 - f(0) = 0 \tag{C.64}$$

Therefore,

<u>For $x > 0$</u>

$$\min_{t>0}\Big(f(0) + \frac{(f(x)-f(0))t}{x} - f(t)\Big) \leq 0, \quad \text{(from (C.63))} \tag{C.65}$$

<u>For $x = 0$</u>

$$\min_{t\geq 0}\Big(f(0) + f'(0)t - f(t)\Big) \leq 0. \quad \text{(from (C.64))} \tag{C.66}$$

Hence, from (C.65) and (C.66), I have

$$g_0(x) \leq 0, \forall x \geq 0. \tag{C.67}$$

Also, $g_0(x)$ is a continuous function for $x \geq 0$.

For $\tilde{x} > 0$

$$\begin{aligned}
\lim_{x\to\tilde{x}} g_0(x) &= \lim_{x\to\tilde{x}} \left[\min_{t\geq 0}\left(f(0) + \frac{(f(x)-f(0))t}{x} - f(t)\right)\right] \\
&= \min_{t\geq 0}\left(f(0) + \lim_{x\to\tilde{x}}\left(\frac{(f(x)-f(0))t}{x}\right) - f(t)\right) \\
&= \min_{t\geq 0}\left(f(0) + \frac{(f(\tilde{x})-f(0))t}{\tilde{x}} - f(t)\right) \\
&= g_0(\tilde{x}) \qquad \text{(C.68)}
\end{aligned}$$

For $\tilde{x} = 0$

$$\begin{aligned}
\lim_{x\to 0^+} g_0(x) &= \lim_{x\to 0^+} \left[\min_{t\geq 0}\left(f(0) + \frac{(f(x)-f(0))t}{x} - f(t)\right)\right] \\
&= \min_{t\geq 0}\left(f(0) + \lim_{x\to 0^+}\left(\frac{f(x)-f(0)}{x}\right)t - f(t)\right) \\
&= \min_{t\geq 0}\big(f(0) + f'(0)t - f(t)\big) \\
&= g_0(0) = g_0(\tilde{x}) \qquad \text{(C.69)}
\end{aligned}$$

Consider $\lim_{z\to\infty} g_0(z)$.

$$\begin{aligned}
\lim_{z\to\infty} g_0(z) &= \lim_{z\to\infty} \left[\min_{t\geq 0}\left(f(0) + \frac{(f(z)-f(0))t}{z} - f(t)\right)\right] \\
&= \min_{t\geq 0}\left(f(0) + \lim_{z\to\infty}\left(\frac{f(z)-f(0)}{z}\right)t - f(t)\right) \\
&= \min_{t\geq 0}\,(f(0) + 0 - f(t)) \quad \text{(because } f \text{ is bounded above)} \\
&= \min_{t\geq 0}\,(f(0) - f(t)) \qquad \text{(C.70)}
\end{aligned}$$

Select $z_0 \in (0,\infty)$. Because f is a non-decreasing function, $z_0 > 0$ and $t \geq 0$, $\frac{(f(z_0)-f(0))t}{z_0} \geq 0$. Using this in (C.70), I have

$$\begin{aligned}
\lim_{z\to\infty} g_0(z) &\leq \min_{t\geq 0}\left(f(0) + \frac{(f(z_0)-f(0))t}{z_0} - f(t)\right) \\
&= g(z_0) \qquad \text{(C.71)}
\end{aligned}$$

I prove that there is at least one root for $g_0(z) = 0$ by contradiction. Assume

$g_0(z) = 0$ does not have a root. Then, from (C.67), I know

$$g_0(z) < 0,\ \forall z \geq 0. \tag{C.72}$$

Define $z_m \in [0, \infty)$,

$$z_m \triangleq \arg\max_{z \geq 0} g_0(z) \tag{C.73}$$

Note: *From* (C.71)*, I know that a finite* z_m *can be found. Because from* (C.71)*,* $\lim\limits_{z\to\infty} g_0(z) \leq g(z_m)$*.* $\forall z_m \in [0, \infty)$*.*

<u>If $z_m = 0$</u>

Define $t_m = \arg\min\limits_{t\geq 0}\Big(f(0) + f'(0)t - f(t)\Big)$. I know $t_m > 0$, because from (C.72), $g_0(z_m) < 0$ and $g_0(z_m) = g_0(0) = \min\limits_{t\geq 0}\Big(f(0)+f'(0)t-f(t)\Big) = \Big(f(0)+f'(0)t_m-f(t_m)\Big) < 0$.

Note: *If* $t_m = 0$*,* $g_0(z_m) = \Big(f(0) + f'(0)t_m - f(t_m)\Big) = \Big(f(0) + f'(0) \times 0 - f(0)\Big) = 0$*, which is a contradiction. Hence,* $t_m > 0$*.*

Since $g_0(z_m) = \min\limits_{t\geq 0}\Big(f(0)+f'(0)t-f(t)\Big) = f(0)+f'(0)t_m-f(t_m)$ and $g_0(z_m) < 0$, it follows that

$$\begin{aligned}
f(0) + f'(0)t_m - f(t_m) &< 0\\
f'(0)t_m &< f(t_m) - f(0)\\
f'(0) &< \frac{f(t_m) - f(0)}{t_m} \quad (\because\ t_m > 0)\\
f'(0)t &< \frac{(f(t_m) - f(0))t}{t_m}, \quad \forall t > 0\\
f(0) + f'(0)t - f(t) &< f(0) + \frac{(f(t_m) - f(0))t}{t_m} - f(t), \quad \forall t > 0\\
\min_{t<0}\Big(f(0) + f'(0)t - f(t)\Big) &< \min_{t<0}\Big(f(0) + \frac{(f(t_m) - f(0))t}{t_m} - f(t)\Big)\\
g_0(z_m) &< g_0(t_m)
\end{aligned} \tag{C.74}$$

<u>If $z_m > 0$</u>

Define $t_m = \arg\min\limits_{t>0}\Big(f(0) + \frac{(f(z_m)-f(0))t}{z_m} - f(t)\Big)$. Since $g_0(z_m) = \min\limits_{t>0}\Big(f(0) +$

$\frac{(f(z_m)-f(0))t}{z_m} - f(t)\Big) < 0$, it follows that

$$
\begin{aligned}
f(0) + \frac{(f(z_m)-f(0))t_m}{z_m} - f(t_m) &< 0 \\
\frac{(f(z_m)-f(0))t_m}{z_m} &< f(t_m) - f(0) \\
\frac{(f(z_m)-f(0))}{z_m} &< \frac{f(t_m)-f(0)}{t_m} \quad (\because\ t_m > 0) \\
\frac{(f(z_m)-f(0))t}{z_m} &< \frac{(f(t_m)-f(0))t}{t_m}, \ \ \forall t > 0 \\
f(0) + \frac{(f(z_m)-f(0))t}{z_m} - f(t) &< f(0) + \frac{(f(t_m)-f(0))t}{t_m} - f(t), \ \ \forall t > 0 \qquad \text{(C.75)}
\end{aligned}
$$

$$
\begin{aligned}
\min_{t>0}\Big(f(0) + \frac{(f(z_m)-f(0))t}{z_m} - f(t)\Big) &< \min_{t>0}\Big(f(0) + \frac{(f(t_m)-f(0))t}{t_m} - f(t)\Big) \\
\min_{t\geq 0}\Big(f(0) + \frac{(f(z_m)-f(0))t}{z_m} - f(t)\Big) &< \min_{t>0}\Big(f(0) + \frac{(f(t_m)-f(0))t}{t_m} - f(t)\Big) \\
g_0(z_m) &< \min_{t>0}\Big(f(0) + \frac{(f(t_m)-f(0))t}{t_m} - f(t)\Big) \\
g_0(z_m) &< \min_{t\geq 0}\Big(f(0) + \frac{(f(t_m)-f(0))t}{t_m} - f(t)\Big) \quad (*) \\
g_0(z_m) &< g_0(t_m) \quad \text{(from (C.2))} \qquad \text{(C.76)}
\end{aligned}
$$

According to the definition of z_m in (C.73), this is a contradiction. Hence our assumption was incorrect; i.e. $g_0(x) = 0$ has a solution.

$(*)$ Note: *When $t = 0$,*

$$
\begin{aligned}
f(0) + \frac{(f(z_m)-f(0))t}{z_m} - f(t) &= f(0) + \frac{(f(z_m)-f(0)) \times 0}{z_m} - f(0) = 0 \qquad \text{(C.77)} \\
&> g_0(z_m) \ \ \textit{(from (C.72))}
\end{aligned}
$$

Further, since I know $g(z_m) < 0$ from (C.72), it follows that

$$
\min_{t\geq 0}\left(f(0) + \frac{(f(z_m)-f(0))t}{z_m} - f(t)\right) < 0. \qquad \text{(C.78)}
$$

Hence, from (C.77) and (C.78), I know $\arg\min_{t\geq 0}\Big(f(0) + \frac{(f(z_m)-f(0))t}{z_m} - f(t)\Big) \neq 0.$

Therefore,

$$\min_{t\geq 0}\left(f(0)+\frac{(f(z_m)-f(0))t}{z_m}-f(t)\right)=\min_{t>0}\left(f(0)+\frac{(f(z_m)-f(0))t}{z_m}-f(t)\right). \tag{C.79}$$

C.8 Addition of property P2

In this section I introduce the property **P2** (stated below) and show that the optimization approach in (C.1) reduces to the theorem from Chapter 2.

P2: The second derivative $f''(x)$ has at most one zero in $x>0$.

From Chapter 2, I know if $f''(\tilde{x})\leq 0$ for some $\tilde{x}>0$, then $f''(x)<0\ \forall x\ >\tilde{x}$.

Note that x_0, defined as the largest root of (C.2), has the following property, as shown in (C.35):

$$\begin{aligned}\frac{f(x_0)-f(0)}{x_0}&=f'(x_0)\\ f(x_0)-f(0)-x_0f'(x_0)&=0\\ \tilde{g}(x_0)&=0\end{aligned} \tag{C.80}$$

where $\tilde{g}(x)\triangleq f(x)-f(0)-xf'(x)$ is the function I denoted as $g(x)$ in Chapter 2. Note that x_0 is a root of $\tilde{g}(x)$. Further, if $x_0>0$ is a root of $\tilde{g}(x)$, from the result in (A.13), for $t\geq 0$

$$\begin{aligned}f(0)+\frac{t}{x_0}\big(f(x_0)-f(0)\big)&\geq f(t)\\ f(0)+\frac{t}{x_0}\big(f(x_0)-f(0)\big)-f(t)&\geq 0\end{aligned} \tag{C.81}$$

Therefore, from (C.2), $g(x_0)=0$. Note that $t=x_0$ in (C.2) provides the equality[1]. I have shown that the roots of $g_0(x)$ and $\tilde{g}(x)$ are the same. Therefore, x_0 is equivalent to x^* from (A.2). From the results in (A.6), and **P2**, I also have $f''(x)<0\ \forall x>x_0$.

Proof that $g(y)=0$ does not have any solutions for $y>x_0$

[1] I have only considered $x_0>0$ here. Note that $x_0=0$ is the trivial case where $f(x)$ is concave $\forall x\geq 0$ and the optimal strategy is equal power attack in all bands at all power levels.

I prove this by contradiction. Assume $y_1 > x_0$ is a solution; i.e. $g(y_1) = 0$, where $g(y)$ is defined in (C.4).

$$\min_{t>y_1}\Big(f(y_1) + (t - y_1)f'(y_1) - f(t)\Big) = 0 \tag{C.82}$$

Therefore, $\exists t_1 > y_1$, such that

$$f(y_1) + (t_1 - y_1)f'(y_1) - f(t_1) = 0 \tag{C.83}$$

and

$$f(y_1) + (t_1 \pm \delta - y_1)f'(y_1) - f(t_1 \pm \delta) \geq 0 \tag{C.84}$$

where $\delta > 0$ is a small value such that $t_1 - \delta > y_1$.

Using Taylor's theorem in the Lagrange remainder form, I can write

$$f(t_1 + \delta) = f(t_1) + \delta f'(t_1) + \frac{\delta^2}{2}f''(t_1^*) \tag{C.85}$$

$$f(t_1 - \delta) = f(t_1) - \delta f'(t_1) + \frac{\delta^2}{2}f''(t_2^*) \tag{C.86}$$

where $t_1^* \in (t_1, t_1 + \delta)$ and $t_2^* \in (t_1 - \delta, t_1)$. From (C.84),

$$\begin{aligned}
f(y_1) + (t_1 + \delta - y_1)f'(y_1) - f(t_1 + \delta) &\geq 0 \\
f(y_1) + (t_1 + \delta - y_1)f'(y_1) - \left(f(t_1) + \delta f'(t_1) + \frac{\delta^2}{2}f''(t_1^*)\right) &\geq 0 \quad \text{(from (C.85))} \\
\big(f(y_1) + (t_1 - y_1)f'(y_1) - f(t_1)\big) + \delta f'(y_1) - \delta f'(t_1) - \frac{\delta^2}{2}f''(t_1^*) &\geq 0 \\
0 + \delta\big(f'(y_1) - f'(t_1)\big) - \frac{\delta^2}{2}f''(t_1^*) &\geq 0 \\
f'(y_1) - f'(t_1) &\geq \frac{\delta}{2}f''(t_1^*) \qquad \text{(C.87)}
\end{aligned}$$

Similarly, using (C.84) and (C.86), I can show that

$$-\Big(f'(y_1) - f'(t_1)\Big) \geq \frac{\delta}{2}f''(t_1^*) \tag{C.88}$$

For both inequalities (C.87) and (C.88) to be satisfied for any small δ, $f'(y_1) = f'(t_1)$. (*Note that the proof is identical to that of* (C.35).)

But it is known that $f''(x) < 0 \; \forall x > x_0$, and $x_0 < y_1 < t_1$. Therefore, $f'(y_1) = f'(t_1)$ is a contradiction. It follows that our assumption that $g(y) = 0$ has a solution y_1 is wrong.

Hence, $g(y) = 0$ does not have any solutions greater than x_0. Therefore, N_r in (C.1) is zero, and (C.1) reduces to

$$\sum_{i=1}^{N} f(\tilde{x}_i) \leq \begin{cases} \left(N - \frac{X_T}{x_0}\right) f(0) + \frac{X_T}{x_0} f(x_0), & \text{if } \frac{X_T}{N} \leq x_0 \\ N f\left(\frac{X_T}{N}\right), & \text{if } x_0 < \frac{X_T}{N} \end{cases} \tag{C.89}$$

where $x_0 \equiv x^*$ in the theorem from Chapter 2.

References

[1] Cisco Systems, “Cisco visual networking index: Global mobile data traffic forecast update, 2014-2019.” *White Paper*, February 2015.

[2] X. Zhu and B. Girod, “Video streaming over wireless networks,” in *Proceedings of the European Signal Processing Conference, EUSIPCO-07*, 2007.

[3] “Radio jamming.” Internet: en.wikipedia.org/wiki/Radio_jamming [Accessed on: Sep. 15, 2015].

[4] “Broadcast signal intrusion.” Internet: en.wikipedia.org/wiki/Broadcast_signal_intrusion [Accessed on: Sep. 15, 2015].

[5] S. Haykin, “Cognitive Radio: Brain-empowered wireless communications,” *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201 – 220, Feb. 2005.

[6] ITU-T and ISO/IEC JTC 1, “Advanced video coding for generic audiovisual services,” ITU-T Recommendation H.264 and ISO/IEC 14496-10 (MPEG-4 AVC), Version 1: May 2003, Version 2: May 2004, Version 3: Mar. 2005, Version 4: Sep. 2005, Version 5 and Version 6: June 2006, Version 7: Apr. 2007.

[7] H. Schwarz, D. Marpe, and T. Wiegand, “Overview of the scalable video coding extension of the H.264/AVC standard,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 17, no. 9, pp. 1103–1120, Sept 2007.

[8] I. E. Richardson, *The H.264 advanced video compression standard*, John Wiley & Sons, Hoboken, NJ, USA, 2010.

[9] A. Vosoughi, “Unequal error protection for compressed video over noisy channels,” Ph.D dissertation, Department of Electrical and Computer Engineering, University of California, San Diego, CA, 2015.

[10] Yueh-Lun Chang, “Improving end-user video quality through error concealment and packet importance modeling,” Ph.D dissertation, Department of Electrical and Computer Engineering, University of California, San Diego, CA, 2014.

[11] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread spectrum communications.* Computer science press, 1985, vol. I.

[12] L. Milstein, “Waveform and receiver design considerations on wideband CDMA,” *IEEE Personal Communications*, vol. 6, no. 5, pp. 24–30, Oct. 1999.

[13] S. Hara and R. Prasad, “Overview of multicarrier CDMA,” *IEEE Communications Magazine*, vol. 35, no. 12, pp. 126–133, Dec. 1997.

[14] A. Goldsmith, *Wireless Communications.* New York, NY, USA: Cambridge University Press, 2005.

[15] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication.* New York, NY, USA: Cambridge University Press, 2005.

[16] T. X. Brown and A. Sethi, “Potential cognitive radio Denial-of-Service vulnerabilities and protection countermeasures: A multi-dimensional analysis and assessment,” in *International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, Aug. 2007, pp. 456 –464.

[17] Q. Peng, P. Cosman, and L. Milstein, “Optimal sensing disruption for a cognitive radio adversary,” *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1801 –1810, May 2010.

[18] ——, “Analysis and simulation of sensing deception in fading cognitive radio networks,” in *International Conference on Wireless Communications Networking and Mobile Computing*, Sep. 2010, pp. 1 –4.

[19] ——, “Spoofing or jamming: Performance analysis of a tactical cognitive radio adversary,” *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 903 –911, Apr. 2011.

[20] S. Anand, Z. Jin, and K. Subbalakshmi, “An analytical model for primary user emulation attacks in cognitive radio networks,” in *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Oct. 2008, pp. 1 –6.

[21] H. Li and Z. Han, “Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, Part I: Known channel statistics,” *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3566 –3577, Nov. 2010.

[22] ——, “Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, Part II: Unknown channel statistics,” *IEEE Trans. Wireless Commun.*, vol. 10, no. 1, pp. 274 –283, Jan. 2011.

[23] Z. Jin, S. Anand, and K. Subbalakshmi, “Impact of primary user emulation attacks on dynamic spectrum access networks,” *IEEE Trans. Commun.*, vol. 60, no. 9, pp. 2635 –2643, Sep. 2012.

[24] C. Zhang, R. Yu, and Y. Zhang, “Performance analysis of primary user emulation attack in cognitive radio networks,” in *International Wireless Communications and Mobile Computing Conference*, Aug. 2012, pp. 371 –376.

[25] B. Wang, Y. Wu, K. Liu, and T. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 877–889, April 2011.

[26] W. Conley and A. Miller, "Cognitive jamming game for dynamically countering ad hoc cognitive radio networks," in *IEEE Military Communications Conference, MILCOM 2013*, Nov 2013, pp. 1176–1182.

[27] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proceedings of the IEEE*, vol. 55, no. 4, pp. 523–531, April 1967.

[28] A. Erdelyi, W. Magnus, F. Oberhettinger, and F. G. Tricomi, *Tables of Integral Transforms*, ser. Bateman Manuscript Project, California Institute of Technology. McGraw-Hill Book Company, Inc, 1954, vol. 1.

[29] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions.* Dover Publications, Inc., New York, 1970.

[30] L. Rastrigin, "The convergence of the random search method in the extremal control of a many parameter system," *Automation and remote control*, vol. 24, no. 11, pp. 1337–1342, 1963.

[31] M. K. Simon and M.-S. Alouini, *Digital communication over fading channels*, ser. Wiley series in telecommunications and signal processing. Hoboken, N.J. Wiley-Interscience, 2005.

[32] H. Kwon, I. Song, S. Y. Kim, and S. Yoon, "Noncoherent constant false-alarm rate schemes with receive diversity for code acquisition under homogeneous and nonhomogeneous fading circumstances," *IEEE Trans. Veh. Technol.*, vol. 56, no. 4, pp. 2108–2120, July 2007.

[33] Q. Qu, L. Milstein, and D. Vaman, "Cognitive radio based multi-user resource allocation in mobile ad hoc networks using multi-carrier cdma modulation," *IEEE Journal on Selected Areas in Communications,*, vol. 26, no. 1, pp. 70 –82, Jan. 2008.

[34] W. Xu and L. Milstein, "Performance of multicarrier DS CDMA systems in the presence of correlated fading," in *IEEE Vehicular Technology Conference*, vol. 3, May 1997, pp. 2050–2054 vol.3.