UC San Diego

UC San Diego Electronic Theses and Dissertations

Title

Tradeoff between spoofing and jamming a Cognitive Radio link

Permalink

https://escholarship.org/uc/item/61f5h924

Author

Wang, Jing

Publication Date

2010

Peer reviewed|Thesis/dissertation

eScholarship.org Powered by the California Digital Library
University of California

UNIVERSITY OF CALIFORNIA, SAN DIEGO

Tradeoff between Spoofing and Jamming a Cognitive Radio Link

A Thesis submitted in partial satisfaction

of the requirements for the degree Master of Science

in

Electrical Engineering (Computer Engineering)

by

Jing Wang

Committee in charge:

Professor Milstein Laurence, Chair
Professor Pamela Cosman
Professor Bhaskar Rao

2010

The Thesis of Jing Wang is approved and it is acceptable in quality and form for publication on microfilm and electronically:

Chair

University of California, San Diego

2010

TABLE OF CONTENTS

Signature Page iii

Table of Contents iv

List of Figures vi

Acknowledgements viii

Abstract x

Chapter 1 Introduction

1.1 Background 1

1.2 Cognitive radio review 3

Chapter 2 Spectrum sensing techniques

2.1 Overview 6

2.2 Matched filter 7

2.3 Energy detector 8

2.4 Cyclostationary feature detection 9

2.5 Problem statement 10

2.5.1 Scenario I 11

2.5.2 Scenario II 12

Chapter 3 System model

3.1 Introduction 14

3.2 Theoretical analysis ……15

3.2.1 Scenario I ……15

3.2.2 Scenario II ……17

Chapter 4 Simulation model and results (Scenario I)

4.1 Simulation model …… 27

4.2 Simulation results …… 29

Chapter 5 Numerical results (Scenario II)

5.1 $N_{R,PU}=1, N_{R,SU}=1$ …… 36

5.2 $N_{R,PU}=1, N_{R,SU}=10$ …… 44

5.3 $N_{R,PU}=1, N_{R,SU}=100$ …… 54

5.4 $N_{R,PU}=10, N_{R,SU}=10$ …… 60

5.5 $N_{R,PU}=100, N_{R,SU}=10$ …… 68

5.6 Conclusions …… 70

References…… 72

LIST OF FIGURES

Figure 1.1. Spectrum utilization measurements ……2

Figure 1.2. Basic cognitive cycle ……5

Figure 2.1. Energy detector diagram ……9

Figure 3.1. System model …… 14

Figure 3.2. Spectrum bands ……14

Figure 3.3. Frame structure for cognitive radio ……17

Figure 3.4. System model ……19

Figure 3.5. Attack strategies in sensing duration ……22

Figure 3.6. Attack strategies in transmission duration ……24

Figure 4.1. AWGN model …… 27

Figure 4.2. Optimal number of spoofed bands versus number of allowable bands …… 30

Figure 4.3. Optimal number of spoofed bands versus spoofing-power-to-thermal-noise-power ratio …… 31

Figure 4.4. The average number of false detection versus number of allowable bands with different spoofing powers …… 33

Figure 4.5. The average number of additional false detections …… 34

Figure 5.1. System average throughput with $N_{R,PU}=1, N_{R,SU}=1$ ……36

Figure 5.2. System average throughput versus P/S …… …….…….. 40

Figure 5.3. Log of packet success rate ……..……..…….. 41

Figure 5.4. Log of secondary user throughput components …… 43

Figure 5.5. Throughput of secondary user ……..……..…….. 44

Figure 5.6. System average throughput with $N_{R,PU}=1, N_{R,SU}=10$ ……..…. 46

Figure 5.7. System average throughput versus P/S ……..…… 47

Figure 5.8. System throughput components ……..…… 49

Figure 5.9. Secondary user throughput …….. 50

Figure 5.10. Log of secondary user throughput components …… 52

Figure 5.11. Secondary user throughput ……..……..…….. 54

Figure 5.12. System average throughput with $N_{R,PU}=1, N_{R,SU}=100$ …….... 55

Figure 5.13. System average throughput versus P/S …….. 57

Figure 5.14. Packet success rate …… …… 58

Figure 5.15. Secondary user throughput components ..……59

Figure 5.16. System average throughput with $N_{R,PU}=10, N_{R,SU}=10$ ……. 61

Figure 5.17. System average throughput versus P/S ……..……..62

Figure 5.18. Secondary user throughput components …..……..……63

Figure 5.19. Throughput of secondary users ……..…….. 64

Figure 5.20. Throughput of primary users and secondary users …… 67

Figure 5.21. System average throughput with $N_{R,PU}=100, N_{R,SU}=10$ ...….. 69

ACKNOWLEDGEMENTS

I would like to thank my advisor, Professor Laurence B. Milstein for his guidance and supervision of my Master's research project. I especially appreciate his great patience in correcting my grammar mistakes and typos. Also I am deeply grateful to him for taking the time to read an entire draft of this work and noting the unclear passages. His comments and suggestions have tremendously improved the quality of this thesis. I am very grateful for his constant help during the years I studied at UCSD. I would like to thank him for writing reference letters to help me get the UCSD admission and a job offer.

I would like to thank my friends, Qihang Peng and Dawei Wang for their help and useful suggestions on this work.

I would like to thank my thesis committee members, Professor Bhaskar Rao and Professor Pamela Cosman, for their time, help and effort in serving on my committee.

I would like to express my special thanks to Professor Jack K. Wolf and Professor Bhaskar Rao for their recommendations to help me get a job opportunity.

I would like to express my gratefulness to the ECE department advisors, especially Adolfo Juarez and Megan Scott, for helping me whenever required.

Finally, I would like to express my love and thanks to my parents, my sisters and my husband for their encouragement.

ABSTRACT OF THE THESIS

Tradeoff between Spoofing and Jamming a Cognitive Radio Link

by

Jing Wang

Master of Science in Electrical Engineering (Computer Engineering)

University of California, San Diego, 2010

Professor Milstein Laurence, Chair

Cognitive radio (CR), which employs spectrum sensing technology to realize the spectrum reuse, holds much promise as a technology that will play a significant role in communication systems of the future. The utilization efficiency of spectrum has been improved by allowing for dynamic accessing. However, the sensing before accessing strategy makes a CR network more vulnerable to an intelligent adversary attack. In addition to jamming as in traditional radio systems, the adversary can launch signals to the unused bands to spoof the secondary users in a CR network.

In the first scenario, an optimal spoofing strategy subject to the adversary's

power constraint is briefly introduced. The simulation results match well to numerical results in [15], where the worst-case deception strategy is shown to be equal-power, partial-band spoofing.

In the secondary scenario, the tradeoff between spoofing and jamming a CR network by an intelligent adversary with the presence of primary users is analyzed. Considering an energy constraint, the intelligent adversary negotiates the energy distribution between jamming primary users, and spoofing and/or jamming secondary users to minimize the system average throughput. It is shown that in a cluster-based CR network, once the secondary users require a relatively large fraction of the allowable bands, spoofing is more efficient than jamming the secondary users in terms of minimizing the throughput of the secondary users. Jamming the primary users can always decrease the throughput of the primary users.

Chapter 1 Introduction

1.1 Background

With the steady increase in the requirement for the radio spectrum and the improvement of communications and speeds, spectrum scarcity and low spectrum utilization are becoming more obvious. Even though spectrum efficiency of some radio systems (such as cell phone and WiFi bands) is improving, some bands are still poorly utilized. The spectrum occupancy measurement shows that only a small fraction of the spectrum bands are efficiently used, some are largely unoccupied most of the time and some are only partially occupied. Furthermore, the time scale of the spectrum occupancy varies from milliseconds to hours [1]. As shown in Figure 1.1, the utilization is roughly 30% below 3GHz and 5% in the 3-6 GHz frequency band. Therefore spectrum access is more significant than physical scarcity of spectrum [1].

In considering the significant underutilization of the radio spectrum, in 2002, the Federal Communications Commission published a report prepared by the Spectrum-Policy Task Force aimed at improving the spectrum usage [1]. Spectrum utilization can be improved significantly by making it possible for a

secondary user to access a spectrum hole unoccupied by the primary users at the right location and the time in question. By definition, a spectrum hole is a band of

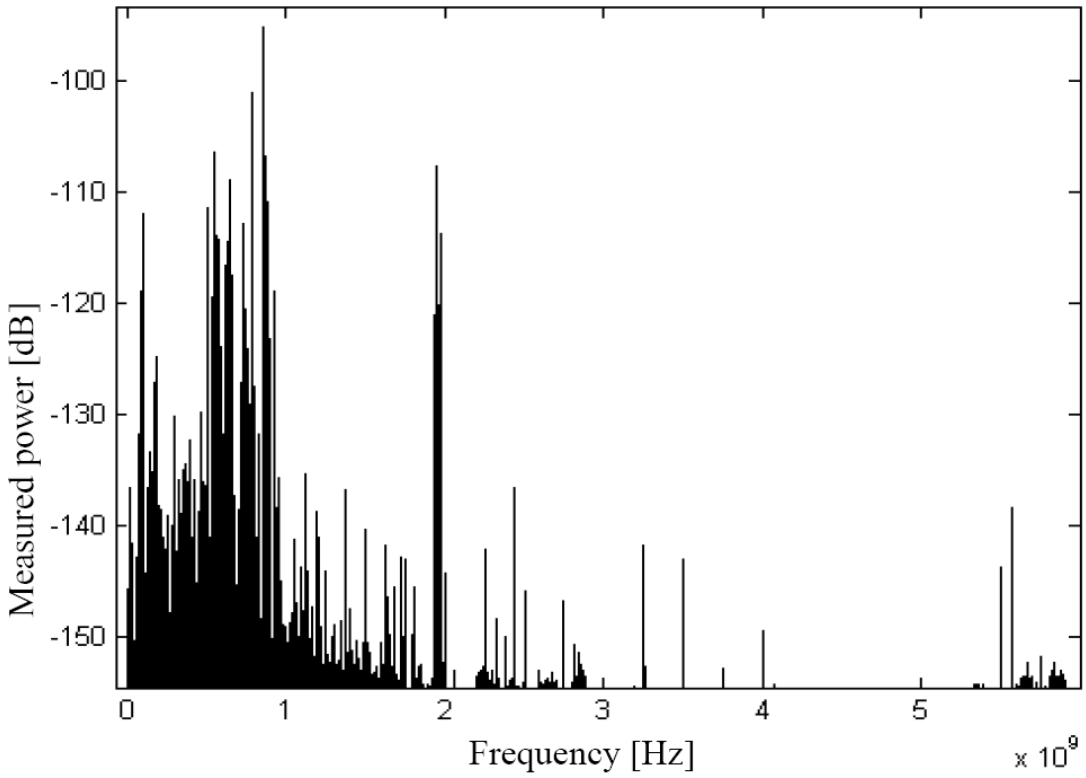


Figure 1.1. Spectrum utilization measurements (0-6GHz) [1]

frequencies initially assigned to a primary user, but, at a particular time and specific geographic location, the band is not being utilized by that user [1].

Cognitive radio, allowing for dynamically accessing unused spectrum bands with only minimal degradation to primary users, holds much promise as a technology that will play a strong role in communication systems of the future. Moreover, the trend in wireless communication systems is going from fully centralized systems to the direction of self-organizing systems where individual

nodes can quickly establish ad hoc networks whose structure is changing over time. Cognitive radios, with the capabilities to sense the operating environment, learn and adapt in real time according to the environment, are also seen as a promising technology [2].

1.2 Cognitive radio review

The term cognitive radio was first suggested by Mitola in 1999. Cognitive radio is an intelligent wireless communication system that is aware of its surrounding environment, and uses the methodology of understanding-by-building to learn from the environment. Thus cognitive radio can make corresponding changes in certain operating parameters (e.g., transmit power, carrier frequency and modulation strategy) in real time, with two primary objectives in mind [3]:

i) Highly reliable communications whenever and wherever needed;

ii) Efficient utilization of the radio spectrum

Cognitive radio consists of three essential components [4]: (1) Spectrum sensing: The secondary users are required to sense and monitor the radio spectrum environment within their operating range to detect the frequency bands that are not occupied by primary users; (2) Dynamic spectrum management:

Cognitive radio networks are required to dynamically select the best available bands for communications; and (3) Adaptive communications: A cognitive radio device can configure its transmission parameters (carrier frequency, bandwidth, transmission power, etc) to opportunistically make best use of the ever-changing available spectrum [2,4,5].

The key issues in the cognitive radio are awareness, intelligence, learning, adaptivity, reliability and efficiency [2]. The aim of the cognitive radio is to use the natural resources efficiently, including frequency, time and transmitted energy.

Basically, cognitive radio has three major tasks which are [3]:

(1) radio-scene analysis

(2) channel identification, and

(3) dynamic spectrum management and transmit-power control.

The transmitter power control and dynamic spectrum management select the transmission power levels and frequency holes for transmission based on the results of radio scene analysis and channel identification. This task is carried out at the transmitter, which also requires some form of feedback between receiver and transmitter. The dynamic spectrum management guarantees dynamic spectrum access, which simply means that no static assignments of frequencies are made.

The three major tasks of the cognitive radio can be characterized with the

cognitive cycle as described in Figure 1.2 [3]. In general, the cognitive cycle is a continuous process comprising of sensing, understanding, deciding and adapting.

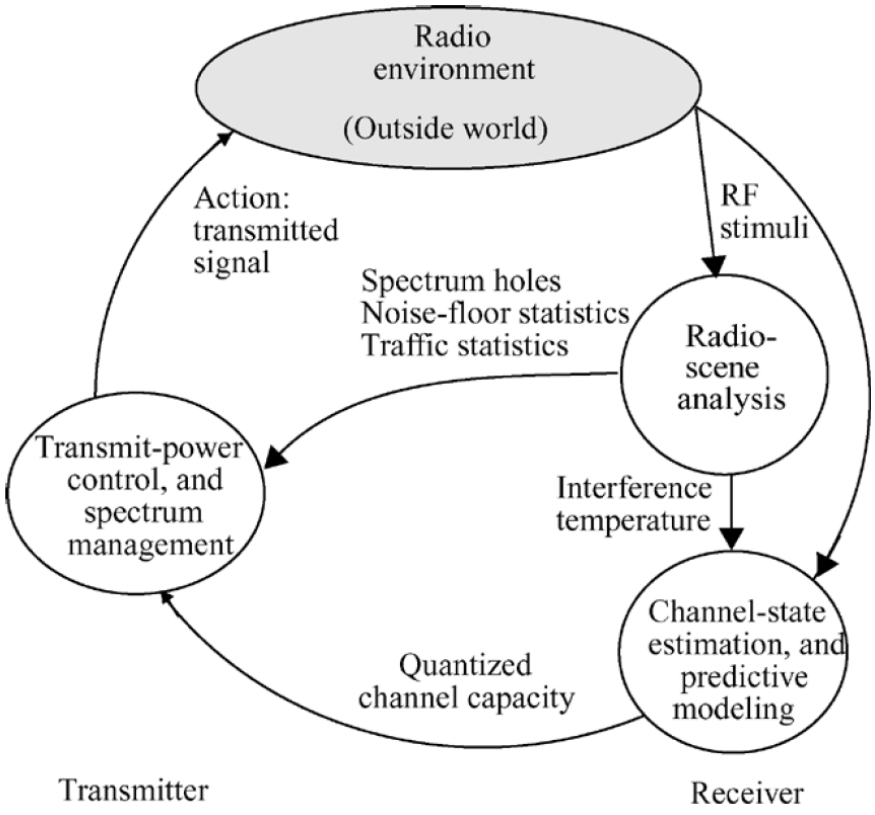


Figure 1.2. Basic Cognitive cycle [3]

Chapter 2 Spectrum sensing techniques

2.1 Overview

Detecting the unused spectrum and sharing it without harmful interference with other (secondary) users, spectrum sensing is an important function of cognitive radio. Spectrum sensing techniques generally can be classified into two categories, which are local spectrum sensing [6] and cooperative spectrum sensing [7, 8]. Actually according to different standards, spectrum sensing techniques can also fall into three categories, which are transmitter detection (also known as local spectrum sensing), cooperative detection and interference based detection.

In cooperative spectrum sensing, the initial sensing decision is made either based on local sensing data or local sensing decisions. Before final decisions about spectrum use are made, all local measurements of several cognitive radio nodes will be combined to provide more reliable information about the availability of the spectrum. Therefore, cooperative detection can be used to improve the performance of spectrum sensing. Cooperative spectrum sensing algorithms also have been extensively studied.

In local spectrum sensing, the sensing decision on whether the band is vacant or not is made individually by the secondary users. Local sensing algorithms include several approaches such as matched filter detection, energy detection and cyclostationary feature detection (refer to the next three sections for details). The detection is a test of the following two hypotheses [6]:

(1) H_0: The input at the pre-filter is noise alone:

a) $y(t) = n(t)$

b) $E[n(t)] = 0$

(2) H_1: The input at the pre-filter is signal plus noise

a) $y(t) = s(t) + n(t)$

b) $E[s(t) + n(t)] = s(t)$

where we assume that $s(t)$ is the input signal and $n(t)$ is additive white Gaussian noise (AWGN) with zero mean and unit spectrum density.

2.2 Matched filter

The matched filter is the optimal linear filter for maximizing the signal to noise ratio (SNR) in the presence of additive white Gaussian noise and is commonly used in radar and sonar systems.

In communications systems, when the secondary user knows the primary

user signal at physical layer, such as modulation and pulse shape, the optimal signal detection method is to use matched filter detection [9]. The principle advantage of a matched filter is that matched filter needs less time to achieve high processing gain due to the coherent detection. The disadvantage for matched filter detection technique is that it requires a priori knowledge of the primary signal to guarantee coherent detection, i.e., a dedicated receiver is required for every primary user. However, the performance can be improved by using pilot symbols (e.g., CDMA system), preambles (e.g., OFDM system), synchronization codes, and equalization of the primary signal [9, 10].

2.3 Energy Detector

The energy detector consists of a square law device followed by a finite time integrator as shown in Figure 2.1. The pre-filter serves to limit the noise bandwidth and the noise at the input to the squaring device has a band-limited, flat spectral density. The output of the integrator at any time is the energy of the input to the squaring device over the interval T seconds in the past. The test statistic at the detector is

$$K = \int_{t-T}^{t} y^2(\tau) d\tau .$$

By comparing the output with the threshold value, the detector makes a

decision whether the spectrum is available or not. In this case, the receiver does not need to know any prior knowledge of the transmitted signal. In other words, the advantage of energy detection is that we do not necessarily need much information about the primary user.

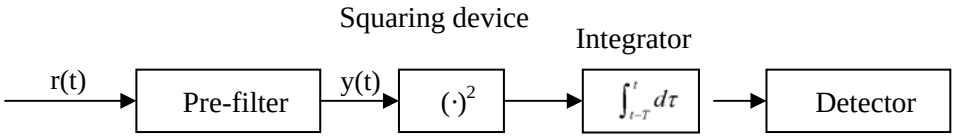


Figure 2.1. Energy detector diagram

Using an energy detector to measure the energy in the received waveform over an observation window when the transmitted signal is unknown was studied in many classic papers [6, 11, 12]. Assuming deterministic signals transmitted over a flat band-limited Gaussian noise channel, Urkowitz [6] derived both the probability of detection and the probability of false alarm. Kostylev [11] gave the derivation of the probability of detection for signal transmission over a variety of fading channels.

In our work, we assume that the primary signaling is unknown at the receiver side and thus energy detection is adopted for spectrum sensing. See the next chapter for more information.

2.4 Cyclostationary feature detection

In cyclostationary feature detection [13], modulated signals are coupled with sine wave carriers, pulse trains, hopping sequences or cyclic prefixes, which results in built-in periodicity. The idea of cyclostationary feature detection is to utilize the built-in periodicity of the modulated signal.

The advantage of cyclostationary feature detection is that it is robust against random noise and thus has better performance than matched filter or energy detector detection at low SNR [2].

2.5 Problem statement

As mentioned above, spectrum sensing provides a solution to the contradiction between spectrum shortage and low spectrum utilization by allowing for dynamic access of unused bands. However, spectrum sensing, as the key technique in cognitive radio, exposes vulnerabilities [14] that an intelligent adversary, whose goal is to disrupt the system performance, can exploit. That is, in the sensing duration the adversary can launch a spoofing signal in unused bands to deceive the secondary user, or can jam signals in busy bands to increase the symbol error rate. By definition, the busy bands are those that are currently occupied by primary users, while the allowable/unused bands, which can be accessed by secondary users through spectrum sensing, are those that

are not currently used by primary users. In the transmission duration the adversary can further degrade the system performance through traditional jamming techniques. In brief, spoofing reduces the effective available bandwidth for secondary user data transmission, while jamming increases the symbol error rate of primary user and/or secondary user. To analyze the attack strategy of the adversary, in our work the following two scenarios are considered.

2.5.1 Scenario I

The spectrum of interest is divided into multiple bands with identical bandwidth and they can be categorized into two types: busy bands (currently occupied by primary users) and allowable bands (currently not occupied by primary users). In this scenario, we focus on the allowable bands. The adversary can emit signals in the allowable (unused) bands to deceive secondary users into thinking that the unused bands are occupied by primary users, thus preventing the secondary user from accessing the system. A worst case theoretical analysis and derivation of optimal sensing disruption strategies have been studied in [15]. It was shown that the optimal disruption strategy is obtained by maximizing the average number of the secondary users' false detections under a total power constraint of the adversary. Specifically, the optimal strategy is an equal-power

partial-band spoofing. In our work, we will simulate this optimal disruption process and establish whether the simulation results match well with the numerical ones.

2.5.2 Scenario II

We assume that the adversary knows which bands are vacant and which are occupied by primary users. In the previous scenario, we studied how the adversary affects the secondary user's access by spoofing the vacant bands without considering primary users. The problem is what will happen if we take into account the primary user and assume that the adversary also jams the primary users.

We employ a periodic spectrum sensing cognitive radio system. The frame structure consists of a sensing slot and a data transmission slot in each frame. The primary users don't need to sense before accessing while the secondary users need to. To make the problem simple, we assume that the adversary can correctly detect which bands are occupied by primary users and which ones are available for secondary users. The goal of the adversary is to minimize the total throughput of the system under the adversary's total energy constraint. In the following chapter, we will analyze the worse-case performance of both primary users and secondary users, which is measured by total throughput of all users.

Numerical results indicate that there is a tradeoff between spoofing and jamming, as well as between jamming primary users and jamming secondary users.

Chapter 3 System model

3.1 Introduction

The system of interest in scenario I is shown in Figure 3.1, and the channel is AWGN channel.

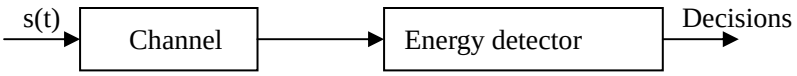


Figure 3.1. System model

The spectrum range of interest in divided into multiple identical bandwidth bands, as shown in Figure 3.2 [15]. Basically there are two types of bands, i.e. busy bands and allowable bands.

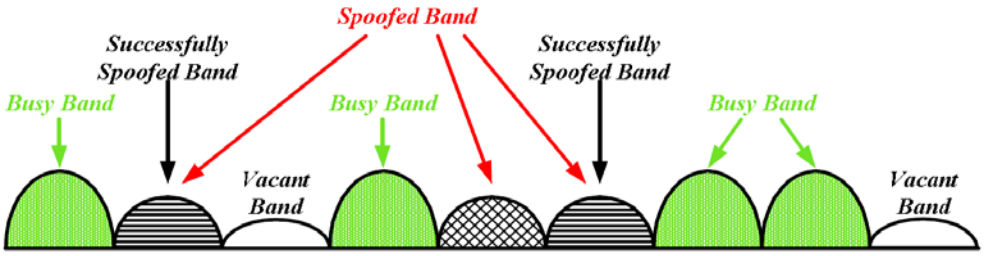


Figure 3.2. Spectrum bands elaboration [15]

We know the allowable bands are those that are not currently used by primary users. However, not all the allowable bands will be accessed by the secondary users, because of the present of background noise. The actual

available bands for the secondary users are further reduced in a malicious sensing environment. Since the primary users are not required to sense before accessing, what we consider here only applies to secondary users. In other words, in order to know the effect of background noise and adversary to the secondary users, we just need to consider the allowable bands. Before going further, we first give some definitions that are going to be used for different bands. The allowable bands in which the adversary chooses to launch signals are termed spoofed bands, while the allowable ones that are not spoofed are called vacant bands. The probability that an allowable band is determined by a secondary user to be busy (due to thermal noise or both thermal noise and spoofed power) is called the *false detection probability*. The probability that a vacant bands (only with thermal noise) is sensed by a secondary user to be busy is termed the *false alarm probability* [15].

3.2 Theoretical analysis

3.2.1 Scenario Ⅰ

In order to avoid any kind of confusion, here we list the following notation that will be used in the following chapters:

N = number of allowable bands

N_J = average number of false detections

N^* = optimal number of spoofed bands

ΔN_J = average number of additional false detections due to spoofing

P = power of adversary

K = energy threshold value used by energy detector

TW = time bandwidth product

σ_n^2 = Gaussian noise variance

p_f = probability of false alarm

p_d = probability of detection

$p_m = 1 - p_d$ = probability of missing

We assume that at a specific time, there are N allowable bands and some of them are detected to be busy due to either thermal noise or adversary spoofing or both. The purpose of the adversary is to minimize the available bandwidth by maximizing N_J, subject to the adversary's power P constraint.

Reference [6] shows that under Gaussian approximations, the false alarm probability can be expressed as:

$$p_f = Q\left(\frac{K}{2\sqrt{TW}\sigma_n^2} - \sqrt{TW}\right) \tag{3.1}$$

where $Q(\cdot)$ is the Gaussian tail function given by

$$Q(x) = \frac{1}{2\pi} \int_{x}^{+\infty} e^{-t^2/2} dt \tag{3.2}$$

We assume the adversary is zero mean Gaussian distributed "noise" and the power emitted to each spoofed band is P_k. It is shown in [15] that the probability of determining the kth allowable band to be busy is given by:

$$p_k(P_k) = Q\left(\frac{K}{2\sqrt{TW}(P_k + \sigma_{n,k}^2)} - \sqrt{TW}\right) \tag{3.3}$$

The solution to this worst case sensing deception problem is to maximize the following summation [15]

$$\max_{P_k} \sum_{k=1}^{N} Q\left(\frac{K}{2\sqrt{TW}(P_k + \sigma_{n,k}^2)} - \sqrt{TW}\right) \tag{3.4}$$

subject to

$$\sum_{k=1}^{N} P_k - P = 0 \text{ and } P_k \geq 0, k = 1, 2, ..., N \text{ .} \tag{3.5}$$

3.2.2 Scenario II

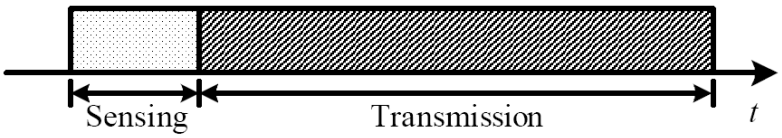


Figure 3.3. Frame structure for cognitive radio [16]

To make the problem simple, we assume that the adversary can correctly

detect the number of allowable bands (N_V) and busy bands (N_P), and that it knows the system timing (sensing/transmission time duration as shown in Figure 3.3). The adversary can launch signals in either busy bands or vacant bands or both.

a) Busy bands

In this case, we get two effects:

(1) increase the packet error rate through jamming primary users

(2) increase the probability of detection of secondary users, which is not desired by the adversary.

b) Vacant bands

This increases the probability of false alarm and thus decreases the average number of allowable bands to access by secondary users.

The object of the adversary is to

$$\min(\Gamma(P)+\Gamma(S)) \tag{3.6}$$

subject to $E = \text{Constant}$

where $\Gamma(P)$ and $\Gamma(S)$ are the throughput of the primary users and the secondary users, respectively. E is the total energy of the adversary.

A. Probability of Packet Error

First let's derive the probability of packet error with jamming. The block diagrams in Figure 3.4 [16] show the transmitter and receiver of the *j*th primary user.

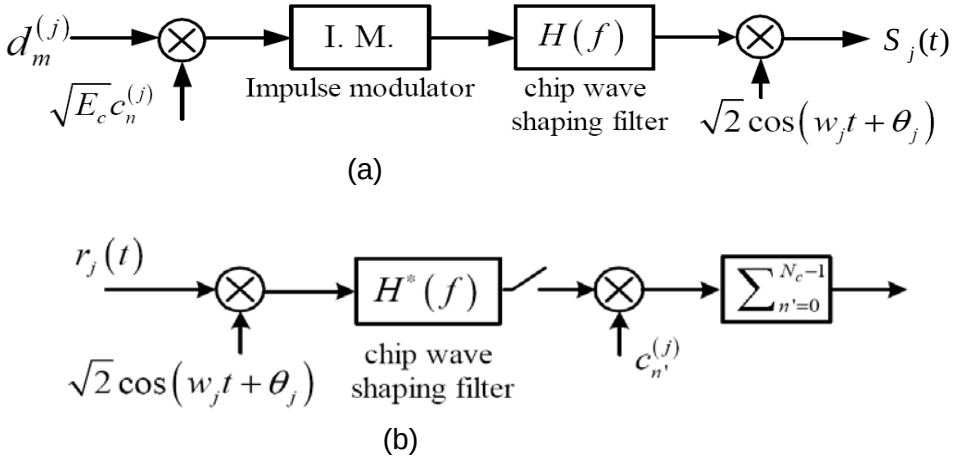


Figure 3.4. System model (a) transmitter, (b) receiver [16]

Here $d_m^{(j)}$ is a random binary data sequence, $c_n^{(j)}$ is a PN sequence, N_c is the number of chips per symbol and E_c is the chip energy. $m = \left\lfloor n/N_c \right\rfloor$, $h(t)$ is the impulse response of the chip wave shaping filter, and θ_j is a random carrier phase uniformly distributed over $[0, 2\pi]$ [16, 17].

The transmitted signal is given by [16]

$$S_j(t) = \sqrt{2E_c}\sum_{n=-\infty}^{\infty} d_m^{(j)} c_n^{(j)} h(t - nT_c)\cos(\omega_j t + \theta_j) \qquad (3.7)$$

and the transmitted signal is corrupted by AWGN and a Gaussian jamming signal due to the intelligent adversary. We assume the jammer is independent of the

background additive Gaussian noise. The spectrum of the jamming signal in each band is rectangular and has a bandwidth equal to the bandwidth of that band. Also we assume that $X(f) = H(f)H^*(f)$, which is a raised-cosine filter with β as a measure of the excess bandwidth, and satisfies the Nyquist criterion to guarantee that the DS waveforms don't overlap in adjacent bands.

The received signal is then given by [16]:

$$r(t) = \sum_{j=1}^{\Omega_k} \sqrt{2E_c} \sum_{n=-\infty}^{\infty} d_m^{(j)} c_n^{(j)} h(t - nT_c) \cos(\omega_j t + \theta_j) + n_w(t) + n_J(t) \qquad (3.8)$$

where $n_w(t)$ is AWGN with double-sided psd of $\eta_0/2$ and $n_J(t)$ is the received jamming signal with a double-sided psd $\eta_J/2$ in each jammed band. We have that $\eta_J = P_{J,P,k}/W$, where $P_{J,P,k}$ is the jamming power in the *k*th primary user band and W the bandwidth of that band. We assume the jamming strategy is equal-power, partial-band jamming, which means the jamming power in each jammed band is equal.

In the sensing duration, the symbol error rate of the *j*th primary user with BPSK modulation in the *k*th jammed band is approximately given by [16-20]

$$SER_{sensing,P,k}^{(j)} = Q\left(\sqrt{\frac{2N_c E_c}{(\Omega_k - 1)(1 - \beta/4)E_c + \eta_J + \eta_0}}\right) \qquad (3.9)$$

where Ω_k represents the number of users in each band. Hence the packet error rate is:

$$PER_{sensing,P,k}^{(j)} = 1-(1-SER_{sensing,P,k}^{(j)})^{z} \tag{3.10}$$

B. $p_{N,i}$ *due to jamming in sensing duration*

In sensing duration, the adversary may spoof some vacant bands and deceive the secondary users that those bands are occupied by primary users. The false detection probability (i.e., the probability that vacant bands are sensed to be busy by secondary users due to both thermal noise and spoofing) in the *k*th band is given by [15]

$$p_k(P_{D,k}) = Q(\frac{K/2\sqrt{T_0W}}{P_{D,k}+\sigma_n^2} - \sqrt{T_0W}) \tag{3.11}$$

where $P_{D,k}$ is the spoofing power in the *k*th band. Here we assume that the spoofing strategy is partial band equal power spoofing. Note that the false alarm probability (due to thermal noise only) in the *k*th vacant band is given by

$$p_f = Q(\frac{K/2\sqrt{T_0W}}{\sigma_n^2} - \sqrt{T_0W}) \tag{3.12}$$

Therefore the probability that i out of N_V bands is detected to be vacant by secondary user is [15]:

$$
\begin{aligned}
p_{N_V,1} &= C^1_{N_{V,spoof}} (1-p_k)\, p_k^{(N_{V,spoof}-1)}\, p_f^{(N_V-N_{V,spoof})} \\
&+ p_k^{N_{V,spoof}}\, C^1_{N_V-N_{V,spoof}} (1-p_f)\, p_f^{(N_V-N_{V,spoof}-1)} \\
\\
p_{N_V,2} &= C^2_{N_{V,spoof}} (1-p_k)^2\, p_k^{(N_{V,spoof}-2)}\, p_f^{(N_V-N_{V,spoof})} \\
&+ C^1_{N_{V,spoof}} (1-p_k)^1\, p_k^{(N_{V,spoof}-1)} C^1_{N_V-N_{V,spoof}} (1-p_f)\, p_f^{(N_V-N_{V,spoof}-1)} \\
&+ p_k^{N_{V,spoof}}\, C^2_{N_V-N_{V,spoof}} (1-p_f)^2\, p_f^{(N_V-N_{V,spoof}-2)} \\
&\cdots\cdots \\
p_{N_V,N_V} &= (1-p_k)^{N_{V,spoof}}\, (1-p_f)^{N_V-N_{V,spoof}}
\end{aligned}
\tag{3.13}
$$

where $N_{V,spoof}$ is the number of spoofed bands.

Now we analyze the throughput in the sensing and the transmission duration.

C. Throughput in sensing duration

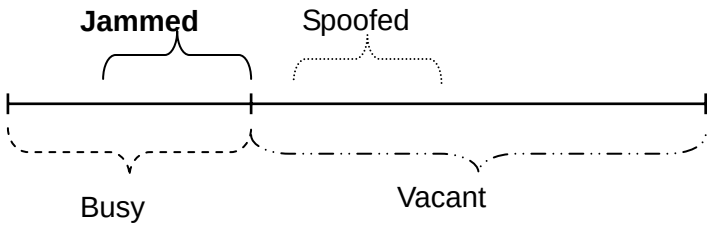


Figure 3.5. Attack strategies in sensing duration

In the sensing duration, the adversary may jam some primary users' (PU)

occupied bands and spoof some vacant bands as shown in Figure 3.5. The throughput of the primary user is considered here.

Let $\Gamma^{(j)}_{sen\sin g,P,k}$ be the throughput of the *j*th primary user in the *k*th band during the sensing duration. It equals [16]

$$\Gamma^{(j)}_{sen\sin g,P,k} = (1 - PER^{(j)}_{sen\sin g,P,k}) z \log_2 M \tag{3.14}$$

where z is the number of symbols per packet and $\log_2 M$ is the number of bits per symbol and $PER^{(j)}_{sen\sin g,P,k}$ is the probability of packet error of the *j*th primary user in the *k*th band (see (3.9) and (3.10)).

The sum throughput of the primary users in the *k*th band can be expressed as:

$$\Gamma_{sen\sin g,P,k} = \sum_{j=1}^{\Omega_k} \Gamma^{(j)}_{sen\sin g,P,k} \tag{3.15}$$

where Ω_k is the number of primary users in the *k*th band.

The average sum throughput of the primary users in the sensing slot is given by:

$$\Gamma_{sen\sin g,P} = \sum_{k=1}^{N_P} \Gamma_{sen\sin g,P,k} \tag{3.16}$$

where N_P is the number of bands that are occupied by primary users.

D. Throughput in transmission duration

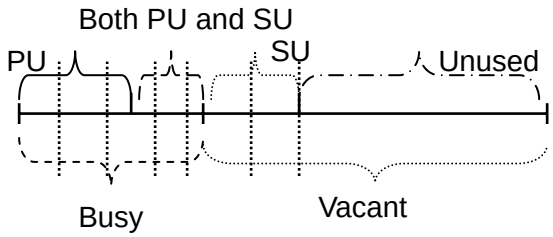


Figure 3.6. Attack strategies in transmission duration

Figure 3.6 shows the attack strategies of the adversary in transmission duration. The secondary users (SU) will send signals to the bands that are detected to be vacant and hence in some bands the primary user and secondary user may coexist. Also the number of required bands by secondary users and the number of vacant bands may different. To make the problem simple, we assume that the secondary users can correctly detect the bands that are occupied by primary users.

Here, the throughput of the primary users and the secondary users are both considered. The throughput of the primary users in the transmission slot is given by [16]

$$\Gamma_{tran,P} = \sum_{k=1}^{N_P} \sum_{j=1}^{\Omega_k} \Gamma_{tran,P,k}^{(j)} = N_P \Omega_k \Gamma_{tran,P,k}^{(j)} \tag{3.17}$$

where

$$\Gamma_{tran,P,k}^{(j)} = (1 - PER_{tran,P,k}^{(j)}) z \log_2 M \tag{3.18}$$

$$PER_{tran,P,k}^{(j)} = 1-(1-SER_{tran,P,k}^{(j)})^{z} \tag{3.19}$$

$$SER_{tran,P,k}^{(j)} = Q(\sqrt{\frac{2N_cE_c}{(\Omega_k-1)(1-\beta/4)E_c+\eta_J+\eta_0}}) \tag{3.20}$$

The throughput of the secondary users is [16]

$$\Gamma_{tran,S} = \sum_{i=1}^{N_V} p_{N_V,i} \sum_{k=1}^{i} \sum_{j=1}^{\Omega_k} \Gamma_{tran,S,k}^{(j)} \tag{3.21}$$

where $p_{N_V,i}$ is the probability that i out of N_V bands are detected to be vacant by secondary users as given in (3.13), and

$$\Gamma_{tran,S,k}^{(j)} = (1-PER_{tran,S,k}^{(j)})z'\log_2 M' \tag{3.22}$$

$$PER_{tran,S,k}^{(j)} = 1-(1-SER_{tran,S,k}^{(j)})^{z'} \tag{3.23}$$

$$SER_{tran,S,k}^{(j)} = Q(\sqrt{\frac{2N_c'E_c'}{(\Omega_k'-1)(1-\beta'/4)E_c'+n_J'+n_0}}) \tag{3.24}$$

$$n_J' = \frac{P_{J,S,k}'}{W} \tag{3.25}$$

Here z', M', Ω_k', β', N_c', E_c' are parameters of the secondary user, with the same meaning as the corresponding parameters for the primary users. To make the problem simple, we assume that all the parameters are the same as those of the primary users.

Now if we add the throughput of the primary users and secondary users

together we then get the total system throughput, which can be expressed as:

$$\Gamma = \Gamma_{sen\sin g,P} + \Gamma_{tran,P} + \Gamma_{tran,S} \tag{3.26}$$

The object is to minimize the system throughput, subject to

$$(1+\alpha)T_0 \sum_{k=1}^{N_P} P_{J,P,k} + T_0 \sum_{k=1}^{N_V} P_{D,k} + \alpha T_0 \sum_{k=1}^{N_V} P_{J,S,k} = E \tag{3.27}$$

where $P_{J,P,k}$, $P_{D,k}$ and $P_{J,S,k}$ are the jamming power in the *k*th primary user band, spoofing power in the *k*th vacant band, and jamming power in the *k*th secondary user occupied band, respectively.

Chapter 4 Simulation model and results (Scenario I)

4.1 Simulation model

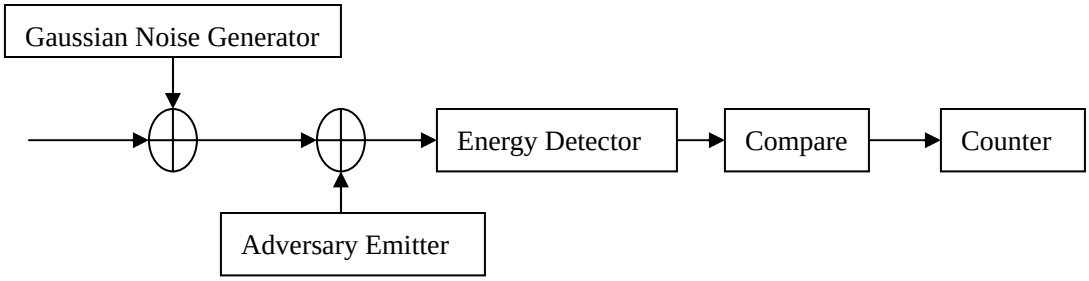


Figure 4.1. AWGN model

Figure 4.1 shows the receiver side block diagram of an AWGN channel. It consists of Gaussian noise generator, adversary emitter, energy detector and comparator.

Gaussian Noise Generator

Generally we can use the random variables that are uniformly distributed in the interval (0, 1) to generate some other random variables with a different probability density function (PDF). For example, we desire to generate a random variable v with cumulative distribution function (CDF) $F(v)$. Since $F(v)$ is limited in the interval (0, 1), so we can first generate a (0, 1) interval uniformly

distributed random variable u. Let $F(v)=u$, then we have $v=F^{-1}(u)$. Thus the desired random variable v with CDF $F(v)$ is generated.

For AWGN channel, the thermal noise is Gaussian white noise with PDF,

$$f(v)=\frac{1}{\sqrt{2\pi}\sigma}e^{-v^2/2\sigma^2} \tag{4.1}$$

where σ^2 is the standard derivation of v. It is CDF is

$$F(v)=\int_{-\infty}^{v} f(x)dx \tag{4.2}$$

We know random variable R with Rayleigh distribution has the following CDF,

$$F(R)=\begin{cases}0 & R<0\\ 1-e^{-R^2/2\sigma^2} & R>0\end{cases} \tag{4.3}$$

This random variable R is related to a pair of Gaussian random variables U and V through the following transformation,

$$\begin{aligned}U&=R\cos\Theta\\ V&=R\sin\Theta\end{aligned} \tag{4.4}$$

where Θ satisfies uniform distribution in the interval $(0,2\pi)$ and σ^2 is the variance of U and V.

Let

$$F(R)=u \tag{4.5}$$

We have

$$R=\sqrt{2\sigma^2\ln(\frac{1}{1-u})}\,, \tag{4.6}$$

where u is a random variable uniformly distributed in the interval (0, 1).

Now if we generate another in the (0, 1) interval uniformly distribution random variable v and define

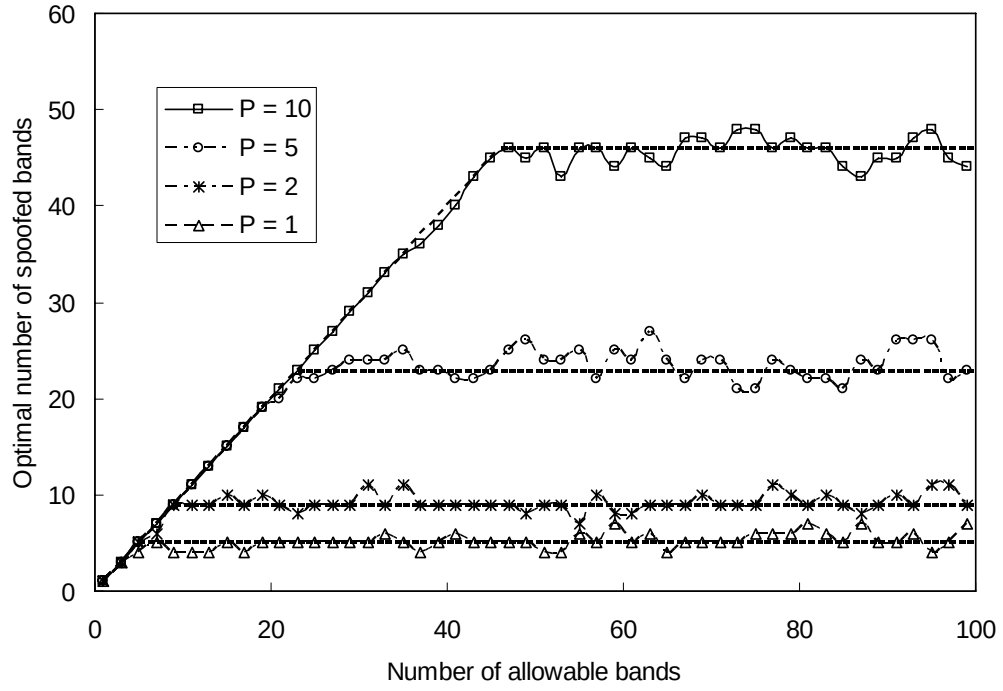
$$\Theta = 2\pi v \tag{4.7}$$

then using u and v we can generate two statistically independent Gaussian random variables U and V by employing the transformation function.

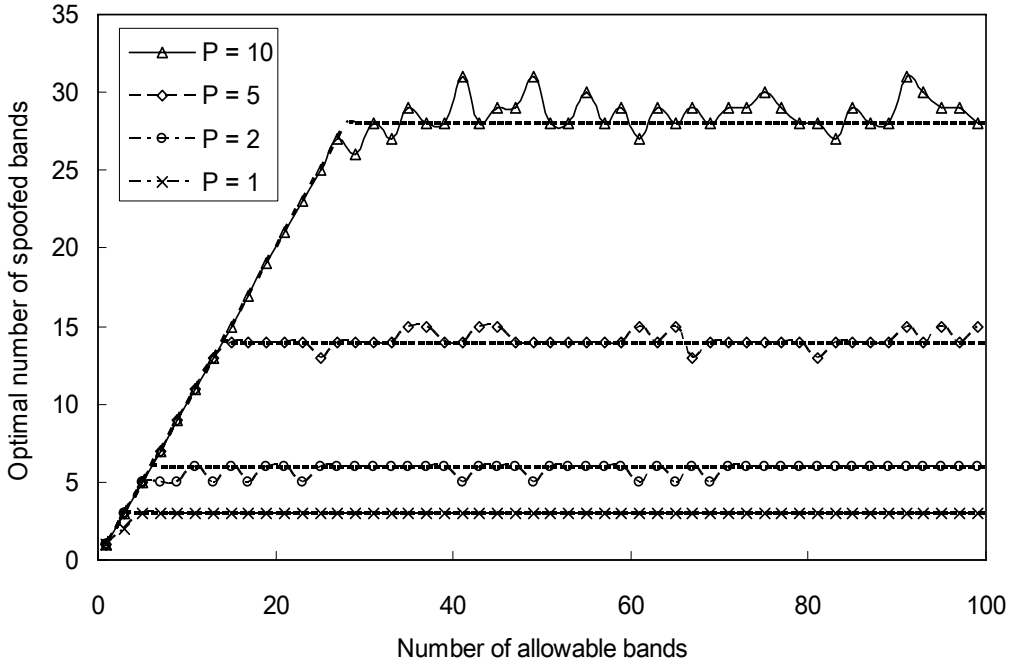
If the channel is a Rayleigh fading channel, we just need to add a Rayleigh random number generator to the block diagram. Rayleigh random number can be generated using either formula $R = \sqrt{2\sigma^2 \ln(\frac{1}{1-u})}$ or formula $R = \sqrt{U^2 + V^2}$, where U and V both satisfy a Gaussian distribution.

4.2 Simulation results

Figure (4.2) shows how the optimal number of spoofed bands N^* varies with the number of allowable bands N parameterized by the total spoofer power. The threshold value corresponds to noise power $\sigma_n^2 = 1$, $TW = 100$, $p_f = 0.05$ and $p_f = 0.005$ respectively. It is seen that all the simulated data points are distributed around the numerical results. The fluctuation is due to the random nature of the thermal noise. Comparing 4.2 (a) and (b), it shows for the same



(a)



(b

Figure 4.2. Optimal number of spoofed bands versus number of allowable bands *N* with different spoofing powers *P*

($\sigma_n^2 = 1, TW = 100$) (a) $p_f = 0.05$, (b) $p_f = 0.005$

spoofing power the saturation value of optimal number of spoofed bands for $p_f = 0.05$ is larger than that for $p_f = 0.005$. This is because N^* is a function of false detection probability and a lower false alarm probability gives a lower false detection probability and thus a smaller optimal number of spoofed bands.

In Figure (4.3) the optimal number of spoofed bands is plotted versus the spoofing power to noise power ratio for a fixed time-bandwidth product $TW = 100$. The simulated data points are corresponding to different threshold value for different false alarm probability. It is seen that increasing p_f indicates an increase

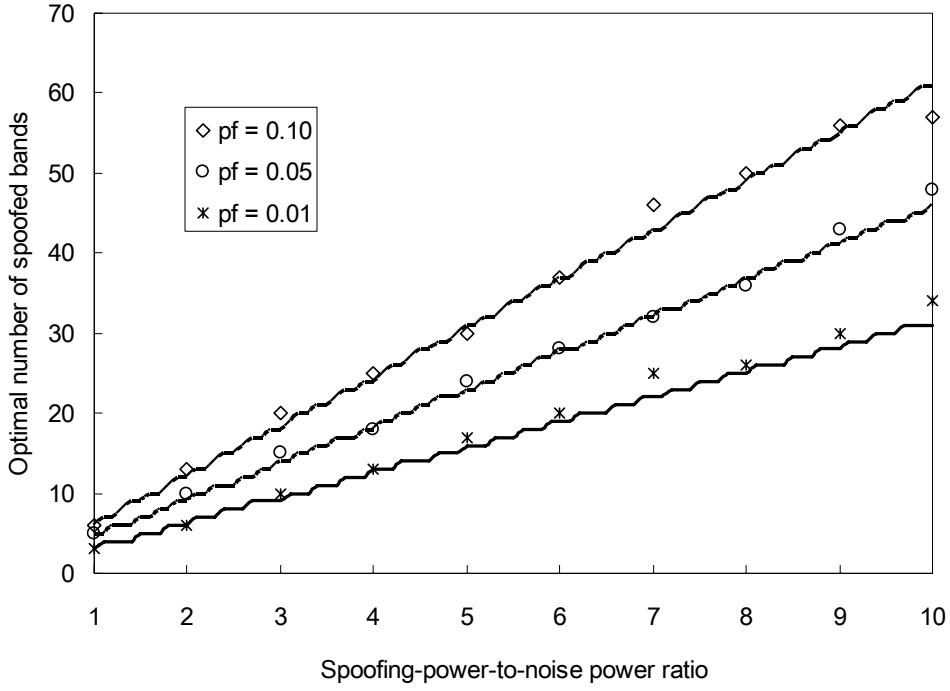
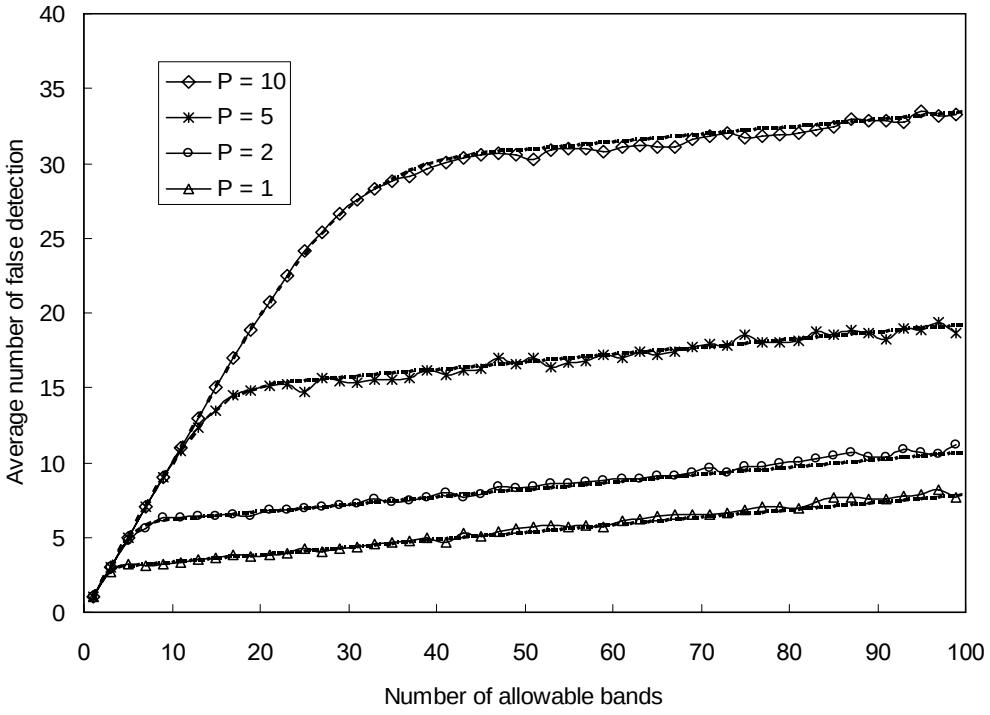


Figure 4.3. Optimal number of spoofed bands N^* versus spoofing-power-to-thermal-noise-power ratio with different values of p_f. ($TW = 100$)

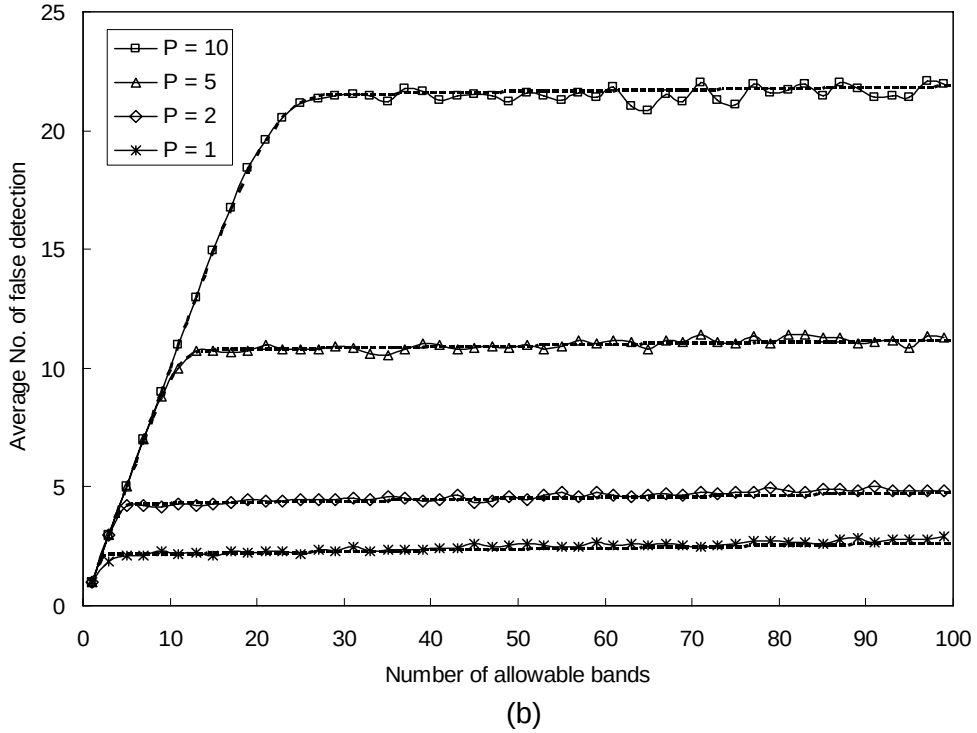
of N^*.

In Figure 4.4, the average number of false detection versus the number of allowable bands is plotted. It is seen that the simulated results distribute around the numerical results. Comparing (a) with (b), we see that for the same spoofing power, the average number of false detection is larger in (a) than in (b).

With the same parameters as in Figure 4.4, the average number of additional false detections due to spoofing versus the number of allowable bands is plotted in Figure 4.5. Note that when the number of allowable bands N is large, the number of average additional false detection ΔN_J becomes constant. This is because of the adversary energy budget and there will be no spoofing power put into more than N^* bands.



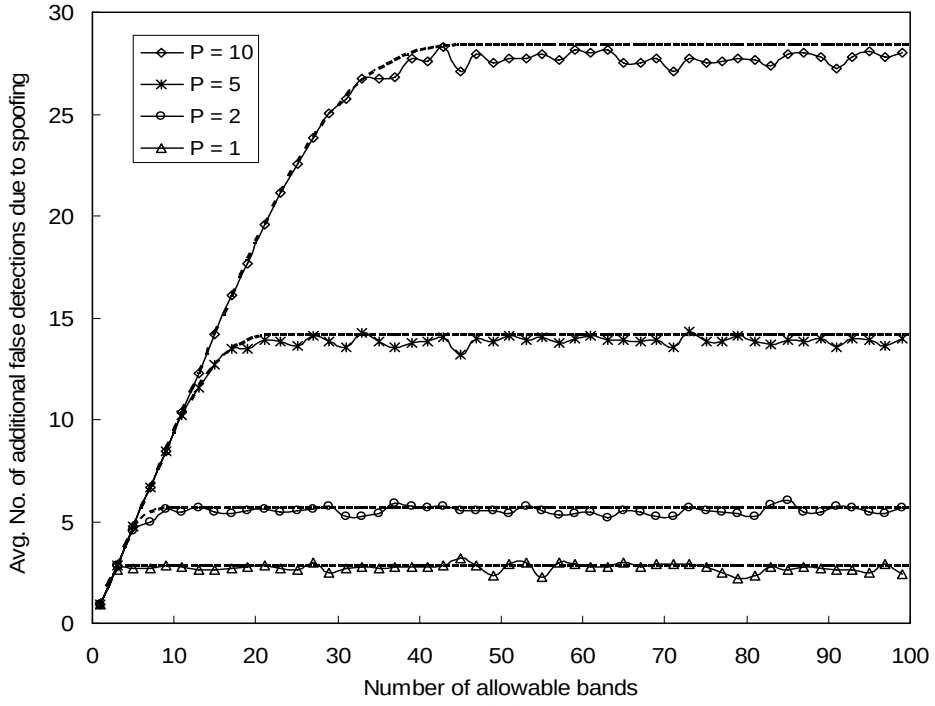
(a)



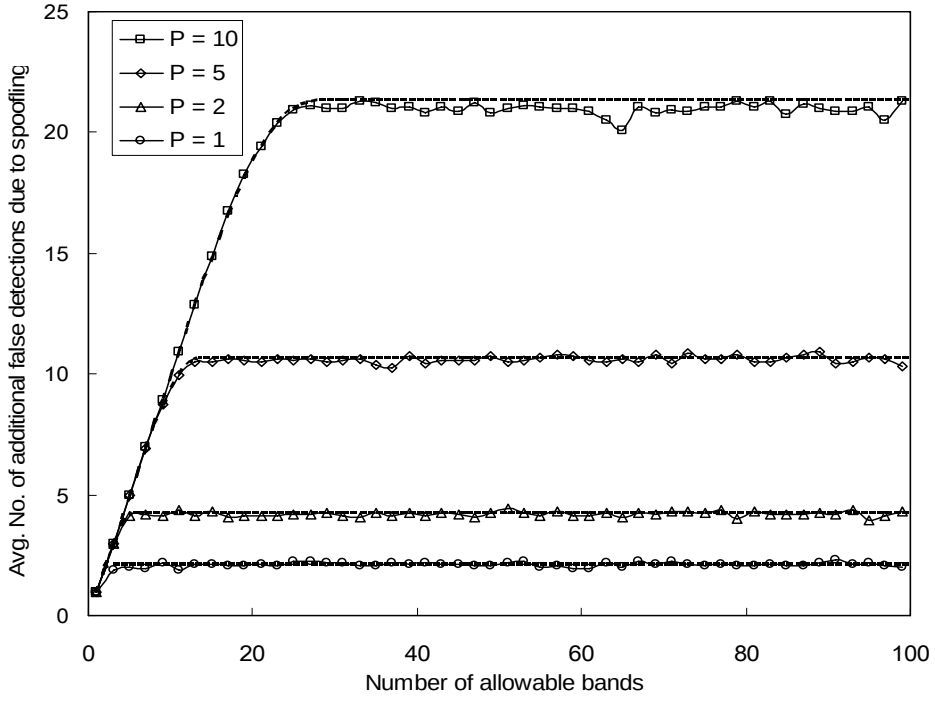
(b)

Figure 4.4. The average number of false detection versus number of allowable bands with different spoofing powers

($\sigma_n^2 = 1, TW = 100$) (a) $p_f = 0.05$ (b) $p_f = 0.005$



(a)



(b)

Figure 4.5. The average number of additional false detection due to spoofing versus number of allowable bands with different spoofing powers ($\sigma_n^2 = 1, TW = 100$) (a) $p_f = 0.05$ (b) $p_f = 0.005$

Chapter 5 Numerical results (Scenario II)

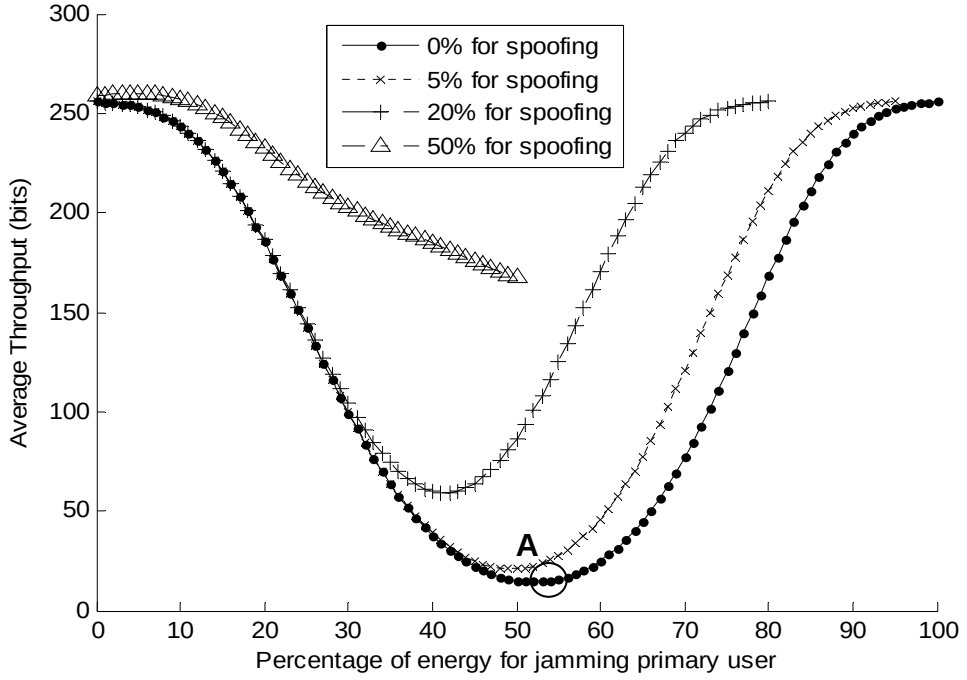
In this chapter, numerical results for the performance analysis of the above cognitive radio adversary are provided. Here all the parameters are the same as in [16]. The transmission to sensing duration ratio α is set to 10 [14], the measure of the excess bandwidth β is set to 0.5, the number of symbols per packet z equals 256 and the number of chips per symbol is set to 128. The thermal noise power in one allowable band at the energy detection receiver σ_n^2 is normalized to unity and the maximum number of users that can coexist in each band is 10. We assume that the average received energy of each user is identical and E_b/η_0 is set to 10dB. As in [16], we also define J/S as the jamming-to-signal power ratio, where J is the jamming power when the adversary puts all energy into jamming secondary users, i.e. $J = E/\alpha T$ with T as the time duration of sensing. The J/S value of interest is 21dB [16].

In the following, the adversary performance in different scenarios that are categorized by the number of spectrum vacancies required by secondary users (i.e. $N_{R,SU}$) is analyzed. To make the problem simple, we assume that the adversary knows which bands are occupied by primary users and are allowable to

secondary users.

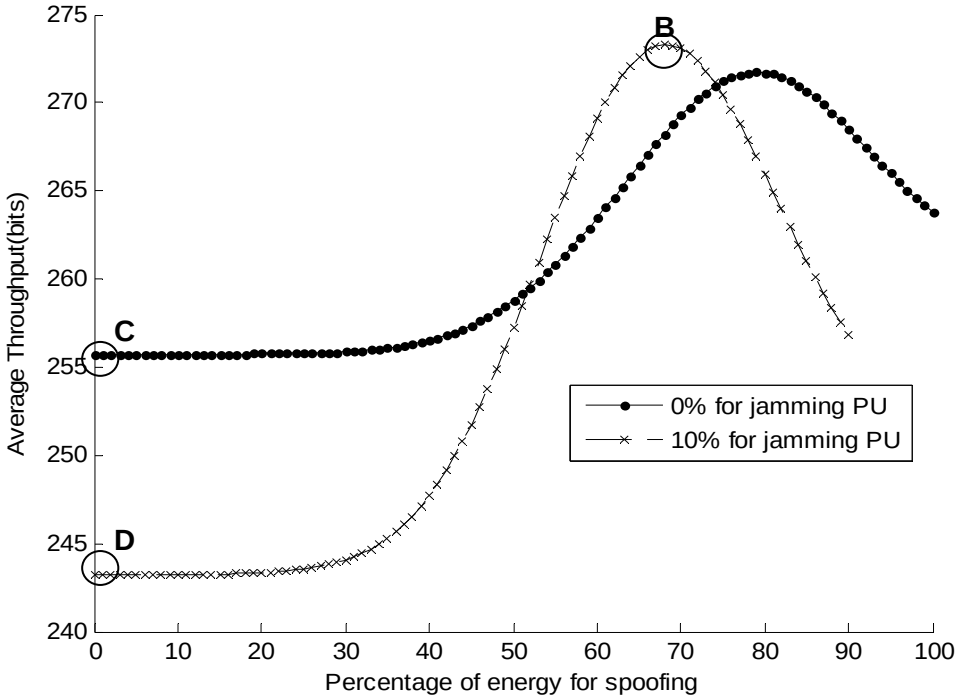
5.1 $N_{R,PU}=1, N_{R,SU}=1$

In Figures 5.1(a) the system average throughput versus the percentage of energy for jamming the primary user is plotted and in Figure 5.1(b), (c) the system average throughput versus the percentage of energy for spoofing are plotted. It is seen that the minimum throughput is achieved when no adversary energy is allocated to spoofing, i.e., the optimal strategy in this case is just to jam the primary user and secondary user. From Figure 5.1(a), it is seen that the

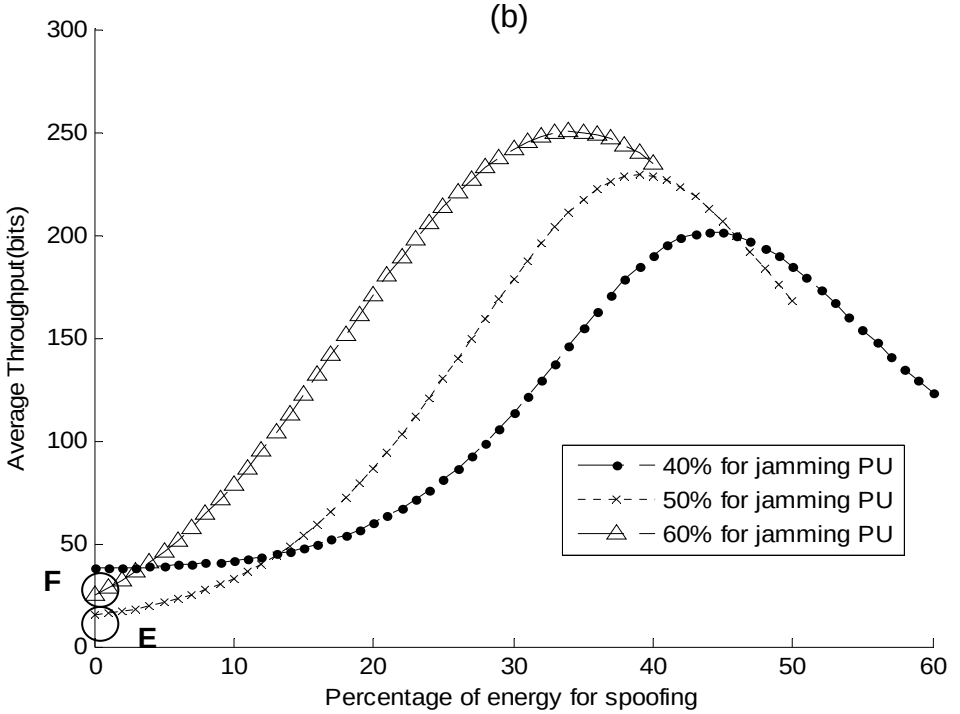


(a)

Figure 5.1. System average throughput versus (a) percentage of energy for jamming primary user, (b)/(c) percentage of energy for spoofing ($N=21, TW=25, p_f=10^{-4}, J/S=21dB$)



(b)



(c)

Figure 5.1. (*continued*) System average throughput versus (a) percentage of energy for jamming primary user, (b)/(c) percentage of energy for spoofing ($N = 21, TW = 25, p_f = 10^{-4}, J/S = 21dB$)

throughput is minimized when the adversary puts roughly 52% of its energy in jamming the primary user and the remaining 48% in jamming secondary user. From Figures 5.1(b) and (c), it is seen that for a specific percentage of energy for jamming primary user, the system average throughput increases as the percentage of energy for spoofing increases, i.e., 0% spoofing gives the corresponding minimum system average throughput. From Figure 5.1(c), we can see that the system average throughput at zero spoofing decreases as the percentage of energy for jamming the primary user increases until point F, while after this point it increases as the percentage of energy for jamming the primary user increases (from point E to F).

Now let's analyze the results further. We concluded that the optimal attack strategy is to put 52% of the energy in jamming the primary user and 48% of the energy in jamming the secondary user. Note that $\frac{52\%}{48\%} \approx \frac{\alpha+1}{\alpha}$, ($\alpha = 10$, i.e., the transmission to sensing duration ratio), which means the ratio of jamming the primary user and jamming the secondary user is close to the transmission duration ratio of them. This makes sense because the adversary also jams the primary user in the sensing duration, while the secondary user does not contribute to the throughput yet.

In order to better understand the results in these Figures, in the following we present numerical results for three cases (1) spoofing only: the adversary puts all energy in spoofing in the sensing duration; (2) jamming primary user only: the adversary puts all energy in jamming the primary user; (3) jamming secondary

user only: the adversary puts all energy in jamming the secondary user in the transmission duration.

Figure 5.2 shows the system average throughput versus the adversary-power-to-signal-power ratio. Note that for jamming only, the adversary power actually is the jamming power, while for spoofing only it is the spoofing power. It is seen that for the same P/S ratio, the system average throughput with jamming is smaller than that with spoofing. Therefore in this case jamming is more effective than spoofing. On the other hand, for a given adversary power the system average throughput with jamming the primary user only and the system average throughput with jamming the secondary user only are the same, i.e., jamming the primary user and jamming the secondary user are almost equal efficient. However, the data transmission durations of the primary user and secondary user are not the same, with the former being longer. Therefore, the adversary puts a little bit more energy into jamming the primary user, which is consistent with our previous analysis.

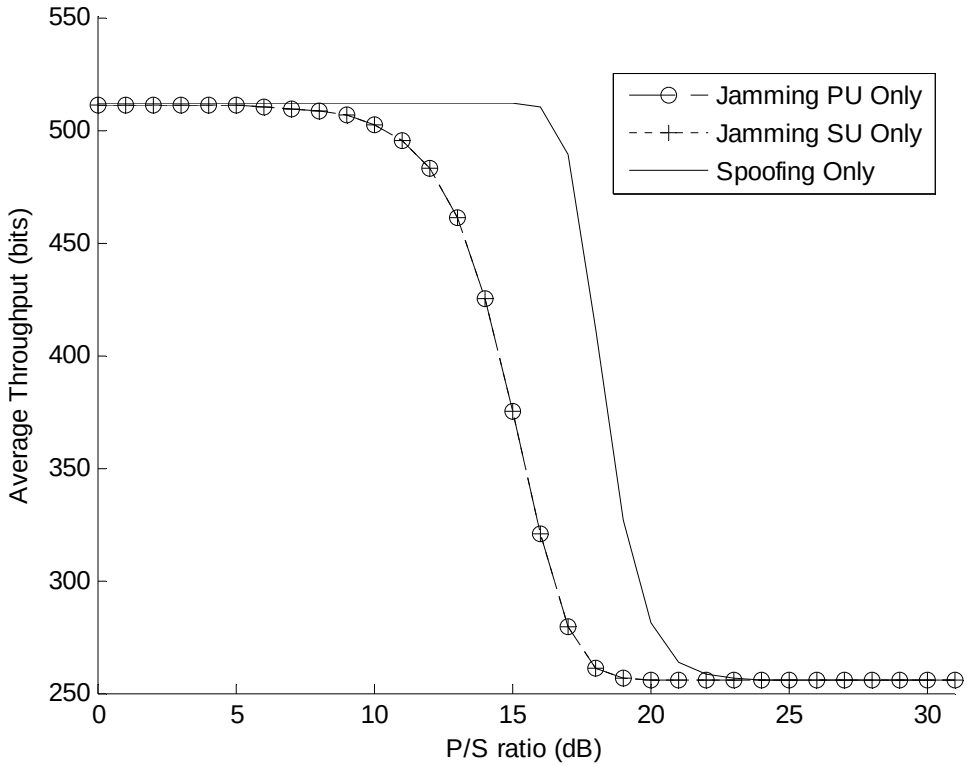


Figure 5.2. System average throughput versus P/S ratio

($N = 21, TW = 25, p_f = 10^{-4}$)

In the following, we explain the behavior of the average throughput in Figures 5.1(a) and (b). We know that the system throughput consists of two parts: (1) the primary user throughput and (2) the secondary user throughput. The primary user throughput is proportional to $(1-PER)$ (referred to as the packet success rate) due to jamming, while the secondary user throughput is proportional to both $(1-PER)$ due to jamming and $(1-p_k)$ (referred to as the probability of access) due to spoofing.

Figure 5.3 shows the primary user and secondary user packet success

rates versus the percentage of energy for jamming the primary user with 0% of the energy for spoofing. We know the throughput of the secondary user is

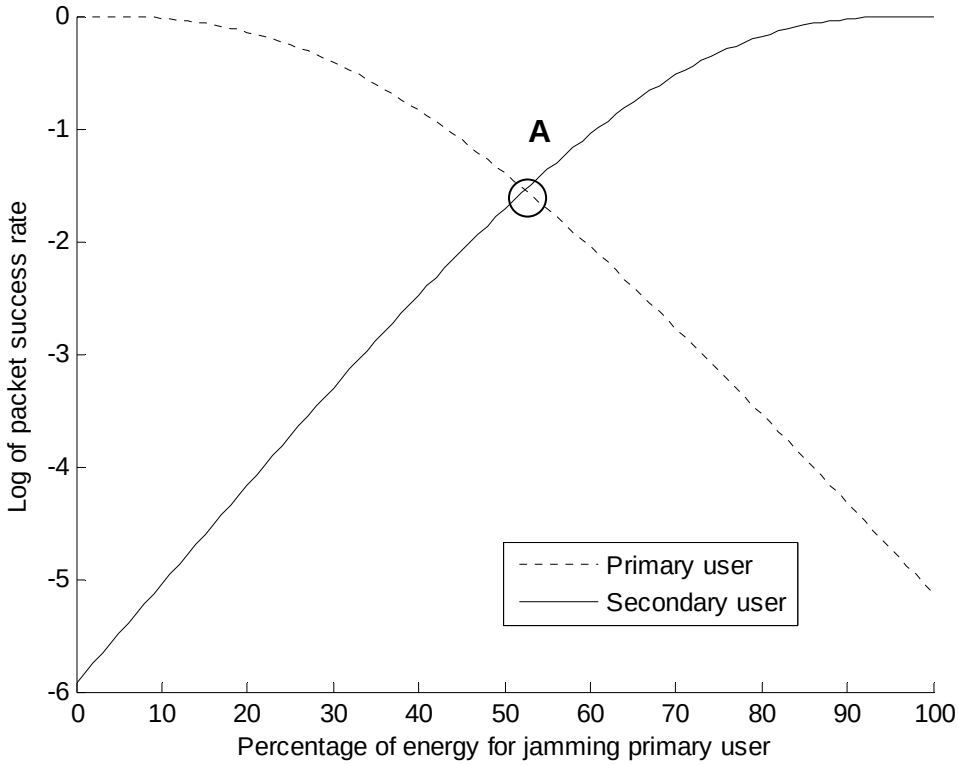


Figure 5.3. Log of packet success rate versus the percentage of energy for jamming primary user ($N = 21, TW = 25, p_f = 10^{-4}, J/S = 21dB$)

proportional to two terms: the probability of access and the packet success rate. However, for a fixed percentage of energy for spoofing, the probability of access of the secondary user is a constant. Thus, the throughput of the secondary user is proportional to the packet success rate only, as is the throughput of the primary user. It is seen that on the left side of point A, the secondary user packet success rate is smaller compared to the primary user packet success rate. So the system

average throughput is dominated by the primary user, i.e., decreases as the percentage of energy for jamming the primary user increases. Similarly, on the right side of point A, the system average throughput is dominated by the secondary user, i.e., increases as the percentage of energy for jamming the primary user increases. Therefore the system throughput is minimized at point A, which is consistent with the results in Figure 5.1(a).

We know that for a given percentage of energy for jamming the primary user, the throughput of the primary user is constant. Thus, the trend of the system average throughput is the same as the trend of the throughput of the secondary user. It can be seen from Figure 5.4 that as the spoofing energy increase, the packet success rate of the secondary user increases sharply until roughly point B and then decreases as the spoofing energy further increases. Meanwhile, the probability of access of the secondary user first is constant and then decreases. When the percentage of energy for spoofing is on the left of Point B, the packet success rate increases more sharply than the decrease of the probability of access. Thus, the trend of the average throughput in this region is dominated by the packet success rate. Similarly, the trend of the average throughput on the right of Point B is dominated by the decrease of the probability of success. Therefore, the system average throughput should first increases to point B and then decreases. This is consistent with the curve in Figure 5.1 (b).

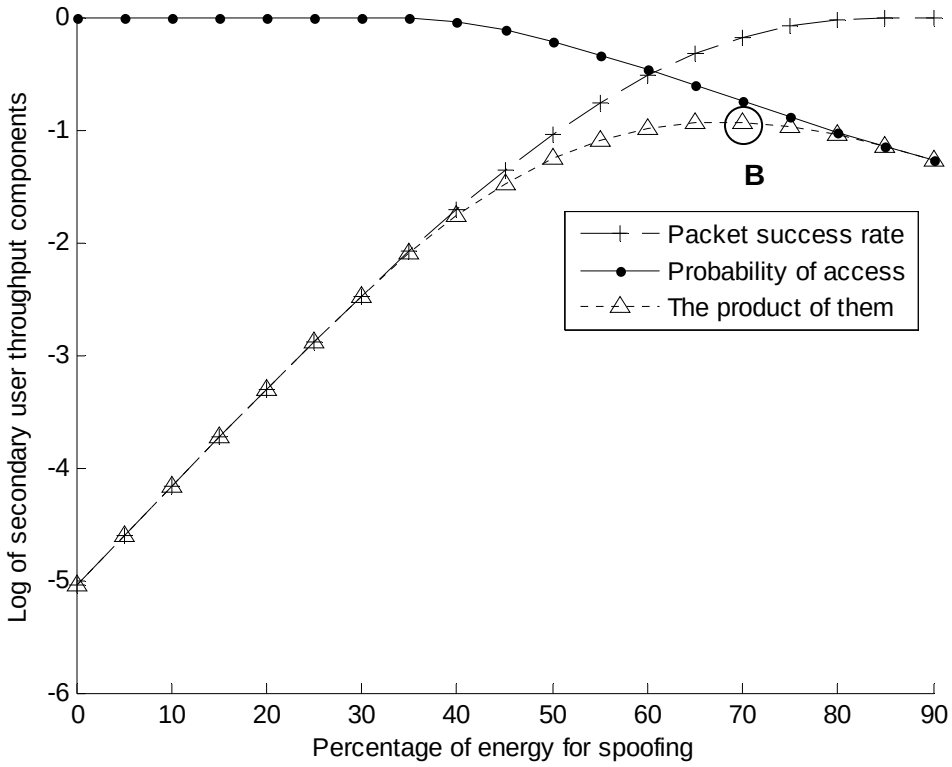


Figure 5.4. Log of secondary user throughput components versus the percentage of energy for spoofing with 10% of the energy used for jamming the primary user ($N = 21, TW = 25, p_f = 10^{-4}, J/S = 21dB$)

Now let's consider the primary user. It contributes less to the system throughput with 10% of the energy used for jamming it than with 0%. The difference is roughly 12 bits (from Figure 5.1 (b), it equals the throughput at point C minus the throughput at point D.) As shown in Figure 5.5, the throughput of the secondary user with 10% of the energy for jamming the primary user is larger than that with 0% of the energy for jamming the primary user. However, this small superiority cannot compensate the throughput degradation of the primary user

due to the 10% jamming energy except for the region between lines ① and ②, i.e., the secondary user throughput difference between these two lines is greater than 12 bits. This is consistent with the results in Figure 5.1(b).

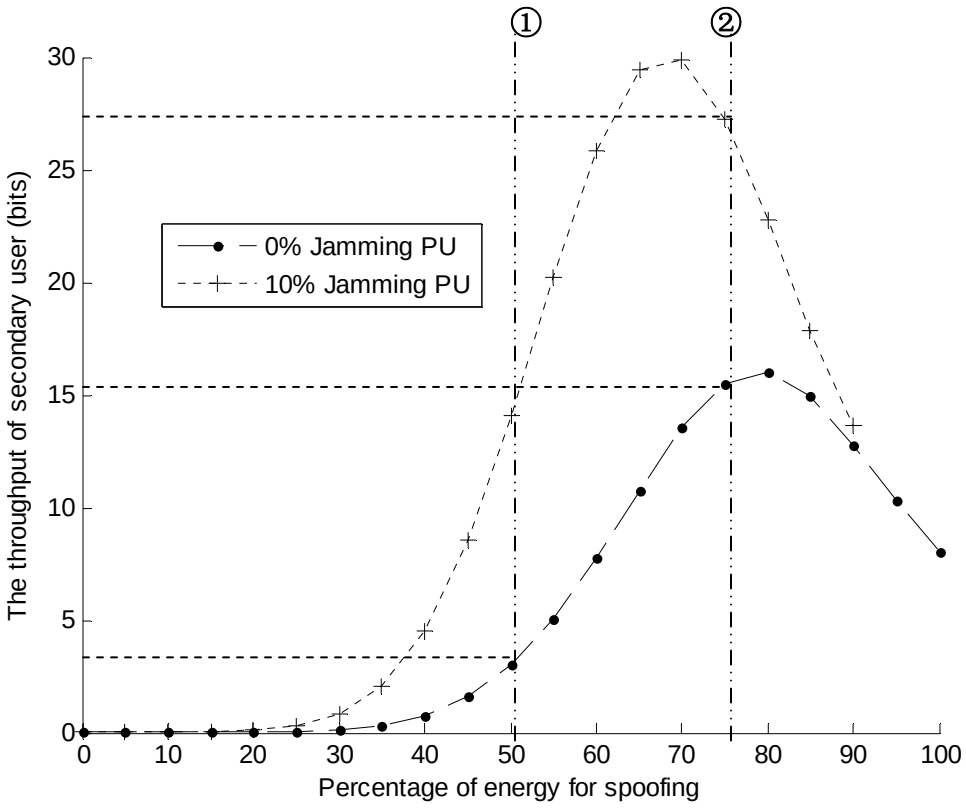


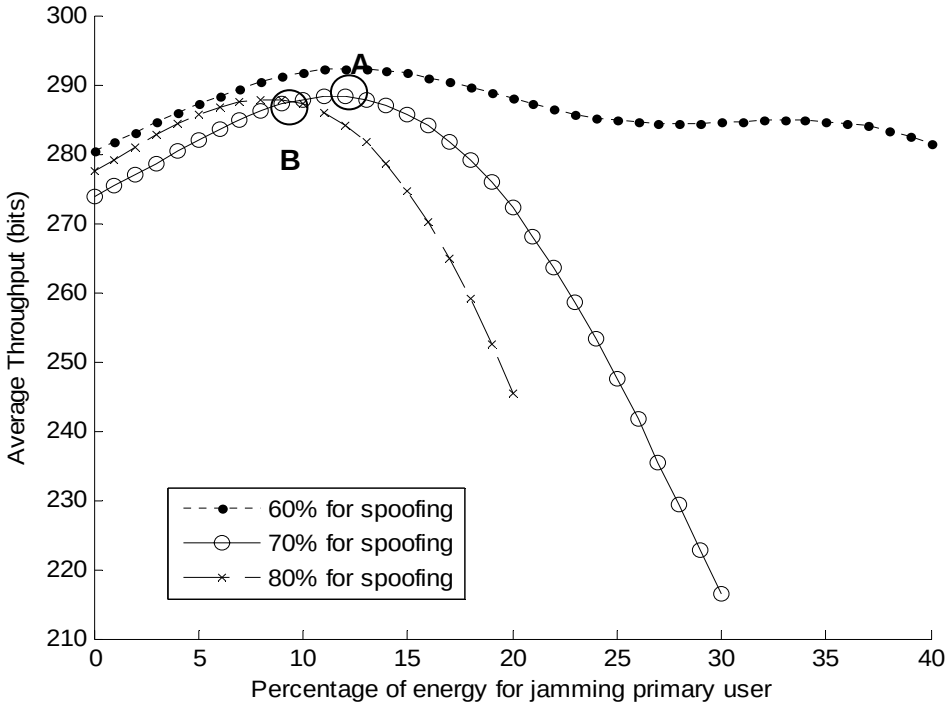
Figure 5.5. Throughput of secondary user versus the percentage of energy for spoofing ($N = 21, TW = 25, p_f = 10^{-4}, J/S = 21dB$)

5.2 $N_{R,PU} = 1, N_{R,SU} = 10$

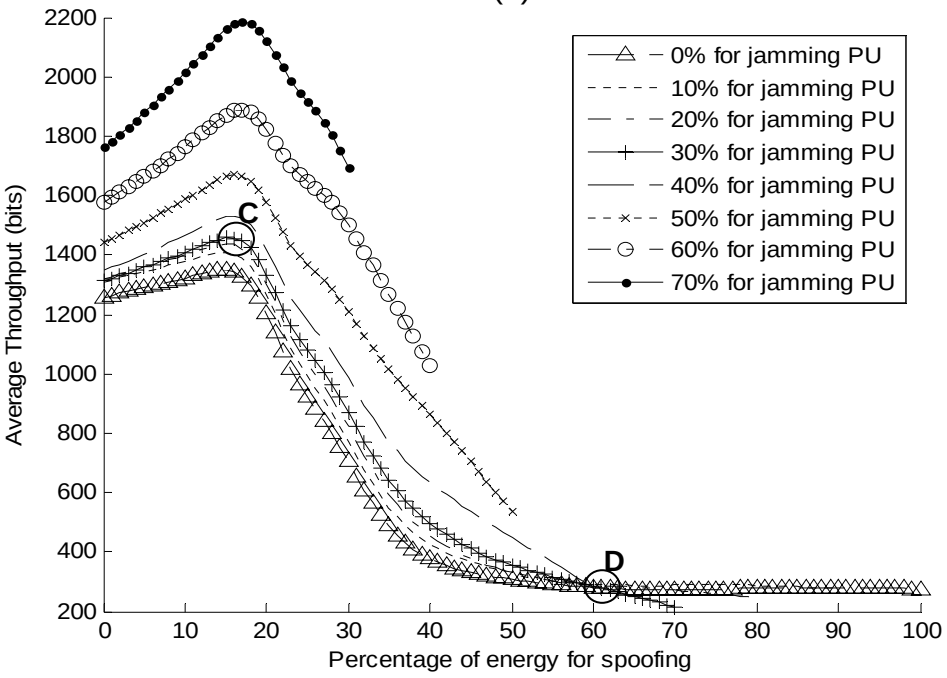
The system average throughput versus the percentage of energy for jamming the primary user and the percentage of energy for spoofing are plotted in

Figures 5.6 (a) and (b), respectively. It is seen that when the adversary puts roughly 70% of the energy in spoofing and 30% of the energy in jamming the primary user, the system average throughput is minimized. From [16], if there is no primary user, with the same parameter settings, the throughput is minimized when the adversary puts roughly 70% of the energy in spoofing, which is similar to our results. For the remaining 30% of the energy, jamming the primary use is more efficient than jamming the secondary user (Figure 5.6 (a)).

In order to further understand these results, in the following, we present numerical results for three cases (the same as the previous part) as shown in Figure 5.7. It is seen from Figure 5.7 (a) that for P/S equals 21dB, spoofing is more effective than jamming the secondary users. Therefore, the optimal strategy is to put energy in spoofing rather than jamming to minimize the throughput of the secondary user, and put the remaining energy in jamming primary user to minimize the throughput of the primary user.



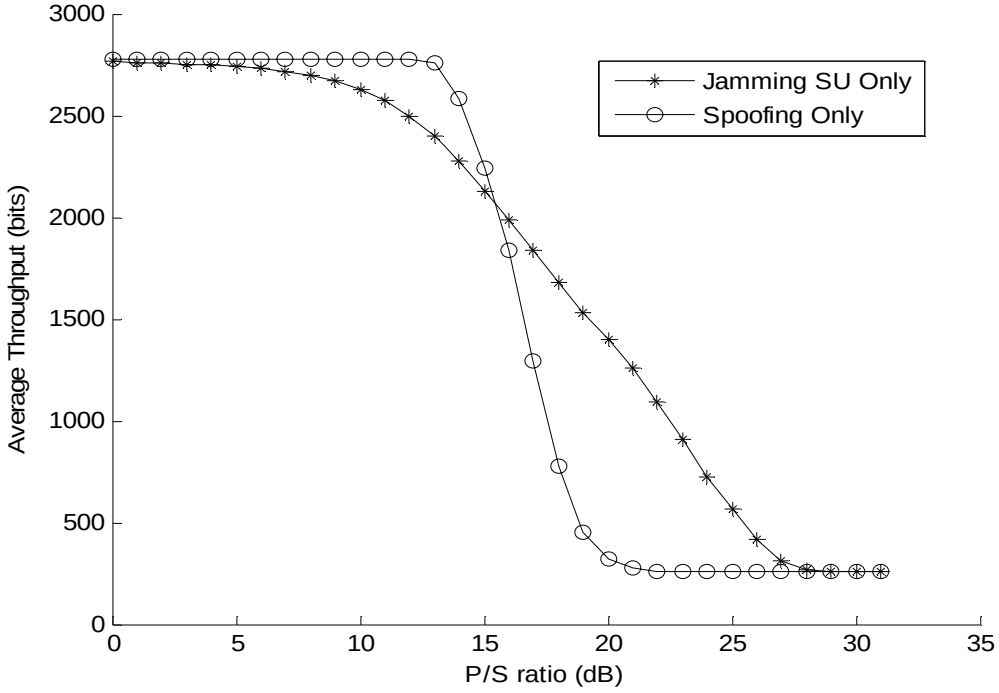
(a)



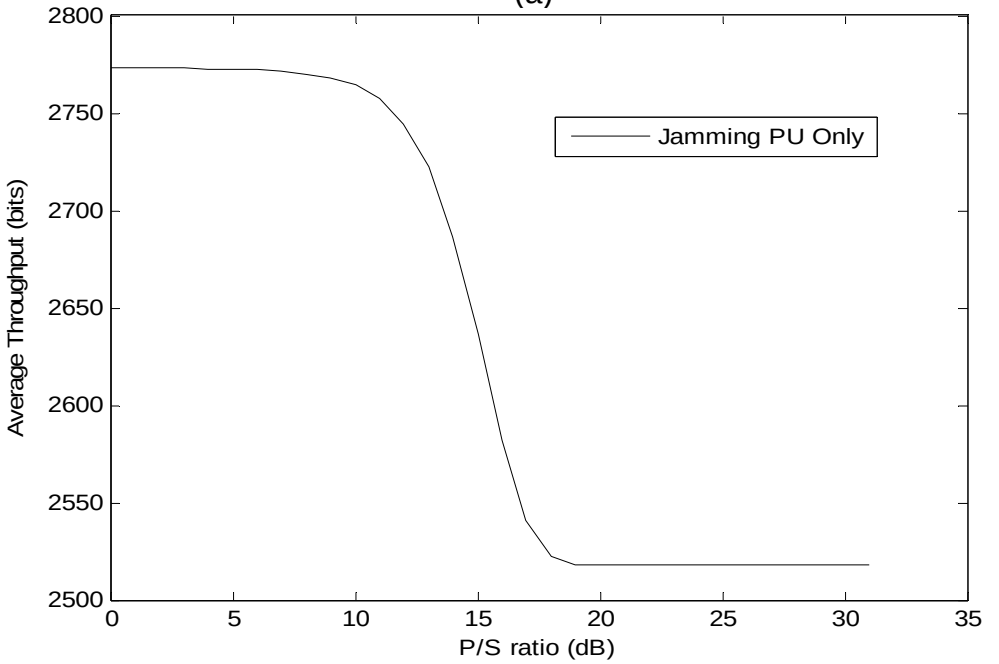
(b)

Figure 5.6. System average throughput versus (a) the percentage of energy for jamming primary user and (b) the percentage of energy for spoofing

($N = 21, TW = 25, p_f = 10^{-4}, J/S = 21dB$)



(a)



(b)

Figure 5.7. System average throughput versus P/S with (a) jamming the secondary user only/ spoofing only (b) jamming the primary user only ($N = 21, TW = 25, p_f = 10^{-4}$)

From Figure 5.7 (b), we can see for a large P/S ratio, the average throughput with jamming primary users only will reach a saturation value, which is the throughput of the secondary users. This makes sense, because if the adversary has enough energy and all of it is put in jamming primary users, the system average throughput will be dominated by the throughput of the secondary users.

Now in the following, we will present some other numerical results to explain the behavior of the system average throughput in Figure 5.6. In Figure 5.8, the primary user and secondary user packet success rates versus the percentage of energy for jamming the primary user, with 70% of the energy for spoofing, are plotted. It is seen that to the left of point A the increase of secondary user packet success rate is greater than the decrease of the primary user packet success rate as the energy for jamming the primary user increases (note that point A is not the cross point, and the increase or decrease speed depends on the slope of the curve). Thus, the trend of the system throughput is dominated by the secondary user, i.e., increases as the percentage of energy for jamming the primary user increases until point A. Similarly, to the right side of point A, the system average throughput is dominated by the decrease of primary user packet success rate, i.e. system throughput decreases as the percentage of energy for jamming the primary user increases. This is consistent with the results in Figure 5.6 (a).

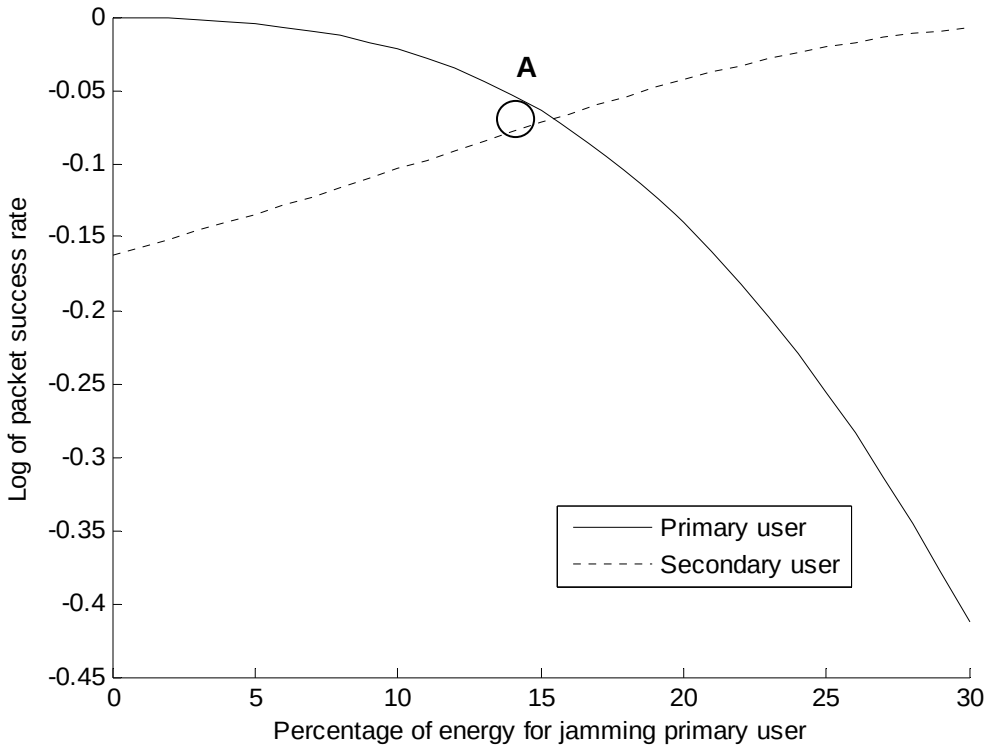


Figure 5.8. Log of packet success rate versus the percentage of energy for jamming the primary user with 70% of the energy for spoofing ($N = 21, TW = 25, p_f = 10^{-4}, J/S = 21dB$)

We know that the primary user throughput is proportional to the packet success rate, which is a function of the percentage of energy for jamming the primary user. Hence, the throughput of the primary user with a given percentage of energy for jamming the primary user is fixed. Therefore, the trend of the system average throughput is dominated by the throughput of the secondary users. Figure 5.9 shows the secondary user throughput versus the percentage of energy for jamming the primary user, with 70% and 80% of the energy for spoofing. It is seen that the secondary user throughput with 80% of the energy for spoofing is

larger than that with 70% of the energy for spoofing until point B, and then the curves cross. This is consistent with the results in Figure 5.6 (a), where the system average throughput with 80% of the energy for jamming the primary user is larger than that with 70% of the energy for jamming the primary user until point B, and then becomes less than that with 70% for jamming the primary user.

As shown in Figure 5.10, the secondary user packet success rate and the probability of access versus the percentage of energy for spoofing with

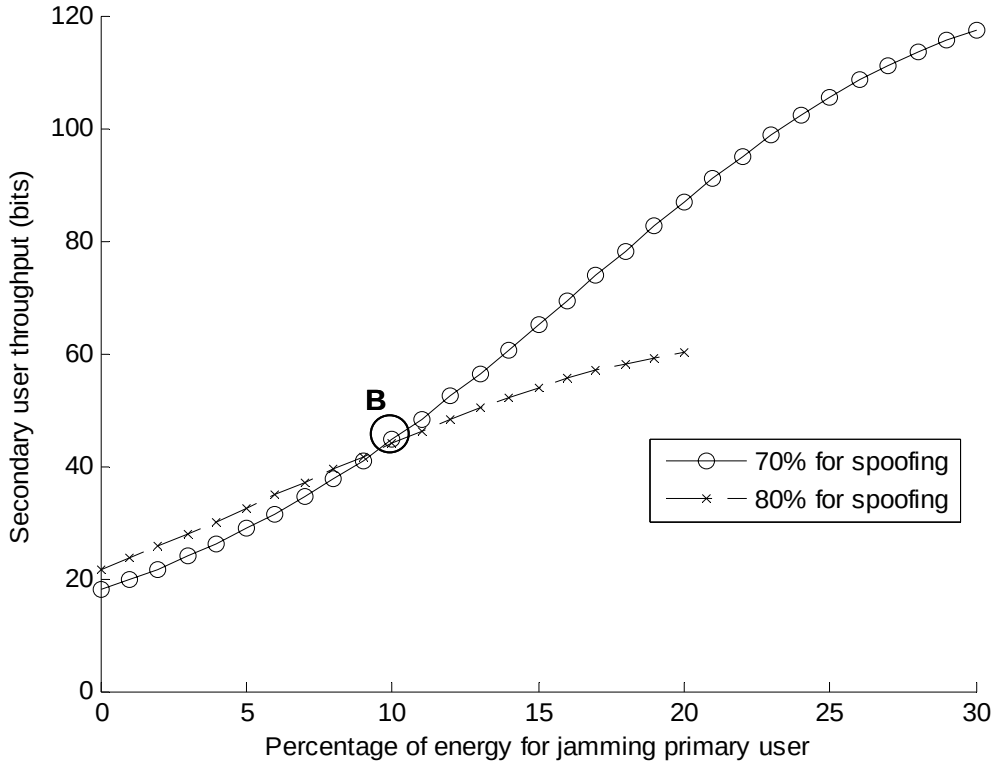


Figure 5.9. Secondary user throughput versus the percentage of energy for jamming the primary user ($N = 21, TW = 25, p_f = 10^{-4}, J/S = 21dB$)

30% of the energy for jamming the primary user are plotted. For a given

percentage of energy for jamming the primary user, the throughput of the primary user is a constant value. The trend of the system average throughput is thus determined by the trend of the secondary user throughput, which is proportional to the secondary user packet success rate and the probability of access. It is seen that the trend of secondary user throughput first is dominated by the packet success rate, and then, after point C, is dominated by the probability of access. This is consistent with the curve in Figure 5.6 (b), where the system throughput slowly increases as the spoofing energy increases until point C, where its maximum is achieved. After point C, the system throughput sharply decreases as the spoofing energy increases, and then its minimum is achieved.

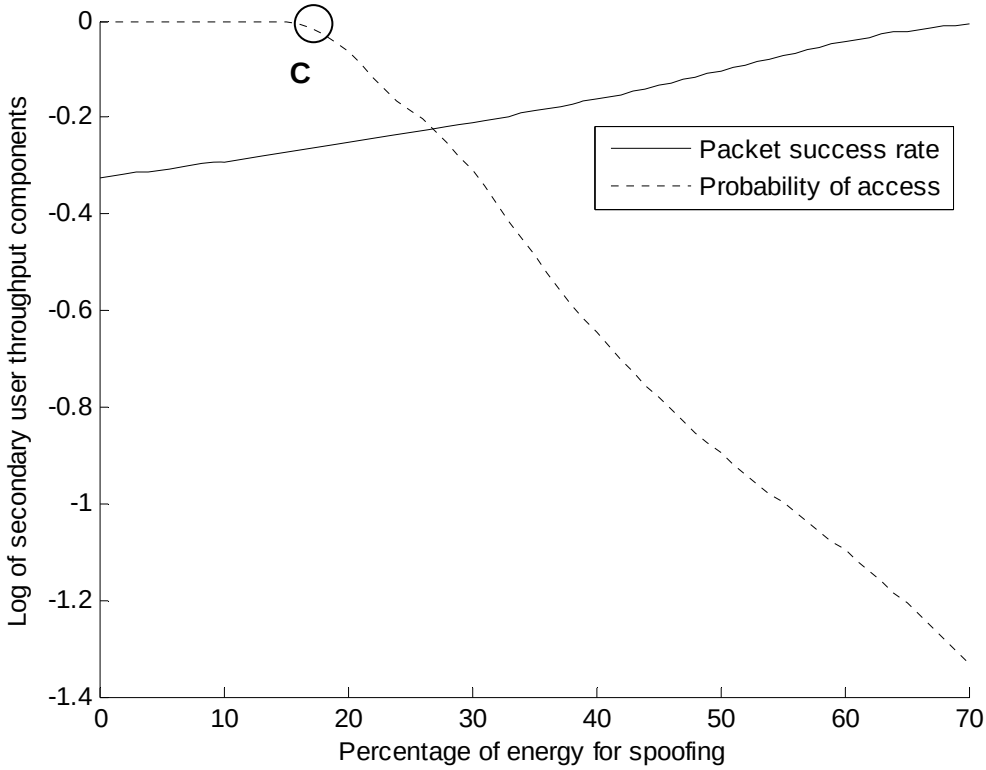


Figure 5.10. Log of secondary user throughput components versus the percentage of energy for spoofing with 30% of the energy for jamming the primary user ($N = 21, TW = 25, p_f = 10^{-4}, J/S = 21dB$)

Comparing the primary user throughput with 30% and 0% of the energy for jamming the primary user, we find that it decreases by about 157 bits with 30% of the jamming energy. The throughput of the secondary user versus the percentage of energy for spoofing, with 0% and 30% of the energy for jamming the primary user, are plotted in Figure 5.11. It is seen that to the left of point D, the throughput with 30% of the energy for jamming the primary user is larger than that with 0% of the energy for jamming the primary user. And the difference (greater than 157 bits) can compensate for the throughput degradation caused by the primary user.

Therefore, the system throughput is dominated by the secondary user until point D, i.e., the system average throughput with 30% of the energy for jamming the primary user is larger than that with 0% of the energy for jamming the primary user. However to the right side of point D, even through the secondary user throughput with 30% primary user jamming energy is still larger than that with 0% primary user jamming energy, the difference cannot compensate for the degradation caused by jamming the primary user. Thus, the system throughput with 30% of the energy for jamming the primary user is smaller than that with 0% of the energy for jamming the primary user, which is consistent with the results in Figure 5.6 (b).

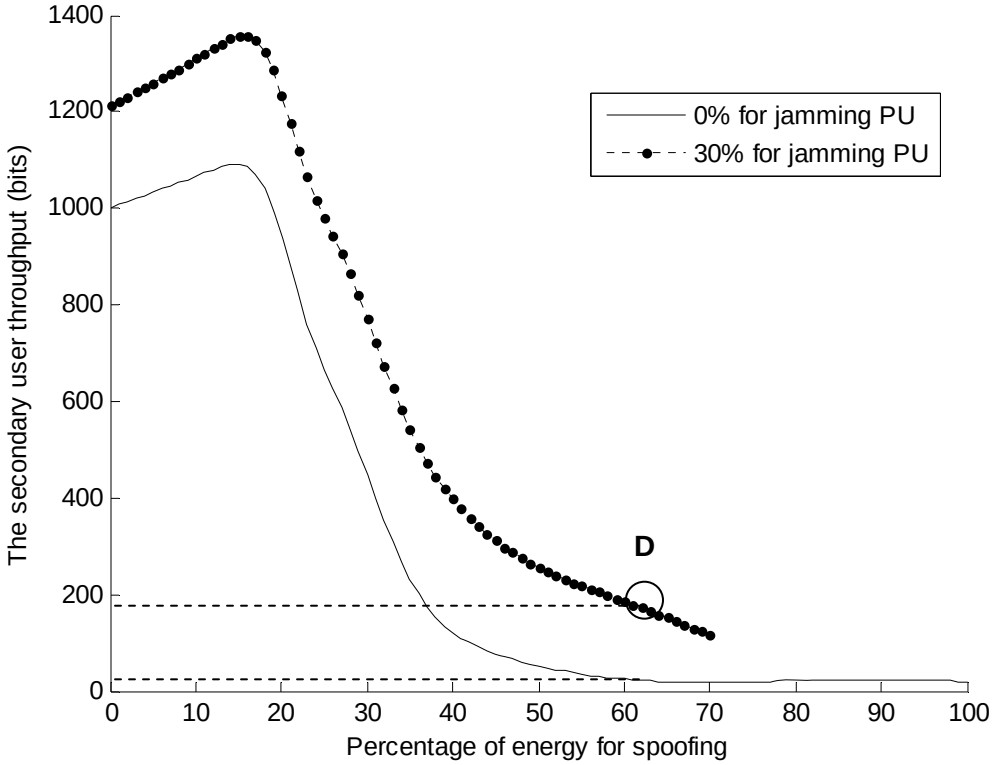
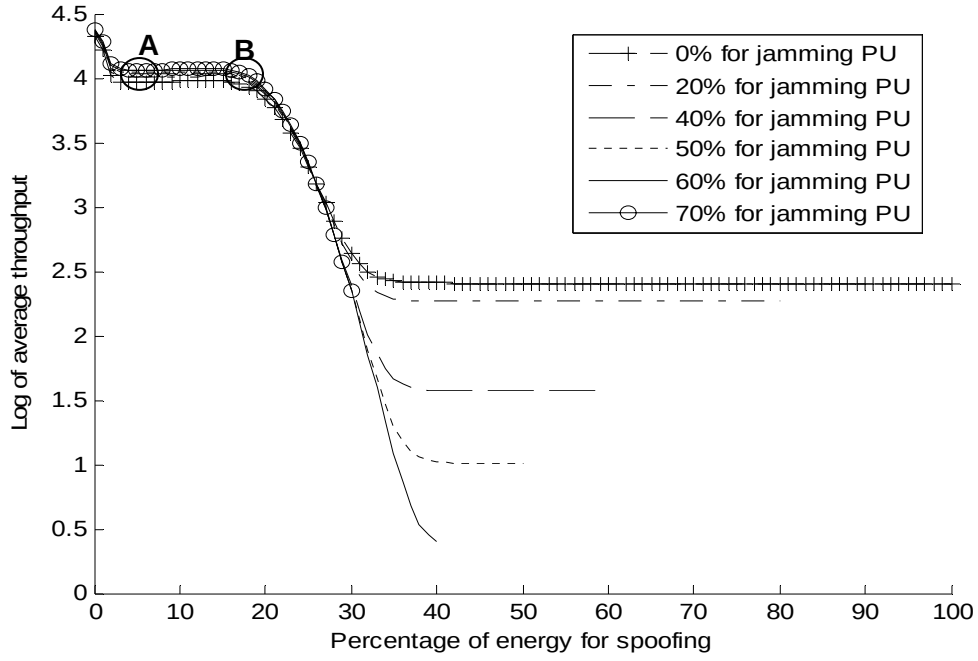


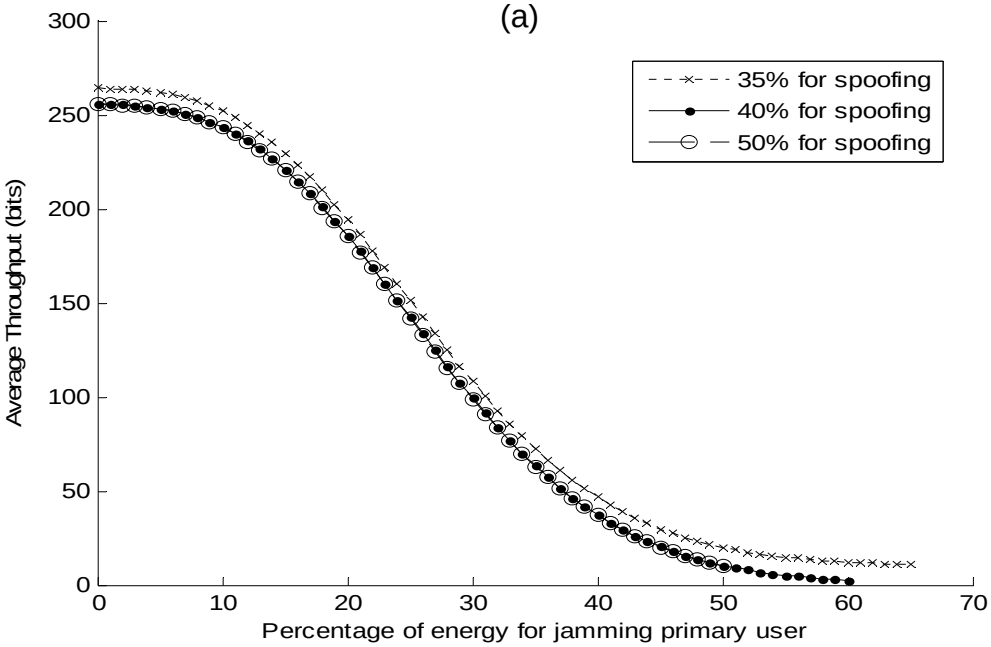
Figure 5.11. Secondary user throughput versus the percentage of energy for spoofing ($N = 21, TW = 25, p_f = 10^{-4}, J / S = 21dB$)

5.3 $N_{R,PU} = 1, N_{R,SU} = 100$

In Figures 5.12(a) and (b), the system average throughput versus the percentage of energy for spoofing and the percentage of energy for jamming the primary user are plotted. From Figure 5.12(a), it is seen that the system average throughput decreases as the percentage of energy for spoofing increases, and it exhibits a knee when the adversary puts more than 40% of the energy for



(a)



(b)

Figure 5.12. System average throughput versus (a) the percentage of energy for spoofing, (b) the percentage of energy for jamming the primary user and ($N = 21, TW = 25, p_f = 10^{-4}, J/S = 21dB$)

spoofing. In other words, extra percentage over 40% of the energy for spoofing can not degrade the system throughput anymore, i.e., spoofing is less efficient than jamming the primary user. The system average throughput is minimized when the adversary puts 40% of the energy in spoofing and the remaining 60% of the energy in jamming the primary user. From Figure 5.12(b), it is seen that with 40% of the energy for spoofing the minimum system throughput is achieved when all of the remaining energy is used for jamming the primary user. This is consistent with Figure 5.12(a).

In order to understand the results more clearly, in the following, we present numerical results for two cases, i.e., spoofing only and jamming secondary users only (Figure 5.13). It is seen from Figure 5.13 that spoofing is more efficient than jamming secondary user (e.g. P/S equals 21dB), thus the adversary optimally puts energy in spoofing rather than jamming to minimize the throughput of the secondary user.

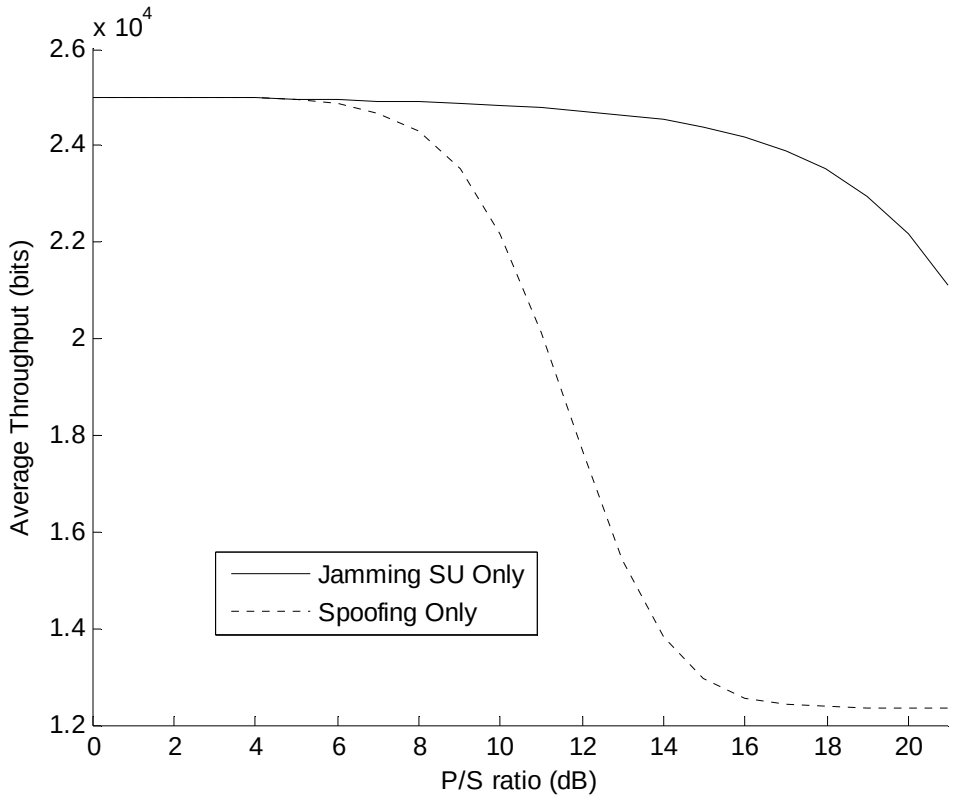


Figure 5.13. System average throughput versus P/S ratio

($N = 21, TW = 25, p_f = 10^{-4}$)

When 40% of the energy is put in spoofing, the packet success rate of a primary user and a secondary user versus the percentage of energy for jamming primary users is plotted in Figure 5.14. Obviously the decrease of primary user packet success rate is mostly larger than the increase of the secondary user packet success rate. Thus, the trend of the system average throughput is dominated by the primary user packet success rate, i.e., decreases as the percentage of energy for jamming primary user increases, which is consistent with Figure 5.12(b).

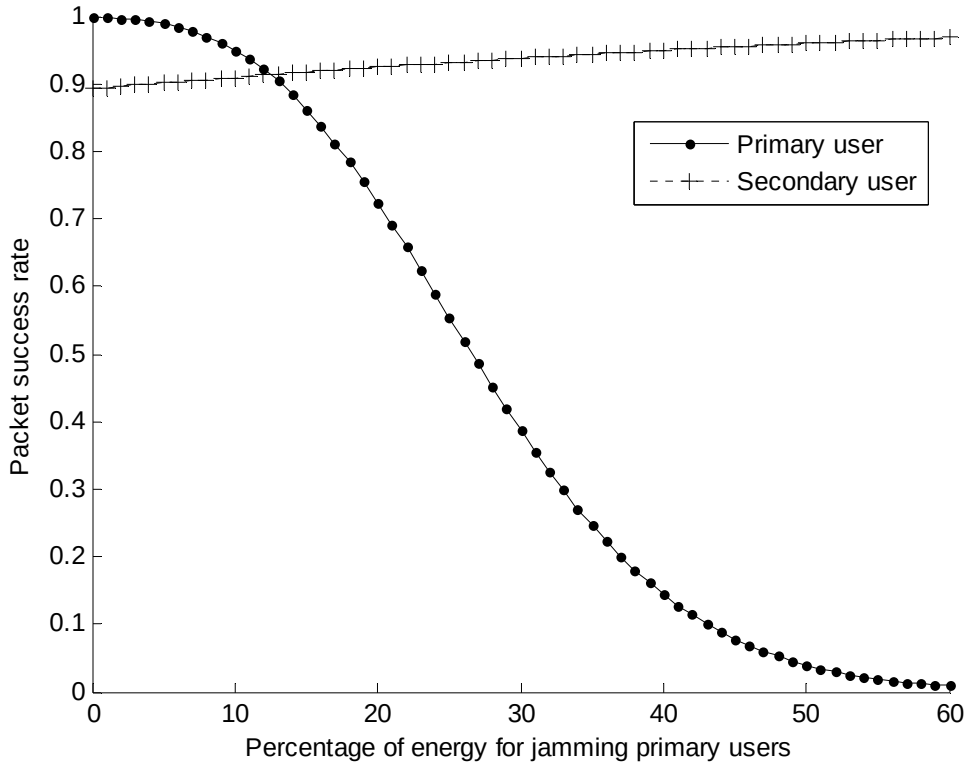


Figure 5.14. Packet success rate versus the percentage of energy for jamming the primary users with 40% of the energy for spoofing ($N = 21, TW = 25, p_f = 10^{-4}, J/S = 21dB$)

Now we analyze the trend of the system average throughput in Figure 5.12 (a). We know that the throughput of the primary user is just proportional to the packet success rate, i.e., the percentage of energy for jamming the primary user. For a given percentage of energy for jamming the primary user, the throughput of the primary user is a constant value. We find the primary user throughput with 60% of the energy for jamming the primary user is roughly 253 bits. The trend of the system throughput is thus dominated by the throughput of the secondary

users. In Figure 5.15, the components of secondary user throughput versus the percentage of energy for spoofing are plotted. Clearly, the secondary user throughput is dominated by the probability of access, i.e., it decreases sharply as the percentage of energy for spoofing increases until point A, roughly stead in certain value until point B and then decreases again until the minimum value is achieved. This is consistent with the results in Figure 5.12 (a)

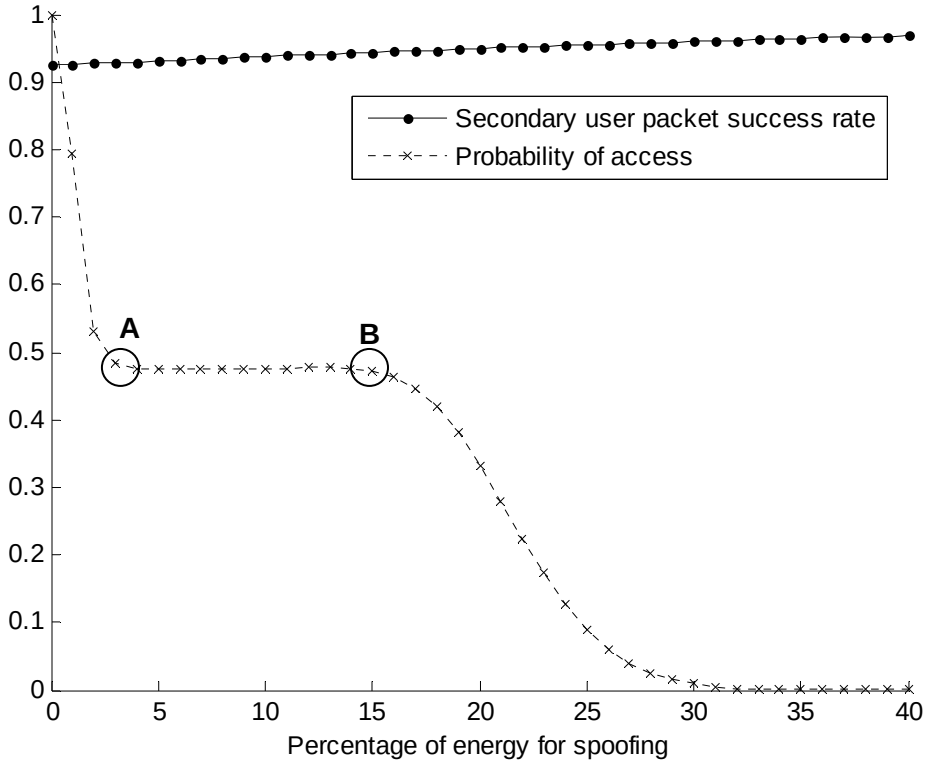
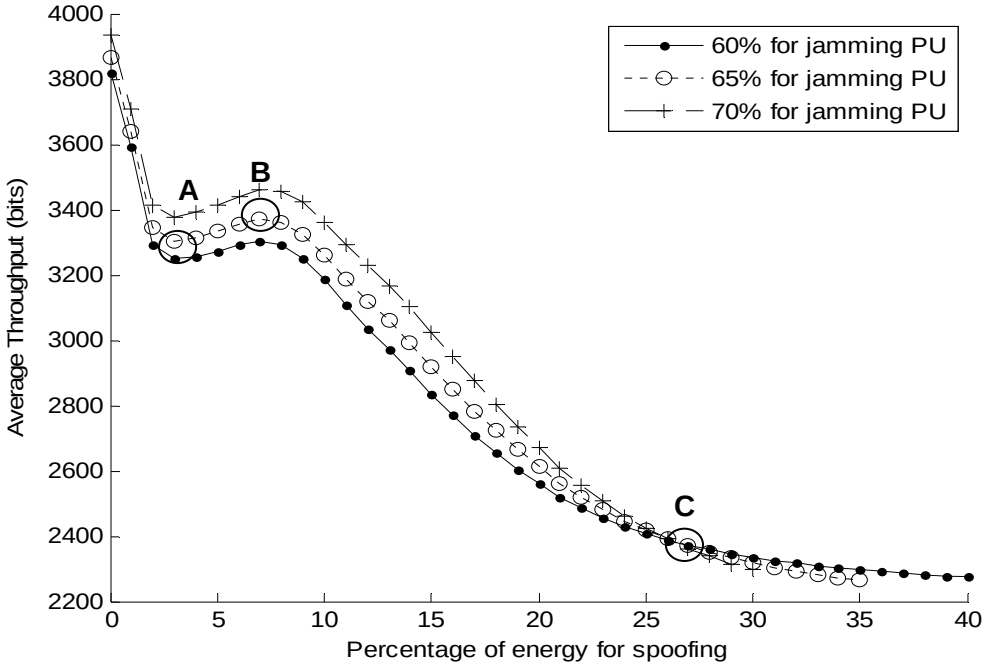


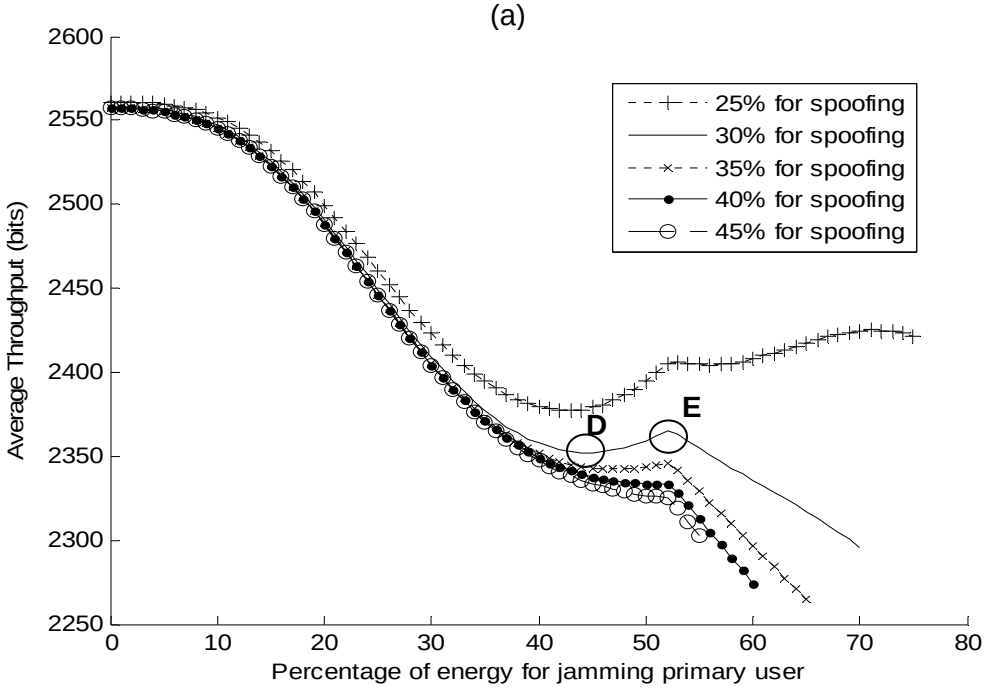
Figure 5.15. Secondary user throughput components versus the percentage of energy for spoofing with 60% energy for jamming primary user ($N = 21, TW = 25, p_f = 10^{-4}, J / S = 21dB$)

5.4 $N_{R,PU} = 10, N_{R,SU} = 10$

In this case, we assume that ten bands are occupied by the primary users and there is only one user in each band. The other ten bands are allowable for the secondary users. The system average throughput versus the percentage of energy for spoofing and the percentage of energy for jamming primary user are plotted in Figures 5.16 (a) and (b), respectively. Comparing these two Figures, it is seen that the system average throughput is minimized when the adversary puts roughly 65% of the energy in jamming primary users and 35% of the energy in spoofing. Specifically, with the percentage of energy for spoofing increases, the corresponding minimum system average throughput is achieved when all of the remaining energy is put in jamming the primary user as seen from Figure 5.16(b). In the following, the system average throughput versus the adversary- to-signal power ratio with jamming secondary users only and spoofing only are presented in order to explain the results more clearly. From Figure 5.17 (a), we can see that in order to decrease the throughput of the secondary user, spoofing is always more efficient than jamming the secondary users. In other words, the optimal attack strategy is to put energy in spoofing to minimize the throughput of the secondary user and put the rest of the energy in jamming primary users to minimize the throughput of the primary users.



(a)



(b)

Figure 5.16. System average throughput versus (a) the percentage of energy for spoofing and (b) the percentage of energy for jamming primary user ($N = 20, TW = 25, p_f = 10^{-4}, J/S = 21dB$)

Now in order to further understand the system average throughput behavior in Figure 5.16, we present some other numerical results. The secondary user throughput component versus the percentage of energy for spoofing with 65% of the energy for jamming the primary users is plotted in Figure 5.18. Similar

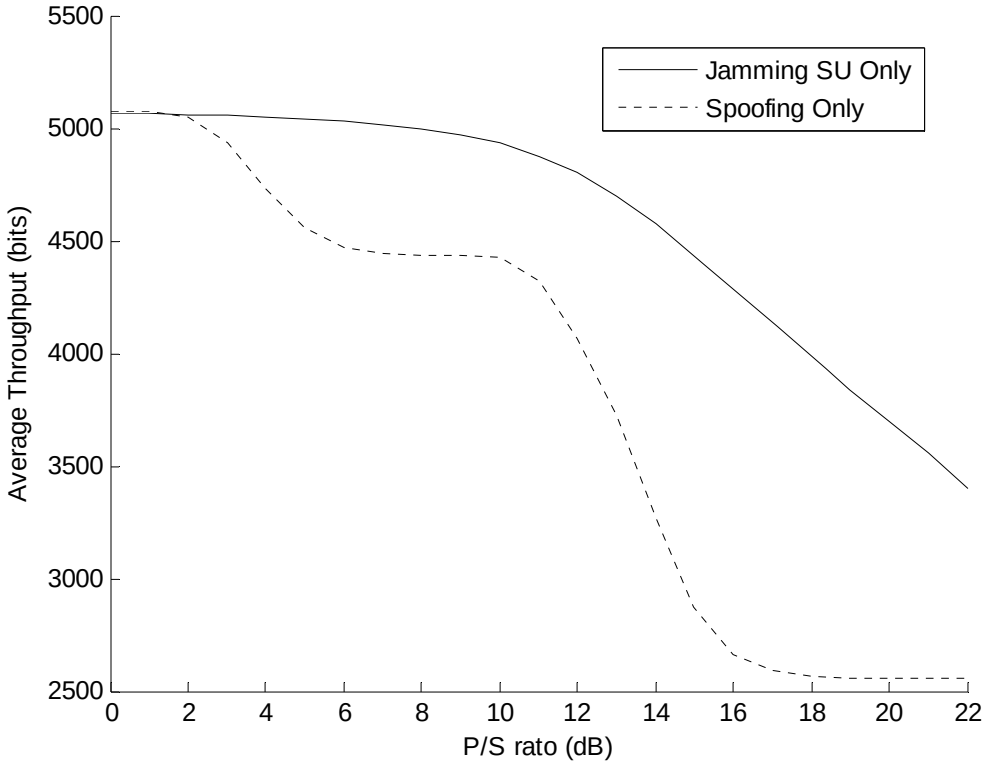


Figure 5.17. System average throughput versus the P/S ratio with jamming secondary user/ spoofing only ($N = 20, TW = 25, p_f = 10^{-4}$)

to our analysis in the previous part, the throughput of the primary users with a given percentage of energy for jamming the primary users is a constant. The trend of the system average throughput is determined by the trend of the secondary user throughput. It is seen that on the right side of point A the secondary user

throughput is dominated by the probability of access, i.e., it decreases as the percentage of energy for spoofing increases. In the range from point A to B, the throughput is dominated by the packet success rate, while on the left side of point B it is dominated by the probability of access again. This is consistent with the

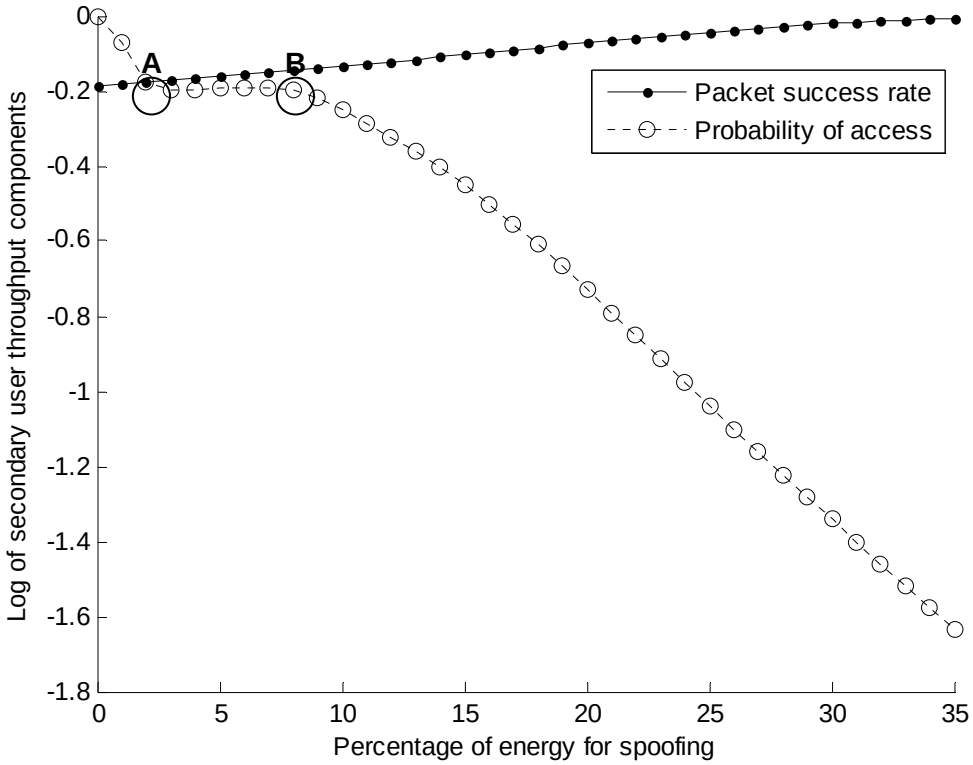


Figure 5.18. Secondary user throughput components versus the percentage of energy for spoofing with 65% of the energy for jamming primary users ($N = 20, TW = 25, p_f = 10^{-4}, J/S = 21dB$)

curve in Figure 5.16 (a), where the system average throughput sharply decreases until point A and slowly increases from point A to B and then decreases again until the minimum throughput is achieved as the percentage of energy for spoofing

increases.

Comparing the throughput of the primary users with 60% of the energy for jamming the primary users and 65% of the energy for jamming the primary users, we find it decreases for about 50 bits due to the extra 5% jamming energy. With the 60% and 65% of the energy for jamming the primary users, the throughput of the secondary users versus the percentage of the energy for spoofing is plotted in Figure 5.19. It is seen that the throughput of the secondary users with 65% of the

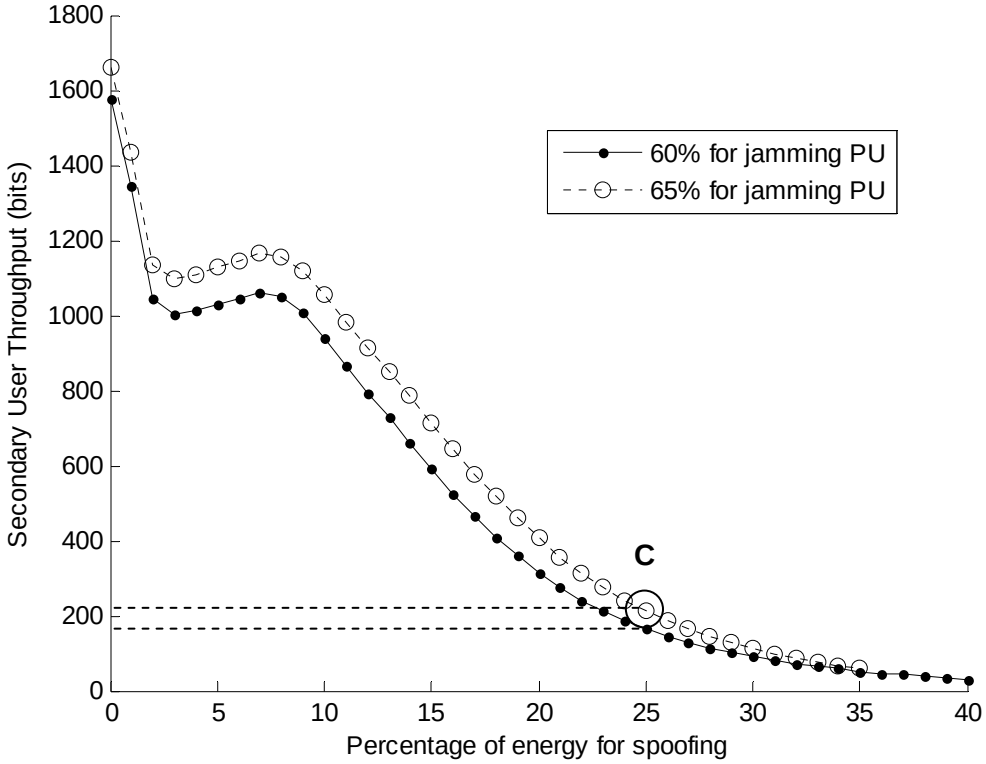


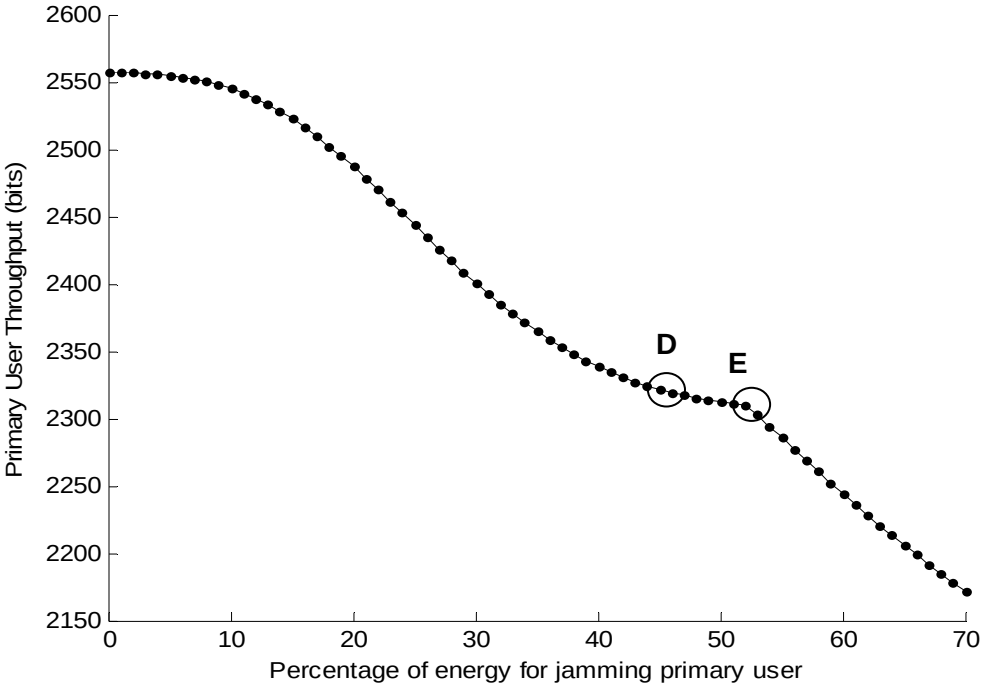
Figure 5.19. The throughput of secondary users versus the percentage of energy for spoofing ($N = 20, TW = 25, p_f = 10^{-4}, J/S = 21dB$)

energy for jamming the primary users is always larger than that with 60% of the

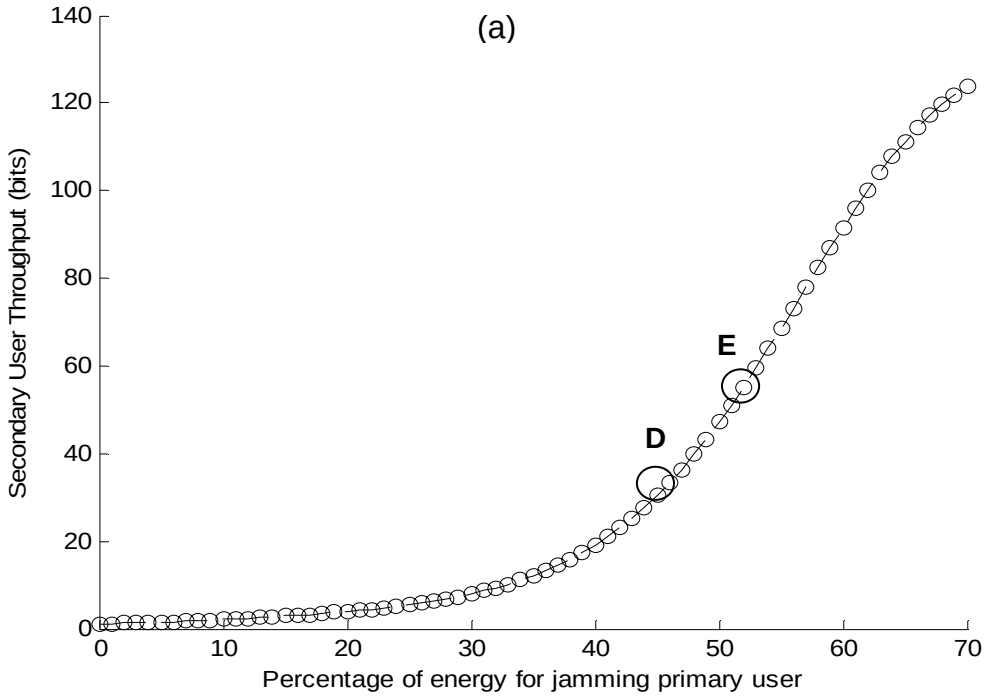
energy for jamming primary users, and the difference can compensate for the throughput degradation of the primary users due to that extra 5% jamming energy until point C. This means the system average throughput with 65% of the energy for jamming the primary users is larger than that with 60% of the energy for jamming the primary users until point C, which is consistent with the curves in Figure 5.16 (a).

The throughput of the primary users and secondary users versus the percentage of energy for jamming the primary users with 30% of the energy for spoofing are plotted in Figure 5.20 (a) and (b), respectively. It is seen that the throughput of the secondary users increases as the percentage of the energy for jamming primary users increases. This is because that with a given percentage of energy for spoofing, the probability of access as a component of secondary user throughput is constant. The secondary user throughput is proportional to the packet success rate of secondary users. With more energy put into jamming primary users, the packet success rate of the secondary users will increase, while that of the primary users will decrease. The non-smooth decrease of the primary user throughput as shown in Figure 5.20 (a) is due to the optimal jamming strategy of the adversary. The adversary optimally determines the number of bands that are jammed, based on the percentage of energy that is distributed to jam the primary users. On the left side of point E, the number of spoofed bands is

a constant, and it increases to another constant after this point. However, on the right side of point D, the slow decrease of primary user throughput cannot compensate for the increase of the secondary user throughput until point E. Hence there is a light increase of the system average throughput from point D to E, and then it drops again, which is consistent with the curve in Figure 5.16 (b).



(a)



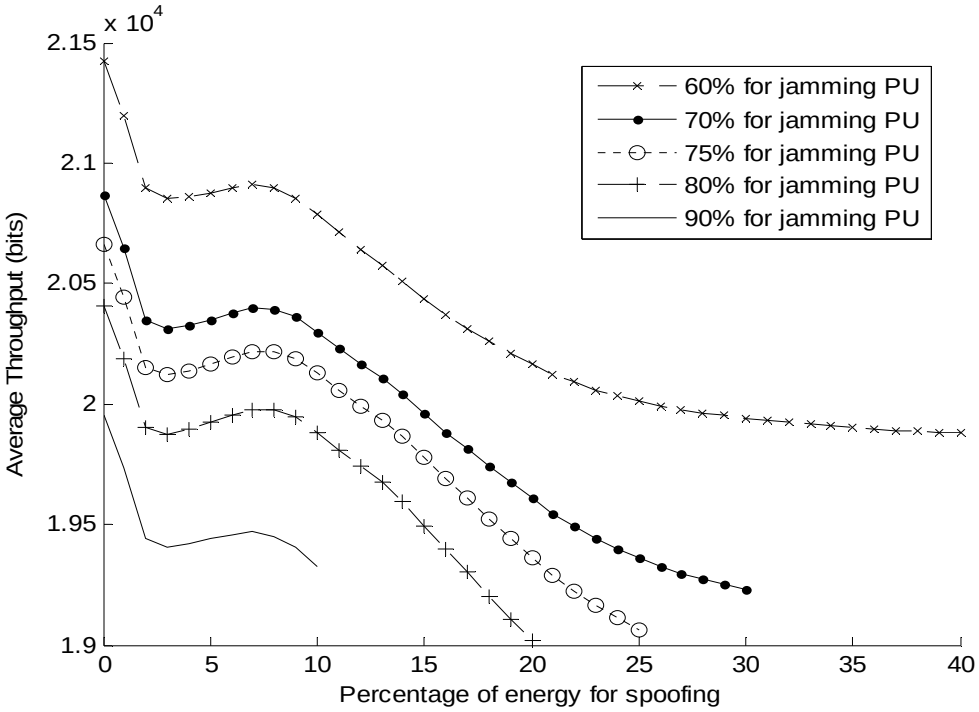
(b)

Figure 5.20. The throughput of (a) primary users and (b) secondary users versus the percentage of energy for jamming primary users

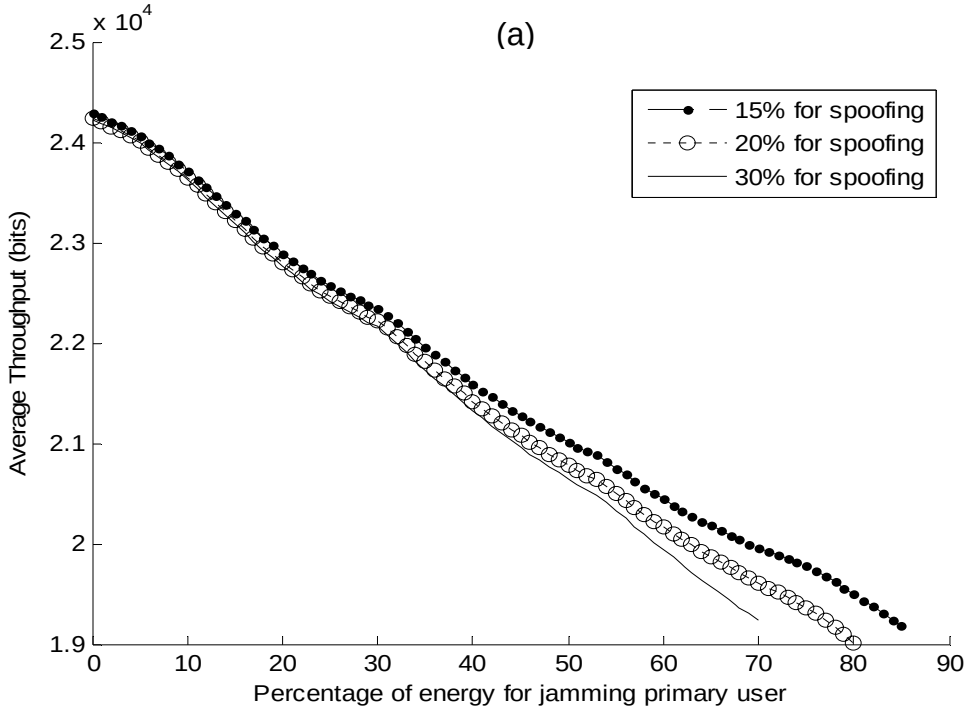
($N = 20, TW = 25, p_f = 10^{-4}, J / S = 21dB$)

5.5 $N_{R,PU} = 100, N_{R,SU} = 10$

In this case we assume that ten bands are occupied by primary users and all of them are fully occupied, i.e., there are ten users in each band. In Figure 5.21, the system average throughput versus the percentage of energy for spoofing and the percentage of energy for jamming primary users are plotted. It is seen that the optimal attack strategy is to put roughly 20% of the energy in spoofing and 80% in jamming primary users. Similarly, we can analyze the behavior of the system average throughput as the previous part. However, from Figure 5.21 (a), we can see that the system average throughput with 80% of the energy for jamming primary users is always smaller than that with 75% of the energy for jamming primary users, which is different from the results in Figure 5.16. This is because in this case the throughput of the primary users takes a larger fraction of the system average throughput. The degradation of the primary users' throughput due to the extra 5% jamming energy is evident, and cannot be compensated by the increase of secondary user throughput due to less spoofing energy.



(a)



(b)

Figure 5.21. System average throughput versus the percentage of energy for (a) spoofing and (b) jamming primary users

($N = 20, TW = 25, p_f = 10^{-4}, J/S = 21dB$)

5.6 Conclusions

In the above scenarios, we assume the adversary knows which bands are occupied by primary user, and which bands are vacant after sensing. The adversary wants to minimize the system throughput, which consists of both the throughput of the primary users and the throughput of the secondary users. The throughput of the primary users decreases as the percentage of energy for jamming primary users increases. For the secondary users, the throughput is proportional to the product of two terms: the packet success rate (jamming) and the probability of access (spoofing). If more than one band is occupied by primary users, the adversary optimally determines the number of jammed bands based on the energy distributed to jamming the primary users. The numerical results show that:

(1) $N = 21, TW = 25, p_f = 10^{-4}, J/S = 21dB, N_c = 128, \beta = 0.5, N_{R,PU} = 1, N_{R,SU} = 1$

In this case, jamming the secondary user is more efficient than spoofing. The optimal strategy is to put roughly 52% of the energy in jamming the primary user and the remaining 48% of the energy in jamming the secondary user.

(2) $N = 21, TW = 25, p_f = 10^{-4}, J/S = 21dB, N_c = 128, \beta = 0.5, N_{R,PU} = 1, N_{R,SU} = 10$

For a large P/S value (e.g. 21dB), spoofing is more efficient than jamming the secondary users. The results show that the optimal strategy is to put 70% of

the energy in spoofing and 30% of the energy in jamming primary user.

(3) $N = 21, TW = 25, p_f = 10^{-4}, J/S = 21dB, N_c = 128, \beta = 0.5, N_{R,PU} = 1, N_{R,SU} = 100$

For this case, spoofing is always more efficient than jamming secondary users. The optimal strategy is to put 40% of the energy in spoofing and 60% of the energy in jamming the primary user.

(4) $N = 20, TW = 25, p_f = 10^{-4}, J/S = 21dB, N_c = 128, \beta = 0.5, N_{R,PU} = 10, N_{R,SU} = 10$

The optimal strategy in this case is to put roughly 35% of the energy in spoofing and 65% of the energy in jamming primary users.

(5) $N = 20, TW = 25, p_f = 10^{-4}, J/S = 21dB, N_c = 128, \beta = 0.5, N_{R,PU} = 100, N_{R,SU} = 10$

The optimal strategy is to put roughly 20% of the energy in spoofing and 80% of the energy in jamming primary users.

In going from case (2) to (4) to (5), the number of primary users increases, and the throughput ratio of the primary users and the system increases, and the adversary puts more energy in jamming primary users. In going from case (1) to (2) to (3), spoofing is more efficient than jamming secondary users, as more spectrum vacancies are required by secondary users. The adversary puts more energy in spoofing as the number of secondary users increases. However, when there are enough secondary users to occupy the spectrum vacancies (e.g., case (5)), extra percentage over 40% of the energy for spoofing is less efficient than jamming the primary user, a result that is similar to [16].

References

[1] Federal Communications Commission, “Spectrum policy task force report, FCC 02-155,” Nov. 2002.

[2] M. Matinmikko et al, “Cognitive radio: An intelligent wireless communication system”, March 2008

[3] S. Haykin, “Cognitive Radio: Brain-Empowered Wireless Communications”, IEEE J. on Selected Areas in Communications, VOL. 23, NO. 2, FEBRUARY 2005

[4] Yang Xiao, Hu Fei, “Cognitive Radio Networks”, CRC Press, Taylor & Francis Group, 2009

[5] Y. C. Liang, Y. H. Zheng, E. C. Y. Peh, and A. T. Hoang, “Sensing-throughput tradeoff for cognitive radio networks,” IEEE Transactions on Wireless Communications, vol. 7, no. 4, pp. 1326-1337, Apr. 2008.

[6] H. Urkowitz,“Energy detection of unknown deterministic signals,” in Proceedings of the IEEE, vol. 55, no. 4, pp. 523-531, Apr. 1967.

[7] S. M. Mishra, A. Sahai, and R. W. Brodersen, “Cooperative sensing among cognitive radios,” in Proc. IEEE Int. Conf. Commun., Jun. 2006, vol. 4, pp. 1658–1663.

[8] Z. Quan, S. Cui, and A. H. Sayed, “Optimal linear cooperation for spectrum sensing in cognitive radio networks,” IEEE J. Sel. Topics Signal Process., vol. 2, no. 1, pp. 28–40, Feb. 2008.

[9] John Proakis, Digital Communications, 4th edition, 2001, McGraw-Hill

[10] S. M. Kay, “Fundamentals of statistical signal processing: Detection theory,” Printice Hall PTR, vol. 2, 1998.

[11] F. Digham, M. Alouini, M. Simon, “On the energy detection of unknown signals over fading channels,” Proc. IEEE ICC 2005, vol. 5, pp. 3575–3579, 2003.

[12] V. I. Kostylev, “Energy Detection of a Signal with Random Amplitude,” IEEE, vol.3, pp 1606 – 1610, August 2002
[13] H. S. Chen and W. Gao, “Text on cyclostationary feature detector—For informative annex on sensing techniques,” IEEE 802.22 Meeting Documents, Jul. 2007.

[14] T. X. Brown and A. Sethi, “Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: a multi-dimensional analysis and assessment,” IEEE International Conf. on Cognitive Radio Oriented Wireless Networks and Communications, pp. 456-464, Aug. 2007.

[15] Q. H. Peng, P. C. Cosman, and L. B. Milstein, “Optimal sensing disruption for a cognitive radio adversary,” IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 59, NO. 4, MAY 2010

[16] Q. H. Peng, P. C. Cosman, and L. B. Milstein, “Spoofing or Jamming: Performance Analysis of a Tactical Cognitive Radio Adversary,” submitted

[17] W. Xu and L. B. Milstein, “Performance of multicarrier DS CDMA systems in the presence of correlated fading,” Proc. Of VTC, vol. 3, pp. 2050-2054, 1997.

[18] S. Kondo and L. B. Milstein, “Performance of multicarrier DS CDMA systems,” IEEE Transactions on Communications, vol. 44, no. 2, pp. 238-246, Feb. 1996.

[19] Pickholtz, RL, Schilling, DL, & Milstein, LB (1982). Theory of spread spectrum communications — a tutorial. IEEE Transactions on Communications Com30(5), 855–885

[20] C. Lo, E. Masry, and L. B. Milstein, “Design and analysis of a fast frequency-hopped DBPSK communication system, Part II. Error performance in AWGN plus partial-band noise jamming,” IEEE Transactions on Communications, vol. 41, no. 11, pp. 1723-1735, Nov. 1993.