Dynamic resource allocation for cognitive radio

Pei, Yiyang

2011

Pei, Y. (2011). Dynamic resource allocation for cognitive radio. Doctoral thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/50648>

<https://doi.org/10.32657/10356/50648>

DYNAMIC RESOURCE ALLOCATION FOR COGNITIVE RADIO

PEI YIYANG

School of Electrical & Electronic Engineering

A thesis submitted to the Nanyang Technological University
in partial fulfillment of the requirement for the degree of
Doctor of Philosophy

2011

Acknowledgements

First and foremost, I would take this opportunity to express my deep and sincere gratitude to my supervisor, Dr. Liang Ying Chang from Institute for Infocomm Research (I²R). It was the fruitful experience of working with him for my Industry Attachment and Final Year Project during my undergraduate studies in Nanyang Technological University (NTU), that sparked my interest in the research subject and boosted my confidence in considering pursuing a Ph.D degree. Had it not been for his valuable technical advice and sharp professional insights throughout the years, the completion of the thesis would certainly not be possible.

Secondly, I am greatly indebted to my supervisors, Prof. Teh Kah Chan and Prof. Li Kwok Hung from NTU, for their continued inspiration and attentive supervision. Special thanks go to their extreme patience and valuable time taken in discussing my work and revising my papers.

Next, I would like to thank my fellow groupmates, Dr. Zhang Lan, Dr. Kang Xin, Mr. Edward Peh Chu Yeow, Mr. Ebrahim Avazkonandeh Gharavol, and Mr. Zheng Shoukang, for their selfless sharing and valuable discussion in our weekly group meeting.

My special gratitude goes to Agency for Science, Technology, and Research (A*STAR), which provided me with the financial support during my Ph.D studies and the precious opportunities for attending international conferences. I would also like to make a grateful acknowledgement for many professors and researchers from NTU and I²R for inviting the top scientists and researchers abroad to give various useful seminars in

Singapore. Both the conferences and the seminars have greatly broadened my knowledge on the state-of-the-art research in the area, and was very helpful in reinvigorating my research and generating new ideas.

Lastly but not least, most significant acknowledgement of all goes to my parents, husband and friends for their devoted love and continued support throughout my life.

Contents

Acknowledgements	i
Contents	iii
Abstract	vii
List of Figures	ix
List of Tables	xii
List of Abbreviations	xiii
List of Notations	xv
1 Introduction	1
1.1 Dynamic Spectrum Access (DSA)	1
1.2 Cognitive Radio (CR)	3
1.2.1 CR for DSA	4
1.2.2 Regulatory Efforts	4
1.2.3 Standardization Activities	5
1.2.4 Cognitive Radio Models	6
1.3 Motivation	10
1.4 Objective	12
1.5 Summary of Contributions	14

1.6	Organization of the Thesis	16
2	Literature Review	18
2.1	Opportunistic Spectrum Access (OSA)	18
2.1.1	Spectrum Sensing Approaches	20
2.1.2	Signal Detection Schemes	24
2.1.3	Sensing-Access Designs	30
2.2	Spectrum Sharing	38
2.2.1	Perfect CSI	39
2.2.2	Imperfect CSI	42
2.3	Security Issues in CRNs	44
2.3.1	Security Aspects of Spectrum Sensing	44
2.3.2	Information Theoretic Security	46
3	Sensing-Access Design in OSA: Parallel Channel Sensing	50
3.1	System Models and Problem Formulation	52
3.2	Optimization under the Average Transmit Power Constraint	57
3.3	Optimization under the Peak Transmit Power Constraint	60
3.4	Numerical Results and Discussions	62
3.5	Conclusions	64
4	Sensing-Access Design in OSA: Sequential Channel Sensing	66
4.1	System Model	69
4.1.1	Network Description	69
4.1.2	Energy Efficiency	71
4.2	Problem Formulation	73
4.3	Optimal Sensing-Access Strategies	76
4.3.1	Parametric Problem	76
4.3.2	(Dynamic Programming) DP for the Parametric Problem	77

4.3.3	The Optimal Sensing-Access Strategies	79
4.4	Joint Design of Sensing Order and Sensing-Access Strategies	82
4.4.1	Problem Formulation and the Optimal Strategies	82
4.4.2	Computational Complexity	85
4.5	Numerical Results	86
4.5.1	Given Sensing Order	87
4.5.2	Optimal Sensing Order	93
4.6	Conclusions	95
5	Secure Transmission in Spectrum Sharing with Perfect CSI	97
5.1	System Model and Problem Formulation	99
5.2	Optimal Solution	106
5.2.1	Semidefinite Program (SDP) Transformation	106
5.2.2	Auxiliary CRN (ACRN) Transformation	107
5.2.3	Computational Complexity	110
5.3	Suboptimal Solutions	111
5.3.1	Scaled Secret Beamforming	111
5.3.2	Projected Secret Beamforming	113
5.3.3	Projected Cognitive Beamforming	114
5.3.4	Computational Complexity	115
5.4	Numerical Results and Discussions	116
5.4.1	Optimal Solutions	116
5.4.2	Suboptimal Solutions	119
5.5	Conclusions	124
6	Secure Transmission in Spectrum Sharing with Imperfect CSI	125
6.1	System Model and Problem Formulation	126
6.2	Optimal Solution	131

6.2.1	Quasiconvex Optimization Approach	131
6.2.2	ACRN Transformation	133
6.2.3	SDP Transformation	136
6.3	Suboptimal Solutions	138
6.4	Numerical Results and Discussions	142
6.5	Conclusions	147
7	Conclusions and Future Work	149
7.1	Conclusions	149
7.2	Future Work	151
	List of Publications	154
	Bibliography	156
	Appendices	173
	Appendix A Proof of Proposition 3.1	174
	Appendix B Proof of (5.16)	176
	Appendix C Proof of (5.18)	177
	Appendix D Proof of Concavity of $\mathcal{G}(q)$	180
	Appendix E Proof of Proposition 6.8	181
	Appendix F Proof of Proposition 6.9	182
	Appendix G Proof of Quasiconcavity of (6.40)	183
	Appendix H Sample Simulation Code	185

Abstract

Cognitive radio (CR) has been recognized as an effective way to improve the spectrum utilization by allowing unlicensed secondary users (SUs) to coexist either opportunistically or concurrently with the licensed primary users (PUs). Two models of CR operation have attracted most attention, namely, opportunistic spectrum access (OSA) and spectrum sharing. While the former allows only opportunistic transmission of the SUs through spectrum sensing, the latter one permits concurrent transmission by imposing the interference power constraint. In both models, SUs have to strike a balance between optimizing its own performance and maintaining sufficient protection to the PUs. Therefore, efficient resource allocation methods need to be investigated to balance this tradeoff. In this thesis, two major resource allocation problems are studied, namely, sensing-access design in the OSA model and secure transmission in the spectrum sharing model.

In the OSA model, the thesis investigates the sensing-access design which aims to balance the intrinsic tradeoffs between the sensing requirement to protect the PUs and the access need to improve the SUs' own performance under two different multi-channel sensing schemes. Specifically, for the case of parallel channel sensing where an SU can sense multiple channels simultaneously, the sensing-access design includes the sensing strategy specifying the optimal sensing time and the access strategy determining the optimal power level upon transmission. The objective is to maximize the sum achievable throughput under the sum transmit power constraint such that the PUs are well protected on each channel by a fixed probability of detection constraint. For the case

of sequential channel sensing where an SU can sequentially sense the channels one at a time, the sensing-access design includes the sensing strategy determining when to stop sensing and start transmission, the access strategy specifying the transmit power level upon transmission, and the sensing order design telling the SU which channel to sense next if the current channel is given up for transmission. The objective is to maximize the energy efficiency of the sequential channel sensing process such that the PU is sufficiently protected under a fixed probability of detection constraint. In both schemes, we derive the structures of the optimal sensing-access strategies and propose efficient algorithms to compute the optimal solutions.

In the spectrum sharing model, the thesis investigates the secure transmission from the information-theoretic perspective. In particular, the communication over a secure multiple-input single-output CR channel where a multi-antenna SU transmitter (SU-Tx) sends confidential information to a legitimate SU receiver in the presence of a single-antenna PU-Rx and a single-antenna eavesdropper receiver is considered. The performance is measured in terms of secrecy rate, which is defined as the rate at which the information can be reliably transmitted to the SU-Rx but is kept secret from the ED-Rx, at the same time interference power constraint is satisfied. While the secrecy capacity is characterized for the case of perfect channel state information (CSI) at the SU-Tx, the worst-case secrecy rate under Gaussian signaling without preprocessing of information is characterized for the case of imperfect CSI. Under either case of CSI, the capacity/rate involves a nonconvex optimization problem of the transmit covariance matrix. Two numerical approaches are proposed to compute the optimal transmit covariance matrix and the corresponding secrecy capacity/rate. A few beamforming solutions are also proposed to trade off secrecy rate and computational complexity.

List of Figures

1.1	The cognitive cycle for DSA.	4
1.2	An illustration of spectrum usage in the OSA model.	7
1.3	An illustration of the spectrum sharing model.	9
2.1	Main PHY and MAC layer functions in OSA model.	19
2.2	Illustration of Passive Sensing of PU-Txs	22
2.3	The basic point-to-point channels in the spectrum sharing model. . . .	39
2.4	The wiretap channel.	47
3.1	The transmission frame structure.	53
3.2	The schematic illustration of the parallel channel sensing: A separate energy detector with threshold ε_k is used on each narrowband channel k , for $k = 1, \dots, K$	54
3.3	The average achievable throughput vs. sensing time under average or peak power constraints with different transmit power levels.	63
3.4	The optimal sensing time vs. the total transmit power under average or peak power constraints.	64
4.1	Illustration of the sequential channel sensing process with the sensing order given as $\{1, 2, \dots, K\}$	70
4.2	Comparison of computational complexity between the exhaustive search and the proposed method.	86

4.3	Energy efficiency vs sensing time for $K = 6$ (constant transmission time).	88
4.4	Energy efficiency vs sensing time (constant transmission time).	89
4.5	Energy efficiency vs sensing time (constant frame time).	90
4.6	Maximum energy efficiency vs number of channels.	91
4.7	Optimal sensing time vs number of channels.	91
4.8	Energy efficiency comparison of the energy-efficient and the throughput-efficient designs for $K = 8$ (constant transmission time).	92
4.9	Throughput efficiency comparison of the energy-efficient and the throughput-efficient designs for $K = 8$ (constant transmission time).	93
4.10	Energy efficiency vs sensing time with $\theta_k = 0.8$, $k = 1, \dots, K$	94
4.11	Energy efficiency vs sensing time with the idle probabilities given by $\{\theta_1, \dots, \theta_K\} = \{0.1, 0.3, 0.5, 0.7, 0.8\}$	95
5.1	System model for the secure MISO CR channel.	99
5.2	System model for the conventional MISO CR channel.	108
5.3	Capacity comparison of the secure CR channels with the conventional CR channels and the conventional wiretap channels at $Q = 0$ dB. . . .	117
5.4	Secrecy capacity comparison of the secure MISO and SISO CR channels at $Q = 0$ dB for different number of transmit antennas.	117
5.5	Secrecy capacity comparison of the secure MISO and SISO CR channels at $Q = 0$ dB for different variance of the eavesdropper channel.	118
5.6	Secrecy capacity comparison of the secure MISO and SISO CR channels at $Q = 0$ dB for different variance of the primary channel.	118
5.7	Performance comparison of the achievable secrecy rates by the SSB, PSB and PCB at $Q = 20$ dB.	120
5.8	Performance comparison of the achievable secrecy rates by the SSB, PSB and PCB at $Q = -20$ dB.	121

5.9	Performance comparison of the achievable secrecy rates by the SSB, PSB and PCB at $P = 10$ dB.	122
5.10	Performance comparison of the achievable secrecy rates by various schemes at $Q = 0$ dB for $(2, 1, 1)$	122
5.11	Performance comparison of the achievable secrecy rates by various schemes at $Q = 0$ dB for $(1, 1, 2)$	123
5.12	Performance comparison of the achievable secrecy rates by various schemes at $Q = 0$ dB for $(1, 2, 1)$	123
6.1	System model for the secure MISO CRN.	127
6.2	System model for the conventional MISO CRN with 2 PUs.	134
6.3	Achievable secrecy rate vs transmit power with $N = 4$ antennas at $Q = -10$ dB for different levels of channel uncertainties.	143
6.4	Achievable secrecy rate vs interference power with $N = 4$ antennas at $P = 15$ dB for different levels of channel uncertainties.	144
6.5	Achievable secrecy rate vs number of transmit antennas at $P = 20$ dB and uncertainty level $(10^{-3}, 10^{-3}, 10^{-2})$	145
6.6	Achievable secrecy rate vs interference temperature limit at $P = 15$ dB and uncertainty levels (i) $(10^{-3}, 10^{-3}, 10^{-2})$ and (ii) $(10^{-2}, 10^{-2}, 10^{-1})$	146

List of Tables

1.1	Comparisons of the OSA and the spectrum sharing models.	7
3.1	Throughput Loss	64
4.1	Parameter Settings	87
6.1	Complexity Comparison of Various Approaches	147
6.2	Number of Variables and Size of Constraints in Standard Form	147

List of Abbreviations

AWGN	additive white Gaussian noise
CR	cognitive radio
CRN	cognitive radio network
CSCG	circularly symmetric complex Gaussian
CSI	channel state information
DSA	dynamic spectrum access
FCC	Federal Communications Commission
IDA	Infocomm Development Authority
IA	interference alignment
i.i.d.	independent and identically distributed
KKT	Karush-Kuhn-Tucker
LO	local oscillator
MAC	medium access control
MIMO	multiple-input multiple-output
MISO	multiple-input single-output
NPRM	notice of proposed rulemaking
Ofcom	Office of Communication
OSA	opportunistic spectrum access
PDF	probability density function
POMDP	partially observable Markov decision process

PHY	physical (layer)
PSD	power spectral density
PU	primary user
PU-Tx	primary user transmitter
PU-Rx	primary user receiver
QoS	quality-of-service
SDP	semidefinite program
SINR	signal-to-interference-plus-noise ratio
SISO	single-input single-output
SNR	signal-to-noise ratio
SU	secondary user
SU-Tx	secondary user transmitter
SU-Rx	secondary user receiver
s.t.	subject to
WRAN	wireless regional area network
w.r.t.	with respect to
ZF	zero-forcing

List of Notations

$\triangleq$	defined as
$\mathcal{CN}(0, \sigma^2)$	the distribution of a CSCG random variable with zero mean and variance σ^2
$\mathbb{C}^{M \times N}$	the complex space of a matrix of dimension $M \times N$
$H(\cdot), H(\cdot \cdot)$	the entropy, the conditional entropy
$I(\cdot, \cdot)$	the mutual information
$\arg \max_x f(x)$	the value of x that maximizes the function $f(x)$
$\mathbf{p}_X(x)$	the probability density function of random variable X
$\mathbb{E}[\cdot]$	the expectation operator
$\mathcal{Q}(\cdot)$	the $\mathcal{Q}$ -function, i.e., $\mathcal{Q}(x) = \frac{1}{\sqrt{2\pi}} \int_x^{+\infty} \exp\left(-\frac{t^2}{2}\right) dt$
$\text{Re}(x)$	the real part of x
$\text{Im}(x)$	the imaginary part of x
$\lceil x \rceil$	the smallest integer not less than x
$\ \mathbf{x}\ $	the Euclidean norm of vector $\mathbf{x}$
$\check{\mathbf{x}}$	the unit-norm vector of vector $\mathbf{x}$, i.e., $\check{\mathbf{x}} = \mathbf{x}/\ \mathbf{x}\ $
$\mathbf{X}^\dagger$	the conjugate transpose of matrix $\mathbf{S}$
$\text{tr}(\mathbf{X})$	the trace of matrix $\mathbf{S}$
$\mathbf{X} \succeq 0$	matrix $\mathbf{S}$ is positive semidefinite
$\mathbf{I}_N$	the $N \times N$ identity matrix
$\mathbf{0}_{M \times N}$	zero matrix of dimension $M \times N$

Chapter 1

Introduction

1.1 Dynamic Spectrum Access (DSA)

As we know, radio spectrum is the enabler for wireless communications. As a natural resource, the radio spectrum is usually accessed under the regulation of government agencies, such as the Federal Communications Commission (FCC) in the United States (US), the Office of Communications (Ofcom) in the United Kingdom (UK), and the Infocomm Development Authority (IDA) in Singapore. Currently, most of the radio spectrum is allocated based on the command-and-control policy [1], also known as fixed or static spectrum allocation policy [2–4]. Under such a policy, every spectrum user has to obtain a license to gain access to certain spectrum and the license allows the user to have exclusive rights to operate over the spectrum licensed on a long-term basis for large geographical regions.

The static spectrum allocation policy has been working well at mitigating interference between different license holders over the past decades, and we have seen the rapid development of wireless communication applications and services. With the popularity of smart mobile devices over recent years, the demand for ubiquitous wireless services will continue to grow substantially and the wireless traffic will evolve from the simple voice traffic to the bandwidth-demanding multimedia data. However, a glance at any

spectrum allocation chart, e.g. in the United States [5] or in Singapore [6], reveals that most of the spectrum has already been allocated. The question is how we can find swath of spectrum to accommodate the accelerating demand from the already crowded radio spectrum chart.

Inspiringly, preliminary measurements conducted by the FCC have revealed that large portions of the allocated radio spectrum are used only sporadically [1]. Similar observations were also reported in several measurement campaigns conducted world-wide subsequently, e.g., in US [7], Singapore [8], Germany [9], New Zealand [10] and China [11]. These findings suggest that current spectrum scarcity problem is largely due to the inefficiency of static spectrum allocation rather than physical shortage of spectrum.

Therefore, there necessitates a paradigm shift towards a more efficient and flexible way of spectrum management. The concept of *dynamic spectrum access* (DSA) has been brought out under such context as a remedy to the current spectrum scarcity and inefficiency problems. In DSA, users without licenses, also known as secondary users (SUs), are allowed to either access the temporarily unused spectrum, also known as spectrum holes or white space [12], and/or share the spectrum that belongs to license holders dynamically, also known as primary users (PUs). However, as the license holders who have the priority in using the spectrum, PUs should be prevented from any degradation in quality of service (QoS) due to SUs' access. Generally, PUs are not expected to cooperate with the SUs for interference management since changing their systems may be costly. Hence, it is usually the sole responsibility of the SUs to ensure the PU protection. In the case that PUs are allowed to lease their temporarily unused spectrum to SUs, the leasing fees paid by the SUs will give them an incentive to provide certain form of cooperation. This will greatly ease the burden of SUs and hence facilitate DSA [13–15]. In either case, if the interference can be properly controlled, SUs can then coexist with the PUs either opportunistically or concurrently.

Consequently, we can not only improve the utilization of the spectrum, but also provide sufficient bandwidth to meet the growing demand for emerging wireless applications and services.

Note that the aforementioned DSA is also known as the hierarchical access model [2] since users' priorities of accessing the spectrum are differentiated based on whether they are licensed or not. In the literature, another model of DSA over the spectrum where the access of it does not require any license, has also received considerable attention [16–19]. In this model, since there are no license holders, all users, possibly from different networks, have equal right to access the spectrum. However, this thesis will focus on the hierarchical DSA instead.

1.2 Cognitive Radio (CR)

To enable DSA, *cognitive radio* (CR) [20, 21] has been widely recognized as key technology. Since its first inception in 1999, many variants of definitions of CR have been offered in the literature [2, 3, 22–24] etc. Generally speaking, a CR refers to an intelligent radio system that can dynamically and autonomously adapt its transmission strategies (e.g., carrier frequency, bandwidth, transmit power, antenna beam or modulation scheme, etc.) based on the interaction with the surrounding environment and its awareness of its internal states (e.g., hardware and software architectures, spectrum use policy, user needs, etc.) to achieve the best performance. Besides the reconfiguration capability that is inherited from its predecessor software-defined radio (SDR) where the transmission strategies can be adjusted through computer software [25], CR is built with additional “cognition” which allows it to observe the environment through sensing, to analyze and process the observed information through learning, and to decide the best transmission strategy through reasoning. While the idea of CR may potentially benefit future wireless communication systems in a broader sense, e.g., to enable the inter-operability of heterogeneous networks, the main focus of most current

CR research is on the exploration and realization of cognitive capability to facilitate DSA. Hence, in the literature, sometimes, the term CR is used as a synonym for DSA.

1.2.1 CR for DSA

Figure 1.1 shows a typical cognitive cycle for DSA. An SU equipped with CR has to constantly monitor/sense the spectrum, and gather the information such as spectrum holes and the channel state information (CSI). Based on the collected information, it determines the best operational parameters to optimize its own performance while meeting the requirement to protect the PUs and then reconfigures its system accordingly. The information collected over time can also be used to analyze the radio environment so that the CR device can learn to perform better in future dynamic adaption.

Figure 1.1: The cognitive cycle for DSA.

1.2.2 Regulatory Efforts

While enabling DSA with CR is certainly a technical issue which involves multidisciplinary efforts from various research communities, such as signal processing, information theory, communications, computer networking, and machine learning [23], the

realization of it also largely depends on regulators' willingness to open the spectrum for unlicensed access. Fortunately, over the past decades, we have seen worldwide efforts from regulatory bodies on eliminating regulatory barriers to facilitate DSA. For example, in the US, the FCC set forth a few proposals for removing unnecessary regulations that inhibit the development of secondary spectrum markets in November, 2000 [26]. Later, in December 2003, the FCC recognized the importance of CR and promoted the use of it for improving spectrum utilization [22]. In May 2004, the FCC issued a notice of proposed rulemaking (NPRM) that proposes to allow the unlicensed devices (both fixed and personal/portable) to reuse the temporarily unused spectrum of TV channels, i.e., TV white space [27], and the rules for such unlicensed use was finalized in September 2010 [28]. In the national broadband plan released in March 2010, the FCC also indicated its intention to enable more flexible access of spectrum for unlicensed and opportunistic uses [29]. The TV white space is considered to be very promising for a wide range of potential applications due to its favorable propagation characteristics [28], and hence it has also drawn attention from other regulators worldwide. For example, in the UK, the Ofcom proposed to allow licence-exempt CR devices to operate over the spectrum freed up due to analog to digital TV switchover in the statement of the Digital Dividend Review Project released in December, 2007 [30]. In Singapore, the IDA has also recognized the potential of TV white space technology and is currently conducting trials for testing the feasibility and developing regulatory framework to facilitate it [31].

1.2.3 Standardization Activities

Besides regulators' efforts on spectrum "deregulation", various standardization communities have also been actively working on developing industrial standards that expedite the commercialization of CR-based applications. Following the FCC's NPRM in May 2004, the IEEE 802.22 working group was formed in November 2004 that aims to de-

velop the first international standard that utilizes TV white space based on CR [32, 33]. The standard specifies an air interface (both physical (PHY) layer and medium access control (MAC) layer) for a wireless regional area network (WRAN), which is designed to provide wireless broadband access for rural or suburban areas for licensed-exempt fixed devices through secondary opportunistic access over the VHF/UHF TV broadcast bands between 54 MHz to 862 MHz. The finalized version has been recently published in July, 2011 [34]. The first international CR standard on the use of personal/portable devices over TV White Spaces is Ecma 392 [35]. The first edition of the standard was finalized in December, 2009 by Ecma International based on the draft specification contributed from cognitive networking alliance (CogNeA) [35]. It specifies an air interface as well as a MUX sublayer for higher layer protocols [36], which is targeted for in-home, in-building and neighborhood-area applications in urban areas [35]. Other standards based on CR that are currently under development include IEEE 802.11af, IEEE 802.19 and IEEE SCC 41 (previously known as IEEE 1900) [15, 37].

1.2.4 Cognitive Radio Models

As constant sources of innovation, academic research has contributed and will continue to contribute to the standardization of various CR-based applications. Therefore, the focus of the thesis is on the theoretical analysis, modeling and design of the CR for DSA. From the theoretical perspective, the level of cognition that a CR has determines the type of cognitive messages [38] (also referred to as network side information [24]) it can collect from the environment. Depending on the type of information that the CR collects, the operation of CR can be generally classified into two categories, namely, *opportunistic spectrum access* (OSA) and *spectrum sharing*. The main differences between these two models are summarized in Table 1.1 and will be explained shortly. Some models that use mixed strategies of OSA and spectrum sharing can also be found in [39–43].

	OSA	Spectrum Sharing
Cognitive Message	spectrum holes	CSI from SU-Tx to PU-Rx
Access Mode	opportunistic	concurrent
Enabling Techniques	spectrum sensing, geolocation database	intelligent mechanism to obtain CSI

Table 1.1: Comparisons of the OSA and the spectrum sharing models.

Opportunistic Spectrum Access (OSA)

As the name suggested, in the OSA model (Fig. 1.2), SUs can access the spectrum in an opportunistic fashion over only the spectrum bands which are temporarily left unused by the PUs, i.e., spectrum holes. This model is perhaps the most appealing model that has attracted significant attention from research, regulatory, and standardization communities. It is also referred to by some authors as spectrum overlay [2], or interweave paradigm [24].

To enable this mode of CR operation, SUs need to know accurately the on and off status of the PUs over the bands of interest and thereby access only the spectrum holes or spectrum white space so that PUs' QoS will not be affected. There are basically two enabling approaches.

One is through the use of a geolocation database which records the information on the geographical and temporal spectrum usage. Before transmission, an SU has to

Figure 1.2: An illustration of spectrum usage in the OSA model.

obtain its own geographic coordinates possibly through a locally installed positioning system, and then checks the database for the list of channels that are currently available at its location. More details on how geolocation database can be implemented for reusing TV white space can be found in [44].

The other is to incorporate the capability of *spectrum sensing*, which allows the SUs to monitor the radio spectrum and to determine the presence/absence of the PUs either individually or collaboratively [45–50]. Unlike the geolocation database where the accurate spectrum usage information is recorded, spectrum sensing is basically a signal detection technique [51], which is imperfect due to the presence of noise, multipath fading or shadowing. The performance of it is primarily determined by the following two metrics, *probability of detection* which is the probability of detecting the PU as being present when the PU is active, and *probability of false alarm* which is the probability of detecting the PU as being present when the PU is actually inactive. The former can be considered as an indication to the level of protection to the PUs since a higher probability of detection reduces the chance that the SU accesses the spectrum over which the PU is operating; whereas the latter is related to the amount of transmission opportunities for the SUs since the lower the false alarm, the better that the SU can reuse the spectrum. Generally speaking, these two metrics are conflicting with each other. For example, for a given detection scheme, an increase in the probability of detection can improve the protection to the PU; however, this is achieved at the expense of increasing probability of false alarm which leads to decreasing spectrum access opportunities to the SU. Therefore, to improve the performance of spectrum sensing, there has been a lot of work on designing different detection schemes or allowing multiple SUs to cooperatively perform spectrum sensing [45–50].

The geolocation database may be a good choice for reusing the spectrum where the PU's spectrum usage is highly predictable [4, 15] and the PU is willing to publicize such information since it provides accurate spectrum usage information and allows the

spectrum to be utilized more efficiently [44]. For example, in the final rules set by the FCC for unlicensed access over TV bands, the use of spectrum sensing is eliminated and the unlicensed devices solely rely on the geolocation database for incumbent protection [28]. However, for the spectrum bands where the spectrum usage is highly unpredictable and the PUs are not willing to offer such information, spectrum sensing is still an essential tool for enabling DSA and deserves continued development from the research communities. It is further noted that although spectrum sensing is not mandatory for the unlicensed access over TV white space, the current standards developed such as IEEE 802.22 and Ecma 392 still use a combination of geolocation database and spectrum sensing [34, 36, 52].

Spectrum Sharing

In the spectrum sharing model, also referred to as spectrum underlay in [24], or concurrent spectrum access in [4] (Fig. 1.3), SUs are allowed to access the spectrum simultaneously with the PUs. However, to do this, the SU transmitter (SU-Tx) has to adjust its transmission strategies (e.g., transmit power, antenna beams) to strictly control the amount of interference power caused at the PU receivers (PU-Rxs), i.e., *interference temperature* [23], to be below a predetermined threshold, also known as *interference temperature limit*. This type of protection is usually known as interference power constraint. Generally speaking, the improvement of SU's transmission is usually at the expense of increase in the interference power at the PU-Rxs. To balance this

Figure 1.3: An illustration of the spectrum sharing model.

tradeoff, many research works have been conducted to identify the optimal transmission strategy to achieve *cognitive transmission*, i.e., optimize SUs' performance (e.g., transmission rate, signal-to-noise ratio (SNR), or transmit power) under the interference power constraint [38]. In particular, the use of multiple antennas has been found to improve cognitive transmission substantially because of the additional spatial degree of freedom it offers for the SU-Tx to direct the interference away from the PU-Rx while enhancing the rate of its own transmission [53].

The viability of this model of CR operation lies highly on the availability of the relevant CSI, especially the channel from the SU-Tx to the PU-Rx, so that the interference temperature can be predicted. Without PUs' cooperation, such information may not be easily obtained. This limits the interest of the spectrum sharing model currently only to academic research. However, the concurrent mode of transmission in the spectrum sharing model generally allows the spectrum to be utilized more efficiently than the OSA model wherein only orthogonal transmission is allowed [38]. Besides, there have also been some ongoing endeavor that look into the issue how to practically obtain such CSI, e.g., in [54–58]. Hence, the spectrum sharing model is still a competitive candidate to enable future DSA.

1.3 Motivation

Spectrum sensing is widely considered as the most important capability to enable CR devices to operate in the OSA model. Due to hardware limitations, sensing and transmission cannot be performed simultaneously. This prevents the SUs from monitoring the spectrum during the transmission. To avoid the collision with the possibly reappearing PUs, SUs have to suspend their normal transmission periodically to sense the availability of a channel. From the PUs' perspective, channels should be sensed as long as possible to achieve more accurate detection, as frequently as possible to avoid collision due to PUs' reappearance, and as many as possible to detect the spectrum

opportunity as fast as possible. However, this will introduce more overhead to the SUs' transmission and hence will reduce the effective amount of time left for transmission, which will thus affect SUs' throughput, delay, energy consumption, etc. There necessitates careful designs to balance the intrinsic tradeoff between the sensing requirement to protect the PUs and the access need to improve the SUs' own performance. A design that investigates such kind of tradeoff between sensing and access is termed as *sensing-access design* in this thesis. A pioneer work on such kind of design that optimizes the spectrum sensing time to balance the tradeoff between sensing requirement and the access need to maximize an SU's throughput for a single channel can be found in [59] under the name of sensing-throughput tradeoff. Generally, SUs are allowed to explore spectrum opportunities over a wideband of channels. Depending on the hardware capability, multiple channels can be sensed either simultaneously or one at a time. The sensing-access design for multiple channels involves different design considerations under different multi-channel sensing schemes. This is usually not the same as the optimization performed individually for each channel. For example, when multiple channels can be sensed simultaneously, which is termed as *parallel channel sensing* in this thesis, since sensing and transmission have to be synchronized over multiple channels, the design has to be performed jointly. When only a single channel can be sensed at a time, a good way for the SUs is to sense multiple channels sequentially, which is termed as *sequential channel sensing* in this thesis. This scheme allows the SUs to explore the diversity not only in the PUs' activities but also in the SU's own channel condition among different channels so that it can quickly locate an idle channel that is good enough to achieve its own desire. The design thus has to determine when to stop sensing and start transmission and in what order sensing should be performed. Therefore, this motivates the study in this thesis to investigate the multi-channel sensing-access design to optimize SU's own transmission for different performance measures at the same time to ensure the PUs' QoS is not affected under

these two multi-channel sensing schemes.

In the spectrum sharing model, most existing studies focus on the design of transmission strategies to improve cognitive transmission mainly in terms of achievable rate or SNR. However, wireless networks are susceptible to eavesdropping due to the openness of wireless transmission medium. In future CRNs, eavesdropping becomes much easier for a malicious user due to the capability of a future CR device to sense a wide range of radio spectrum. Although eavesdropping is a critical issue, little attention has been received in the literature of CR research, especially from the information-theoretic perspective. This motivates the study in the thesis to address the security issue for the cognitive transmission in the presence of an eavesdropper.

1.4 Objective

Despite the theoretical differences in modeling, design and analysis, in both models, SUs have to strike a balance between optimizing its own performance and maintaining sufficient protection to the PUs. Therefore, efficient resource allocation methods should be investigated to balance this tradeoff. In this thesis, several such resource allocation problems are identified and studied. The objectives and the constraints are problem-specific. The aim is to optimize various system resources such as transmit power, sensing/transmission time, antenna beams, channel selection, etc. In particular, two major resource allocation problems are considered: sensing-access design in the OSA model and secure transmission in the spectrum sharing model.

In the OSA model, both cases of parallel and sequential channel sensing are of interest. Specifically, for the case of parallel channel sensing, the objective is to maximize the sum achievable throughput under the sum transmit power constraint such that the PUs are well protected on each channel by a fixed probability of detection constraint. The sensing-access design includes the sensing strategy specifying the optimal sensing time and the access strategy determining the optimal power level upon transmission.

For the case of sequential channel sensing, the objective is to maximize the energy efficiency of the sequential channel sensing process such that the PU is sufficiently protected under a fixed probability of detection constraint. The design includes the sensing-access strategies as well as the sensing order. The sensing strategy determines when to stop sensing and start transmission. The access strategy specifies the transmit power level upon transmission. The sensing order tells the SU which channel to sense next if the current channel is given up for transmission.

The secure transmission in the spectrum sharing model is addressed from the information-theoretic perspective. This approach is also known as physical-layer security, which is to be differentiated from the traditional cryptography approach to treat security at the application layer [60]. Specifically, the communication over a *secure multiple-input single-output (MISO) CR channel* where a multi-antenna SU transmitter (SU-Tx) sends confidential information to a legitimate SU receiver (SU-Rx) in the presence of a single-antenna PU receiver (PU-Rx) and a single-antenna eavesdropper receiver (ED-Rx) is considered. The performance of the secure transmission is measured in terms of *secrecy rate*, which is defined as the rate at which the information can be reliably transmitted from the SU-Tx to the SU-Rx but is kept secret from the ED-Rx, at the same time interference power constraint is satisfied. The secrecy rate is affected by the quality of the CSI of the secondary channel (i.e., channel from the SU-Tx to the SU-Rx), the eavesdropper channel (i.e., channel from the SU-Tx to the ED-Rx) and the primary channel (i.e., channel from the SU-Tx to the PU-Rx). The objective is to characterize the secrecy rate in this channel and to design the transmission strategy in terms of the transmit covariance matrix such that the achievable secrecy rate is maximized under both cases of perfect and imperfect CSI at the SU-Tx.

1.5 Summary of Contributions

The main contributions of the thesis are summarized as follows.

Sensing-Access Design in the OSA Model

The sensing-access design for the case of parallel channel sensing is formulated as an optimization problem that maximizes the sum throughput under the probability of detection and sum transmit power constraint. The optimal power allocation strategy is determined to be a waterfilling form using convex optimization techniques. The waterlevel for a particular channel is shown to be independent of the status of the PUs on other channels under the average sum transmit power constraint; whereas it is dependent under the instantaneous sum transmit power constraint. The optimal sensing time can be determined through exhaustive search in the general settings while in the numerical results provided, unique optimal sensing time is observed and can be determined with more efficient search algorithm.

The sensing-access design that aims to maximize the energy efficiency of sequential channel sensing is formulated as a finite-horizon stochastic sequential decision-making problem [61]. Through mathematical transformation and analysis, an algorithm is proposed to compute the optimal strategies numerically. Besides, it is found analytically that the optimal sensing strategy has a threshold structure, which indicates that the SU should stop sensing and start transmission if the current channel condition is good enough. The optimal access strategy which specifies the transmit power level upon transmission has a water-filling structure with the water level determined by the long-term energy efficiency and the perceived spectrum opportunity of the transmission channel. The optimal sensing order will choose the channel to be sensed as the one with maximum expected future net reward among the set of remaining channels. Lastly, numerical results show that a larger set of channels that an SU is allowed to sense improves energy efficiency and reduces the optimal sensing time.

Secure Transmission in the Spectrum Sharing Model

When the CSI of the secondary channel, the eavesdropper channel and the primary channel is perfectly known at the SU-Tx, the secrecy capacity, which is the maximum secrecy rate, is characterized in terms of a nonconvex optimization problem of the transmit covariance matrix. In the case of imperfect CSI when the SU-Tx only knows the uncertainty sets where the actual CSI is contained, the worst-case secrecy rate under Gaussian signaling without preprocessing of information is characterized in terms of a maximin non-convex semi-infinite optimization problem, which is mathematically more complex than the case of perfect CSI. Under both cases of CSI, the optimal transmit covariance matrix and the corresponding secrecy capacity/rate can be computed from the two numerical approaches proposed. Moreover, when CSI is perfectly known, it is shown analytically that beamforming is the optimal transmission strategy for the secure MISO CR channel. Furthermore, a few beamforming solutions are proposed to trade off secrecy rate and computational complexity. Lastly, it is shown in the numerical results that the effectiveness of using multiple antennas to preserve information confidentiality as well as to protect the PU-Rx.

Application of Optimization Techniques

It is demonstrated throughout the main content of the thesis the effectiveness of various optimization techniques such as convex optimization and dynamic programming to model and analyze the resource allocation problems. In addition, several novel mathematical transformation techniques for the problems described above are also proposed. These techniques not only allow the application of efficient algorithms but also help gain insights into the structure of the optimal solutions. Specifically, for the problem that addresses energy-efficient sequential channel sensing, the design is formulated as a sequential decision-making problem. This formulation not only allows to integrate the adaptive power allocation design, the sensing strategy design and sensing order

design, but also takes into account the imperfection of spectrum sensing. The optimal energy-efficient sensing-access strategies are identified through the transformation into a parametric problem, which can be interpreted as an energy-aware design. The resulting problem has an additive and separable structure which allows dynamic programming (DP) [61] to be applied to find the corresponding optimal strategy. Based on the relationship between these two designs and the monotonicity structure of the energy-aware design, an algorithm is then developed to compute the optimal sensing-access strategies numerically. For the problems that address the secure transmissions in the spectrum sharing model, the secrecy capacity/rate is expressed as the result of a non-convex optimization problem. Under the both cases of perfect and imperfect CSI, two efficient numerical approaches are proposed to obtain the optimal transmit covariance matrix. In the first approach, through novel reformulation, the seemingly nonconvex problem can be recast into a convex semidefinite program (SDP) and hence can be solved very efficiently through semidefinite programming. In the second approach, the original problem can be shown to be equivalent to a sequence of capacity-achieving designs in the conventional CR channel with two PU-Rxs and no ED-Rxs, which can be shown to be a convex SDP. The second approach, though computationally more complex than the first one, allows to draw the relationship between secure CR channel and conventional CR channel and hence gains insight into the optimality of beamforming strategies for the case of perfect CSI. It is further noted that the derivation of the two approaches in the case of imperfect CSI is facilitated through the use of the S-Procedure [62].

1.6 Organization of the Thesis

The remainder of the thesis is organized as follows. In Chapter 2, a detailed review on various resource allocation schemes under the two basic CR models, namely, OSA and spectrum sharing, is provided. The designs of sensing-access strategies in the OSA

model are studied for the cases of parallel channel sensing in Chapter 3, and sequential channel sensing in Chapter 4, respectively. The transmitter designs to achieve the physical-layer security for the secure MISO CR channel are studied for the cases of perfect and imperfect CSI, in Chapter 5 and Chapter 6, respectively. Lastly, the thesis is concluded in Chapter 7, where possible future directions of work in the area of subject are also pointed out.

Chapter 2

Literature Review

The fundamental challenge to the successful deployment of DSA is to ensure that the PUs' QoS is not affected. As mentioned in Chapter 1, the OSA model typically explores the use of spectrum sensing to facilitate protection; whereas in the spectrum sharing model, this is usually accomplished through the interference power constraint. In this chapter, literature review on various resource allocation methods that balance the tradeoff between optimizing SUs' own performance and maintaining sufficient protection to the PUs under these two models are presented. In addition, for the complete functioning of CRNs, security is also very important. The security issues involved are also discussed. However, given the large number of existing works on CR, the references to be mentioned, though numerous, is far from being exhaustive.

2.1 Opportunistic Spectrum Access (OSA)

Spectrum sensing is the key enabling function for a CR to operate in the OSA model, the incorporation of which makes the spectrum access significantly different from that in the conventional wireless networks. The main functions for the PHY and MAC layers of CR networks (CRN) in the OSA model is illustrated in Fig. 2.1. The additional spectrum sensing functionality is realized in both layers. The PHY layer focuses on

Figure 2.1: Main PHY and MAC layer functions in OSA model.

signal detection, which is how to identify spectrum holes based on the observed data from the environment. Spectrum sensing approaches can be different based on whether detecting the signal from the PU-Tx, or the PU-Rx, which will be introduced in Section 2.1.1. In either of these approaches, sensing is basically a signal detection problem, and various existing signal detection schemes will be reviewed in Section 2.1.2. The main function for sensing in the MAC layer is sensing scheduling, which determines when, which channel, how long and how frequently sensing should be performed, etc. As mentioned in Chapter 1, spectrum sensing is closely coupled with spectrum access. The latter includes the MAC layer access scheduling which determines when to access the spectrum and how to coexist with multiple users; and the PHY layer transceiver optimization which is concerned with power control, modulation and coding, antenna beam design, etc. The efficient implementation of CRNs requires the coordination of both spectrum sensing and spectrum access. On one hand, spectrum access is largely guided by the outcomes of spectrum sensing. On the other hand, spectrum sensing has to be optimized to achieve the ultimate goal of efficient spectrum access. Such coordination is determined by an additional sensing-access controller in the MAC layer. The sensing-access design can be considered as the basic responsibility of the sensing-access controller and the existing work on this will be presented in Section 2.1.3.

2.1.1 Spectrum Sensing Approaches

In the OSA model, the SUs can only access the spectrum holes, the detection of which is based on spectrum sensing. To be more precise, a spectrum band can be considered as a spectrum hole if the use of it by the SUs will not affect the successful reception at any PU-Rx of the signal from the corresponding PU-Tx [47, 63]. Thus, the SUs have to prevent any harmful interference generated at the PU-Rxs. The range of which the transmission by an SU causes unacceptable interference to any PU-Rx within is termed as the *interference range* of the SU-Tx, which is generally determined by the transmit power of the SU-Tx and the maximum allowable interference to the PU-Rx. Therefore, the objective of spectrum sensing is to detect if there is any PU-Rx within the interference range of the SU-Tx before it transmits. If there are no PU-Rxs found, the spectrum band can be considered as a spectrum hole, and it is safe to be accessed by the SU-Tx. The approach aims to directly detect PU-Rxs is termed as *direct sensing* in this thesis. However, generally receivers do not intentionally transmit any signal when it is active, which makes the direct sensing for PU-Rxs very challenging. To overcome this, the approach commonly taken in the literature is to infer the presence of any active PU-Rxs based on the detection of signal(s) from the PU-Tx(s). In this case, spectrum sensing can be further classified into two approaches based on the knowledge used to make such inference, namely, *indirect sensing by worst-case location information* and *indirect sensing by PUs' link control feedback*. The details on the rationales behind these approaches are introduced as follows and their pros and cons are also discussed.

Direct Sensing

Although receivers do not intentionally transmit any signal when it is active, it has been pointed out in [64] that there is inevitably power leaked from any active radio frequency (RF) receiver. The leakage is generated because at the active receiver, when the incoming RF signal is down-converted to intermediate frequency at the local oscil-

lator (LO), some of the LO power couples back through the input port and emits out of the antenna. Hence, it was proposed in [64] to exploit the LO reverse leakage power to detect the presence of PU-Rxs. However, the leakage signal is normally extremely weak, which limits the detection to short distance detection with long detection time. For example, it has been shown in [64] that if SUs are situated 20 meters away from a TV receiver, the time for reliable detection would take on the order of seconds. To make this sensing approach more practical, it was further proposed in [64] to place tiny low-cost sensors in close proximity to the PU-Rxs, and to allow the sensor upon detecting the LO leakage power to communicate the channel usage information to the SUs using additional control channels. The feasibility of this proposal still depends on the PUs' willingness to incorporate the additional sensor nodes. Besides, even though the SUs could receive the channel usage information on the control channels, they may still require additional location information from the sensors to assess the possibility of interference on the channels intended to use.

Indirect Sensing by Worst-Case Location Information

As mentioned previously, without the aid of sensor nodes, detecting PU-Rxs in the general scenario is highly impractical. The most popular approach taken in the literature turns to detecting the presence of signals from the PU-Txs and treats the detection result as an indication to the presence of any nearby PU-Rxs. The basic idea is illustrated in Fig. 2.2 [2, 4, 47, 65]. An SU-Tx at location A is seeking transmission on a licensed channel. In order not to interfere with the PUs, the SU-Tx has to ensure no PU-Rxs are within its interference range denoted as d_I . Without information on the locations of either PU-Txs or PU-Rxs, the SU-Tx in this case takes a worst-case approach. In the worst case, a PU-Rx could be located on the boundary of its interference range, e.g., at location B and the corresponding PU-Rx could be located as far as a distance $d_I + d_p$ away, e.g., at location C, where d_p denotes the maximum transmission range of

Figure 2.2: Illustration of Passive Sensing of PU-Txs

the PU-Tx. In this case, if the SU-Tx can ensure no PU-Tx is located within a range of $d_I + d_p$, then it can ensure no PU-Rx is located within its interference range and therefore it is safe to transmit. This requires the SU-Tx to have a sensing capability to detect PU-Txs' signals at a distance as far as $d_I + d_p$, which is termed as its *sensing range*.

However, this approach of sensing the existence of PU-Txs suffers two major drawbacks. First, this approach is conservative and potentially leads to low spectrum utilization. This is because even though the SU-Tx successfully detects the presence of PU-Txs within the sensing range, it does not necessarily indicate the presence of PU-Rxs within the interference range. For example, the detected PU-Tx may communicate to the PU-Rx situated at location D or E, which is outside the interference range of the SU-Tx. In this case, it is in fact a spectrum hole to the SU-Tx, but the access of it is unfortunately prohibited in this approach of sensing. Secondly, even though transmitters' power emission is much stronger than the LO leakage power from the receivers, the signal detection range in this approach also increases from d_I as in the approach of direct sensing to $d_I + d_p$. Since the SU-Tx can be potentially located outside the coverage range of the PU-Txs, the primary signal received at the SU-Tx can sometimes be very weak for signal detection. In some undesired cases when the

SNR of the primary signal is lower than some threshold, which is known as the SNR wall, the detection becomes impossible even with infinitely long detection time [66].

Indirect Sensing by PUs' Link Control Feedback

Many communication systems are bidirectional in which the receiver can feedback the link information such as channel quality, reception acknowledgements (ACK/NAK) to the transmitter so that the latter can adjust its transmission strategies such as, transmit power, access probability, retransmission strategies to maintain or improve the QoS of the transmission link. In [54, 67, 68], the power control feedback (PCF) between the PU-Tx and the PU-Rx is exploited for the purpose of spectrum sensing. Unlike the previous two approaches in which the SU-Tx only passively listens to the presence of signals, in this approach it proactively sends a sounding signal, and then detects if there is any power fluctuation of the primary signal in response. If there is any PU-Rx in the SU-Tx's interference range, the sounding signal would temporarily interfere with the PU-Rx and hence would trigger the PCF, which would result in the increase in transmit power level at the corresponding PU-Tx. If there is no PU-Rx nearby, the level of the primary signal would remain the same. Therefore, by detecting if there is any change in the power level during and after the sounding interval, the SU-Tx can determine the presence of any PU-Rx nearby. Ideally, only when a PU-Rx is indeed in the SU-Tx's interference range can such change in power be observed. Hence, this approach improves the spectrum utilization as compared to the one based on worst-case location information.

However, a few practical concerns have to be carefully justified: First, the sounding signal may cause temporary interference to the PU-Rxs and thus the design of the sounding interval is critical. On one hand, it should be long enough to trigger the PUs' PCF, which however increase the detection time. On the other hand, it should be short enough to allow only "insignificant" degradation to the PUs. Otherwise, incentive for

PUs to accept such performance degradation should be sought. Next, without the knowledge of when the PCF will be triggered, the detection performance is sensitive to the detection timings. Furthermore, the quantization levels of the PUs' transmit power control will also affect how well the detector is able to detect changes in the power levels.

It is worth mentioning that besides spectrum sensing, the PCF has also been explored for primary channel estimation in [54, 58, 69]. In addition, other forms of link control feedback employed by PUs have been investigated as well for the design of DSA [70–72].

2.1.2 Signal Detection Schemes

In either of the spectrum sensing approaches introduced in Section 2.1.1, spectrum sensing is reduced to a signal detection problem that involves discerning between signal and noise or between different types of signals. Such a problem is usually formulated as a hypotheses test. In this section, the focus is given to the detection schemes specially developed for the indirect sensing approach with worst-case location information, which represents the main stream of literature in spectrum sensing and is also used for the multi-channel sensing-access designs in Chapters 3 and 4¹. In this case, the aim is to decide between the two hypotheses, $\mathcal{H}_0$ representing the absence of the primary signal, and $\mathcal{H}_1$ denoting the presence of the primary signal. Mathematically, it is expressed as follows:

$$\mathcal{H}_0 : y(t) = w(t), \quad (2.1)$$

$$\mathcal{H}_1 : y(t) = x(t) + w(t) \quad (2.2)$$

where $y(t)$ is the received signal at the SU; $x(t)$ is the signal from the PU-Tx received at the SU; and $w(t)$ is the additive white Gaussian noise (AWGN). A number of

¹The detection schemes adapted to the other two sensing approaches can be found in [64, 67, 68]

detection schemes has been proposed in the literature to solve this hypotheses test problem. These schemes differ in operational rationale, levels of knowledge of the primary signal needed, complexity, performance, etc, some of which will be briefly reviewed subsequently.

Energy Detection

When the SUs have completely no knowledge of any characteristics of the primary signals, one simple approach is to use energy detection, also known as radiometry, which measures the energy level of the received signal and makes a decision based on a properly chosen threshold ϵ_{ED} , [73, 74]

$$T_{ED} = \frac{1}{L} \sum_{t=0}^{L-1} |y(t)|^2 \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\geq}} \epsilon_{ED}, \quad (2.3)$$

where L is the number of sensing samples collected.

The advantage of energy detection is the simplicity in implementation and the robustness to change in signal characteristic since no *a priori* knowledge of primary signals is required. On the other hand, such simplicity renders it not able to differentiate the primary signals from any interference signal, which may increase the probability of false alarm in the presence of unknown sources of interference. Besides, the setting of detection threshold for energy detector requires perfect knowledge of noise power, which may not be obtained precisely in practice. Hence, energy detection is very susceptible to noise uncertainty.

Matched Filter Detection

When the SUs have perfect knowledge of the primary signal, it is optimal to use matched filter to detect known signal in the presence of AWGN since it maximizes the SNR of the received signal [75]. Mathematically, the matched filter correlates the received signal with the known primary signal and the decision is based on the

comparison with a predefined threshold ϵ_{MF} ,

$$T_{MF} = \frac{1}{L} \sum_{t=0}^{L-1} y(t)x^*(t) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \epsilon_{MF}. \quad (2.4)$$

The main advantage of the matched filter detection is the short time required to achieve good detection performance [76]. However, due to the coherent detection, the SUs have to maintain synchronization with the PUs, which may complicate the practical implementation [77]. In addition, future DSA may allow the SUs to explore spectrum opportunities over a wide range of spectrum that may belong to different primary systems. In this case, the SUs should know all types of signals, which may further lead to high implementation complexity. In practice, when perfect information on the primary signals is not possible, pilots, preambles, etc. used by the primary systems, if known, can also be used for coherent detection.

Cyclostationary Detection

Radio signals in most communication systems are in fact cyclostationary, i.e., their statistical properties (e.g., mean and autocorrelation) vary periodically with time [78]. The periodicity usually emerges as a result of modulation and coding, pulse shaping, frequency hopping, etc., or is even intentionally introduced to facilitate synchronization and channel estimation. The periodicity introduces spectral redundancy and causes correlation between widely separated spectral components and hence can be used to distinguish cyclostationary signals from noise, which is generally considered a stationary process that exhibits no spectral correlation [78–80]. A Detection scheme based on it is known as cyclostationary detection, which has been considered for spectrum sensing in [77, 81–83] etc.

Mathematically, the correlation between spectral components separated in frequency by an amount of α , can be evaluated from the cyclic autocorrelation function

(CAF) of the received signal $x(t)$ [84],

$$R_y^\alpha(\tau) = \lim_{T \rightarrow \infty} \frac{1}{T} \int_{-\frac{\tau}{2}}^{\frac{\tau}{2}} y\left(t + \frac{\tau}{2}\right) y^*\left(t - \frac{\tau}{2}\right) e^{-j2\pi\alpha t} dt \quad (2.5)$$

where α is called the cyclic frequency, which is the integer multiples of the fundamental frequencies, i.e, reciprocals of periods in $y(t)$. The value of $R_y^\alpha(\tau)$ is not identically zero as a function of τ at some $\alpha \neq 0$ for cyclostationary signals whereas it is identically zero for stationary signals [79]. Equivalently, it can also be observed from the cyclic spectral density function, also known as spectrum correlation function [79],

$$S_y^\alpha(f) = \int_{-\infty}^{\infty} R_y^\alpha(\tau) e^{-j2\pi f\tau} d\tau \quad (2.6)$$

which is the Fourier transform of the CAF and measures the density of correlation between spectral components at frequencies $f - \frac{\alpha}{2}$ and $f + \frac{\alpha}{2}$. The implementation details of cyclostationary detection can be found in [81].

The merit of cyclostationary detection is that it can differentiate the cyclostationary primary signal with the stationary interference and noise. Besides, it is more robust to noise uncertainty than energy detection [81]. Nevertheless, SNR wall still exists for cyclostationary detection, however, it is better than that of energy detection but strictly worse than matched filter detection [85].

Covariance-Based Detection

The primary signal received at the SUs is usually correlated due to the time dispersion of the propagation channel, oversampling, or the use of multiple antennas for spectrum sensing [86]; whereas noise components are usually independent and identically distributed (i.i.d.) and are not correlated. This observation results in different structures

in statistical covariance matrix of the received signal under the two hypotheses:

$$\mathbf{R}_y = \mathbb{E} \{ \mathbf{y}(t) \mathbf{y}^H(t) \} = \begin{cases} \mathbf{R}_s + \sigma^2 \mathbf{I}_N, & \mathcal{H}_1 \\ \sigma^2 \mathbf{I}_N, & \mathcal{H}_0 \end{cases} \quad (2.7)$$

where $\mathbf{y}(t) = [y(t), y(t-1), \dots, y(t-N+1)]$; $\mathbf{R}_s$ is the statistical covariance matrix of the received primary signal; σ^2 is the noise power; and $\mathbf{I}_N$ is an identity matrix of dimension $N \times N$. It is typically nondiagonal under $\mathcal{H}_1$ but diagonal under $\mathcal{H}_0$. Such a difference can be used to differentiate between primary signal and noise. In practice, with limited number of signal samples, the sample covariance matrix

$$\hat{R}_y = \frac{1}{L} \sum_{t=0}^{L-1} \mathbf{y}(t) \mathbf{y}^H(t) \quad (2.8)$$

is used as an approximation to (2.7), based on which a number of test statistics has been proposed, e.g., using the ratio of its diagonal and off-diagonal elements in [86], the ratio of maximum and minimum eigenvalues in [87], its maximum eigenvalue in [88]. The exact threshold for the detection based on the maximum and minimum eigenvalues has been derived in [89]. Since covariance-based detection does not require *a priori* knowledge of the noise power, the signal or the channel, it is robust to noise uncertainty and change in primary signals. However, complexity arises due to the need to compute sample covariance matrix and perform eigenvalue decomposition.

Other Detection Schemes

While the aforementioned signal detection schemes mainly focus on narrowband signal detection, there are also research works that specifically address the detection of wideband signals. For example, when the power spectral density (PSD) of the wideband signal exhibits smoothness within each subband but discontinuous changes between adjacent subbands, a wavelet-based detection approach has been proposed in [90] to

detect and estimate the irregular edge in PSD, which carries critical information on the location and intensities of spectrum holes. When the wideband signal is sparse in the frequency domain, which is usually the case due to low spectrum utilization as evident from various measurement campaigns, compressed sensing [91], also known as compressive sensing or compressive sampling, has been applied to spectrum sensing in [92, 93] etc. Unlike other detection schemes that utilize the samples obtained at Nyquist rate, compressed sensing only relies on the signal sampled at sub-Nyquist rate, which greatly relaxes the sampling requirement at the analog-to-digital converter for detecting wideband signals.

All of the schemes reviewed so far can be considered as block-based detection, which means that the decision is made after collecting and processing a fixed number of samples. There have also been research works that investigate sample-by-sample-based detection, where after collecting each sample, a decision has to be made on whether confirming either of the two hypotheses and hence quit detection or continuing observation [94–98]. For the detection of signal on a single narrowband channel, this detection scheme can find its roots either in sequential probability ratio test (SPRT) assuming all the samples collected during the entire period of observation follow the same statistical distribution, or in quickest change detection assuming the samples have a abrupt change in distribution at some unknown time due to the change of PU status [99]. Generalization of these two scenarios to multiple channels can be found in [94, 97, 98]. The advantage of this type of detection is that it may effectively reduce the detection time since the number of samples collected is a random variable that adapts to the realizations of the observations.

Furthermore, by allowing multiple spatial located SUs to cooperate and therefore exploiting the spatial diversity in their sensing information, the performance of all the aforementioned detections schemes can be improved. This is known as cooperative spectrum sensing in which the final decision is made at a fusion center based on the

sensing information from multiple independent SUs. The sensing information combined can be in terms of hard information (e.g., decision or quantized sensing information), or soft information (e.g., original sensing observations or test statistics). The rule that specifies how such sensing information is combined is known as the fusion rule, which has been well investigated in the literature under various detection schemes [45–50].

2.1.3 Sensing-Access Designs

The inability of simultaneous sensing and transmission for a CR presents a fundamental challenge and necessitates the sensing-access design to balance the general tradeoff between the SU's desire for performance and the PU's requirement for protection. In addition to the channel characteristics between the SU-Tx and the SU-Rx, such designs will also be affected by sensing capability due to hardware limitation and the PU traffic characteristics. The emphasis of the sensing-access design under different considerations is generally different and will be discussed and reviewed in this section. To demonstrate the basic tradeoff in sensing-access design, the focus in this chapter and the rest of the thesis is essentially on the single user abstraction of a CRN where there is only a single pair of SUs. The design for a multi-user network is more involved due to the need to manage issues such as competition among SUs and aggregate interference to the PUs. Existing MAC protocols designed for CRNs can be found in the survey paper [100].

Sensing Capability due to Hardware Limitation

Parallel Channel Sensing

Parallel channel sensing allows the simultaneous sensing and transmission over multiple frequency channels. As mentioned in Chapter 1, for the case of parallel channel sensing, practical implementation prefers the synchronization of sensing and transmission over multiple channels. Hence, the sensing-access strategies cannot be separately

optimized for each channel. Instead, the design should be taken as a joint approach. This involves making compromise among the performances of different channels so that a system-wide optimal design can be achieved. In [45, 101], a multiband joint detection scheme was proposed to jointly optimize the detection thresholds over multiple parallel channels so that the aggregate throughput of the SU (expressed in terms of weighted sum of false alarm probabilities) is maximized subject to interference constraint (represented in terms of weighted sum of miss detection probabilities). Under some regulatory conditions, the problem can be transformed into a convex optimization problem and optimal thresholds can be thus efficiently computed.

Sequential Channel Sensing

When only one channel can be sensed at a time, an SU can sense multiple channels sequentially, and dynamically determine how many channels should be sensed before a transmission. This approach allows the SU to explore diversity in primary channel occupancy among different licensed channels. Hence, in case that one channel is sensed busy, the SU can quickly identify a spectrum opportunity by continuing to sense other channels. Furthermore, it allows the SU to explore diversity in the secondary channel fading statistics so that the SU can possibly take advantage of a better channel to maximize its own desire. In this sensing approach, each time after spectrum sensing, the SU has to make a decision on whether to continue to sense the next channel or to stop sensing and start transmission. The rule that determines when channel sensing should be stopped is known as the stopping rule², which is the essential objective in the sensing-access design for the sequential channel sensing. Intuitively, sensing more channels can better exploit the diversity among different channels. However, this could lead to degradation in the SU's performance because of the increasing sensing overhead. Therefore, optimal stopping rule should properly balance such a tradeoff.

In [102], the authors considered the case that multiple channels can be used for

²It is noted that in this thesis, a stopping rule can be considered a sensing strategy for the case of sequential channel sensing.

transmission and explored only the diversity in primary channel occupancy. In [103] and [104], the authors considered the transmission over the last sensed channel and explored the diversity among both the primary channel occupancy and secondary fading statistics. In [105], the authors further allowed the transmission over previous sensed channel, which is called “retire”, as well as the unsensed channels, which is called “guessing”. The focus of [102–106] is to design the stopping rule so as to maximize some forms of throughputs of the SU. The designs are based on the optimal stopping framework or DP. When the sensing order is given, it has been shown in [103, 104] that the optimal stopping rule has a threshold structure which allows stopping only when the achievable rate of the current channel is above some thresholds. When retire and guessing are allowed, it has been shown in [105] that the optimal strategy is also threshold-based, which indicates that to stop and retire when the best channel condition among all sensed channels is good enough, to stop and guess when it is bad enough, and to continue to sense when it is in between. When the achievable rates on different channels are known *a priori* and the channel is sensed according to descending order of them, it has been shown in [106] that the optimal stopping rule is to stop at the first idle channel sensed.

Besides the stopping rule, the sensing-access design also involves the sensing order design which affects how quickly a good enough spectrum opportunity can be found. In [104], the sensing order was investigated together with the stopping rule using DP and the optimal order in general depends on the realizations of the PU states and the SU channel conditions in the sequential channel process. In [107], the channel sensing order was designed to minimize the mean sensing time to find idle channels that satisfy a predefined rate constraint. A necessary condition for the optimal order was derived using the interchange arguments approach as in the scheduling problem considered in [61, p. 178]. For the case of homogeneous SU channels where the achievable rates are the same for all channels and known *a priori*, this necessary condition is also sufficient

and the optimal order is to sense according to the ascending order of ratios between channel sensing durations and the corresponding idle probabilities. In the general case, the optimal order cannot be predetermined and is dependent on the realizations of the PU states. In [108], the authors investigated the sensing order to maximize the average probability to find an idle channel. Considering homogeneous SU channels, the optimal sensing order is to sense in the descending order of channel idle probabilities.

Selective Parallel Channel Sensing

Selective parallel channel sensing considers the case that only a subset of the channels can be sensed simultaneously each time. Hence, the key task of the sensing-access design is to select which subset of channels to sense in each frame. Under this sensing scheme, the authors in [2, 109, 110] considered a CRN in which the PU states across different frames follow a Markov chain with known transition probabilities. The objective is to jointly design the sensor operating point which is essentially the detector threshold, the sensing strategy that specifies which channel(s) to sense, and the access strategy that determines whether to access the sensed channel(s) based on sensing outcome(s)³ such that the long-term throughput over a finite time horizon is maximized subject to a collision constraint. The optimal design has to jointly balance the tradeoff between false alarm and miss detection through the tuning of the sensor operating point, the tradeoff between gaining immediate access and gaining information for future decision through the sensing strategy, and the tradeoff between being aggressive and being conservative through the access strategy. Due to the partial channel observability, the problem is formulated as a constrained partially observable Markov decision process (POMDP). The sufficient statistics for determining the sensing-access strategies in each frame is the statistical information about the current system state of the underlying Markov process given the sensing and observation history, and can be recursively updated via

³These papers do not assume that the access strategy trusts the sensing outcome, which means that a busy sensing outcome may not prevent the SU from accessing the channel and an idle outcome may not lead to a subsequent transmission.

the Bayesian rule. In the case that the PU activities are independent on different channels, it reduces to the set of conditional idle probabilities. In the general case of constrained POMDP, the optimal strategies are usually randomized, which means that the optimal strategy is a mapping from the sufficient statistics to the probability that a channel should be chosen to be sensed. However, it has been shown in [110] that when only one channel can be sensed and accessed in each frame, the design of the sensing strategy can be decoupled from that of the sensor operating point and the access strategy. As a result, the design of the sensor operating point and the access strategy reduces to a static optimization problem which admits closed-form solutions; and the design of the sensing strategy reduces to an unconstrained POMDP, which leads to a deterministic strategy. In the case that the PU states of all the channels follow independent and identical Markov chains, it has been shown in [111] that the myopic sensing strategy that maximizes the immediate access has a simple structure and that it achieves optimality for the two-channel case and is conjectured for the general case.

Some variations of this basic problem have also been studied. For example, the sensing-access designs in [112, 113] further take into consideration of energy consumption during sensing and transmission. While the basic problem assumes homogeneous SU channels, the authors in [114] further utilized the SU channel conditions in the design of the sensing-access strategies. In [70], the authors extended the basic model to further address the scenario of reactive PUs whose access probabilities over a particular channel are related to the SU's past access history.

Slotted or Unslotted PU Traffic

When the PU system is time-slotted in which its transmission is divided into frames of equal duration, the change in PU status can only be at the frame boundary. If in this case the SU is able to synchronize with the PUs and performs sensing at the

beginning of each frame, the protection of PUs can be simply restricting the probability of detection to a predefined threshold, assuming transmission is allowed only sensing indicates the channel to be idle. However, when the PU system is slotted but the SU is not able to be synchronized with or when the PU system is unslotted in which the busy and idle periods are alternating and randomly distributed, the protection will be much harder since the PU may return during the SU' transmission even if spectrum sensing is perfect. Hence, besides the miss detection, an additional form of collision due to the return of the PUs must be carefully controlled. The amount of collision can be quantified in terms of the number of collisions/collided packets [115–119] or overlapping transmission time between the PUs and the SU [115, 120, 121].

One important parameter in the sensing-access design to cater for the unslotted PUs is the transmission time. Intuitively, the shorter the transmission time, the less likely that the PU will reappear once the SU starts transmission, and therefore the better the protection to the PUs. However, shorter transmission time means less effective time for transmission. Therefore, the transmission time should be properly designed to balance the tradeoff between the PU protection and the SU performance. In [120, 121], a fixed transmission time is optimized, whereas in [115] a randomly distributed transmission time is designed.

The detection of a PU during spectrum sensing (even it is perfect) does not always lead to collision-free transmission. In this case, the SU may not always want to access an idle channel, and whether or not to access will probably be determined by the perceived residual idle/busy time based on past sensing observations. Hence, the access strategy that determines whether or not to access a channel based on the sensing history is also an important ingredient for the sensing-access design. In [116], an unslotted PU system and a slotted SU are considered in a single channel CRN. An access strategy is designed to maximize the SU's throughput subject to the PU's collision constraint. The case of multi-channel CRN has been studied in [117], in which assuming one channel can be

sensed in each frame and with the sensing strategy fixed to be a round Robin fashion, the aim is to design the access strategy that specifies in each frame which channel the SU should access (possibly different from what it has just sensed) based on the sensing and observation history to maximize the long-term throughput in an infinite time horizon subject to the collision constraint. Due to the special sensing strategy used and assuming exponentially distributed PU busy and idle periods, the problem is formulated as a constrained Markov decision process (CMDP). The optimal strategy, which is randomized, is found via a linear program. Two suboptimal strategies have also been proposed to tradeoff the performance and complexity. A similar problem was also addressed in [118]. When the collision constraint is stringent, it has further been shown in [119] that the memoryless (i.e., independent of time and observation history) suboptimal access strategy that allows probabilistic transmission only in the channel just sensed achieves optimality.

The existing works typically assume the activities of the PUs remain constant during the entire sensing period. However, due to the busy nature of PU traffic, it is also possible for the PU to change status even during sensing period. In [122], the authors address this problem by considering a slotted PU system with which the SU is not able to synchronize and the states of which are modeled as a Markov chain across different time slots. Several sequence detection algorithms have been applied to uncover the sequence of PU states within the sensing period based on the sequence of sensing observations under a Bayesian formulation that assigns different costs for miss detection and false alarm. However, the work in [122] focused more on the sensing design in the PHY layer but not on the joint sensing-access design.

Known or Unknown PU Traffic Statistics

The efficient sensing-access design highly depends on the knowledge on the statistics of the PU traffic. It has been mentioned that such information can be utilized to de-

sign the channel sensing order for the sequential channel sensing. When the PU traffic statistics is not known *a priori*, an SU has to learn such information through past sensing observations, and hence the SU has to balance the tradeoff between exploitation which refers to the possible short-term gain (i.e., immediate channel access opportunities) that results from sensing the channel with highest idle probability based on the current knowledge, and exploration which refers to the update of the learnt statistical information by possibly choosing other channels to sense in order to benefit future decision-making. Such a tradeoff resembles the classic multi-armed bandit problem and has been identified and studied in [123] for a slotted selective parallel channel sensing system where the idle probabilities of multiple channels are unknown but are assumed to be i.i.d. across different frames. The sensing-access design is to determine which channel(s) to sense and access in every frames based on the sensing history. Assuming the joint distribution of the idle probabilities is known, optimal sensing-access strategy is found using DP. Some nonparametric strategies with asymptotically optimal performance have also been proposed to relax the assumption on the prior knowledge on such distribution. For the case that the states of PUs are Markovian across different frames as considered in [2, 109, 110], the channel idle probabilities are dynamically varying and are updated by both the sensing history and the known temporal correlation of the underlying Markov chain. The optimization of the sensing strategy based on the perceived conditional channel idle probabilities is also to balance such exploitation versus exploration tradeoff. When the transition probabilities of the Markov chain are not known, it was mentioned in [122] that Baum-Welch algorithm can be used for the estimation. The distribution statistics of an alternating busy and idle periods have been studied in [108] using maximum likelihood estimation.

2.2 Spectrum Sharing

Unlike the OSA model which exploits the temporal unused spectrum of the PUs through spectrum sensing, the spectrum sharing model permits concurrent transmission. Hence, interference to the PUs is inevitable and SUs have to impose interference power constraints to restrict the resulting interference to the PU-Rxs within acceptable levels [124]. Intuitively, an SU's reception quality benefits from a higher transmit power. However, this will result in a high interference power to the PU-Rxs. Tradeoff between performance and protection has to be carefully balanced. In the case of multiple antennas, the additional degree of freedom in the spatial domain can be further exploited. Resource allocation schemes that have been studied in the literature for the spectrum sharing model usually optimize the SUs' performance under various criteria subject to the interference power constraints by adjusting the transmission power and/or antenna beams. The performance measure can be in terms of achievable rate as from the information-theoretical perspective, or SNR / signal-to-interference-plus-noise ratio (SINR) / mean squared error (MSE) as from the signal processing perspective. Some of the resource allocation problems are convex and hence can be solved numerically through interior-point methods implemented by many convex solvers. Closed-form solutions are sometimes available by analyzing the Karush-Kuhn-Tucker (KKT) conditions for a convex problem or using some other mathematical techniques. Many of the resource allocation problems are in fact nonconvex and some novel transformation techniques have to be explored to facilitate optimal and efficient solutions.

The most basic point-to-point channel model for the resource allocation problems is illustrated in Fig. 2.3(a) where the interference from any PU-Tx is generally treated as Gaussian noise and is omitted from the figure. When such interference is not considered as noise, the channel model depicted in Fig. 2.3(b) is sometimes considered. In some existing works, the design of the resource allocation methods requires additional knowledge of the channel from the PU-Tx to the PU-Rx, and in this case, channel

models in Fig. 2.3(c) and Fig. 2.3(d) are considered. The optimization of the resources is in general sensitive to the knowledge of the CSI of the relevant channels. In this section, resource allocation in the literature is first reviewed for the case that the SU-Tx is able to obtain perfect knowledge of various CSI and then introduced for the case when such CSI is imperfect.

Figure 2.3: The basic point-to-point channels in the spectrum sharing model.

2.2.1 Perfect CSI

When the SU-Tx knows the CSI of all the relevant channels, keeping the interference power below a predefined threshold is a simple task for the case that each of the terminals has a single antenna, i.e., single-input single-output (SISO) CR channel. The transmit power is limited by either the transmit power limit or the normalized interference temperature limit. When there are multiple antennas at the SU-Tx, the transmit covariance matrix (or equivalently, the precoding matrix and the power allocation matrix) becomes the design parameter, the computation of which is generally much more involved. In [53], the authors considered a multiple-input multiple-output (MIMO) CR channel where all terminals are equipped with multiple antennas. The design of the capacity-achieving transmit covariance matrix under the joint transmit power and interference power constraints is formulated as a convex optimization prob-

lem, which can be solved only numerically in the general case. In the special case when the receiving terminals are equipped with a single antenna each, i.e., the MISO CR channel, the optimal transmit covariance has been proved to be a rank-one matrix, which shows that beamforming is the optimal strategy. Closed-form solution for the optimal beamforming vector has also been derived through a geometrical approach. In addition, the use of multiple antennas has been found to improve cognitive transmission substantially because of the additional spatial degree of freedom it offers for the SU to direct the interference away from the PU-Rx while enhancing the rate of its own transmission. This basic model has also been extended to various multi-antenna multi-user CR channels, such as multiple access channel [125, 126], broadcast channel [127], multicast channel [128], and interference channel [129].

In some cases, the PU-Rx may even impose a very strict constraint by further restricting the interference temperature limit to be zero. One way for the SU-Tx to achieve this is to use zero-forcing (ZF) beamforming, where the precoding matrix is chosen to be in the null space of the channel matrix from the SU-Tx to the PU-Rx. Depending on the rank of the channel matrix, precoding matrix obtained based on ZF criterion can be null, which prevents the cognitive transmission of the SU-Tx. With the additional information on the CSI from the PU-Tx to the PU-Rx, the idea of interference alignment (IA) has been applied to design the resource allocation of a MIMO CR channel (based on the model in Fig. 2.3(d)). This idea was originally proposed to study the degree of freedom of the interference channel [130]. The rationale is to design the precoding matrix such that all the resulting interference is aligned to the unused spatial directions of the primary transmission. In this way, the SU-Tx can achieve spatially orthogonal transmission with respect to (w.r.t) the primary transmission. Then the decoding matrix and the power allocation matrix are optimized to enhance the rate of the cognitive transmission. The advantage of the IA-based design over the ZF-based design has also been shown in [131] through simulations.

When fading channels are considered, another form of protection, known as the average interference power constraint can also be used. Compared to the normal form of the constraint that restricts the interference power at all times (referred as peak interference power constraint in this case), the average power constraint only limits the average interference power over all fading states to be below the predefined limit. Hence, in certain unfavorable fading states, the temporal interference power could possibly exceed this limit. In [132–135], the authors studied the optimal power allocation to achieve the ergodic and/or outage capacity under various combinations of peak/average interference power constraints and/or peak/average transmit power constraints for the SISO fading CR channels where the SU-Tx, the SU-Tx and the PU-Rx are equipped with a single antenna each. In [136], the authors further investigated the optimal power allocation to achieve the ergodic sum capacity of a fading SISO multiple access CR channel and a fading SISO broadcast CR channel. Intuitively speaking, the average interference power constraint is less restrictive than the peak interference power constraint. As a result, the capacity achieved by the SU is expected to be higher under the average interference power constraint and the protection to the PU is expected to be better too. However, it has been shown in [137] that although the former is true, the capacity loss of the PU in the case of average interference power constraint is surprisingly less than that of the peak interference power constraint due to the “interference diversity” phenomenon.

It is also noted that besides the interference power constraint, another form of constraint that limits the amount of PU’s transmission outage to a predefined threshold has recently been proposed to ensure the protection to the PU [138, 139] for a point-to-point fading SISO CR channel. While the interference power constraint can guarantee the capacity loss of the PU within a bounded value, which is generally independent of the CSI on the primary channel [53], this new form of constraint provides a more direct way to quantify the amount of performance degradation to the PU and exploits

the additional CSI in the channel between the PU-Tx and the PU-Rx (assumed to be available) to better utilize the PU's outage state due to its own adverse channel fading for cognitive transmission. It has been shown through simulations that the optimal power allocation based on this new form of constraint can substantially improve the SU's performance over the conventional interference power constraint [139].

2.2.2 Imperfect CSI

The assumption that perfect CSI of all the relevant channels is available at the SU-Tx in general represents ideal scenarios and the performance results obtained thereby can only serve as the upper bounds for the actual cognitive transmission. In practice, this CSI may not be obtained perfectly due to the channel estimation and quantization errors, and the loose cooperation between the SU and the PU. Therefore, in the context of imperfect knowledge of the relevant channels at the SU-Tx, robust design techniques have to be identified so that the cognitive transmission strategy is less sensitive to the uncertainty in the CSI. To address the system design in the context of imperfect CSI, two popular approaches have been adopted in the literature, namely, stochastic approach and worst-case approach.

In the stochastic approach, the channel is often modeled by a Gaussian random variable with only the mean and covariance known to the transmitter. In such a case, system is usually design to optimize some statistical measures of the performance. From the information theory perspective, this corresponds to maximize the ergodic capacity [140]. Important works in the non-CR context include [141] and [142], which address the capacity achieving transmitter design for the MISO and MIMO channels, respectively. From the signal processing perspective, the system measure is in terms of, e.g., average SNR, average mean square error etc. Prior work along this line for multi-antenna channels can be found in [143, 144].

In the context of CR, with only imperfect CSI of the primary channel, the optimal

power allocation scheme to achieve the ergodic capacity of a fading SISO CR channel under the average interference power constraint was studied in [135]. Furthermore, probabilistic interference power constraint which limits the probability that the interference power exceeds the predefined threshold has also been proposed to study the designs of the optimal power allocation in the OFDM CR channel in [145] and the optimal beamforming vectors for the MIMO CR channel in [146], respectively.

On the other hand, in the worst-case approach, the CSI is assumed be bounded in a known set of possible values but the actual value of the CSI is not known to the transmitter. Under this scenario, the system is usually designed to optimize the performance for the worst case of the CSI value. This approach is commonly used in the signal processing community. For example, robust transmitter designs to maximize the worst-case SNRs have been addressed in [147] and [148] for MIMO channels. In the information-theoretic jargon, a channel with such kind of uncertainty is termed as a compound channel and the maximum worst-case achievable rate is defined as the compound capacity. In particular, the capacity-achieving transmitter strategy has been found to be beamforming for the rank-one Ricean MIMO compound channel in [149].

In the context of CR, the robust transmitter designs in the worst case have been initiated by [150] for the MISO CR channel where only the uncertainty in the primary channel is considered. In particular, in [150], beamforming has been found to be the optimal strategy to maximize the rate of the secondary channel while keeping the interference power below the predefined threshold even for the worst-case condition of the primary channel. The optimal beamforming vector is derived in closed form. Similar to the case of perfect CSI, the closed-form solution for the optimal transmit covariance matrix in the MIMO case with uncertainty in the primary channel is generally not available. Numerical approach has been proposed in [151] to address the robust design. The extension to the case of distributed MIMO CR channels have recently been studied

in [152]. Worst-case robust design has also been investigated from the signal processing perspective for a number of CR channel models where the uncertainty exists in both the secondary and primary channels. Specifically, the optimal beamforming vectors are designed under the worst-case interference power constraints to maximize the worst-case SNR in [153] for the point-to-point MISO CR channel, to optimize under various performance measures in [128] for the multicast CR channel, to balance the worst-case SINR in [154] and to minimize the total transmit power in [155] for the MISO broadcast CR channel.

2.3 Security Issues in CRNs

In the above sections, we have discussed the operational aspects of CRNs and reviewed the existing works. In this section, we will have a brief discussion on the security aspects and introduce some basics on the information theoretic security, with which we take to address the secure transmission in the spectrum sharing in Chapters 5 and 6.

2.3.1 Security Aspects of Spectrum Sensing

Like other wireless networks, security aspects are also very important to the proper functioning of CRNs. Although many of the security measures against malicious attacks could be reused, the unique characteristic of CR also presents new form of security threats and challenges. Since the behavior of a CR is adapted according to its perceived environment from its own sensing observation or interaction with other CRs, a malicious user could cause serious disruptions to the function of the CR by spoofing during the process of environment observation. In [156], the author analyzed the impacts of spoofing on various phases of the cognitive cycle. A detailed discussion on the security threats and challenges to CR and SDR as well as a review on the existing protection

mechanisms can be found in a recent survey paper in [157]. Since spectrum sensing is the basic way for environment observation in the OSA model, the security aspects of spectrum sensing has also attracted considerable attention in the literature. In particular, two types of attacks are of interest, namely, *PU emulation attack* (PUEA) and *sensing data falsification attack* (SDFA).

The highly reconfigurable nature of a future CR makes a malicious user very easily launch a PUEA. In such an attack, the malicious user masquerades as a PU by transmitting a PU-like signal during the SUs' sensing period. The legitimate SUs could mistakenly detect this signal as the PU's and thus refrain from transmission. In this way, the malicious user could prevent the access of the spectrum by these users and hence causes denial of service to them. Additionally, the malicious user could even take advantage of the spectrum opportunity for its own transmission. The PUEA was first identified in [158] and a number of mechanisms to defend against it has been proposed so far. Specifically, in [158] and [159], the authors proposed a solution to identify a PUEA by comparing the location and signal characteristics of the signal with the known PU location and signal. The location of the signal is estimated by a proposed localization technique through the use of an additional sensor network. Without the use of any location information, the authors developed an analytical model to analyze the PUEA in [160], based on which an SPRT-based test was proposed to distinguish between the attacker and the PU in [161]. Assuming the PUEA has been launched, a cooperative spectrum sensing technique was further proposed in [162] to detect if there is any PU signal in the presence of the attacker's signal. Instead of proactively identifying the PUEA as in [158–161], the authors in [163] and [164] proposed to probabilistically avoid the PUEA by allowing the SU to randomly select which channel to sense. With a perfect knowledge of the channel occupancy statistics, the problem was modeled as a zero-sum game between the legitimate SUs and the attacker in [163]. The defending strategy for the legitimate SU, i.e., the channel selection strategy in this case,

and the attacking strategy for the attacker, under the Nash Equilibrium was found. In the absence of such knowledge and with arbitrarily varying attacking strategy, the defense strategy, was found under the adversarial bandit framework.

Another type of attack that is of great interest in the literature is the SDFA in the cooperative spectrum sensing. In such an attack, a malicious user intentionally reports false sensing information with a purpose to distort the global spectrum sensing decision at the fusion center. To defend this, several reputation-based methods have been proposed so as to limit or exclude the attackers' sensing data from the fusion process [165–167]. A reputation reflects an SU' accuracy over past spectrum sensing activities, and is usually obtained by checking the consistency of the local sensing decision with respect to the global sensing decision. Furthermore, the authors in [168] and [169] also proposed to detect the malicious users based on the outlier detection, which is a powerful technique in data mining to identify abnormalities in the data samples.

2.3.2 Information Theoretic Security

Both the PUEA and the SDFA can be considered as *active attacks* where malicious users actively inject some information or modify the information to disrupt the systems. In this thesis, the security issue of interest is *passive attacks* where eavesdroppers quietly monitor the transmission process in a hope to interpret the information transmitted. Hence, our aim is thus to protect the confidentiality of the transmitted information from the potential eavesdropper.

Conventionally, such a problem is usually addressed by using cryptographic encryption, in which a transmitter encrypts the source information with a key, and the encrypted information can be extracted only by a legitimate receiver with a corresponding key. Any eavesdropper, even through having an access to the encrypted information, cannot obtain the source information without the knowledge of the de-

encryption key. In practice, the eavesdropper can be assumed to possess only limited time and computational resources and hence, it is not able to test all the possible keys to extract the source information.

Alternatively, the problem can be addressed from an information theoretic approach, which was initiated by Wyner [170]. The basic idea is to exploit the difference between the channel to the legitimate receiver and to the eavesdropper, which is introduced by the randomness of the communication channel due to noise and/or channel fading, and devise an encoding scheme to guarantee that the source information can be successfully obtained by the legitimate receiver without being intercepted by the eavesdropper.

As compared to cryptography, this approach does not use encryption and decryption keys, and hence achieves significant reduction in complexity and savings in resources by eliminating the need for key management (including key generation and distribution) [60]. Another advantage is that the confidentiality of the source information can be achieved even when the eavesdropper has unlimited resources, and knowledge of the communication strategy employed including encoding and decoding algorithms [60].

The wiretap channel is the basic model to study information theoretic security, an illustration of which is shown in Fig. 2.4 and introduced as follows. The channel describes the communication scenario involving three terminals: a transmitter, a legitimate receiver and an eavesdropper. The transmitter intends to transmit a source message W at rate R_s in n channel use to the legitimate receiver but wants to keep it

Figure 2.4: The wiretap channel.

secret from the eavesdropper⁴. The message is uniformly distributed over a message set $\mathcal{W} = \{1, 2, \dots, 2^{nR_s}\}$, and hence has entropy $H(W) = nR_s$. At the transmitter, the encoder maps each message w to a codeword $x^n = (x_1, \dots, x_n)$. The codeword x^n is transmitted over a discrete memoryless channel, which outputs two sequences y^n and z^n at the legitimate receiver and the eavesdropper, respectively. The transition probability of this channel is denoted as $\mathbf{p}_{YZ|X}$. At the legitimate receiver, a decoder maps each received sequence y^n to an estimated message $\hat{w} \in \mathcal{W}$.

For such a transmission, the message should be guaranteed to be received both reliably and securely at the legitimate receiver. The reliability is measured by the average probability of error, which is defined for a code of length n as $\mathcal{P}_e^{(n)} = \Pr\{\hat{W} \neq W\}$. The level of secrecy is measured by the equivocation rate, which is defined as the entropy rate of the confidential information conditioned on the eavesdropper's observation,

$$R_e^{(n)} \triangleq \frac{1}{n} H(W|Z^n). \quad (2.9)$$

It shows the level of uncertainty that the eavesdropper has about the message W after observing Z^n . Clearly, higher equivocation rate indicates higher level of secrecy.

In this thesis, we are interested in the case of *perfect secrecy*. A rate R_s is said to be achievable with perfect secrecy (also known as secrecy rate) if for any $\varepsilon > 0$, there exists a sequence of codes $(2^{nR_s}, n)$, such that for any $n \geq n(\varepsilon)$, we have

$$\mathcal{P}_e^{(n)} \leq \varepsilon, \quad (2.10)$$

$$R_e^{(n)} \geq R_s - \varepsilon. \quad (2.11)$$

In this case, we can see $\frac{1}{n} I(W; Z^n) = \frac{1}{n} H(W) - \frac{1}{n} H(W|Z^n) = R_s - R_e^{(n)} \leq \varepsilon$, where $I(\cdot; \cdot)$ denotes the mutual information, indicating that the eavesdropper cannot decode at any positive rate and hence the message W is completely hidden from the eaves-

⁴In this section, the parameters W, X, Y, Z are denoted as random variables and the realizations of which are represented by w, x, y, z , respectively.

dropper. The *secrecy capacity* C_s is defined as the maximum of the achievable perfect secrecy rate.

In [171], Csiszár and Körner obtained a single-letter expression for the secrecy capacity of the general discrete memoryless wiretap channel described above as

$$C_s = \max_{\mathbf{p}_{UX}} I(U; Y) - I(U; Z) \quad (2.12)$$

where U is an auxiliary variable satisfying the Markov relation $U \rightarrow X \rightarrow (Y, Z)$, i.e., $\mathbf{p}_{YZ|UX} = \mathbf{p}_{YZ|X}$, where $\mathbf{p}$ denotes the probability density function (PDF). The details on the coding techniques to achieve this secrecy capacity and the converse proof to show the optimality of such techniques can be found in a recent monograph on information theoretic security in [60]. Note that the secrecy capacity C_s is achieved by optimizing over all the joint distributions $\mathbf{p}_{UX}$ satisfying the Markov relation.

Following the works by Wyner in [170], Csiszár and Körner in [171], many researchers have been working on extending the discrete memoryless wiretap channel to many other specific channel models and studying the corresponding secrecy capacity, e.g., for Gaussian channels in [172], fading channels in [173, 174], multi-antenna channels in [175–179], and many multi-user channels in [180–183], etc.

Chapter 3

Sensing-Access Design in OSA: Parallel Channel Sensing

As mentioned in Chapter 1, due to the hardware limitation, the sensing and transmission have to be synchronized over multiple channels for the case of parallel channel sensing. This necessitates the design to be in a joint approach over multiple channels. In this chapter, we take such an approach to address the sensing-access design for parallel channel sensing. Unlike [45] and [101] which focused more on the joint sensing design that determines the sensing thresholds, we are interested in the sensing-access design with the sensing strategy specifying the optimal sensing time and the access strategy determining the optimal power level upon transmission. The duration of sensing time affects the sensing accuracy and the time left for transmission. The power allocation, which depends on sensing results, affects how total transmission power has to be allocated across different channels and hence affects the transmission throughput.

Specifically, our objective is to maximize the sum achievable throughput under the sum transmit power constraint such that the PUs are well protected on each channel by a fixed probability of detection constraint. Two types of transmit power constraints are considered, namely, average power constraint and peak power constraint. The sensing-access design is formulated as an optimization problem. In particular, through

mathematically analysis, we find that the optimal power allocation strategy is determined to be a water-filling form using convex optimization techniques. The water level for a particular channel is shown to be independent of the status of the PUs on other channels under the average sum transmit power constraint; whereas it is dependent under the peak sum transmit power constraint. The optimal sensing time can be determined through exhaustive search in the general settings while in the numerical results provided, unique optimal sensing time is observed and can be determined with more efficient search algorithm.

It is further noted that although the parallel channel sensing and selective parallel channel sensing bear similar names in our classification, the sensing-access designs under two sensing approaches are significantly different. First, due to the hardware limitation, spectrum sensing is not able to be performed over all the channels simultaneously under selective parallel channel sensing. Therefore, how to select the subset of channels for spectrum sensing and subsequent transmission is usually of interest. However, for parallel channel sensing, no channel selection is needed since spectrum sensing can be performed over all the channels. Second, to enable dynamic selection of channels, existing work in parallel channel sensing considers the PU activities vary in a Markovian fashion across different frames such that the perceived idle probability, which is the criterion for selection, vary over time frames. However, for parallel channel sensing, the sensing-access design, especially the sensing design, e.g., the duration of spectrum sensing, is considered as a fixed parameter over time for the ease of synchronization and practical implementation. The design will not be affected by the instantaneous variation of time-varying perceived channel idle probability. Therefore, we can assume independent PU activities across different frames and consider only long-term traffic statistics.

The rest of the chapter is organized as follows. The system model and problem formulation are presented in Section 3.1. The optimization of sensing time and power

allocation under the average and peak power constraints are studied in Sections 3.2 and 3.3, respectively. Section 3.4 presents the simulation results and finally, Section 3.5 draws the conclusion.

3.1 System Models and Problem Formulation

We consider a CRN which can opportunistically access a set of K licensed frequency channels. For simplicity, we assume that the channels are of the same bandwidth, though the design methodology proposed here can be directly extended to channels with unequal bandwidth. Since these channels may be discontinuous on a wideband of spectrum and potentially belong to different primary networks, the PU's activity on each channel can be assumed to be independent of each other. The probability that the PU is idle on channel k is assumed to be known as θ_k , which can be estimated through long-term spectrum usage measurements before the CRN is deployed. In practice, it is more worthwhile for the SU to explore spectrum opportunity of a channel which has low usage, i.e., $1 - \theta_k$ is small.

We consider the case where the CRN consists of a single pair of SU-Tx and SU-Rx. This single-user model can be considered as an abstraction of the multi-user scenario where there is a centralized control such that the central controller each time grants exclusive rights for parallel channel sensing to a single pair of SUs. It can also represent the multi-user scenario where all SUs have to contend on a common control channel first and then only the one who wins the contention can proceed to parallel channel sensing and transmission. In both cases, the multiuser scenario reduces to a single-user scenario where there is only one pair of SUs perform spectrum sensing and access.

Spectrum sensing is an enabling function to facilitate SU's opportunistic access. SU has to suspend its normal transmission periodically to sense the availability of a channel, and it can only access the channel where the PU is not present. The overall transmission frame thus consists of two parts, namely, channel acquisition and

transmission as shown in Fig. 3.1.

Figure 3.1: The transmission frame structure.

We denote the channel acquisition time as τ , which consists of both the spectrum sensing time and possibly channel estimation time if the channel is detected to be idle. To ensure sufficient protection to the PUs, spectrum sensing time is usually much longer than the channel estimation time. For example, if the PUs are TV bands where each channel occupies 6MHz bandwidth as in the case of IEEE802.22 WRAN, for a typical sensing time in terms of a few milliseconds, it will result in thousands of samples [59]. However, for channel estimation, a few pilot symbols would be enough. For example, in IEEE802.11a, only 4 pilot symbols are used for channel estimation [184]. Hence, in our analysis, we simply ignore the channel estimation time. We further denote the duration of the entire transmission frame as T .

The parallel channel sensing allows the SU to sense the K channels simultaneously. However, due to the hardware limitation, all channels should follow the same frame structure as in Fig. 3.1. The wideband spectrum sensor and detector are shown in Fig. 3.2. Spectrum sensing on channel k is simply a binary hypotheses test to determine between $\mathcal{H}_0$ and $\mathcal{H}_1$. Spectrum sensing is subject to sensing errors, and the performance of a spectrum sensor is measured by the probability of detection $\mathcal{P}_{d,k}$ and probability of false alarm $\mathcal{P}_{f,k}$. Given a probability of detection $\mathcal{P}_{d,k}$ on channel k , the probability of false alarm by using energy detection and assuming complex-valued PU signal can

Figure 3.2: The schematic illustration of the parallel channel sensing: A separate energy detector with threshold ϵ_k is used on each narrowband channel k , for $k = 1, \dots, K$.

be approximated by [59]

$$\mathcal{P}_{f,k} = \mathcal{Q} \left(\sqrt{2\gamma_k + 1} \mathcal{Q}^{-1}(\mathcal{P}_{d,k}) + \sqrt{\tau f_s \gamma_k} \right) \quad (3.1)$$

where γ_k is the worst-case received SNR of the PU's signal on channel k ; and f_s is the sampling frequency. In practice, the probability of detection of $\mathcal{P}_{d,k} = 0.9$ has to be ensured when the worst-case PU signal is as low as $\gamma_k = -20\text{dB}$ as in the case of IEEE802.22 WRAN [59].

After the spectrum sensing stage, the SU-Tx will then send pilot signals to the SU-Rx over the idle channels to estimate the fading channel gain. Then the SU-Rx feeds the estimated channel gain back to the SU-Tx⁵. It is assumed that the probability distributions of all the channels are known *a priori* through previous long-term channel measurements.

In the opportunistic spectrum access model, there are two scenarios when an SU can access the channel: 1) Under hypothesis $\mathcal{H}_0$, the SU will access channel k if the SU detector makes no false alarm of the presence of the PU; 2) Under hypothesis $\mathcal{H}_1$, the

⁵In this thesis, our design is to ensure very high detection probability, e.g., $\mathcal{P}_{d,k} = 0.9$ when PU's worst-case SNR is as low as, e.g., $\gamma_k = -20\text{dB}$. Under such conditions, when there is misdetection, we assume that the SU-Rx is still able to receive the pilot signals, correctly estimate the channel and then successfully communicate back to the SU-Tx due to the weak interference from the PU. In practice, the PU signal level may not be so low and the actual detection probability will be even higher. Hence, misdetection is very rare and can be ignored.

SU can access channel k if the SU detector falsely detects the PU as absence due to the imperfection of spectrum sensing. The probability that channel k will be accessed by the SU is given by

$$\mathcal{P}_{a,k}(\tau) = \theta_k(1 - \mathcal{P}_{f,k}) + (1 - \theta_k)(1 - \mathcal{P}_{d,k}). \quad (3.2)$$

In the following, we refer to a channel that is accessed by the SU as an “active channel”.

Due to the variations on traffic loads of different PUs, at a particular period of time, only some of the K channels are available. When spectrum sensing indicates that multiple channels are available, the SU will transmit data simultaneously on them, which is termed as *channel aggregation*. In the case of K channels in the CRN, there are $M = 2^K - 1$ possible scenarios for the SU to use the channels (i.e., at least one channel is active). Note that the scenario that all channels are inactive is excluded for consideration. The probability that scenario m occurs can be expressed as

$$\mathcal{P}_{s,m}(\tau) = \prod_{k \in \Phi_m} \mathcal{P}_{a,k}(\tau) \prod_{k' \in \Phi_m^C} (1 - \mathcal{P}_{a,k'}(\tau)), \quad (3.3)$$

where the symbol $\prod$ represents the product of a sequence of terms; Φ_m is the set of active channels in scenario m ; and Φ_m^C is the complementary set of Φ_m , representing the set of inactive channels in scenario m .

Note that, in any scenario, when the SU detects channel k as available, whether it is successful detection (no false alarm) under $\mathcal{H}_0$ or miss-detection under $\mathcal{H}_1$, the transmitter of the SU will use the same amount of power on this channel, because the SU cannot differentiate these two cases. As mentioned above, for protection purposes, the target probability of detection has to be ensured even when the PUs’ signals are very weak, i.e., γ_k is extremely low. Hence, this worst-case achievable throughput will be of interest. As a consequence, in this chapter, we can ignore the interference from the PU under $\mathcal{H}_1$ in this worst-case analysis. Therefore, the transmission rate on

channel k for both cases in scenario m is thus given by [185]

$$r_{k,m} = \log_2 \left(1 + \frac{h_k p_{k,m}}{N_0} \right), \quad (3.4)$$

where h_k represents the peak channel power gain of the secondary channel k and it is assumed to be independent and ergodic; N_0 is the variance of the AWGN noise at the SU's receive antenna which is assumed to be the same for different channels; and $p_{k,m}$ is the power allocated to channel k in scenario m .

In this chapter, we are interested in maximizing the aggregate average achievable throughput of all the secondary links such that prescribed probability of detection is guaranteed to the PU on each channel. Therefore, the sensing-access design for the parallel channel sensing can be formulated as

$$\max_{\tau, \mathbf{P}} \quad R(\tau, \mathbf{P}) = \sum_{m=1}^M \frac{T - \tau}{T} \mathcal{P}_{s,m}(\tau) C_m \quad (3.5)$$

$$\text{s.t.} \quad \mathcal{P}_{d,k} = \bar{\mathcal{P}}_{d,k}, \quad k = 1, \dots, K, \quad (3.6)$$

where $\mathbf{P} = \{p_{k,m}\}_{k=1,\dots,K;m=1,\dots,M}$; $\bar{\mathcal{P}}_{d,k}$ is the target probability of detection on channel k ; C_m is the sum-rate of the active channels in scenario m which is given by

$$C_m = \sum_{k \in \Phi_m} \mathbb{E} \left\{ \log_2 \left(1 + \frac{h_k p_{k,m}}{N_0} \right) \right\}. \quad (3.7)$$

Note that the throughput given in (3.5) takes into account the activity statistics of the PUs, and the imperfection of spectrum sensing (e.g., false alarm, miss detection, sensing time). Basically, it gives a measure of the actual throughput the SU can achieve on average.

Different from the single-channel setup [59], in our multiple-channel formulation, we are not only interested in identifying the optimal sensing time duration, but also designing the optimal power allocation strategies for each channel k in each scenario

m . Therefore, the SU is also subject to the total transmit power constraint on top of the probability of detection constraints. In the following sections, we will study the above problem under two different power constraints, namely, average transmit power constraint and peak transmit power constraint.

3.2 Optimization under the Average Transmit Power Constraint

In this section, we study the optimization problem formulated in Section 3.1 under the additional average transmit power constraint, which can be expressed mathematically as

$$\sum_{m=1}^M \mathcal{P}_{s,m}(\tau) \sum_{k \in \Phi_m} \mathbb{E}\{p_{k,m}\} \leq \bar{P}_{avg}, \quad (3.8)$$

where $\bar{P}_{avg}$ is the prescribed average power limit. The average power is usually imposed to maintain the long-term power budget [133].

For any given sensing time τ , it is easy to verify the convexity of the problem in $p_{k,m}$. Then, we can have the Lagrangian corresponding to this optimization problem as

$$\mathcal{L} = \sum_{m=1}^M \mathcal{P}_{s,m}(\tau) \sum_{k \in \Phi_m} \mathbb{E} \left\{ \frac{T-\tau}{T} \log_2 \left(1 + \frac{h_k p_{k,m}}{N_0} \right) - \lambda p_{k,m} \right\} + \lambda \bar{P}_{avg}, \quad (3.9)$$

where $\lambda \geq 0$ is the Lagrange multiplier.

We take the partial derivative with respect to $p_{k,m}$ and obtain

$$\frac{\partial \mathcal{L}}{\partial p_{k,m}} = \mathcal{P}_{s,m}(\tau) \left(\frac{T-\tau}{T \ln 2} \frac{1}{\frac{N_0}{h_k} + p_{k,m}} - \lambda \right) \mathbf{p}_{\mathbf{h}_m}(\mathbf{h}_m) = 0, \quad (3.10)$$

for $k \in \Phi_m$, where $\mathbf{h}_m = \{h_k\}_{k \in \Phi_m}$ and $\mathbf{p}_{\mathbf{h}_m}(\mathbf{h}_m)$ is the joint PDF of $\mathbf{h}_m = \{h_k\}_{k \in \Phi_m}$.

The optimal power allocation can then be found to be a water-filling solution given by

$$p_{k,m} = \left(\frac{T - \tau}{T\lambda \ln 2} - \frac{N_0}{h_k} \right)^+ = \left(\mu - \frac{N_0}{h_k} \right)^+, \quad (3.11)$$

where $(x)^+ = \max(x, 0)$, and $\mu \geq 0$ is the water level. Note that a common water level is used for all the possible access scenarios. Hence, once the water level has been determined, the optimal power allocation strategy for a given active secondary channel k is independent of the activities of the other channels. Equivalently, the allocation remains the same in different scenarios. Hence, we can simplify the notation of $p_{k,m}$ to p_k . The optimal water level can be found when the equality holds for (3.8). The numerical method to obtain it will be given in the sequel.

Proposition 3.1. With the power allocation given in (3.11), the problem in Section 3.1 under the constraint (3.8) is equivalent to the following problem

$$\max_{\tau, \{p_k\}} \sum_{k=1}^K \frac{T - \tau}{T} \mathcal{P}_{a,k}(\tau) \mathbb{E} \left\{ \log_2 \left(1 + \frac{h_k p_k}{N_0} \right) \right\} \quad (3.12)$$

$$\text{s.t.} \quad \sum_{k=1}^K \mathcal{P}_{a,k}(\tau) \mathbb{E}\{p_k\} = \bar{P}_{avg} \quad (3.13)$$

$$\mathcal{P}_{d,k} = \bar{\mathcal{P}}_{d,k}, \quad k = 1, \dots, K. \quad (3.14)$$

Proof. See Appendix A □

Generally, it is not easy to develop a simple algorithm to identify the optimal strategies for $(\tau, \{p_k\})$ due to the complex form of the objective function and the constraint set. However, the problem is still tractable since the optimal sensing time τ can only lie within the interval $(0, T)$, which enables us to solve for the optimal τ by a one-dimensional exhaustive search. Furthermore, for any given τ , we can find the optimal $\{p_k\}$ by solving for the single variable μ as seen from (3.13).

In the following, we will develop the algorithm to find the feasible value of the water

level μ for a given sensing time τ . Denote $\mathcal{F}(\tau, \mu) = \sum_{k=1}^K \mathcal{P}_{a,k}(\tau) \mathbb{E}\{p_k\} - \bar{P}_{avg}$, we have

$$\mathcal{F}(\tau, \mu) = \sum_{k=1}^K \mathcal{P}_{a,k}(\tau) \int_{\frac{N_0}{\mu}}^{+\infty} \left(\mu - \frac{N_0}{h_k} \right) \mathbf{p}_{h_k}(h_k) dg_k - \bar{P}_{avg}, \quad (3.15)$$

where $\mathbf{p}_{h_k}(h_k)$ is the PDF of the channel gain h_k .

Then, by taking the first and second partial derivatives of $\mathcal{F}(\tau, \mu)$ w.r.t. μ , we obtain

$$\mathcal{F}'(\tau, \mu) = \sum_{k=1}^K \mathcal{P}_{a,k}(\tau) \int_{\frac{N_0}{\mu}}^{+\infty} \mathbf{p}_{h_k}(h_k) dg_k > 0, \quad (3.16)$$

and

$$\mathcal{F}''(\tau, \mu) = \sum_{k=1}^K \mathcal{P}_{a,k}(\tau) \frac{N_0}{\mu^2} \mathbf{p}_{h_k} \left(\frac{N_0}{\mu} \right) > 0. \quad (3.17)$$

From (3.16) and (3.17), we can see that $\mathcal{F}(\tau, \mu)$ is a monotonically increasing and convex function of μ . Moreover,

$$\lim_{\mu \rightarrow 0^+} \mathcal{F}(\tau, \mu) = -\bar{P}_{avg} < 0. \quad (3.18)$$

Therefore, we can conclude that there is a unique $\mu^* \geq 0$ satisfying $\mathcal{F}(\tau, \mu^*) = 0$ for a given τ . To solve for the root μ^* of $\mathcal{F}(\tau, \mu^*) = 0$ for a given τ , Newton's method as shown in Algorithm 1 below can be employed, which guarantees the convergence when a function is convex and increasing and the starting point is chosen as $\mu^{(0)} > \mu^*$ [186]. It is noted that when $\mu^{(0)} < \mu^*$ is chosen, it can be verified that $\mu^{(1)} > \mu^*$ by the first-order convexity of $\mathcal{F}(\tau, \mu)$ and the algorithm starts to converge from the second iteration. Finally, the optimal sensing time can then be found by exhaustive search over $(0, T)$.

Algorithm 1 Algorithm for finding the optimal μ for a given τ

- 1) Initialization: $j \leftarrow 0; \mu^{(j)}$;
 - 2) Repeat
 - a) $j \leftarrow j + 1$;
 - b) Calculate $\mu^{(j)} = \mu^{(j-1)} - \frac{\mathcal{F}(\tau, \mu^{(j-1)})}{\mathcal{F}'(\tau, \mu^{(j-1)})}$;
 - 3) Until $|\mathcal{F}(\tau, \mu^{(j)})| \leq \bar{\varepsilon}$;
- where $\bar{\varepsilon}$ is a predefined small constant number.
-

3.3 Optimization under the Peak Transmit Power Constraint

In this section, we study the problem formulated in Section 3.1 under the additional peak transmit power constraint. The peak power constraint is imposed usually due to the nonlinearity of practical power amplifiers [133]. Therefore, the total transmit power cannot exceed a prescribed peak power limit in any access scenario. Mathematically, the constraints can be expressed as

$$\sum_{k \in \Phi_m} p_{k,m} \leq \bar{P}_{pk}, \quad m = 1, \dots, M, \quad (3.19)$$

where $\bar{P}_{pk}$ is the peak power limit. Note that this power constraint is more strict than the average power constraint in (3.8) since it requires that the total transmit power to be below the prescribed level in each access scenario.

Unlike the average power constraint given in (3.8) where the transmit power and the sensing time are coupled, (3.19) only depends on the transmit power. This allows us to optimize the transmit power and the sensing time separately. Therefore, the problem can be solved by optimizing over the transmit power first and then over the sensing time.

Firstly, notice that the transmit power is constrained for each scenario m indepen-

dently and hence we have the following subproblem for each scenario m :

$$\max_{\{p_{k,m}\}_{k \in \Phi_m}} C_m = \sum_{k \in \Phi_m} \mathbb{E} \left\{ \log_2 \left(1 + \frac{h_k p_{k,m}}{N_0} \right) \right\}, \quad (3.20)$$

$$\text{s.t.} \quad \sum_{k \in \Phi_m} p_{k,m} \leq \bar{P}_{pk}. \quad (3.21)$$

The optimal power allocated to channel k in scenario m follows the well-known water-filling form

$$p_{k,m} = \left(\mu_m - \frac{N_0}{h_k} \right)^+, \quad (3.22)$$

where μ_m is the water level for scenario m and it can be found by

$$\sum_{k \in \Phi_m} \left(\mu_m - \frac{N_0}{h_k} \right)^+ = \bar{P}_{pk}. \quad (3.23)$$

Note that, unlike the previous section where we have a common water level in spite of different access scenarios, in this section, the optimal water level has to be varied according to the number of active channels and the joint channel condition of the active secondary links. Therefore, the SU will have to vary their power allocation strategies according to the number of active channels in the network. Specifically, the SU transmitter has to be informed of the results of all the narrowband energy detection before allocating the power to each individual channel.

With the optimal power allocation, we can find C_m for scenario m . Then the optimal sensing time can be obtained by solving the following subproblem:

$$\max_{\tau} \quad \sum_{m=1}^M \frac{T-\tau}{T} \mathcal{P}_{s,m}(\tau) C_m \quad (3.24)$$

$$\text{s.t.} \quad \mathcal{P}_{d,k} = \bar{\mathcal{P}}_{d,k}, \quad k = 1, \dots, K. \quad (3.25)$$

In general, $\frac{T-\tau}{T} \mathcal{P}_{s,m}(\tau)$ may not be a concave function of τ . Hence, we have to exhaus-

tively search for the optimal sensing time over $(0, T)$.

3.4 Numerical Results and Discussions

In this section, numerical results for the sensing-access design for parallel channel sensing will be presented. We use a fixed frame of $T = 100$ ms for the secondary network and the target probability of detection is set to $\bar{\mathcal{P}}_{d,k} = 0.9$ for all the channels. The probability that the primary user is present is assumed to be $\theta_k = 0.8$ on each channel. The noise power levels at all secondary receive antennas are set to $N_0 = 1$. The bandwidth for each narrowband channel and the equivalent narrowband channel sampling frequency are fixed at 6 MHz. $K = 3$ such narrowband channels are considered whose worst-case SNRs of the primary users' signals received at the secondary detectors are -12 dB, -15 dB and -20 dB, respectively. It is further assumed that the secondary channels are block faded and the channel power gains are ergodic, stationary and exponentially distributed with unit mean. The basic Matlab code for the simulation can be found in Appendix H.

The aggregate average achievable throughputs versus the sensing time under average or peak power constraints with different transmit power levels are shown in Fig. 3.3. The curves are obtained by calculating the throughput numerically for a series of given sensing time within the interval $(0, T)$. Under both the average and peak power constraints, it is seen from the figure that the throughputs are concave functions of the sensing time. A unique optimal sensing time can be found to achieve the maximum throughput in each case. Moreover, the achievable throughputs under the peak power constraints are always slightly lower than those under the average power constraints. This is because the average power constraint is generally a looser constraint which allows the transmitter to allocate more power than the peak power constraint under favorable channel conditions.

Since the sensing time is a fixed parameter for the CRN, it can be computed offline.

Figure 3.3: The average achievable throughput vs. sensing time under average or peak power constraints with different transmit power levels.

Instead of using exhaustive search to identify the optimal sensing time, we can use a more efficient bisection search method if the throughput can be visually observed to be a unimodal function of the sensing time. In this case, as seen from the concavity of the curves in Fig. 3.3, efficient bisection search can be used. The optimal sensing time versus the total transmit power under the two different power constraints is depicted in Fig. 3.4. We can observe that the optimal sensing time increases with the increasing total transmit power for both cases. It is thus implied from the figure that the SU will have to change its sensing time for different total transmit power. However, for practical implementation, it is better to fix the sensing time for a good protocol design. As observed from Fig. 3.3, the achievable throughputs only vary slightly around the peak values, especially for the lower total transmit power cases. The sensing time can therefore be chosen at a value that is more favorable to higher transmit power situation. In particular, if we choose the optimal sensing time at 20 dB of total transmit power as the sensing time, the resultant throughput losses are listed in Table 3.1. It can be

seen that the losses are insignificant for the choices of other total transmit power.

Figure 3.4: The optimal sensing time vs. the total transmit power under average or peak power constraints.

Table 3.1: Throughput Loss

Total transmit power	5 dB	10 dB	15 dB
peak power constraint	0.22%	0.09%	0.02%
Average power constraint	0.4%	0.15%	0.03 %

3.5 Conclusions

In this chapter, we have studied the sensing-access design that determines the sensing time and power allocation for parallel channel sensing to maximize the average achievable throughput of the multiple-channel CRN subject to the constraint that all PUs can be correctly detected most of the time. We have investigated the problem under both the average and peak sum transmit power constraints. In particular, it has been shown that under the average transmit power constraint, once the water level has been fixed, the amount of transmit power that can be allocated to a channel only depends

on its own channel availability and fading channel information; while under the peak transmit power constraint, the allocation also depends on the availability and channel conditions of the other channels. Numerical results show that, under both cases, for a CR network with three 6MHz channels, if the frame duration is 100ms and the target probability of detection is 90% for the worst-case SNR of PUs being -12dB , -15dB and -20dB , respectively, the optimal sensing time is around 6ms and it is almost insensitive to the total transmit power.

Chapter 4

Sensing-Access Design in OSA: Sequential Channel Sensing

In this chapter, we are interested to study the sensing-access design for the case of sequential channel sensing. However, unlike Chapter 3 and majority of the current research which have focused on improving the throughput of CRNs, we will focus on the energy-efficient transmission instead. Such transmission that takes into account the energy consumption is very important to battery-powered devices since they are energy limited. As an initial attempt to address the energy-efficient transmission, specifically in a CRN employing sequential channel sensing, we use energy efficiency⁶ as the performance metric. Energy efficiency is defined as the number of bits transmitted per unit of energy consumption. Both sensing and transmission consume energy. For a given level of transmit power, sensing more channels can help explore the diversity among different channels, and possibly find an idle channel with higher transmission rate. However, this increases the overall energy consumption and may also reduce the amount of time left for transmission in the case that the total sensing and transmission time is fixed. There are multiple tradeoffs involved in the design. Besides, since the

⁶For the energy-efficient design in the non-CR setup, please refer to [187] [188] and the references therein.

amount of transmit power used will affect both the throughput and energy consumption, adaptive power allocation is also important to achieve higher energy efficiency. Furthermore, the PU's activity and the SU's channel fading (large-scale and small-scale) statistics may not be identical among different channels. The order of channel sensing affects how quickly a spectrum opportunity can be identified and hence affects the total energy expenditure.

The objective of this chapter is to design the sensing-access strategies together with the sensing order to maximize the energy efficiency of the sequential channel sensing process. The sensing strategy determines when to stop sensing and start transmission. The access strategy specifies the transmit power level upon transmission. The sensing order design tells the SU which channel to sense next if the current channel is given up for transmission.

The contributions of the chapter can be summarized as follows. Firstly, we formulate the above design problem under the framework of finite-horizon stochastic sequential decision-making problem [61]. This formulation allows us to integrate the adaptive power allocation design, the sensing strategy design and sensing order design and also to take into account the imperfection of spectrum sensing. Secondly, to identify the optimal energy-efficient sensing-access strategies, we investigate a parametric formulation of the above problem, which can be interpreted as an energy-aware design. This formulation treats throughput as rewards and imposes explicit cost for energy consumption. The resulting problem has an additive and separable structure which allows DP to be applied to find the corresponding optimal strategy. Then, by exploring the relationship between these two designs and making use of the monotonicity structure of the energy-aware design, an algorithm is developed to identify the optimal sensing-access strategies for the energy-efficient design. Furthermore, it is found that the optimal sensing strategy has a threshold structure, which indicates that the SU should stop sensing and start transmission if the current channel condition is good enough. The

optimal access strategy which specifies the transmit power level upon transmission has a water-filling structure with the water level determined by the long-term energy efficiency and the perceived spectrum opportunity of the transmission channel. The optimal sensing order will choose the channel to be sensed as the one with maximum expected future net reward among the set of remaining channels.

Some of the related works are reviewed and the differences between them and our work are highlighted. Two groups of literature are most relevant. Firstly, as reviewed in Chapter 2, the design of sensing-access strategies with sequential channel sensing has been studied in [102–104, 106] etc. However, all of them focused on maximizing the transmission throughput. In this case, maximum transmit power is always preferred and no design of power allocation is needed. When energy efficiency is of concern, power allocation affects the design through both the throughput and the energy consumption. Hence, maximum transmit power may not be optimal from the perspective of energy efficiency. There is a need to incorporate power allocation design in the study of energy efficiency. To incorporate the adaptive power allocation into the energy-efficient sensing-access design, we formulate our problem in the framework of general finite-horizon stochastic decision-making problem, instead of the standard optimal stopping framework used in [102–104, 106]. This approach gives us more freedom in analyzing the problem and more insights into the structure of the proposed strategies. Secondly, cognitive transmissions considering energy consumption have been studied in [112, 113, 189, 190], under the model of periodic sensing where spectrum sensing is performed only once in each frame. In [112] and [113], the authors considered the Markovian PU occupancy across different frames and studied the sensing-access strategies for the selective parallel channel sensing under the POMDP. The objective is to maximize the throughput within a finite energy budget in [112] and to maximize a utility-based objective function which penalizes energy consumption in [113]. The absolute energy efficiency is not of their concern and the transmit power/energy levels

are based on some predefined values. The energy efficiency of CR has been studied in [190] and [189] with the assumption that the primary occupancy status is independent across different frames. In [190], the authors focused on parallel channel sensing where spectrum sensing was considered perfect. In [189], the authors considered a single channel scenario, which can be considered as a special case of our work. Since the strategy in each frame can be designed independently, the resultant design reduces to simply a static optimization of the transmit power. In contrast, when we consider sequential channel sensing, a sequence of decisions is made in each sensing and transmission process. The design problem becomes a finite-horizon stochastic sequential decision-making problem, which is mathematically much more involved.

The remainder of the chapter is organized as follows. In Section 4.1, we introduce the system model of interest. We formulate the design of the energy-efficient sensing-access strategies for a given sensing order as a sequential decision-making problem in Section 4.2. The corresponding optimal design strategy is identified in Section 4.3. In Section 4.4, we further investigate the design that incorporates the optimal sensing order. We evaluate our proposed design for a given sensing order and optimal sensing order through numerical results in Section 4.5. Finally, Section 4.6 concludes the chapter.

4.1 System Model

4.1.1 Network Description

Similar to Chapter 3, we consider a CRN which can access a set of K licensed frequency channels of equal bandwidth B . The set of channels is indexed by $\{1, 2, \dots, K\}$. The probability that the PU is idle on channel k is denoted as θ_k . Same as Chapter 3, we concentrate on a single pair of SU-Tx and SU-Rx, which is an abstraction of the multi-user scenario where a single pair of SUs is granted exclusive right to perform

sequential channel sense and access either through centralized control or contention on a common control channel.

Due to the hardware limitation, the SU can only sense one channel at a time. Hence, sequential channel sensing is employed. An example of it is shown in Fig. 4.1 and is described as follows: The SU starts with one channel. If it is sensed busy, the SU continues to sense the other channels sequentially until it finds an idle one. If the channel is idle, the SU performs channel estimation to determine the channel gain and makes a decision on whether to select a power level to transmit over this channel or to continue to sense the other channels until it decides to transmit. It is assumed that the SU-Tx and the SU-Rx are always synchronized through a dedicated control channel so that they always tune to the same channel for sensing, channel estimation and possibly transmission/reception at the same time.

Figure 4.1: Illustration of the sequential channel sensing process with the sensing order given as $\{1, 2, \dots, K\}$.

Similar to Chapter 3, we denote τ as the sensing time and consider the channel estimation time to be negligible. We further denote T_k as the transmission time if the SU decides to transmit after sensing k channels. We consider two scenarios: constant transmission time and constant frame time. The constant transmission time case represents the scenario when the transmission always takes a constant duration T regardless of the number of channels that have been sensed, i.e., $T_k = T$, for $k = 1, \dots, K$. The constant frame time case denotes the scenario when each channel acquisition and data transmission process takes a constant duration T . The transmission time in this case

if the SU starts transmitting after sensing k channels is $T_k = T - k\tau$.

Let δ_k denote the PU status of channel k , with $\delta_k = 1$ or 0 indicating that channel k is busy or idle, respectively. Hence, we have $Pr(\delta_k = 0) = \theta_k$. Denote $\hat{\delta}_k$ as the binary decision of spectrum sensing on channel k , with $\hat{\delta}_k = 0$ or 1 representing channel k is idle or busy, respectively. Due to the imperfection of spectrum sensing, the perceived distributions of the PU status on channel k for a given probability of false alarm $\mathcal{P}_{f,k}$ and probability of detection $\mathcal{P}_{d,k}$ are given by

$$Pr(\hat{\delta}_k = 0) = \theta_k(1 - \mathcal{P}_{f,k}) + (1 - \theta_k)(1 - \mathcal{P}_{d,k}) \quad (4.1)$$

and

$$Pr(\hat{\delta}_k = 1) = \theta_k\mathcal{P}_{f,k} + (1 - \theta_k)\mathcal{P}_{d,k}. \quad (4.2)$$

Spectrum sensing is followed by channel estimation if the channel k is detected to be idle as described in Section 3.1. Denote the estimated fading channel gain as h_k . Similarly, it is assumed that the probability distributions of all the channels are known *a priori* through previous long-term channel measurements. Note that unlike the case of parallel channel sensing that the channel gains of all the idle channels can be estimated simultaneously before transmission, channels can only be estimated one-by-one in this case. Hence, channel acquisition at channel k can only reveal the actual channel gain of this channel and the actual channel gain of any channels that are not sensed is unknown at this stage.

4.1.2 Energy Efficiency

In this chapter, we are interested in the energy efficiency, which is defined as

$$\eta = \frac{\text{Average Number of Bits Transmitted}}{\text{Average Energy Consumed}}. \quad (4.3)$$

The SU is allowed to transmit only when a channel is detected to be idle. However, due to the imperfection of spectrum sensing, the channel can be either idle or busy.

Denote the number of bits that can be transmitted over channel k when it is truly idle and truly busy as r_k^0 and r_k^1 , respectively. Obviously, we have $r_k^0 \geq r_k^1$ due to the interference from the PU in the latter case. When channel k is truly idle, the number of bits that can be delivered is given by

$$r_k^0 = T_k B \log_2 (1 + SNR_k / \Gamma) \quad (4.4)$$

where SNR_k represents the received SNR at the SU-Rx, and Γ is considered as the SNR gap to channel capacity. Note that for an uncoded M-QAM, Γ can be approximated as $\Gamma \approx -\frac{\ln(5BER)}{1.5}$ given a bit-error rate, denoted by BER . We denote c as the speed of light, d as the distance between the SU-Tx and the SU-Rx, $f_{c,k}$ as the carrier frequency of channel k , $N_0/2$ as the power spectral density of the noise, N_f as the receiver noise figure, ι as the link margin compensating the hardware process variation and imperfection. Hence, for a given transmit power P_t , we have

$$SNR_k(h_k, P_t) = \frac{\rho_k h_k P_t}{\iota \sigma^2} \quad (4.5)$$

where $\rho_k = \left(\frac{c}{4\pi d f_{c,k}} \right)^2$ captures the propagation loss, and $\sigma^2 = N_0 B N_f$ is the noise power at the receiver front end.

Spectrum sensing, channel estimation and data transmission all consume energy. We denote the sensing power as P_s . The energy consumed for sensing a single channel is then given by τP_s . Since channel estimation takes a very short time and finite power, we assume that the energy consumed in channel estimation is insignificant as compared to the sensing energy and hence is ignored in our analysis. Note that our design can easily incorporate the case when channel estimation consumes relatively high energy. In the data transmission phase, the total power consumed can be expressed as [187]

$$P_{tx} = \frac{\xi}{\zeta} P_t + P_c \quad (4.6)$$

where ξ is the peak-to-average ratio (PAR) of the power amplifier (PA), ζ is the drain efficiency of the PA, P_t is the transmit power, and P_c is the power consumed in various transmit and receive electronic circuit excluding the PA power. The transmit power P_t affects the rate of a transmission and hence the energy efficiency. It is a parameter to be designed in our study. The circuit power P_c is independent of transmission rate and can be considered as a constant.

The overall objective of this chapter is to jointly design the sensing-access strategies and the sensing order to maximize the energy efficiency. The sensing strategy specifies when to stop sensing and carry out transmission. The access strategy specifies the amount of transmit power used upon transmission. The sensing order specifies in which sequence the channels are sensed. For the ease of presentation, we first present the design of sensing-access strategies for a given sensing order in Section 4.2 and Section 4.3. For simplicity, we assume that the channels are sensed according to the logical channel index from 1 to K . Then, we will extend the design to take into account the sensing order in Section 4.4.

4.2 Problem Formulation

In this section, we formulate the above design problem as a K -stage stochastic sequential decision-making problem [61]. In the general settings, such a problem models the situation when a decision-maker has to make a decision at each stage after observing the current system state. Each decision made will gain certain reward and lead the system into a new state, which may not be determined at the time of decision. The process evolves until the last stage. The objective is to maximize the overall reward incurred over all stages. The sequential channel sensing process is a special case of the general sequential decision-making problem which allows problem to be terminated before the last stage. In the followings, we briefly describe the basic components in the analysis of such a problem.

System State: The system state is characterized by the joint knowledge of the PU channel status and the SU channel condition (δ_k, h_k) . Since spectrum sensing is imperfect, we only have an observation $\hat{\delta}_k$ about the true PU channel status δ_k after sensing channel k . Instead we will treat $s_k = (\hat{\delta}_k, h_k)$ as the system state⁷. Since we will not carry out channel estimation when channel k is detected as busy, i.e., $\hat{\delta}_k = 1$, we will assume $h_k = 0$ in this case. We introduce an additional state $s_k = \mathcal{T}$ to denote that the process has been terminated, that is, sequential channel sensing has stopped.

Decision: At each stage k , after observing the system state s_k , a decision u_k has to be made. To protect the PUs, transmission is not allowed when channel k is sensed busy. Hence, the only decision when $s_k = (1, 0)$ is $u_k = \mathcal{C}$, where $\mathcal{C}$ denotes continuing to sense the next channel. However, when channel k is sensed idle, the SU has to decide whether to give up the current channel and continue to sense the next channel, i.e., $u_k = \mathcal{C}$, or to choose a transmit power level P_t and terminate the process, i.e., $u_k = P_t \in [P_{min}, P_{max}]$. Here P_{min} is a predefined small positive value and P_{max} is the maximum transmit power allowed due to the hardware limitation or some other regulations. Note that once transmission starts, i.e., $u_k = P_t$, the system enters the termination state and remains in it, i.e., $s_{k+1} = \dots = s_K = \mathcal{T}$. At the last stage, since all the channels have been sensed, the decision $u_K = \mathcal{C}$ is not available.

Cost Functions: Since energy efficiency is related to both the throughput and the energy consumption, we define two cost functions at each stage. The first one is the throughput. When $s_k \neq \mathcal{T}$, $\hat{\delta}_k = 0$, $u_k = P_t$, the throughput of channel k is given by

$$g_k^R(s_k, u_k) = \mathbb{E}_{\delta_k|\hat{\delta}_k}[r_k] = \omega_k r_k^0 + (1 - \omega_k) r_k^1 \approx \omega_k r_k^0 \quad (4.7)$$

⁷When the state δ_k cannot be observed perfectly, the problem becomes a sequential decision-making problem with imperfect state information. According to [61], the conditional probability $Pr(\delta_k|\hat{\delta}_1, \dots, \hat{\delta}_k)$ can serve as a sufficient statistic for decision making. Due to the independence of the PUs' status on each channel, this sufficient statistic depends only on the current observation $\hat{\delta}_k$. Hence, it is equivalent to treat $\hat{\delta}_k$ as the sufficient statistic and hence as the system state together with h_k .

where $\omega_k = \frac{\theta_k(1-\mathcal{P}_{f,k})}{\theta_k(1-\mathcal{P}_{f,k})+(1-\theta_k)(1-\mathcal{P}_{d,k})}$ is the *posterior* probability of $\delta_k = 0$ given $\hat{\delta}_k = 0$; and $g_k^R(s_k, u_k) = 0$, otherwise. The approximation is due to the fact that $\bar{\mathcal{P}}_d^k \approx 1$ and $r_k^0 \geq r_k^1$ [59]. The second cost function is energy consumption. The energy consumed at stage k can be written as

$$g_k^E(s_k, u_k) = \begin{cases} 0, & \text{if } s_k = \mathcal{T}, \\ \tau P_s + T_k(\alpha P_t + P_c), & \text{if } s_k \neq \mathcal{T} \text{ and } u_k = P_t, \\ \tau P_s, & \text{otherwise,} \end{cases} \quad (4.8)$$

where $\alpha = \xi/\zeta$.

The objective of our design is to find a sequence of functions $\mu_k, k = 1, 2, \dots, K$, mapping each state s_k into a control $u_k = \mu_k(s_k)$, to maximize the energy efficiency of the whole process, which is defined as

$$\eta = \frac{\mathbb{E} \left\{ \sum_{k=1}^K g_k^R(s_k, \mu_k(s_k)) \right\}}{\mathbb{E} \left\{ \sum_{k=1}^K g_k^E(s_k, \mu_k(s_k)) \right\}} \quad (4.9)$$

where the expectation is taken over $s_k, k = 1, \dots, K$.

The sequence of functions $\phi = \{\mu_1(s_1), \dots, \mu_K(s_K)\}$ is referred to as a policy, which is the sensing-access strategies that specify when to stop sensing and the corresponding transmit power level used for transmission. Denoting the energy efficiency achieved using policy ϕ as η_ϕ , an optimal policy ϕ^* is then given by $\phi^* = \underset{\phi}{\operatorname{argmax}} \eta_\phi$.

Remark. Note that when there is only one channel, i.e., $K = 1$, the system becomes the one for periodic sensing, which is the problem studied in [189]. The design of the sensing-access strategies is reduced to designing the transmit power only. Mathematically, the problem becomes

$$\max_{P_t(h_1)} \frac{\theta_1(1 - \mathcal{P}_{f,1})T_1 B \mathbb{E} \left\{ \log_2 \left(1 + \frac{1}{\Gamma} SNR_1(h_1, P_t(h_1)) \right) \right\}}{\tau P_s + (\theta_1(1 - \mathcal{P}_{f,1}) + (1 - \theta_1)(1 - \bar{\mathcal{P}}_{d,1})) T_1 (\alpha \mathbb{E}\{P_t(h_1)\} + P_c)} \quad (4.10)$$

where the expectation is taken w.r.t. h_1 .

4.3 Optimal Sensing-Access Strategies

The problem formulated in Section 4.2 cannot be solved directly. Instead, we first study a parametric formulation of this problem, which allows us to derive a simple solution. Then, we will explore the relationship between the two problems and present the solution for the main problem of interest.

4.3.1 Parametric Problem

Sequential decision-making problem with an additive cost function as the objective can be usually solved through DP [61]. However, the problem formulated above is the ratio of two additive cost functions, which makes DP more difficult to be applied directly. Since fractional programming (FP) deals with problems of optimizing ratio-type functions, it is suggested in [191] to make use of the solution techniques of FP to transform the sequential decision making problem of ratio-type objective function into a parametric formulation so that DP can be readily applied. Specifically, we form a new sequential decision-making problem with the states and decisions defined same as the one in Section 4.2. However, the cost function at stage k , $k = 1, \dots, K$, is defined as follows:

$$\begin{aligned} G_k(s_k, u_k; \lambda) &= g_k^R(s_k, u_k) - \lambda g_k^E(s_k, u_k) \\ &= \begin{cases} 0, & \text{if } s_k = \mathcal{T}, \\ \mathcal{F}_k(h_k, P_t, \lambda) - \lambda \tau P_s, & \text{if } s_k \neq \mathcal{T} \text{ and } u_k = P_t, \\ -\lambda \tau P_s, & \text{otherwise,} \end{cases} \end{aligned} \quad (4.11)$$

where $\lambda \geq 0$ is a parameter whose value is assumed to be known for the time being, and

$$\mathcal{F}_k(h, p, \lambda) = \omega_k T_k B \log_2(1 + \text{SNR}_k(h, p)/\Gamma) - \lambda T_k(\alpha p + P_c). \quad (4.12)$$

For a given value of λ , the objective of the new problem is to find a sequence of functions, $\phi(\lambda) = \{\mu_1(s_1; \lambda), \dots, \mu_K(s_K; \lambda)\}$, mapping each (s_k, λ) into a control $u_k =$

$\mu_k(s_k; \lambda)$, such that the following objective function is maximized:

$$J_{\phi(\lambda)}(\lambda) = \mathbb{E} \left\{ \sum_{k=1}^K G_k(s_k, \mu_k(s_k, \lambda); \lambda) \right\}. \quad (4.13)$$

In the sequel, we denote the problem parameterized by λ as *Problem* $\mathbb{P}(\lambda)$. *Problem* $\mathbb{P}(\lambda)$ can be interpreted as an energy-aware version of the sensing-access design. The physical meaning of it can be seen as follows. If we treat the throughput $g_k^R(s_k, u_k)$ as the monetary reward of the process, then the parameter λ can be treated as the price for per unit of energy consumption. As a result, (4.13) can be interpreted as the expected net reward of the whole process, which is similar to the utility function which is used to study the energy-aware design for the multiuser cooperative and noncooperative power control games in [192] and [193], and the sensing-access strategies in the periodic sensing [113]. Clearly, when we impose different prices for energy consumption, we may result in different optimal policies and different values of maximum net reward. Hence, depending on the value of λ , we have many different parametric problems.

4.3.2 (Dynamic Programming) DP for the Parametric Problem

By adopting the parametric formulation, we have an additive and separable objective function, which enables DP to be applied. For a given λ , we denote the expected net reward for a process of $K - k + 1$ stages, starting from state s_k , as $J_k(s_k; \lambda)$. Next, we will present the basic idea of DP.

We start from the last stage. If we observe the system state as s_K ($s_K \neq \mathcal{T}$), then the maximum net reward can be calculated as

$$J_K(s_K; \lambda) = \max_{u_K} G_K(s_K, u_K; \lambda) = \begin{cases} -\lambda\tau P_s, & \text{if } s_K = (1, 0), \\ -\lambda\tau P_s + \mathcal{F}_K^*(h_K, \lambda), & \text{otherwise,} \end{cases} \quad (4.14)$$

where $\mathcal{F}_k^*(h, \lambda) = \max_{u \in [P_{min}, P_{max}]} \mathcal{F}_k(h, u, \lambda)$, and it can be solved using the method of

Lagrange multipliers.

Hence, the optimal strategy when the channel is sensed idle, i.e., $\hat{\delta}_K = 0$, and the channel is estimated to be h_K , is

$$\mu_K(s_K; \lambda) = \operatorname{argmax}_{u_K \in [P_{min}, P_{max}]} \mathcal{F}_K(h_K, u_K, \lambda) = \left[\frac{\omega_K B}{\lambda \alpha \ln(2)} - \frac{\iota \Gamma \sigma^2}{\rho_K h_K} \right]_{P_{min}}^{P_{max}}, \quad (4.15)$$

where $[\cdot]_a^b = \max(a, \min(\cdot, b))$. $\mathbb{E}\{J_K(s_K; \lambda)\}$ can be computed by taking the expectation of (4.14) w.r.t. s_K . Note that for a given λ , $\mathbb{E}\{J_K(s_K; \lambda)\}$ is a constant once it is computed.

Following that, the expected net reward for the $(K - k + 1)$ -stage problem starting from state s_k can be calculated using backward induction from $k = K - 1$ to $k = 1$. Specifically, for $k = 1, \dots, K - 1$, we have

$$J_k(s_k; \lambda) = \max_{u_k} G_k(s_k, u_k; \lambda) + \mathbb{E}\{J_{k+1}(s_{k+1}; \lambda)\}. \quad (4.16)$$

When channel k is sensed busy, i.e., $s_k = (1, 0)$, we have

$$J_k(s_k; \lambda) = -\lambda \tau P_s + \mathbb{E}\{J_{k+1}(s_{k+1}; \lambda)\} \quad (4.17)$$

and when channel k is sensed idle, i.e., $s_k = (0, h_k)$, we have

$$J_k(s_k; \lambda) = -\lambda \tau P_s + \max \{ \mathcal{F}_k^*(h_k, \lambda), \mathbb{E}\{J_{k+1}(s_{k+1}; \lambda)\} \}. \quad (4.18)$$

The optimal strategy after observing channel k is idle, i.e., $s_k \neq (1, 0)$, is given by

$$\mu_k(s_k; \lambda) = \begin{cases} \left[\frac{\omega_k B}{\lambda \alpha \ln(2)} - \frac{\iota \Gamma \sigma^2}{\rho_k h_k} \right]_{P_{min}}^{P_{max}}, & \text{if } \mathcal{F}_k^*(h_k, \lambda) \geq \mathbb{E}\{J_{k+1}(s_{k+1}; \lambda)\}, \\ \mathcal{C}, & \text{otherwise,} \end{cases} \quad (4.19)$$

for $k = 1, \dots, K - 1$. Note that the condition

$$\mathcal{F}_k^*(h_k, \lambda) \geq \mathbb{E}\{J_{k+1}(s_{k+1}; \lambda)\} \quad (4.20)$$

specifies the optimal sensing strategy of *Problem* $\mathbb{P}(\lambda)$ at stage k , i.e., when the SU should stop sensing and start transmission. The function $\mathcal{F}_k^*(h_k, \lambda)$ can be considered as the maximum immediate net reward associated with transmitting over channel k . In (4.20), we compare the maximum immediate net reward with the expected future net reward if channel k is given up. Since it can be shown that the function $\mathcal{F}_k^*(h_k, \lambda)$ is a nondecreasing function of h_k , (4.20) is equivalent to $h_k \geq \bar{h}_k$, where $\bar{h}_k$ is the minimum of h_k satisfying (4.20). Therefore, the optimal sensing strategy has a threshold structure. It indicates that we will transmit over an idle channel only when the channel condition is good enough. Otherwise we will continue to sense the next channel. The corresponding decision when (4.20) is satisfied indicates the amount of transmit power used upon transmission. We note that the optimal power allocation strategy has a water-filling structure. The water level is determined by the price for energy consumption λ and the perceived spectrum opportunity of channel k . Hence, when energy consumption is priced heavier, the SU will be restrained from transmitting with higher power; and when the perceived spectrum opportunity is larger, the SU will be willing to inject more power.

The procedure can be repeated backwards from $k = K - 1$ to 1. Denote the maximum net reward for the problem parameterized by λ as $J_{\phi^*(\lambda)}(\lambda)$, i.e., $J_{\phi^*(\lambda)}(\lambda) = \max_{\phi(\lambda)} J_{\phi(\lambda)}(\lambda)$. Then, we have $J_{\phi^*(\lambda)}(\lambda) = \mathbb{E}\{J_1(s_1; \lambda)\}$.

4.3.3 The Optimal Sensing-Access Strategies

The relationship between the original problem and the parametric problem is established as follows.

Proposition 4.1. Denote the optimal policy of the original problem as

$$\phi^* = \{\mu_1^*(s_1), \dots, \mu_K^*(s_K)\}. \quad (4.21)$$

Then, we have $\eta_{\phi^*} = \lambda^*$ if and only if $J_{\phi^*}(\lambda^*) = 0$.

Proof. When $s_1 \neq \mathcal{T}$, we have $g_1^E(s_1, u_1) > 0$, and $g_k^E(s_k, u_k) \geq 0$, for $k = 2, \dots, K$.

Thus, we have $\mathbb{E}\{\sum_{k=1}^K g_k^E(s_k, \mu_k(s_k))\} > 0$.

When $\eta_{\phi^*} = \lambda^*$, we can obtain $\eta_{\phi} = \frac{\mathbb{E}\{\sum_{k=1}^K g_k^R(s_k, \mu_k(s_k))\}}{\mathbb{E}\{\sum_{k=1}^K g_k^E(s_k, \mu_k(s_k))\}} \leq \lambda^*$, and $\eta_{\phi^*} = \frac{\mathbb{E}\{\sum_{k=1}^K g_k^R(s_k, \mu_k^*(s_k))\}}{\mathbb{E}\{\sum_{k=1}^K g_k^E(s_k, \mu_k^*(s_k))\}} = \lambda^*$. Since $\mathbb{E}\{\sum_{k=1}^K g_k^E(s_k, \mu_k(s_k))\} > 0$, we have $J_{\phi}(\lambda^*) = \mathbb{E}\left\{\sum_{k=1}^K G_k(s_k, \mu_k(s_k); \lambda^*)\right\} \leq 0$ and the maximum value $J_{\phi^*}(\lambda^*) = \max J_{\phi}(\lambda^*) = 0$ can be achieved using the policy $\phi^* = \{\mu_1^*(s_1), \dots, \mu_K^*(s_K)\}$.

Conversely, when $J_{\phi^*}(\lambda^*) = 0$, we have $\mathbb{E}\left\{\sum_{k=1}^K G_k(s_k, \mu_k(s_k); \lambda^*)\right\} \leq 0$ and $\mathbb{E}\left\{\sum_{k=1}^K G_k(s_k, \mu_k^*(s_k); \lambda^*)\right\} = 0$. Since $\mathbb{E}\{\sum_{k=1}^K g_k^E(s_k, \mu_k(s_k))\} > 0$, we have $\eta_{\phi} = \frac{\mathbb{E}\{\sum_{k=1}^K g_k^R(s_k, \mu_k(s_k))\}}{\mathbb{E}\{\sum_{k=1}^K g_k^E(s_k, \mu_k(s_k))\}} \leq \lambda^*$. The maximum energy efficiency $\eta_{\phi^*} = \lambda^*$ is achieved with the policy $\phi^* = \{\mu_1^*(s_1), \dots, \mu_K^*(s_K)\}$ $\square$

As pointed out previously, we can have many parametric problems, i.e., energy-aware designs, by setting different values for the price λ . This may lead to different optimal policies and maximum objective values. Proposition 1 tells us that if we can find a problem parameterized by λ^* such that the optimal value of *Problem* $\mathbb{P}(\lambda^*)$ is 0, then the corresponding optimal policy for *Problem* $\mathbb{P}(\lambda^*)$ is also optimal for the original problem. This means that the most energy-efficient design is the energy-aware design of zero expected net reward and the prices for this energy-aware design is the maximum energy-efficiency that can be achieved.

Since for each λ we can solve *Problem* $\mathbb{P}(\lambda^*)$ using DP, this suggests that we can find the optimal policy of the original problem by searching over the possible values of λ . The following proposition reveals the property of the parametric problem such that efficient search algorithm can be applied.

Proposition 4.2. $J_{\phi^*(\lambda)}(\lambda)$ is a monotonously decreasing function of λ .

Proof. We consider two parametric problems with parameters λ_1 and λ_2 , respectively. Denote their corresponding optimal policies as $\phi^*(\lambda_1) = \{\mu_1^*(s_1; \lambda_1), \dots, \mu_K^*(s_K; \lambda_1)\}$ and $\phi^o(\lambda_2) = \{\mu_1^o(s_1; \lambda_2), \dots, \mu_K^o(s_K; \lambda_2)\}$, respectively. Assume that $\lambda_1 < \lambda_2$, we have

$$J_{\phi^o(\lambda_2)} = \mathbb{E} \left\{ \sum_{k=1}^K G_k(s_k, \mu_k^o(s_k, \lambda_2); \lambda_2) \right\} \quad (4.22)$$

$$< \mathbb{E} \left\{ \sum_{k=1}^K G_k(s_k, \mu_k^o(s_k, \lambda_2); \lambda_1) \right\} \quad (4.23)$$

$$\leq \max_{\phi(\lambda_1)} \mathbb{E} \left\{ \sum_{k=1}^K G_k(s_k, \mu_k(s_k, \lambda_1); \lambda_1) \right\} \quad (4.24)$$

$$= \mathbb{E} \left\{ \sum_{k=1}^K G_k(s_k, \mu_k^*(s_k, \lambda_1); \lambda_1) \right\} = J_{\phi^*(\lambda_1)}. \quad (4.25)$$

□

With the monotonicity of $J_{\phi^*(\lambda)}(\lambda)$, we can simply use the following bisection algorithm (Algorithm 2) to search over an interval $[\lambda_{min}, \lambda_{max}]$, which is known to contain λ^* . At each λ within the interval, we solve the parametric problem and check its maximum objective value $J_{\phi^*(\lambda)}$. The algorithm stops when $\lambda_{max} - \lambda_{min} \leq \bar{\varepsilon}$, where $\bar{\varepsilon}$ is a predefined small constant to control the accuracy of convergence. Then, replacing λ in (4.15) and (4.19) with λ^* , we have the optimal sensing-access strategies for the original problem. Note that for the energy-efficient design, the water level of the power allocation strategy is determined by the maximum energy efficiency λ^* instead.

Algorithm 2 Algorithm for finding the optimal λ^*

- 1) **Given:** $\lambda \in [\lambda_{min}, \lambda_{max}]$;
 - 2) **Repeat**
 - a) $\lambda \leftarrow (\lambda_{min} + \lambda_{max})/2$;
 - b) Solve *Problem* $\mathbb{P}(\lambda)$ and calculate $J_{\phi^*(\lambda)}$;
 - c) if $J_{\phi^*(\lambda)} \leq 0$: set $\lambda_{max} \leftarrow \lambda$;
 else: set $\lambda_{min} \leftarrow \lambda$;
 - 3) **Until** $\lambda_{max} - \lambda_{min} \leq \bar{\varepsilon}$;
-

4.4 Joint Design of Sensing Order and Sensing-Access Strategies

In the preceding sections, we have studied the design of the energy-efficient sensing-access strategies assuming that the order of sequential channel sensing has been fixed. However, since the PUs' activities on different channels may be different and the SU's fading and propagation loss across different channels are also different, the order of channel sensing affects how quickly we can identify an available and good channel and hence affects the energy efficiency that can be achieved. In this section, we take into consideration the order of channel sensing. Specifically, our goal is to design the sensing-access strategies that determine in what order sequential channel sensing is performed and when sensing has to stop and how much power is used upon transmission so that energy efficiency is maximized.

4.4.1 Problem Formulation and the Optimal Strategies

The design of the energy-efficient sensing-access strategies that takes into consideration the sensing order can also be formulated as a sequential decision-making problem, which can be described as follows. The SU first selects a channel to start the channel acquisition and transmission process. If the channel is sensed to be busy, the SU has to continue to sense another channel and hence it needs to determine which channel to be sensed next. If the channel is sensed to be idle, the SU has to decide whether to choose a power level and transmit over the channel or to select another channel to sense in the next stage. Since before starting the process, the SU has to make a decision on which channel to sense first, we have an additional decision stage. To be consistent with the notation of the previous analysis, we index the moment when the SU has sensed k channels as stage k , and the moment before starting to sense the first channel as stage 0.

State: We denote the index of the channel sensed at stage k and the set of channels which has not been sensed at stage k as i_k and Ω_k , respectively. Then the state at stage k can be described by the joint variables (s_{i_k}, Ω_k) . Note that we have $\Omega_0 = \{1, \dots, K\}$ and $\Omega_K = \emptyset$, where $\emptyset$ is an empty set. We denote the state at stage 0 as $(\emptyset, \Omega_0)$. Similar to the previous analysis, we denote the state when the process has been terminated as $\mathcal{T}$.

Decision: At stage 0, the SU has to determine a channel to sense. Mathematically, this decision is denoted as $u_0 = j, j \in \Omega_0$. At stage k , the SU observes s_{i_k} . If channel i_k is sensed to be busy, then the SU has to choose another channel for sensing in the next stage, i.e., $u_k = j, j \in \Omega_k$. Otherwise, it has an additional option to transmit over channel i_k , i.e., $u_k = P_t, P_t \in [P_{min}, P_{max}]$ and hence terminate the process.

Cost Functions: The two cost functions for the throughput and the energy consumption are denoted by $g_k^R(s_{i_k}, \Omega_k, u_k)$ and $g_k^E(s_{i_k}, \Omega_k, u_k)$, respectively. They are defined similar as (4.7) and (4.8) by replacing s_k with (s_{i_k}, Ω_k) and $u_k = \mathcal{C}$ with $u_k = j, j \in \Omega_k$. For stage 0, we have $g_0^R(\emptyset, \Omega_0, u_0) = g_0^E(\emptyset, \Omega_0, u_0) = 0$.

The objective is to find a sequence of functions $\phi = \{\mu_0(\emptyset, \Omega_0), \mu_1(s_{i_1}, \Omega_1), \dots, \mu_K(s_{i_K}, \emptyset)\}$, with $\mu_k, k = 0, 1, \dots, K$, mapping each state (s_{i_k}, Ω_k) into a control $u_k = \mu_k(s_{i_k}, \Omega_k)$, to maximize the energy efficiency of the whole process,

$$\eta = \frac{\mathbb{E} \left\{ \sum_{k=0}^K g_k^R(s_{i_k}, \Omega_k, \mu_k(s_{i_k}, \Omega_k)) \right\}}{\mathbb{E} \left\{ \sum_{k=0}^K g_k^E(s_{i_k}, \Omega_k, \mu_k(s_{i_k}, \Omega_k)) \right\}}. \quad (4.26)$$

It can be easily shown that the parametric transformation still applies and hence we can use Algorithm 2 to solve this problem. Therefore, we restrict our attention to solving the parametric problem. By using DP, we have, at stage K , the expected net

reward given by

$$J_K(s_{i_K}, \emptyset; \lambda) = \begin{cases} -\lambda\tau P_s, & \text{if } s_{i_K} = (1, 0), \\ -\lambda\tau P_s + \mathcal{F}_{i_K}^*(h_{i_K}, \lambda), & \text{otherwise.} \end{cases} \quad (4.27)$$

The optimal strategy at stage K when channel i_K is sensed to be idle is the same as that in (4.15).

Then we use backward induction. For the problem starting from stage k and $s_{i_k} \neq \mathcal{T}$, we can express the expected net reward, for $k = 1, \dots, K - 1$, as

$$J_k(s_{i_k}, \Omega_k; \lambda) = -\lambda\tau P_s + \max_{j \in \Omega_k} \mathbb{E}\{J_{k+1}(s_j, \Omega_k - j; \lambda)\} \quad (4.28)$$

when $s_{i_k} = (1, 0)$, and otherwise, we have

$$J_k(s_{i_k}, \Omega_k; \lambda) = -\lambda\tau P_s + \max \left\{ \mathcal{F}_{i_k}^*(h_{i_k}, \lambda), \max_{j \in \Omega_k} \mathbb{E}\{J_{k+1}(s_j, \Omega_k - j; \lambda)\} \right\}. \quad (4.29)$$

The optimal strategy at stage k , $k = 1, \dots, K - 1$, is given by

$$\mu_k(s_{i_k}, \Omega_k; \lambda) = \operatorname{argmax}_{j \in \Omega_k} \mathbb{E}\{J_{k+1}(s_j, \Omega_k - j; \lambda)\} \quad (4.30)$$

when channel i_k is detected to be busy; and when channel i_k is sensed to be idle, it is given by

$$\begin{aligned} & \mu_k(s_{i_k}, \Omega_k; \lambda) \\ = & \begin{cases} \left[\frac{\omega_k B}{\lambda \alpha \ln(2)} - \frac{\iota \Gamma \sigma^2}{\rho_k h_k} \right]_{P_{min}}^{P_{max}}, & \text{if } \mathcal{F}_{i_k}^*(h_{i_k}, \lambda) \geq \max_{j \in \Omega_k} \mathbb{E}\{J_{k+1}(s_j, \Omega_k - j; \lambda)\}, \\ \operatorname{argmax}_{j \in \Omega_k} \mathbb{E}\{J_{k+1}(s_j, \Omega_k - j; \lambda)\}, & \text{otherwise.} \end{cases}, \end{aligned} \quad (4.31)$$

Note that the optimal sensing strategy at stage k indicates transmission only occurs

when the immediate net reward on channel i_k is larger than the expected net reward associated with continuing the process by sensing any of the remaining channels. It is also a threshold based structure because of the monotonicity of $\mathcal{F}_{i_k}^*(h_{i_k}, \lambda)$. The optimal power allocation strategy has the same structure as that in Section 4.3. The optimal sensing order is to choose to sense the channel from the set of remaining channels associated with the maximum expected future net reward.

The procedure can be repeated until stage 0. Then the maximum expected reward for the problem parameterized by λ is given as

$$J_{\phi^*(\lambda)} = J_0(\emptyset, \Omega_0; \lambda) = \max_{j \in \Omega_0} \mathbb{E}\{J_1(s_j, \Omega_0 - j; \lambda)\}. \quad (4.32)$$

Hence, at the beginning, we should sense from the channel index given by

$$\mu_0(\emptyset, \Omega_0; \lambda) = \operatorname{argmax}_{j \in \Omega_0} \mathbb{E}\{J_1(s_j, \Omega_0 - j; \lambda)\}. \quad (4.33)$$

Finally, the maximum energy efficiency λ^* satisfies $J_{\phi^*(\lambda^*)} = 0$ and can be searched using Algorithm 2.

4.4.2 Computational Complexity

Another way to find the optimal sensing order is to exhaustively search over all the possible sensing orders. For each given sensing order, we can use the algorithm proposed in Section 4.3 to compute the energy efficiency. Then we can choose the sensing order that gives the maximum energy efficiency. The computational complexity of the exhaustive search and the approach proposed in this section is compared as follows. We count the number of times that $\mathbb{E}\{J_k\}$ is computed. When the sensing order and λ are fixed, at each stage, we calculate $\mathbb{E}\{J_k\}$ once. Hence, for each given sensing order, the computation complexity is βK , where $\beta = \lceil \log_2 \left(\frac{\lambda_{max} - \lambda_{min}}{\varepsilon} \right) \rceil$ is the number of iterations that the bisection search algorithm takes to terminate and $\lceil (\cdot) \rceil$ represents the

smallest integer not less than $(\cdot)$ [194]. Hence, the overall complexity of the exhaustive search is $\beta K!K$, i.e., $\mathcal{O}(K!K)$. For the approach proposed in this section, for each given λ , we find the best sensing order using DP and then we perform bisection search over λ . When λ is given, at stage k , we have to compute $\mathbb{E}\{J_k\}$ for each possible combination of (i_k, Ω_k) . There are $K \binom{K-1}{K-k}$ combinations. Therefore, the overall complexity of the proposed approach is $\beta K \sum_{k=1}^K \binom{K-1}{K-k}$, i.e., $\mathcal{O}\left(K \sum_{k=1}^K \binom{K-1}{K-k}\right) = \mathcal{O}(2^K K)$. The computational complexities of the two approaches in terms of the number of computations for $\mathbb{E}\{J_k\}$ are compared in Fig. 4.2. It can be seen that our proposed approach is much simpler than the exhaustive search.

Figure 4.2: Comparison of computational complexity between the exhaustive search and the proposed method.

4.5 Numerical Results

The numerical results for our proposed energy-efficient sequential channel sensing designs are presented in this section. Unless otherwise stated, the values of the parameters

used are listed in Table 4.1. The basic Matlab code for the simulation can be found in Appendix H.

Table 4.1: Parameter Settings

Bandwidth B	6 MHz
Noise PSD $N_0/2$	-204 dBW/Hz
Noise Figure N_f	10 dB
Distance d	200 m
Carrier Frequency $f_{c,k}$	$f_{c,1} = 700$ MHz $f_{c,k+1} - f_{c,k} = B$ $k = 1, \dots, K - 1$
Link Margin ι	10 dB
Bit error rate BER	10^{-5}
Minimum Transmit Power P_{min}	1 mW
Maximum Transmit Power P_{max}	166.62 mW
Circuit Power (excluding the PA) P_c	210 mW
Sensing Power P_s	110 mW
Transmission/Frame Time T	100 ms
PU Idle Probability θ_k	0.8
SU Channel condition h_k	$\{1, 2, 3, 4, 5\}$ with probability $\{0.64, 0.23, 0.09, 0.03, 0.01\}$
PU Worst-Case SNR γ_k	-20 dB
Target Detection Probability $\mathcal{P}_{d,k}$	0.9
PAR ξ	6 dB
Drain Efficiency ζ	0.35

4.5.1 Given Sensing Order

In this subsection, we will show the maximum energy efficiency achieved when the sensing order is according to the logical channel index from 1 to K . Note that in general the average channel condition is getting worse as the channel index increases since increasing carrier frequency causes larger propagation loss while other conditions remain the same among all channels [195].

We first compare our design with two suboptimal schemes for $K = 6$. The first suboptimal scheme refers to the scheme that the SU always transmits over the first available channel but with adaptive power allocation. No secondary channel diversity

is explored in this case. This corresponds to removing the decision $u_k = \mathcal{C}$ when $\hat{\delta}_k = 0$. The second suboptimal scheme refers to the scheme that the SU is allowed to explore channel diversity but it always uses the maximum transmit power. No adaptive power allocation is explored in this case. This corresponds to setting $u_k = P_{max}$ when transmitting. The power allocation for the first scheme and the sensing policy for the second scheme can be computed similarly to what we have presented in Section 4.3. The energy efficiencies of the optimal and the two suboptimal schemes are plotted versus sensing time in Fig. 4.3 for the case of constant transmission time. The theoretical

Figure 4.3: Energy efficiency vs sensing time for $K = 6$ (constant transmission time).

results are obtained based on the approach proposed in Section 4.3. Simulated results are obtained using Monte-Carlo simulations which implement the optimal policy. It is observed that the theoretical and simulated results match well for all the three cases. Thus, in the subsequent figures, we will only show the theoretical results. We can also see that our design outperforms the other two schemes because we both explore channel diversity and use adaptive power allocation. Since both the optimal and the first suboptimal scheme are much better than the second suboptimal one, we can

observe that the adaptive power control is more important from the point of view of energy efficiency. It is further observed that the gap between the optimal scheme and the first suboptimal scheme becomes smaller as sensing time increases. This is because the increasing energy consumption in sensing additional channel prevents the SU from exploring channel diversity. For the case of constant frame time, the results and observations are similar and thus are omitted.

Next, we show the maximum energy efficiency achieved under a range of sensing time for different number of channels. The results for the constant transmission time and constant frame time are shown in Figs. 4.4 and 4.5, respectively. First, we

Figure 4.4: Energy efficiency vs sensing time (constant transmission time).

can observe the sensing-energy-efficiency tradeoff phenomenon, which is similar to the sensing-throughput tradeoff presented in [59]. This can be explained as follows. When sensing time is small, we will suffer from high false alarm and miss the transmission opportunities. Therefore, throughput is reduced and energy efficiency is also reduced. When sensing time is increased to certain value, the reduced false alarm and therefore higher throughput may not offset the increasing energy consumption for spectrum sens-

Figure 4.5: Energy efficiency vs sensing time (constant frame time).

ing. Hence, energy efficiency will drop. Hence, we observe the tradeoff phenomenon. Secondly, it is observed that when sensing time is relatively small, the energy efficiency is increased with the increasing number of channels. This is because small sensing time allows the SU to explore multi-channel diversity with negligible sensing energy cost. In contrast, when sensing time is relatively large, more channels do not necessarily help to increase the energy efficiency. This is partly because exploring multi-channel diversity is restrained by the increasing cost for spectrum sensing. In addition, each additional channel is on average getting worse in channel condition. For the case of constant frame time, sensing each additional channel also reduces the transmission time. Thus, when sensing time is relatively large, the decrease in energy efficiency with the number of channels is more obvious than the case of constant transmission time. However, usually, we are more interested in the operating point where the sensing time achieves the maximum energy efficiency for each K . The maximum energy efficiency and the corresponding optimal sensing time are shown against the number of channels in Figs. 4.6 and 4.7, respectively. It is observed that the maximum energy efficiency is in-

Figure 4.6: Maximum energy efficiency vs number of channels.

Figure 4.7: Optimal sensing time vs number of channels.

creased and the optimal sensing time is reduced with the larger set of channels. In this case, we can see the benefit of exploring multi-channel diversity.

Furthermore, we compare our energy-efficient design with the throughput-efficient design, which maximizes the throughput efficiency of the sequential channel sensing and transmission process. To maximize the throughput efficiency, maximum transmit power is always preferred. The corresponding optimal sensing strategy can be derived by replacing the cost function on energy consumption with time consumption and following the same analytical approach as the proposed energy-efficient design. The achievable energy efficiency and the throughput efficiency of the two designs for $K = 8$ and the constant transmission scenario are compared in Figs. 4.8 and 4.9, respectively.

Figure 4.8: Energy efficiency comparison of the energy-efficient and the throughput-efficient designs for $K = 8$ (constant transmission time).

We can observe that although the proposed energy-efficient design can achieve around half of the throughput as that in the throughput-efficient design, it can achieve an energy efficiency more than three times higher than that of the throughput-efficient design, which means that within a finite energy budget, it transmits more than three

Figure 4.9: Throughput efficiency comparison of the energy-efficient and the throughput-efficient designs for $K = 8$ (constant transmission time).

times the amount of data. In general, the sensing-access strategies that maximize the energy efficiency do not achieve the highest throughput efficiency, and vice versa, since the two designs aim for different objectives. In practice, the energy-efficient design can be used for applications that are energy-constrained but do not have very high rate requirements. For applications that require rates higher than what can be supported by the energy-efficient design, the studied parametric formulation, which can be considered as an energy-aware design, can be used to balance the tradeoff between throughput and energy consumption by varying the price per unit energy.

4.5.2 Optimal Sensing Order

In this subsection, we evaluate the energy efficiency achieved when we jointly design the sensing order and the sensing-access strategies. We consider only the case of constant transmission time with $K = 5$ channels.

In Fig. 4.10, we show the energy efficiency versus sensing time when the PU idle

probability equals to $\theta_k = 0.8$, for $k = 1, \dots, K$. The results of our proposed design and

Figure 4.10: Energy efficiency vs sensing time with $\theta_k = 0.8$, $k = 1, \dots, K$.

the exhaustive search method are observed to coincide. We also compare the design that uses optimal sensing order with the design which always uses a fixed sensing order. The fixed sensing order is considered to be according to the logical channel index from 1 to 5. This sensing order corresponds to the decreasing order of the SU's average channel condition and can be considered as an intuitive sensing order since the PU statistics is identical among different channels. We observe that the joint design can achieve higher energy efficiency and this intuitive sensing order is generally not optimal. Note that Since the sensing order is designed to maximize the energy efficiency and sensing time is an important factor that affects the energy efficiency, the optimal sensing order will in general be different with different sensing time. The optimal sensing order under the optimal sensing time in this case is given by [4 3 2 1 5].

Next, we consider the scenario when the primary idle probabilities are set to $\{\theta_1, \dots, \theta_5\} = \{0.1, 0.3, 0.5, 0.7, 0.8\}$ in Fig. 4.11. Two fixed sensing orders are considered. One is from channel index 5 to 1, which corresponds to the decreasing order

PU idle probability. The other is from channel index 1 to 5, which corresponds to the decreasing order of SU average channel gain. We can see again the superiority of the joint design and neither of the two fixed sensing orders is optimal. In this case, the optimal sensing order under the optimal sensing time in this case is given by [2 3 5 4 1].

Figure 4.11: Energy efficiency vs sensing time with the idle probabilities given by $\{\theta_1, \dots, \theta_K\} = \{0.1, 0.3, 0.5, 0.7, 0.8\}$.

4.6 Conclusions

In this chapter, we have studied the energy-efficient transmission in a multi-channel CRN which employs sequential channel sensing. The design of the sensing-access strategies to maximize the energy efficiency has been formulated as a stochastic sequential decision-making problem. To solve it, we have studied a parametric formulation, which can be solved efficiently using DP. An algorithm has been developed by exploring the relationship between the two formulations and making use of the monotonicity prop-

erty of the parametric formulation. We have further investigated the design that takes the sensing order into account. We have found that the optimal sensing strategy has a threshold structure, which allows the SU to transmit only if the current channel condition is good enough. The optimal access strategy, i.e., the optimal power allocation strategy, has a water-filling structure with the water level determined by the long-term energy efficiency and the perceived spectrum opportunity of the transmission channel. The optimal sensing order is to choose to sense the channel from the set of remaining channels associated with the maximum expected future net reward. Finally, the performance of our design has been evaluated through numerical results.

Chapter 5

Secure Transmission in Spectrum Sharing with Perfect CSI

As reviewed in Chapter 2, majority of the research in the spectrum sharing CRNs focus on improving the rate or SNR of the SU while keeping interference well controlled under the interference temperature limit. No attention has been received in the literature to address the security issues during this transmission process under this model. The unique characteristics of CR make CRNs even more susceptible to security threats than any conventional wireless communication systems. In particular, eavesdropping becomes much easier for a malicious user because of the capability of a future CR device to explore a wide range of radio spectrum. In this chapter, we are the first to study techniques to protect the confidentiality of information from the potential eavesdroppers in the spectrum sharing model and we focus on the information-theoretic techniques as introduced in Section 2.3.2. Note that the security threat addressed in this thesis is considered as passive attack while the existing work on security issues all focus on active attacks in the OSA model.

Specifically, we consider the communication over a secure MISO CR channel where a multi-antenna SU-Tx sends confidential information to a legitimate SU-Rx in the presence of a single-antenna PU-Rx and a single-antenna eavesdropper receiver (ED-

Rx). The channel from the SU-Tx to the SU-Rx, the PU-Rx and the ED-Rx is denoted as the secondary channel, the primary channel and the eavesdropper channel, respectively. The secrecy capacity of this channel is defined as the maximum rate such that the information can be reliably transmitted from the SU-Tx to the SU-Rx but is kept perfect secret from the ED-Rx, at the same time the resulting interference power received at the PU-Rx is kept below the interference temperature limit.

The main contributions of this chapter are summarized as follows. The secrecy capacity of the secure MISO CR channel is first characterized, which is a quasiconvex optimization problem of finding the capacity-achieving transmit covariance matrix under the joint transmit power and interference power constraints. Two efficient numerical approaches are proposed to obtain the optimal transmit covariance matrix: 1) Through novel reformulation, the seemingly nonconvex problem can be recast into a convex SDP and hence can be solved efficiently through semidefinite programming. Therefore, this approach is called SDP transformation. 2) By exploiting the relationship between the secure CR channel and the conventional CR channel (i.e., the CR channel without secrecy constraint), the original problem is transformed into a sequence of auxiliary conventional CR optimization problems and as a result, beamforming is shown to be the optimal transmission strategy for the secure MISO CR channel. Therefore, this approach is called auxiliary CRN transformation. Furthermore, to reduce the computational complexity, we also propose three suboptimal schemes, namely, *scaled secret beamforming* (SSB), *projected secret beamforming* (PSB) and *projected cognitive beamforming* (PCB) to tradeoff among maximizing the information rate over the secondary channel, minimizing the interference over the primary channel and restricting the information over the eavesdropper channel

The rest of the chapter is organized as follows. Section 5.1 provides the system model of the secure MISO CR channel and formulates the optimization problem to design the capacity-achieving transmit covariance matrix. Section 5.2 presents two

approaches to derive the optimal transmit covariance matrix, namely, SDP transformation and auxiliary CRN transformation. Section 5.3 develops three suboptimal solutions, namely, SSB, PSB, and PCB. Simulation results are given in Section 5.4. Finally, Section 5.5 concludes the chapter.

5.1 System Model and Problem Formulation

In this chapter, we consider a communication scenario in a CRN where an SU-Tx wants to send confidential information to an SU-Rx on the same band as a PU's transmission, and at the same time an eavesdropper is trying to eavesdrop and interpret the message sent by the SU-Tx. Such a communication scenario can be described by a secure CR channel with four terminals: a pair of SU-Tx and SU-Rx, a PU-Rx and an ED-Rx as shown in Fig. 5.1. The SU-Tx is equipped with N antennas, and the SU-Rx, the PU-Rx and the ED-Rx are all equipped with a single antenna each. The channel responses of the resulting MISO secondary channel, primary channel and eavesdropper channel are denoted by $\mathbf{h}_s$, $\mathbf{h}_p$ and $\mathbf{h}_e$, respectively, where $\mathbf{h}_s, \mathbf{h}_p, \mathbf{h}_e \in \mathbb{C}^{N \times 1}$.

Figure 5.1: System model for the secure MISO CR channel.

Similar to [196], we consider that the SU-Tx as a base station of the CRN and both the SU-Rx and the ED-Rx are the SUs of the CRN. The ED-Rx is treated as an eavesdropper only because it is not the intended destination of the confidential

message. We can assume that both the SU-Rx and the ED-Rx have perfect knowledge of the realization of its own channel. This can be done by estimating the channel using the training sequence sent from the SU-Tx. The knowledge of $\mathbf{h}_s$ and $\mathbf{h}_e$ at the SU-Tx can be obtained through feedback channel from the SU-Rx and the ED-Rx⁸ assuming channel reciprocity. Furthermore, the knowledge of $\mathbf{h}_p$ at the SU-Tx can be obtained by periodically sensing the transmitted signal from the PU-Rx when it is in the transmission mode. Since this chapter aims to characterize the information-theoretic limit of the SU's secure transmission, it is assumed that the SU-Tx knows the channel state information (CSI) of all the links perfectly. In the case when such CSI cannot be obtained perfectly at the SU-Tx, the result provided in this chapter can serve as an upper bound of the secure transmission in CRNs.

The signals received at the SU-Rx and the ED-Rx at time index m are expressed as

$$y_m = \mathbf{h}_s^\dagger \mathbf{x}_m + w_m, \quad (5.1)$$

$$z_m = \mathbf{h}_e^\dagger \mathbf{x}_m + v_m, \quad (5.2)$$

respectively, where $\mathbf{x}_m \in \mathbb{C}^{N \times 1}$ is the signal transmitted from the SU-Tx, with positive semidefinite covariance matrix $\mathbf{S} = \mathbb{E}\{\mathbf{x}\mathbf{x}^\dagger\} \succeq 0$; w_m and v_m are the additive noise components at the SU-Rx and the ED-Rx, respectively. It is assumed that $w_m, v_m \sim \mathcal{CN}(0, 1)$.

The secrecy capacity for the discrete memoryless wiretap channel as given in (2.12) can be extended to the case of continuous-alphabet channel with average cost constraint. Hence, the characterization of the secrecy capacity for the secure MISO CR channel can be obtained by evaluating (2.12) for the channel model in (5.1) and (5.2) under the transmit power constraint and interference constraint, which is mathemati-

⁸It is reasonable to assume that ED-Rx feeds back its CSI to the SU-Tx since as another SU-Rx, it may also expect some confidential information from the SU-Tx.

cally shown as

$$C_s(P, Q) \triangleq \max_{\mathbf{p}(\mathbf{u}, \mathbf{x}): \mathbf{u} \rightarrow \mathbf{x} \rightarrow (y, z)} I(\mathbf{u}; y) - I(\mathbf{u}; z) \quad (5.3)$$

$$\text{s.t.} \quad \mathbb{E}\{\mathbf{x}^\dagger \mathbf{x}\} \leq P \quad (5.4)$$

$$\mathbf{h}_p^\dagger \mathbb{E}\{\mathbf{x}^\dagger \mathbf{x}\} \mathbf{h}_p \leq Q, \quad (5.5)$$

where P and Q are the transmit power limit and interference temperature limit, respectively. Note that (5.4) corresponds to the transmit power constraint, while (5.5) is the interference power constraint imposed at the PU-Rx.

Corollary 5.1. The secrecy capacity $C_s(P, Q)$ of the secure MISO CR channel and its capacity achieving transmit covariance matrix can be found as the maximum objective value and the optimal solution of the following optimization problem, respectively.

Problem 5.2.

$$\max_{\mathbf{S} \succeq 0} \log_2(1 + \mathbf{h}_s^\dagger \mathbf{S} \mathbf{h}_s) - \log_2(1 + \mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e) \quad (5.6)$$

$$\text{s.t.} \quad \text{tr}(\mathbf{S}) \leq P \quad (5.7)$$

$$\mathbf{h}_p^\dagger \mathbf{S} \mathbf{h}_p \leq Q. \quad (5.8)$$

Proof. According to [175], the secrecy capacity the above channel under only the transmit power constraint (5.4), which represents the conventional MISO wiretap channel, can be characterized as

$$C_s(P) = \max_{\mathbf{S} \succeq 0, \text{tr}(\mathbf{S}) \leq P} \log_2(1 + \mathbf{h}_s^\dagger \mathbf{S} \mathbf{h}_s) - \log_2(1 + \mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e).$$

However, this result cannot be directly applied to our channel model due to the additional interference power constraint (5.5). To find $C_s(P, Q)$, we have to resort to a more general result for the MISO wiretap channel, which was reported in [176]. Following [176], the secrecy capacity for the MISO wiretap channel under the general covariance

matrix constraint

$$\mathbb{E}\{\mathbf{x}\mathbf{x}^\dagger\} \preceq \mathbf{K}, \quad (5.9)$$

where $\mathbf{K} \succeq 0$, was characterized as

$$C_s(\mathbf{K}) = \max_{0 \preceq \mathbf{S} \preceq \mathbf{K}} \log_2(1 + \mathbf{h}_s \mathbf{S} \mathbf{h}_s^\dagger) - \log_2(1 + \mathbf{h}_e \mathbf{S} \mathbf{h}_e^\dagger). \quad (5.10)$$

As shown in [197], the matrix covariance constraint (5.9) is a rather general constraint in the sense that it can be used to easily derive the achievable rate under any constraint that can be represented in terms of a compact set of $\mathbf{K}$. Hence, for our channel of interest, we define the compact set as $\mathcal{S} = \{\mathbf{K} \mid \text{tr}(\mathbf{K}) \leq P, \mathbf{h}_p^\dagger \mathbf{K} \mathbf{h}_p \leq Q\}$, which corresponds to the set of covariance matrices satisfying both the transmit power constraint and the interference power constraint. We denote $C_s(\mathcal{S})$ as the secrecy capacity under this compact set constraint $\mathcal{S}$. Note that $C_s(\mathcal{S}) = C_s(P, Q)$. Then, according to Lemma 1 of [197], which states that the rate region achievable under the compact set constraint $\mathcal{S}$ is the union of all achievable rate regions for each $\mathbf{K} \in \mathcal{S}$, we have the secrecy capacity of the secure MISO CR channel

$$C_s(P, Q) = \max_{\mathbf{K} \in \mathcal{S}} C_s(\mathbf{K}) \quad (5.11)$$

$$= \max_{\mathbf{K} \in \mathcal{S}} \max_{0 \preceq \mathbf{S} \preceq \mathbf{K}} \log(1 + \mathbf{h}_s \mathbf{S} \mathbf{h}_s^\dagger) - \log(1 + \mathbf{h}_e \mathbf{S} \mathbf{h}_e^\dagger) \quad (5.12)$$

$$= \max_{\mathbf{S} \succeq 0, \mathbf{S} \in \mathcal{S}} \log_2(1 + \mathbf{h}_s \mathbf{S} \mathbf{h}_s^\dagger) - \log_2(1 + \mathbf{h}_e \mathbf{S} \mathbf{h}_e^\dagger). \quad (5.13)$$

□

Corollary 5.1 implies that the secrecy capacity $C_s(P, Q)$ is achieved by choosing $\mathbf{u} = \mathbf{x}$ to be Gaussian. Hence, the problem of finding the secrecy capacity of the secure MISO CR channel is reduced to the problem of designing the transmit covariance matrix $\mathbf{S}$ of the SU-Tx that achieves the maximum value of *Problem 5.2*. In the

case when $\mathbf{S}$ is a rank-one matrix, the transmission strategy is usually termed as beamforming, implying the transmission is only in a single direction. Before we solve *Problem 5.2*, results for some related channel models will be briefly reviewed.

1. *Conventional MISO Channel*: It is well known that in the conventional MISO channel where both the PU and the eavesdropper are not present, the optimal $\mathbf{S}$ is of the form $\mathbf{S} = P\mathbf{v}\mathbf{v}^\dagger$, where $\mathbf{v} = \check{\mathbf{h}}_s$, indicating that the optimal transmission strategy is maximum-ratio-transmission (MRT) beamforming in the direction of the channel $\mathbf{h}_s$. Note that here the unit-form vector of a vector $\mathbf{h}$ is denoted as $\check{\mathbf{h}}$, i.e., $\check{\mathbf{h}} = \mathbf{h}/\|\mathbf{h}\|$.
2. *Conventional MISO CR Channel*: When the eavesdropper is not present, *Problem 5.2* reduces to a problem in the conventional MISO CR channel with one PU. It has been shown in [53] that the optimal strategy is also beamforming with the maximum power and the closed-form solution for the optimal unit-norm beamforming vector is given by

$$\mathbf{v}_{CR}(\mathbf{h}_s, \mathbf{h}_p) = \alpha_{CR}\check{\mathbf{h}}_p + \beta_{CR}\check{\mathbf{h}}_p^\perp, \quad (5.14)$$

where $\mathbf{h}_p^\perp = (\mathbf{I} - \check{\mathbf{h}}_p\check{\mathbf{h}}_p^\dagger)\mathbf{h}_s$ is the projection of $\mathbf{h}_s$ onto the null space of $\mathbf{h}_p$; the complex-valued weights are given by

$$(\alpha_{CR}, \beta_{CR}) = \begin{cases} \left(\frac{\check{\mathbf{h}}_p^\dagger \mathbf{h}_s}{\|\mathbf{h}_s\|}, \frac{(\check{\mathbf{h}}_p^\perp)^\dagger \mathbf{h}_s}{\|\mathbf{h}_s\|} \right), & Q \geq P\|\mathbf{h}_p\|^2 \left(\frac{|\check{\mathbf{h}}_p^\dagger \mathbf{h}_s|}{\|\mathbf{h}_s\|} \right)^2, \\ \left(\lambda \frac{\check{\mathbf{h}}_p^\dagger \mathbf{h}_s}{\|\check{\mathbf{h}}_p^\perp\|}, \sqrt{1 - \lambda^2} \frac{(\check{\mathbf{h}}_p^\perp)^\dagger \mathbf{h}_s}{\|(\check{\mathbf{h}}_p^\perp)^\dagger \mathbf{h}_s\|} \right), & \text{otherwise,} \end{cases} \quad (5.15)$$

and $\lambda = \sqrt{\frac{Q}{P\|\mathbf{h}_p\|^2}}$. Alternatively, it can be shown that the optimal beamforming vector can be expressed as a linear combination of the MRT beamformer $\check{\mathbf{h}}_s$ and ZF beamformer $\check{\mathbf{h}}_p^\perp$ (see Appendix B)

$$\mathbf{v}_{CR}(\mathbf{h}_s, \mathbf{h}_p) = \tilde{\alpha}_{CR}\check{\mathbf{h}}_s + \tilde{\beta}_{CR}\check{\mathbf{h}}_p^\perp, \quad (5.16)$$

where the real-valued weights are given by

$$(\tilde{\alpha}_{CR}, \tilde{\beta}_{CR}) = \begin{cases} (1, 0), & Q \geq P(\|\mathbf{h}_p\| \cos \phi)^2, \\ \left(\frac{\lambda}{\cos \phi}, \sqrt{1 - \lambda^2} - \lambda \tan \phi \right), & \text{otherwise,} \end{cases} \quad (5.17)$$

and $\phi = \arccos(\check{\mathbf{h}}_p^\dagger \mathbf{h}_s / \|\mathbf{h}_s\|)$, which is termed as *cognitive beamforming* in this chapter. It is implied from (5.16) that the cognitive beamforming vector is either solely in the direction of the secondary channel or adjusted so that it is as close to the secondary channel as possible while at the same time being as orthogonal to the primary channel as possible depending on whether the interference power constraint is active or not.

3. *Conventional MISO wiretap channel:* When the interference power constraint (6.17) is not present, *Problem 5.2* reduces to a problem in the conventional MISO wiretap channel. The optimal strategy is again proved to be beamforming with the maximum power and the unit-norm beamforming vector is computed as the normalized eigenvector corresponding to the largest generalized eigenvalue of the matrix pair $(\mathbf{I} + P\mathbf{h}_s\mathbf{h}_s^\dagger, \mathbf{I} + P\mathbf{h}_e\mathbf{h}_e^\dagger)$ [178–180]. Alternatively, it can be shown in Appendix C that the optimal beamforming vector can also be written as a linear combination of the MRC and ZF beamformers

$$\mathbf{v}_{WT}(\mathbf{h}_s, \mathbf{h}_e) = \alpha_{WT}\check{\mathbf{h}}_s + \beta_{WT}\check{\mathbf{h}}_e^\perp, \quad (5.18)$$

where $\mathbf{h}_e^\perp = (\mathbf{I} - \check{\mathbf{h}}_e\check{\mathbf{h}}_e^\dagger)\mathbf{h}_s$; and α_{WT} and β_{WT} are real-valued weights. Note that (5.18) is termed as *secret beamforming* in this chapter. Similar to the conventional CR channel, the optimal beamforming vector is also a linear combination of the MRT and ZF beamformers.

By the monotonicity of the log function, we will deal with the following *Problem 5.3* in the rest of the chapter:

Problem 5.3.

$$\max_{\mathbf{S} \succeq 0} \quad \frac{1 + \mathbf{h}_s^\dagger \mathbf{S} \mathbf{h}_s}{1 + \mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e} \quad (5.19)$$

$$\text{s.t.} \quad \text{tr}(\mathbf{S}) \leq P \quad (5.20)$$

$$\mathbf{h}_p^\dagger \mathbf{S} \mathbf{h}_p \leq Q. \quad (5.21)$$

Notice that *Problem 5.3* is a quasiconvex optimization problem, with the objective function being a quasiconcave function of $\mathbf{S}$ and the constraints specifying a convex set of $\mathbf{S}$ [194]. This type of problem can be generally solved through a sequence of convex feasibility problems [194, p. 145]. As a first step, it requires the equivalent representation of the superlevel sets of a quasiconcave function via a set of convex inequalities. Since our objective function is a ratio of two linear matrix inequalities of nonnegative semi-definite matrix, this can be easily done by taking the epigraph form of the original problem:

$$\max_{\mathbf{S} \succeq 0, \tau \geq 0} \quad \tau \quad (5.22)$$

$$\text{s.t.} \quad 1 + \mathbf{h}_s^\dagger \mathbf{S} \mathbf{h}_s \geq \tau (1 + \mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e) \quad (5.23)$$

$$\text{tr}(\mathbf{S}) \leq P \quad (5.24)$$

$$\mathbf{h}_p^\dagger \mathbf{S} \mathbf{h}_p \leq Q. \quad (5.25)$$

As a result, for each given value of τ , this problem has convex constraints w.r.t. $\mathbf{S}$. Then the optimal solution can be found through testing the feasibility of (5.23)-(5.25) for a sequence of τ through a bisection search method as shown in Algorithm 3.

Note that at each given τ , the feasibility test can be considered as an SDP since all the constraint functions are linear functions of the positive semidefinite variable $\mathbf{S}$. The SDP can be solved using standard optimization software packages such as SeDuMi [198]. Although many numerical solvers can solve the SDPs very efficiently, they are

Algorithm 3 Bisection algorithm for solving *Problem 5.3*

-
- 1) **Given:** $\tau \in [0, \bar{\tau}]$;
 - 2) **Initialize:** $\tau_{\min} \leftarrow 0, \tau_{\max} \leftarrow \bar{\tau}$;
 - 3) **Repeat:**
 - a) $\tau \leftarrow \frac{1}{2}(\tau_{\min} + \tau_{\max})$;
 - b) Check the feasibility of (5.23), (5.24) and (5.25):
If it is feasible, set $\tau_{\min} \leftarrow \tau$; else, set $\tau_{\max} \leftarrow \tau$;
 - 4) **Until** $\tau_{\max} - \tau_{\min} \leq \bar{\varepsilon}$, where $\bar{\varepsilon}$ is a small positive number that controls the accuracy of the algorithm.
-

usually not good at distinguishing between a strictly infeasible problem and a possible numerical difficulty. Therefore, the algorithm based on numerical feasibility test is prone to errors.

5.2 Optimal Solution

In this section, we present two alternative numerical optimization approaches to obtain the optimal transmit covariance matrix.

5.2.1 Semidefinite Program (SDP) Transformation

In this subsection, we transform the quasiconvex *Problem 5.3* into a single convex optimization problem and also establish the equivalency between *Problem 5.3* and the transformed convex problem through mathematical proof.

Since $\mathbf{S}$ is positive semidefinite, we have $1 + \mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e > 0$. Let $\frac{1}{1 + \mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e} = t$ and $\hat{\mathbf{S}} = t\mathbf{S}$, and we obtain

Problem 5.4.

$$\max_{\hat{\mathbf{S}} \succeq 0, t \geq 0} \quad t + \mathbf{h}_s^\dagger \hat{\mathbf{S}} \mathbf{h}_s \quad (5.26)$$

$$\text{s.t.} \quad \text{tr}(\hat{\mathbf{S}}) - tP \leq 0 \quad (5.27)$$

$$\mathbf{h}_p^\dagger \hat{\mathbf{S}} \mathbf{h}_p - tQ \leq 0 \quad (5.28)$$

$$\mathbf{h}_e^\dagger \hat{\mathbf{S}} \mathbf{h}_e + t = 1. \quad (5.29)$$

Proposition 5.5. *Problems 5.3 and 5.4 are equivalent and the optimal transmit covariance matrix of Problem 5.3 is $\mathbf{S}^* = \hat{\mathbf{S}}^o/t^o$, where $(\hat{\mathbf{S}}^o, t^o)$ is the optimal solution of Problem 5.4.*

Proof. Denote the optimal objective values of Problem 5.3 and Problem 5.4 as f^* and f^o , respectively. First, we will show that the optimal objective value f^* of Problem 5.3 is achievable for Problem 5.4, i.e., $f^* \leq f^o$. Since $\mathbf{S}^*$ is the optimal solution of Problem 5.3, it is easy to verify that the pair $(\hat{\mathbf{S}} = \frac{\mathbf{S}^*}{1+\mathbf{h}_e^\dagger \mathbf{S}^* \mathbf{h}_e}, t = \frac{1}{1+\mathbf{h}_e^\dagger \mathbf{S}^* \mathbf{h}_e})$ is feasible for Problem 5.4 and hence, f^* is achievable for Problem 5.4.

Next, we will show that the optimal objective value f^o of Problem 5.4 is also achievable for Problem 5.3, i.e., $f^* \geq f^o$. If $(\hat{\mathbf{S}}^o, t^o)$ is the optimal solution of Problem 5.4 with $t^o \neq 0$, then it is clear that $\mathbf{S} = \hat{\mathbf{S}}^o/t^o$ is also feasible for Problem 5.3 with the same objective value $f^o = t^o + \mathbf{h}_s^\dagger \hat{\mathbf{S}}^o \mathbf{h}_s$. If $(\hat{\mathbf{S}}^o, t^o)$ is the optimal solution of Problem 5.4 with $t^o = 0$ and $\tilde{\mathbf{S}}$ is feasible for Problem 5.3, then $\mathbf{S} = \tilde{\mathbf{S}} + t\hat{\mathbf{S}}^o$ is feasible for Problem 5.3 for all $t \geq 0$. Furthermore, since $\lim_{t \rightarrow \infty} \frac{1+\mathbf{h}_s^\dagger \mathbf{S} \mathbf{h}_s}{1+\mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e} = \mathbf{h}_s^\dagger \hat{\mathbf{S}}^o \mathbf{h}_s$, feasible solutions can be found with objective values arbitrarily close to that of $(\hat{\mathbf{S}}^o, t^o)$. Therefore, f^o is also achievable for Problem 5.3. Proposition 5.5 thus follows. $\square$

It is easy to see that the objective function of Problem 5.4 is a linear function of the nonnegative cone t and the semidefinite cone $\hat{\mathbf{S}}$, and the constraints define a convex set of $(\hat{\mathbf{S}}, t)$. Therefore, Problem 5.4 is an SDP, which is convex and can be solved very efficiently using SeDuMi [198].

5.2.2 Auxiliary CRN (ACRN) Transformation

The SDP transformation, despite having significant reduction in computational complexity as compared to the general approach mentioned in Section 5.1, hardly provides any insights on the structure of the optimal design of $\mathbf{S}$. In this subsection, we will show how the optimal transmission strategy is obtained through transforming the original problem into a sequence of problems related to the conventional CRN.

Figure 5.2: System model for the conventional MISO CR channel.

In the conventional MISO wiretap channel, to ensure secure transmission, the transmitter has to adjust its beamforming vector so as to restrict the power received at the ED-Rx. Similarly, in the conventional MISO CR channel, the SU-Tx also has to restrict the power received at the PU-Rx. The intrinsic relationship between these two channels has been explored in [199, 200]. The nonconvex robust beamforming problem in the conventional MISO wiretap channel has been transformed into a sequence of robust convex optimization problems in the conventional MISO CR channel and can thus be solved numerically. In this chapter, we adopt a similar approach. We construct an auxiliary CRN (ACRN) where there is a pair of SU-Tx and SU-Tx and two PUs as shown in Fig. 5.2. The channels from the SU-Tx to the SU-Rx and the two PU-Rxs are denoted by $\mathbf{h}_s$, $\mathbf{h}_p$ and $\mathbf{h}_e$, respectively. The capacity-achieving transmitter design problem for this constructed ACRN is as follows

Problem 5.6.

$$\mathcal{G}(q) \triangleq \max_{\mathbf{S} \succeq 0} \quad \mathbf{h}_s^\dagger \mathbf{S} \mathbf{h}_s \quad (5.30)$$

$$\text{s.t.} \quad \text{tr}(\mathbf{S}) \leq P \quad (5.31)$$

$$\mathbf{h}_p^\dagger \mathbf{S} \mathbf{h}_p \leq Q \quad (5.32)$$

$$\mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e \leq q, \quad (5.33)$$

where the log function of the objective (5.30) has been omitted due to its monotonicity.

Proposition 5.7. *Problem 5.3 is equivalent to Problem 5.8, which is defined as*

Problem 5.8.

$$\max_{q \geq 0} \frac{1 + \mathcal{G}(q)}{1 + q}. \quad (5.34)$$

Proof. Please refer to Proposition 1 in [199]. □

Since $\mathcal{G}(q)$ can be shown to be a concave function (see Appendix D), *Problem 5.8* is a quasiconvex optimization problem with a single variable q . As a result, efficient one dimensional search algorithm such as golden section search can be used to find the optimal q^* , which is detailed in Algorithm 4. Note that the algorithm searches for the optimal q over the region $[0, \bar{q}]$. At each search step (i.e., for a given q), *Problem 5.6* has to be solved. *Problem 5.6* has been studied in [53], where three numerical algorithms have been proposed to obtain the optimal $\mathbf{S}$, namely, the interior point method, the second-order cone programming (SOCP) and the SDP. Among these three algorithms, the SDP incurs the lowest computational complexity.

Algorithm 4 Golden section search algorithm for solving *Problem 5.8*

- 1) **Given:** $q \in [0, \bar{q}]$, $c = (\sqrt{5} - 1)/2$;
 - 2) **Initialize:** $a = 0$, $b = \bar{q}$, $q_1 \leftarrow (1 - c)b$, $q_2 \leftarrow cb$, compute $\mathcal{G}(q_1)$, $\mathcal{G}(q_2)$;
 - 3) **Repeat:**
 - a) **if** $\frac{1 + \mathcal{G}(q_1)}{1 + q_1} > \frac{1 + \mathcal{G}(q_2)}{1 + q_2}$:
 set $b \leftarrow q_2$, $q_2 \leftarrow q_1$, $\mathcal{G}(q_2) \leftarrow \mathcal{G}(q_1)$, $q_1 \leftarrow b - c(b - a)$; compute $\mathcal{G}(q_1)$;
 - b) **else:** set $a \leftarrow q_1$, $q_1 \leftarrow q_2$, $\mathcal{G}(q_1) \leftarrow \mathcal{G}(q_2)$, $q_2 \leftarrow a + c(b - a)$; compute $\mathcal{G}(q_2)$;
 - 4) **Until** $|b - a| \leq \bar{\varepsilon}$, where $\bar{\varepsilon}$ is a small positive number that controls the accuracy of the algorithm.
-

Although the ACRN transformation results in similar complexity as solving the sequence of SDPs as mentioned in Section 5.1, the benefit for such transformation is revealed by the following corollary.

Corollary 5.9. The optimal transmit covariance matrix for *Problem 5.3* is of rank one.

Proof. For any q , the optimal $\mathbf{S}$ for *Problem 5.6* has been proved to be of rank one in [53]. Corollary 5.9 thus follows. $\square$

Corollary 5.9 implies beamforming is the optimal strategy and hence encoding can be done by simply using a code for the scalar Gaussian wiretap channel.

In general, the closed-form solution for the optimal beamforming vector seems unlikely to exist. However, from the ACRN transformation, it can be implied that the optimal beamforming vector has to be adjusted to be as close to the secondary channel as possible while being as orthogonal to both the eavesdropper and primary channels as possible.

5.2.3 Computational Complexity

The computational complexity of the proposed SDP and the auxiliary CRN transformation algorithms is discussed as follows. Both of these two optimal approaches involve solving SDPs, e.g., *Problem 5.4* for the first one and a sequence of *Problem 5.6* for the second one. To solve an SDP, most of the commercial optimization software packages implement primal-dual interior point methods, which are iterative algorithms. At each iteration, some matrix operations, such as multiplication and factorization, need to be performed, and as a result, the computational complexity depends on the number of variables and the size of the constraints. To have a quantitative understanding of the complexity to solve an SDP, we will consider the following standard-form real-valued SDP first:

$$\min_{\mathbf{x} \in \mathbb{R}^n} \quad \mathbf{b}^T \mathbf{x} \quad (5.35)$$

$$\text{s.t.} \quad \mathbf{A}_0 + \sum_{j=1}^n x_j \mathbf{A}_j \succeq 0, \|\mathbf{x}\|_2 \leq R \quad (5.36)$$

where each of $\mathbf{A}_j$, $j = 0, \dots, n$ is a symmetric block diagonal matrices with m diagonal blocks of size $k_i \times k_i$, $i = 1, \dots, m$. In [201], the upper bound on the number of real arithmetic operations to obtain the ε -optimal solution of this SDP program is given as

$$\mathcal{O}(1) \left(1 + \sum_{i=1}^m k_i\right)^{\frac{1}{2}} n \left(n^2 + n \sum_{i=1}^m k_i^2 + \sum_{i=1}^m k_i^3\right) \ln(1/\varepsilon). \quad (5.37)$$

Then by converting *Problem 5.4* into its dual form, we will find that it has 3 real variables, 1 real positive definite cone constraint of size $2N$ and 3 nonnegative cone of size 1, i.e., $n = 3$, $m = 4$, $k_1 = 2N$, $k_2 = k_3 = k_4 = 1$. A careful examination will reveal that *Problem 5.6* (see equations (45)-(47) in [53]) is of the same size. Then from (5.37) and with some simplifications, we will have the the arithmetic complexity of *Problem 5.4* and *Problem 5.6* is of the order of $\mathcal{O}(N^{3.5})$. For auxiliary CRN transformation, it has to solve a sequence of *Problem 5.6* through golden section search, which takes $\left\lceil \log_c \left(\frac{\varepsilon}{q}\right) \right\rceil$ iterations to terminate. Since the SDP transformation only needs to solve *Problem 5.4*, the auxiliary CRN transformation is therefore more complex, but the overall complexity is still of the order $\mathcal{O}(N^{3.5})$.

5.3 Suboptimal Solutions

In this section, to reduce the computational complexity, we propose three suboptimal schemes that have closed-form solutions for $\mathbf{S}$. Moreover, all the three schemes are obtained based on the transformations of the secure MISO CR channels into the conventional MISO wiretap or CR channels.

5.3.1 Scaled Secret Beamforming

Since it has been shown in Section 5.2.2 that the optimal transmission strategy is beamforming, which involves only a single beamforming vector and the corresponding power, the rationale of the first scheme is to decouple the design of the beamform-

ing vector and the power. In particular, we first choose the beamforming vector as if the interference power constraint is not present and then we design the transmit power level to meet the interference temperature limit. Therefore it is referred as *scaled secret beamforming* (SSB). It is worth noting that by ignoring the interference power constraint, the channel is reduced to the conventional MISO wiretap channel and the beamforming vector is therefore chosen as $\mathbf{v}_{SSB} = \mathbf{v}_{WT}(\mathbf{h}_s, \mathbf{h}_e)$. However, this contributes to the suboptimality of the scheme since the optimal beamforming vector should be related to the CSI of all the three channels $\mathbf{h}_s$, $\mathbf{h}_e$ and $\mathbf{h}_p$, and it is in general different from the beamforming vector obtained solely from $\mathbf{h}_s$ and $\mathbf{h}_e$. After fixing the beamforming vector $\mathbf{v}_{SSB}$, the problem is reduced to

$$\max_p \quad f(p) \triangleq \frac{1 + p|\mathbf{h}_s^\dagger \mathbf{v}_{SSB}|^2}{1 + p|\mathbf{h}_e^\dagger \mathbf{v}_{SSB}|^2} \quad (5.38)$$

$$\text{s.t.} \quad p \leq P \quad (5.39)$$

$$p|\mathbf{h}_p^\dagger \mathbf{v}_{SSB}|^2 \leq Q, \quad (5.40)$$

which is an optimization problem involving only the power p . Note that the objective function $f(p) \geq 1$ since the nonnegative secrecy capacity is ensured by choosing $\mathbf{v}_{SSB} = \mathbf{v}_{WT}(\mathbf{h}_s, \mathbf{h}_e)$. Thus we have $|\mathbf{h}_s^\dagger \mathbf{v}_{SSB}|^2 \geq |\mathbf{h}_e^\dagger \mathbf{v}_{SSB}|^2$. With this, it is easy to see that $\frac{d(f(p))}{dp} \geq 0$, which implies that $f(p)$ is nondecreasing w.r.t. p . Thus the power p is chosen as $p_{SSB} = \min(P, Q/|\mathbf{h}_p^\dagger \mathbf{v}_{SSB}|^2)$. Although the SSB is suboptimal in nature, we will establish the condition under which it achieves optimality.

Proposition 5.10. The SSB is optimal if Q is sufficiently large such that $Q \geq P|\mathbf{h}_p^\dagger \mathbf{v}_{WT}(\mathbf{h}_s, \mathbf{h}_e)|^2$.

Proof. $Q \geq P|\mathbf{h}_p^\dagger \mathbf{v}_{WT}(\mathbf{h}_s, \mathbf{h}_e)|^2$ implies that $\mathbf{S}_{WT} = P\mathbf{v}_{WT}(\mathbf{h}_s, \mathbf{h}_e)\mathbf{v}_{WT}(\mathbf{h}_s, \mathbf{h}_e)^\dagger$ is the solution of the SSB, which also satisfies the interference power constraint (6.17). Then it is clear that $\mathbf{S}_{WT}$ is a feasible solution for *Problem 5.3*. We denote $\mathbf{S}_{\text{opt}}$ as the optimal transmit covariance matrix for *Problem 5.3*. Since the feasible set of *Problem*

5.3 is a subset of that of the conventional wiretap channel, the objective value achieved by $\mathbf{S}_{\text{opt}}$ cannot be greater than that achieved by $\mathbf{S}_{WT}$. Therefore, in this case, $\mathbf{S}_{WT}$ is the global optimal solution. $\square$

5.3.2 Projected Secret Beamforming

The main idea of the second scheme is to impose zero-forcing criterion to the primary channel such that the interference power at the PU-Rx is completely removed. Specifically, we project both $\mathbf{h}_s$ and $\mathbf{h}_e$ onto the null space of the primary channel $\mathbf{h}_p$

$$\tilde{\mathbf{h}}_s = (\mathbf{I} - \check{\mathbf{h}}_p \check{\mathbf{h}}_p^\dagger) \mathbf{h}_s, \quad (5.41)$$

$$\tilde{\mathbf{h}}_e = (\mathbf{I} - \check{\mathbf{h}}_p \check{\mathbf{h}}_p^\dagger) \mathbf{h}_e, \quad (5.42)$$

where $\tilde{\mathbf{h}}_s$ and $\tilde{\mathbf{h}}_e$ are the new secondary and eavesdropper channels after projection, respectively. Then, we choose $\mathbf{v}_{PSB} = \mathbf{v}_{WT}(\tilde{\mathbf{h}}_s, \tilde{\mathbf{h}}_e)$ and $p_{PSB} = P$, which correspond to secret beamforming as in the conventional MISO wiretap channel with the channel pair $(\tilde{\mathbf{h}}_s, \tilde{\mathbf{h}}_e)$. The scheme is thus referred as *projected secret beamforming* (PSB). It can be verified that the interference is indeed 0. Intuitively, $\mathbf{v}_{PSB}$ lies in the 2-D subspace spanned by $\tilde{\mathbf{h}}_s$ and $\tilde{\mathbf{h}}_e$, both of which are orthogonal to $\mathbf{h}_p$ and hence, $\mathbf{v}_{PSB}$ is also orthogonal to $\mathbf{h}_p$. Therefore, in the PSB, the interference power constraint is always satisfied for any $Q \geq 0$. Moreover, since

$$\mathbf{h}_e^\dagger \mathbf{v}_{PSB} = \tilde{\mathbf{h}}_e^\dagger \mathbf{v}_{PSB} + \mathbf{h}_e^\dagger \check{\mathbf{h}}_p \check{\mathbf{h}}_p^\dagger \mathbf{v}_{PSB} = \tilde{\mathbf{h}}_e^\dagger \mathbf{v}_{PSB}, \quad (5.43)$$

perfect secrecy is also achieved as it is ensured by the secret beamforming.

Remark. It is noted that the ZF criterion has also been used as a potentially suboptimal criterion in the conventional CRN to null out the primary channel [53].

5.3.3 Projected Cognitive Beamforming

Similar to the PSB, the third scheme is also based on the ZF criterion. However, it targets at the eavesdropper so as to completely null out the eavesdropper channel. Specifically, we project both $\mathbf{h}_s$ and $\mathbf{h}_p$ onto the null space of the eavesdropper channel

$$\tilde{\mathbf{h}}_s = \left(\mathbf{I} - \check{\mathbf{h}}_e \check{\mathbf{h}}_e^\dagger \right) \mathbf{h}_s, \quad (5.44)$$

$$\tilde{\mathbf{h}}_p = \left(\mathbf{I} - \check{\mathbf{h}}_e \check{\mathbf{h}}_e^\dagger \right) \mathbf{h}_p, \quad (5.45)$$

where $\tilde{\mathbf{h}}_s$ and $\tilde{\mathbf{h}}_p$ are the new secondary and primary channels after projection, respectively. Then, we choose $\mathbf{v}_{PCB} = \mathbf{v}_{CR}(\tilde{\mathbf{h}}_s, \tilde{\mathbf{h}}_p)$ and $p_{PCB} = P$, which correspond to cognitive beamforming as in the conventional MISO CR channel with the channel pair $(\tilde{\mathbf{h}}_s, \tilde{\mathbf{h}}_p)$. The scheme is thus referred as *projected cognitive beamforming* (PCB). It can be verified that the received SNR at the eavesdropper is indeed 0. Intuitively, $\mathbf{v}_{PCB}$ lies in the 2-D subspace spanned by $\tilde{\mathbf{h}}_s$ and $\tilde{\mathbf{h}}_p$, both of which are orthogonal to $\mathbf{h}_e$ and hence, $\mathbf{v}_{PCB}$ is also orthogonal to $\mathbf{h}_e$. Therefore, in the PCB, the eavesdropper is always nulled out. Furthermore, since

$$\mathbf{h}_p^\dagger \mathbf{v}_{PCB} = \tilde{\mathbf{h}}_p^\dagger \mathbf{v}_{PCB} + \mathbf{h}_p^\dagger \check{\mathbf{h}}_e \check{\mathbf{h}}_e^\dagger \mathbf{v}_{PCB} = \tilde{\mathbf{h}}_p^\dagger \mathbf{v}_{PCB}, \quad (5.46)$$

the interference power constraint is also satisfied as it is ensured by the cognitive beamforming.

Lastly, the condition under which the PCB achieves optimality is shown in the following proposition.

Proposition 5.11. The PCB is optimal if the complete nulling of the eavesdropper is further imposed, i.e., $\mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e = 0$.

Proof. With $\mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e = 0$, (6.15) can be written as

$$\begin{aligned} \frac{1 + \mathbf{h}_s^\dagger \mathbf{S} \mathbf{h}_s}{1 + \mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e} &= 1 + \left(\tilde{\mathbf{h}}_s^\dagger + \mathbf{h}_s^\dagger \check{\mathbf{h}}_e \check{\mathbf{h}}_e^\dagger \right) \mathbf{S} \left(\tilde{\mathbf{h}}_s + \check{\mathbf{h}}_e \check{\mathbf{h}}_e^\dagger \mathbf{h}_s \right) \\ &= 1 + \tilde{\mathbf{h}}_s^\dagger \mathbf{S} \tilde{\mathbf{h}}_s, \end{aligned} \quad (5.47)$$

and (6.17) can be written as

$$\left(\tilde{\mathbf{h}}_p^\dagger + \mathbf{h}_p^\dagger \check{\mathbf{h}}_e \check{\mathbf{h}}_e^\dagger \right) \mathbf{S} \left(\tilde{\mathbf{h}}_p + \check{\mathbf{h}}_e \check{\mathbf{h}}_e^\dagger \mathbf{h}_p \right) \leq Q \quad (5.48)$$

$$\tilde{\mathbf{h}}_p^\dagger \mathbf{S} \tilde{\mathbf{h}}_p \leq Q. \quad (5.49)$$

Then *Problem 5.3* becomes

$$\max_{\mathbf{S} \succeq 0} \quad 1 + \tilde{\mathbf{h}}_s^\dagger \mathbf{S} \tilde{\mathbf{h}}_s \quad (5.50)$$

$$\text{s.t.} \quad \text{tr}(\mathbf{S}) \leq P \quad (5.51)$$

$$\tilde{\mathbf{h}}_p^\dagger \mathbf{S} \tilde{\mathbf{h}}_p \leq Q \quad (5.52)$$

$$\mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e = 0. \quad (5.53)$$

Notice that $\mathbf{S}_{PCB} = P \mathbf{v}_{CR}(\tilde{\mathbf{h}}_s, \tilde{\mathbf{h}}_e) \mathbf{v}_{CR}(\tilde{\mathbf{h}}_s, \tilde{\mathbf{h}}_e)^\dagger$ obtained by the PCB is the same as the above problem without the constraint (5.53). Since $\mathbf{h}_e^\dagger \mathbf{S}_{PCB} \mathbf{h}_e = P |\mathbf{h}_e^\dagger \mathbf{v}_{PCB}|^2 = 0$, then $\mathbf{S}_{PCB}$ is optimal for the above problem, and hence *Problem 5.3* with $\mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e = 0$. $\square$

5.3.4 Computational Complexity

As compared to the optimal solutions proposed in Section 5.2 which can only be solved numerically through a number of iterations, the suboptimal schemes proposed in this section can all be computed in closed forms by some simple arithmetic operations. It can be seen that to obtain each of these closed form solutions, the only operation that scaled with the problem size, i.e., N , is the computation of vector inner product. Other

operations, which contain evaluating elementary functions and making comparisons, are of fixed number and do not scale with N . Therefore, the arithmetic complexity of them are of the same complexity, of the order $\mathcal{O}(N)$.

5.4 Numerical Results and Discussions

In this section, computer simulation results are presented to evaluate the performance of the proposed optimal and suboptimal approaches. Unless otherwise stated, it is assumed that the SU-Tx is equipped with $N = 3$ antennas, and that the entries of the channel vectors $\mathbf{h}_s$, $\mathbf{h}_p$ and $\mathbf{h}_e$ are generated by independent CSCG random variables distributed as $\mathcal{CN}(0, 1)$. Monte Carlo simulations with 10,000 randomly generated channel-triplets $(\mathbf{h}_s, \mathbf{h}_p, \mathbf{h}_e)$ are performed and the average achievable rates are plotted versus a range of transmit power P or interference temperature limit Q , where the units of P and Q are defined in dB w.r.t. the noise power. The basic Matlab code for the simulation can be found in Appendix H.

5.4.1 Optimal Solutions

Figure 5.3 compares the secrecy capacity of the secure CR channels with the capacity/secret capacity achieved by the conventional CR and wiretap channels. For the CR channels, the interference temperature limit is set to be $Q = 0$ dB. It is observed that both the SDP and the ACRN approaches achieve the same secrecy capacity since they are both optimal. It is also observed that the secrecy capacity of the MISO CR channel is lower than the capacity/secret capacity of the other two channels due to the additional secrecy constraint or interference power constraint.

Next, we show the secrecy capacity comparison of the secure MISO and SISO (i.e., the SU-Tx has only one antenna) CR channels at $Q = 0$ dB for different number of transmit antennas in Fig. 5.4, for different variance of the eavesdropper channel σ_e^2

Figure 5.3: Capacity comparison of the secure CR channels with the conventional CR channels and the conventional wiretap channels at $Q = 0$ dB.

Figure 5.4: Secrecy capacity comparison of the secure MISO and SISO CR channels at $Q = 0$ dB for different number of transmit antennas.

Figure 5.5: Secrecy capacity comparison of the secure MISO and SISO CR channels at $Q = 0$ dB for different variance of the eavesdropper channel.

Figure 5.6: Secrecy capacity comparison of the secure MISO and SISO CR channels at $Q = 0$ dB for different variance of the primary channel.

in Fig. 5.5, and for different variance of the primary channel σ_p^2 in Fig. 5.6. From these figures, it is observed that the use of multiple antennas at the SU-Tx can improve both the secure and cognitive transmission substantially. Furthermore, as it is known for the SISO case, for secure transmission, positive secrecy capacity can be obtained only when the secondary channel is strictly stronger than the eavesdropper channel [173]; for cognitive transmission, when the interference temperature limit is low, the capacity is limited by the interference power constraint no matter how much transmit power is allowed [133]. However, in the MISO case, the SU-Tx can use beamforming to adapt its transmission so as to avoid harmful interference to the PU while maximizing the secrecy capacity of its own transmission. As seen from Fig. 5.4, the more the number of transmit antennas, the more the degree of freedom and hence the higher the secrecy rate. In addition, it is observed that by using beamforming positive secrecy rate can be achieved even when the eavesdropper channel is on average stronger than the secondary channel as evident from Fig. 5.5, and that the use of multiple antennas allows the secrecy capacity to increase substantially with the increase in the transmit power at this low value of Q even when primary channel is stronger as evident from Fig. 5.6.

5.4.2 Suboptimal Solutions

Figures 5.7 and 5.8 show the achievable secrecy rates of the three suboptimal schemes. The results are also compared with the secrecy capacity obtained using the optimal SDP approach. The secrecy rates are evaluated at $Q = 20$ dB and -20 dB for Figs. 5.7 and 5.8, respectively. Note that $Q = 20$ dB corresponds to looser protection to the PU while $Q = -20$ dB means more stringent protection.

In Fig. 5.7, it is observed that the achievable secrecy rate of the SSB is close to the secrecy capacity at the low transmit power region and deviates from it at the high transmit power region, which is in accordance with Proposition 5.10. It can also be

Figure 5.7: Performance comparison of the achievable secrecy rates by the SSB, PSB and PCB at $Q = 20$ dB.

seen from Fig. 5.7 that the PSB achieves the lowest secrecy rate and in contrast, the PCB is more effective than the PSB. Note that when Q is large, the PU can tolerate a large amount of interference and the interference power constraint is almost inactive. However, the PSB allocates the power into the projected channels (null to the PU) so as to enforce zero interference. This seems redundant and secret beamforming using the projected channels does not necessarily help to improve the secrecy rates. In this case, projecting onto the null space of the eavesdropper channel as done by the PCB is more effective in enhancing the secrecy rates.

In Fig. 5.8, it is observed that the SSB fails when $Q = -20$ dB. When Q is very small, the resulting power allocated by the SSB will be solely determined by $Q/|\mathbf{h}_p^\dagger \mathbf{v}_{WT}(\mathbf{h}_s, \mathbf{h}_e)|^2$, which is close to zero regardless of the transmit power. Hence, the secrecy rate achieved by the SSB is close to zero for the whole range of transmit power P . It is also observed that both the PSB and the PCB achieve secrecy rates close to the secrecy capacity and the PSB performs slightly better than the PCB. Since

Figure 5.8: Performance comparison of the achievable secrecy rates by the SSB, PSB and PCB at $Q = -20$ dB.

PSB always completely nulls out the interference, it is reasonable that PSB achieves close-to-optimal performance at this low interference temperature limit.

In Fig. 5.9, we compare the achievable secrecy rates of the three suboptimal schemes with the secrecy capacity obtained using the optimal SDP approach under a range of interference temperature limit Q from -20 dB to 20 dB and at the transmit power of $P = 10$ dB. The SSB is observed to fail at the low Q region and approach the optimal solution at the high Q region, which is also consistent with Proposition 5.10. It is also observed that the secrecy rate achieved by the PSB is almost insensitive to different interference temperature limits Q since it always forces the interference to be zero regardless of the Q values. It is further observed that the PCB exhibits a near-capacity performance for all the Q values.

In Fig. 5.10-5.12, we compare the achievable secrecy rates of the three suboptimal schemes with the secrecy capacity at $Q = 0$ dB for different channel conditions. The variance of the channel $(\mathbf{h}_s, \mathbf{h}_p, \mathbf{h}_e)$ are taken as $(\sigma_s^2, \sigma_p^2, \sigma_e^2)$ with the corresponding

Figure 5.9: Performance comparison of the achievable secrecy rates by the SSB, PSB and PCB at $P = 10$ dB.

Figure 5.10: Performance comparison of the achievable secrecy rates by various schemes at $Q = 0$ dB for $(2, 1, 1)$.

Figure 5.11: Performance comparison of the achievable secrecy rates by various schemes at $Q = 0$ dB for $(1, 1, 2)$.

Figure 5.12: Performance comparison of the achievable secrecy rates by various schemes at $Q = 0$ dB for $(1, 2, 1)$.

values indicated on the figure legend. These three figures represent the cases when the secondary channel, the eavesdropper channel, and the primary channel is stronger, respectively. It is observed that under the comparatively stringent interference power constraint $Q = 0$ dB for all these channel conditions, the PCB achieves the highest secrecy rate followed by the PSB. The SSB achieves the lowest secrecy rate and it becomes saturated at the high transmit power region because it is limited by the interference temperature limit when the transmit power increases to certain level.

5.5 Conclusions

In this chapter, the secrecy capacity of the secure MISO CR channel has been characterized. Two numerical approaches have been proposed to compute the secrecy capacity and the capacity-achieving transmit covariance matrix. By exploring the inherent convexity, the first approach has transformed the original quasiconvex problem into a single SDP, which can be solved efficiently. By exploring the relationship between the secure CRN with the conventional CRN, the second approach has transformed the original problem into a sequence of optimization problems related to the conventional CRN, which has helped to prove that beamforming is the optimal strategy. In addition, three suboptimal schemes have been proposed to tradeoff between secrecy rate and computational complexity. Finally, simulation results have shown that the three suboptimal schemes can approach the optimal solution under certain conditions.

Chapter 6

Secure Transmission in Spectrum Sharing with Imperfect CSI

The results derived for secure MISO CR channel in Chapter 5 is based on the assumption that perfect CSI of all the relevant channels is available at the SU-Tx. While the results presented can serve as the upper bounds for the secure transmission in the MISO CRN since, this CSI may not be obtained perfectly in practice due to the channel estimation and quantization errors, and the loose cooperation between the SU and the PU. This motivates the study of this chapter, which takes the first attempt to address the secure communication in the MISO CRNs in the context of imperfect knowledge of all the relevant channels at the SU-Tx. In such cases, robust design techniques have to be identified so that the cognitive and secure transmission strategy is less sensitive to the uncertainty in the CSI.

In this chapter, the worst-case approach as introduced in Section 2.2.2 to address imperfect CSI is adopted. Our objective is to design the transmission strategy under Gaussian signaling without preprocessing of information such that the secrecy rate of the secure MISO CRN is maximized and at the same time the PU-Rx is sufficiently protected under the interference power constraint for all the possible realizations of the CSI within the uncertainty sets. The design is formulated as a maximin non-convex

semi-infinite optimization problem, which is difficult to solve in its direct form. Similar to Chapter 5, two approaches are presented to find the optimal solution. In the first approach, we construct an ACRN with two PU-Rxs but no ED-Rx and formulate the associated robust design problem as a maximin convex semi-infinite program. We show that the new problem can be transformed into a convex semi-definite program and solved efficiently. Then, we solve the original problem by transforming it into a sequence of robust design problems in the ACRN through exploring the relationship between them. The second approach exploits the inherent convexity of the original problem and transforms it into a single convex semi-definite program, which significantly reduces the computational complexity. Furthermore, a few beamforming solutions for the ease of implementation are proposed. Finally, the performance of the optimal and suboptimal algorithms is evaluated through computer simulations.

The rest of the chapter is organized as follows. In Section 6.1, we describe the system model of the secure MISO CRN with CSI uncertainties at the SU-Tx and formulate the optimization problem to maximize the secrecy rate under the joint transmit and interference power constraints for all the channel realizations within the uncertainty sets. Optimal and suboptimal algorithms to obtain the transmission strategies are proposed in Sections 6.2 and 6.3, respectively. The performance of the proposed algorithms is evaluated through simulations in Section 6.4. Finally, conclusion is drawn in Section 6.5.

6.1 System Model and Problem Formulation

Similar to Chapter 5, we are interested in a secure MISO CR channel as shown in Fig. 6.1. The channel responses of the secondary channel, primary channel and eavesdropper channel, are denoted by $\mathbf{h}_s$, $\mathbf{h}_p$ and $\mathbf{h}_e$, respectively, where $\mathbf{h}_s, \mathbf{h}_p, \mathbf{h}_e \in \mathbb{C}^{N \times 1}$, N is the number of transmit antennas at the SU-Tx. However, in this chapter, we assume that the SU-Tx does not know the exact channel realizations of all the three channels but

Figure 6.1: System model for the secure MISO CRN.

instead it has a knowledge of the uncertainty regions containing the actual channels, which are assumed to be described by the following ellipsoids:

$$\mathcal{H}_s = \{\mathbf{h}_s | \mathbf{h}_s = \hat{\mathbf{h}}_s + \Delta\mathbf{h}_s, \Delta\mathbf{h}_s^\dagger \mathbf{W}_s \Delta\mathbf{h}_s \leq 1\}, \quad (6.1)$$

$$\mathcal{H}_p = \{\mathbf{h}_p | \mathbf{h}_p = \hat{\mathbf{h}}_p + \Delta\mathbf{h}_p, \Delta\mathbf{h}_p^\dagger \mathbf{W}_p \Delta\mathbf{h}_p \leq 1\}, \quad (6.2)$$

$$\mathcal{H}_e = \{\mathbf{h}_e | \mathbf{h}_e = \hat{\mathbf{h}}_e + \Delta\mathbf{h}_e, \Delta\mathbf{h}_e^\dagger \mathbf{W}_e \Delta\mathbf{h}_e \leq 1\}, \quad (6.3)$$

where $\hat{\mathbf{h}}_s$, $\hat{\mathbf{h}}_p$ and $\hat{\mathbf{h}}_e$ are the erroneous estimates received at the SU-Tx; $\Delta\mathbf{h}_s$, $\Delta\mathbf{h}_p$, $\Delta\mathbf{h}_e$ are the corresponding channel estimation errors; $\mathbf{W}_s, \mathbf{W}_p, \mathbf{W}_e \succ 0$ determine the shape and size of each uncertainty region.

The estimate $\hat{\mathbf{h}}_s$, $\hat{\mathbf{h}}_p$ and $\hat{\mathbf{h}}_e$ can be obtained in the way as mentioned in Chapter 5. However, these estimates are imperfect because of various uncertainties such as the errors in the transmission through the feedback channel, the quantization error due to the limited capacity of the feedback channel, or the outdated feedback due to the time-varying nature of wireless environments. Furthermore, besides the errors mentioned above, the estimation of $\mathbf{h}_p$ can be even more erroneous due to the limited cooperation with the PU. Hence, we consider that the SU-Tx only knows the erroneous estimates of the channels and wishes to ensure secure and cognitive transmission for the channel realizations that fall within the uncertainty regions around the estimates.

These uncertainty regions show the extent to which the SU-Tx wants the secure and cognitive transmission to be. Larger uncertainty regions indicate that the SU-Tx takes a more conservative approach in securing the confidential information and protecting the PU.

In the presence of the presumed uncertainties in the CSI, the objective is to characterize the maximum secrecy rate at which the information can be reliably transmitted from the SU-Tx to the SU-Rx but is kept secret from the ED-Rx, at the same time the resulting interference power received at the PU-Rx is kept below the interference temperature limit for all the possible realizations of the CSI within the uncertainty sets. The communication scenario of interest here can be considered as a special case of a *compound wiretap channel* [202]. Such a channel captures the transmission scenario over a wiretap channel with a number of possible channel realizations and secure transmission in terms of both reliability and secrecy constraints should be guaranteed no matter which realization it takes. When the channel realizations of the secondary channel and eavesdropper channel are $\mathbf{h}_s$ and $\mathbf{h}_e$, the signals received at the SU-Rx and the ED-Rx can be written as

$$y_m(\mathbf{h}_s) = \mathbf{h}_s^\dagger \mathbf{x}_m + w_m, \quad m = 1, \dots, n \quad (6.4)$$

$$z_m(\mathbf{h}_e) = \mathbf{h}_e^\dagger \mathbf{x}_m + v_m, \quad m = 1, \dots, n \quad (6.5)$$

respectively, where m is the time index; $\mathbf{x}_m \in \mathbb{C}^{N \times 1}$ is the signal transmitted from the SU-Tx; w_m and v_m are the zero-mean unit-variance CSCG noise components at the SU-Rx and the ED-Rx, respectively.

The channel input is subject to the following transmit and interference power constraints,

$$\mathbb{E}\{\mathbf{x}\mathbf{x}^\dagger\} \leq P, \quad (6.6)$$

$$\mathbf{h}_p^\dagger \mathbb{E}\{\mathbf{x}^\dagger \mathbf{x}\} \mathbf{h}_p \leq Q, \quad \forall \mathbf{h}_p \in \mathcal{H}_p. \quad (6.7)$$

Note that since the SU-Tx does not know the exact channel realization of the primary channel, to protect the PU at all times, the interference power constraint should be satisfied for all the possible realizations within the uncertainty set $\mathcal{H}_p$.

In general, the characterization of the secrecy capacity for the general compound wiretap channel is an open research topic. In this chapter, instead of characterizing the secrecy capacity for this channel, we restrict our attention to the case of Gaussian signaling with no preprocessing of information. It is pointed out that although such restriction achieves secrecy capacity for the degraded MIMO compound wiretap channel [202], it is potentially suboptimal for the general multi-antenna compound wiretap channels.

Corollary 6.1. Under Gaussian signaling with no preprocessing of information, the maximum achievable secrecy rate of the secure MISO CR channel with channel uncertainties described in (6.1)-(6.3) can be found as the maximum objective value of the following optimization problem involving transmit covariance matrix $\mathbf{S} = \mathbb{E}\{\mathbf{x}\mathbf{x}^\dagger\}$,

Problem 6.2.

$$\max_{\mathbf{S} \succeq 0} \min_{\mathbf{h}_s \in \mathcal{H}_s, \mathbf{h}_e \in \mathcal{H}_e} \log_2 (1 + \mathbf{h}_s^\dagger \mathbf{S} \mathbf{h}_s) - \log_2 (1 + \mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e) \quad (6.8)$$

$$\text{s.t.} \quad \text{tr}(\mathbf{S}) \leq P \quad (6.9)$$

$$\mathbf{h}_p^\dagger \mathbf{S} \mathbf{h}_p \leq Q, \forall \mathbf{h}_p \in \mathcal{H}_p. \quad (6.10)$$

Proof. For a general discrete memoryless compound wiretap channel, it has been shown in [202] that there exists a code to achieve the following secrecy rate⁹

$$R_s = \max_{\mathbf{p}(\mathbf{u}, \mathbf{x})} \min_{\mathbf{h}_s \in \mathcal{H}_s, \mathbf{h}_e \in \mathcal{H}_e} I(\mathbf{u}; y(\mathbf{h}_s)) - I(\mathbf{u}; z(\mathbf{h}_e)), \quad (6.11)$$

where the auxiliary random variable $\mathbf{u}$ satisfying the Markov relation $\mathbf{u} \rightarrow \mathbf{x} \rightarrow$

⁹The details of the coding strategy to achieve this secrecy rate can be found in [202]. The discussion on the practical code design for the wiretap channel can be found in [60] and the references therein.

$(y(\mathbf{h}_s), z(\mathbf{h}_e))$. By setting $\mathbf{u} = \mathbf{x}$, we have the following achievable secrecy rate

$$R_s = \max_{\mathbf{p}(\mathbf{x})} \min_{\mathbf{h}_s \in \mathcal{H}_s, \mathbf{h}_e \in \mathcal{H}_e} I(\mathbf{x}; y(\mathbf{h}_s)) - I(\mathbf{x}; z(\mathbf{h}_e)). \quad (6.12)$$

This result can also be extended to a continuous-alphabet channel with average cost constraint. Hence, by restricting the channel input to be a Gaussian code, i.e., $\mathbf{u} = \mathbf{x} \sim \mathcal{CN}(0, \mathbf{S})$, then, under the general matrix covariance constraint $\mathbf{S} \preceq \mathbf{K}$, where $\mathbf{K} \succeq 0$, we obtain the following achievable secrecy rate

$$R_s(\mathbf{K}) = \max_{0 \preceq \mathbf{S} \preceq \mathbf{K}} \min_{\mathbf{h}_s \in \mathcal{H}_s, \mathbf{h}_e \in \mathcal{H}_e} \log_2 (1 + \mathbf{h}_s \mathbf{S} \mathbf{h}_s^\dagger) - \log_2 (1 + \mathbf{h}_e \mathbf{S} \mathbf{h}_e^\dagger). \quad (6.13)$$

Similar to Chapter 5, we define the compact set as $\mathcal{S} = \{\mathbf{K} \succeq 0 \mid \text{tr}(\mathbf{K}) \leq P, \mathbf{h}_p^\dagger \mathbf{K} \mathbf{h}_p \leq Q, \forall \mathbf{h}_p \in \mathcal{H}_p\}$, which corresponds to the set of covariance matrices satisfying both the transmit power constraint and worst-case interference power constraint. The maximum achievable secrecy rate under Gaussian signaling without preprocessing of information for the secure MISO CR channel with channel uncertainties is the maximum rate under this compact set constraint $\mathcal{S}$, denoted as $R_s(\mathcal{S})$. Then, from Lemma 1 of [197], we have, for the maximum achievable secrecy rate,

$$R_s(\mathcal{S}) = \max_{\mathbf{K} \in \mathcal{S}} R_s(\mathbf{K}) = \max_{\mathbf{S} \succeq 0, \mathbf{S} \in \mathcal{S}} \min_{\mathbf{h}_s \in \mathcal{H}_s, \mathbf{h}_e \in \mathcal{H}_e} \log_2 (1 + \mathbf{h}_s \mathbf{S} \mathbf{h}_s^\dagger) - \log_2 (1 + \mathbf{h}_e \mathbf{S} \mathbf{h}_e^\dagger). \quad (6.14)$$

□

Corollary 6.1 formulates our main problem of interest. In the rest of the chapter, our objective is to determine the optimal transmit covariance matrix $\mathbf{S}$ to achieve this secrecy rate, which is the maximum rate under the assumption of Gaussian signaling without preprocessing of information at which the information can be sent reliably to the SU-Rx but is kept perfectly secret from the ED-Rx and at the same time the PU-Rx is protected under the interference power constraint for all the possible channel

realizations within the predefined channel uncertainty sets (6.1)-(6.3). We will deal with the following problem due to the monotonicity of the log function:

Problem 6.3.

$$\max_{\mathbf{S} \succeq 0} \min_{\mathbf{h}_s \in \mathcal{H}_s, \mathbf{h}_e \in \mathcal{H}_e} \frac{1 + \mathbf{h}_s^\dagger \mathbf{S} \mathbf{h}_s}{1 + \mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e} \quad (6.15)$$

$$\text{s.t.} \quad \text{tr}(\mathbf{S}) \leq P \quad (6.16)$$

$$\mathbf{h}_p^\dagger \mathbf{S} \mathbf{h}_p \leq Q, \forall \mathbf{h}_p \in \mathcal{H}_p. \quad (6.17)$$

It can be shown that *Problem 6.3* is a maximin optimization of quasiconvex semi-infinite problem since the objective function is quasiconcave [194] and the constraint sets are defined by infinitely many linear constraints due to the uncertainty set $\mathcal{H}_p$. Therefore, *Problem 6.3* is challenging and no immediate algorithm can be applied to it in its direct form. In the next section, we will propose a few algorithms to find the optimal solution based on some equivalent transformations.

6.2 Optimal Solution

Since *Problem 6.3* belongs to the family of quasiconvex optimization problems, we first present an algorithm based on the general approach to conquer quasiconvex problems. However, this method may not be reliable for implementation. Similar to Chapter 5, to overcome it, we present two alternative approaches: namely, ACRN transformation and SDP transformation.

6.2.1 Quasiconvex Optimization Approach

The general approach to quasiconvex optimization is to transform it into its equivalent epigraph form

$$\max_{\mathbf{S} \succeq 0, \tau \geq 0} \tau \quad (6.18)$$

$$\text{s.t.} \quad \text{tr}(\mathbf{S}) \leq P \quad (6.19)$$

$$\mathbf{h}_p^\dagger \mathbf{S} \mathbf{h}_p \leq Q, \forall \mathbf{h}_p \in \mathcal{H}_p \quad (6.20)$$

$$1 + \mathbf{h}_s^\dagger \mathbf{S} \mathbf{h}_s \geq \tau(1 + \mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e), \forall \mathbf{h}_s \in \mathcal{H}_s, \mathbf{h}_e \in \mathcal{H}_e. \quad (6.21)$$

Then the bisection method as shown in Algorithm 4 can be applied to test the feasibility of (6.19), (6.20) and (6.21) instead. However, the feasibility of them cannot be determined directly since each of them corresponds to infinite number of constraints due to the uncertainty sets. Hence, reformulation is needed to transform them into finite number of constraints. Note that the uncertainty sets described in (6.1)-(6.3) are quadratic functions of the channel estimation errors. To resolve the semi-infiniteness of the constraints, the S-Procedure [62] is usually used to convert them into a finite number of convex semi-definite constraints. Since the uncertainties in $\mathbf{h}_s$ and $\mathbf{h}_e$ are constrained separately, we can first perform the S-Procedure w.r.t. the certainty set $\mathcal{H}_s$, and (6.21) is equivalently transformed into

$$\begin{bmatrix} \mathbf{S} + s\mathbf{W}_s & \mathbf{S}\hat{\mathbf{h}}_s \\ \hat{\mathbf{h}}_s^\dagger \mathbf{S} & \mathbf{S}_1 \end{bmatrix} \succeq 0, \forall \mathbf{h}_e \in \mathcal{H}_e, \exists s \geq 0, \quad (6.22)$$

where $\mathbf{S}_1 = \hat{\mathbf{h}}_s^\dagger \mathbf{S} \hat{\mathbf{h}}_s + 1 - \tau(\mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e + 1) - s$. To further resolve the semi-definiteness of $\mathcal{H}_e$, we make use of the following extension of the S-Procedure (Theorem 3.5 in [203]).

Theorem 6.4. The relation

$$\begin{bmatrix} \mathbf{H} & \mathbf{F} + \mathbf{G}\mathbf{X} \\ (\mathbf{F} + \mathbf{G}\mathbf{X})^\dagger & \mathbf{C} + \mathbf{X}^\dagger \mathbf{B} + \mathbf{B}^\dagger \mathbf{X} + \mathbf{X}^\dagger \mathbf{A} \mathbf{X} \end{bmatrix} \succeq 0, \forall \mathbf{I} - \mathbf{X}^\dagger \mathbf{D} \mathbf{X} \succeq 0 \quad (6.23)$$

is valid, if and only if,

$$\exists s \geq 0, \begin{bmatrix} \mathbf{H} & \mathbf{F} & \mathbf{G} \\ \mathbf{F}^\dagger & \mathbf{C} - s\mathbf{I} & \mathbf{B}^\dagger \\ \mathbf{G}^\dagger & \mathbf{B} & \mathbf{A} + s\mathbf{D} \end{bmatrix} \succeq 0. \quad (6.24)$$

Then, according to Theorem 1, (6.22) can be finally reduced to a single convex constraint given by

$$\begin{bmatrix} \mathbf{S} + s\mathbf{W}_s & \mathbf{S}\hat{\mathbf{h}}_s & \mathbf{0}_{N \times N} \\ \hat{\mathbf{h}}_s^\dagger \mathbf{S} & \mathbf{S}_2 & -\tau \hat{\mathbf{h}}_e^\dagger \mathbf{S} \\ \mathbf{0}_{N \times N} & -\tau \mathbf{S}\hat{\mathbf{h}}_e & -\tau \mathbf{S} + e\mathbf{W}_e \end{bmatrix} \succeq 0, \exists s, e \geq 0, \quad (6.25)$$

where $\mathbf{S}_2 = \hat{\mathbf{h}}_s^\dagger \mathbf{S}\hat{\mathbf{h}}_s + 1 - \tau(\hat{\mathbf{h}}_e^\dagger \mathbf{S}\hat{\mathbf{h}}_e + 1) - s - e$. Similarly, (6.20) can also be equivalently transformed into the following single convex constraint

$$\begin{bmatrix} -\hat{\mathbf{h}}_p^\dagger \mathbf{S}\hat{\mathbf{h}}_p + Q - p & -\hat{\mathbf{h}}_p^\dagger \mathbf{S} \\ -\mathbf{S}\hat{\mathbf{h}}_p & -\mathbf{S} + p\mathbf{W}_p \end{bmatrix} \succeq 0, \exists p \geq 0. \quad (6.26)$$

With the help of the S-Procedure and its extension, the constraint sets (6.19), (6.25) and (6.26) are finite and, in fact, they are all linear matrix inequalities (LMIs). As a result, the feasibility problem becomes testing the feasibility of an SDP. As pointed out in Chapter 5, although theoretically feasible, this approach is prone to errors as it is based on numerical feasibility test.

6.2.2 ACRN Transformation

In this subsection, we will first study the optimal robust transmitter design problem for a MISO CRN with two PUs in the case of uncertainties in all the relevant channels. Then, the relationship between this auxiliary CRN and our original system of interest is presented. Finally, an algorithm based on this transformation is proposed.

Consider a CRN with a pair of SU-Tx and SU-Rx and two PU-Rxs as shown in Fig. 6.2. Let $\mathbf{h}_s$, $\mathbf{h}_p$ and $\mathbf{h}_e$ denote the channel responses from the SU-Tx to the SU-Rx, PU-Rx1 and PU-Rx2, respectively. Due to the channel estimation or quantization error and limited cooperation with the PUs, it is assumed that the SU-Tx does not have perfect CSI of all the channels, but that it knows the uncertainty sets within which the

Figure 6.2: System model for the conventional MISO CRN with 2 PUs.

exact CSI belongs to, which is defined by (6.1)-(6.3). The transmission strategy design in the presence of channel uncertainties can be formulated as an optimization problem to find the optimal transmit covariance matrix $\mathbf{S}$ such that the compound capacity, defined as the maximum worst-case rate [149] at which the message can be reliably delivered to the SU-Rx, is achieved, and at the same time the interference received at the PU-Rxs is kept below the predetermined thresholds for all the possible channel realizations within the uncertainty sets. Mathematically, it is given as

Problem 6.5.

$$\max_{\mathbf{S} \succeq 0} \min_{\mathbf{h}_s \in \mathcal{H}_s} \log_2 (1 + \mathbf{h}_s^\dagger \mathbf{S} \mathbf{h}_s) \quad (6.27)$$

$$\text{s.t.} \quad \text{tr}(\mathbf{S}) \leq P \quad (6.28)$$

$$\mathbf{h}_p^\dagger \mathbf{S} \mathbf{h}_p \leq Q, \forall \mathbf{h}_p \in \mathcal{H}_p \quad (6.29)$$

$$\mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e \leq q, \forall \mathbf{h}_e \in \mathcal{H}_e. \quad (6.30)$$

Due to the monotonicity of the log function, *Problem 6.5* is equivalent to

Problem 6.6.

$$\mathcal{G}(q) \triangleq \max_{\mathbf{S} \succeq 0} \min_{\mathbf{h}_s \in \mathcal{H}_s} \mathbf{h}_s^\dagger \mathbf{S} \mathbf{h}_s \quad (6.31)$$

$$\text{s.t.} \quad \text{tr}(\mathbf{S}) \leq P \quad (6.32)$$

$$\mathbf{h}_p^\dagger \mathbf{S} \mathbf{h}_p \leq Q, \forall \mathbf{h}_p \in \mathcal{H}_p \quad (6.33)$$

$$\mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e \leq q, \forall \mathbf{h}_e \in \mathcal{H}_e. \quad (6.34)$$

Note that the maximum objective value of the *Problem 6.6* is denoted as $\mathcal{G}(q)$, which is a function of the interference temperature limit q at the PU-Rx2. It can be easily seen that *Problem 6.6* is a maximin convex semi-infinite program since the objective function is linear and the constraint sets are defined by the intersection of infinite number of convex sets. By taking the epigraph form and performing the S-procedure, we have the following convex problem with finite number of constraints:

Problem 6.7.

$$\max_{\mathbf{S} \succeq 0, t, s, p, e \geq 0} t \quad (6.35)$$

$$\text{s.t.} \quad \text{tr}(\mathbf{S}) \leq P \quad (6.36)$$

$$\begin{bmatrix} \hat{\mathbf{h}}_s^\dagger \mathbf{S} \hat{\mathbf{h}}_s - t - s & \hat{\mathbf{h}}_s^\dagger \mathbf{S} \\ \mathbf{S} \hat{\mathbf{h}}_s & \mathbf{S} + s \mathbf{W}_s \end{bmatrix} \succeq 0 \quad (6.37)$$

$$\begin{bmatrix} -\hat{\mathbf{h}}_p^\dagger \mathbf{S} \hat{\mathbf{h}}_p + Q - p & -\hat{\mathbf{h}}_p^\dagger \mathbf{S} \\ -\mathbf{S} \hat{\mathbf{h}}_p & -\mathbf{S} + p \mathbf{W}_p \end{bmatrix} \succeq 0 \quad (6.38)$$

$$\begin{bmatrix} -\hat{\mathbf{h}}_e^\dagger \mathbf{S} \hat{\mathbf{h}}_e + q - e & -\hat{\mathbf{h}}_e^\dagger \mathbf{S} \\ -\mathbf{S} \hat{\mathbf{h}}_e & -\mathbf{S} + e \mathbf{W}_e \end{bmatrix} \succeq 0. \quad (6.39)$$

Problem 6.7 is an SDP with a linear objective function and LMI constraints. Hence, it can be solved very efficiently by some numerical solvers such as SeDuMi [198].

The relationship between the original secure CR channel with uncertainties and this auxiliary CR channel with uncertainties, i.e., *Problem 6.3* and *Problem 6.6*, is revealed in the following proposition.

Proposition 6.8. Denote $\mathbf{S}^o$ as the optimal covariance matrix of *Problem 6.3* and define $q^o = \max_{\mathbf{h}_e \in \mathcal{H}_e} \mathbf{h}_e \mathbf{S}^o \mathbf{h}_e$. Then, $\mathbf{S}^o$ is also optimal for *Problem 6.6* with $q = q^o$.

Proof. Please refer to Appendix E. □

With this relationship, the following transformation for the original *Problem 6.3* can be obtained:

Proposition 6.9. *Problem 6.3* is equivalent to

Problem 6.10.

$$\max_{q \geq 0} \frac{1 + \mathcal{G}(q)}{1 + q}. \quad (6.40)$$

Proof. Please refer to Appendix F. □

As shown in Appendix G, *Problem 6.10* is an unconstrained quasiconvex optimization problem of a single variable q . Therefore, similar to Chapter 5, the efficient golden section search algorithm can be applied. Note that in this case, at each given q , *Problem 6.7* has to be solved to obtain $\mathcal{G}(q)$. Therefore, the original maximin quasiconvex semi-infinite program is transformed into a sequence of convex optimization problems. Compared to the previous approach, no feasibility test of an SDP is involved and hence this approach is more reliable for implementation.

6.2.3 SDP Transformation

In Chapter 5, we have shown that the capacity-achieving transmission strategy design for the secure MISO CR channel with perfect CSI at the SU-Tx can be solved by transforming it into a single SDP. For *Problem 6.3*, it belongs to the family of generalized linear fraction programs since the objective function is the minimum of the ratio between two linear functions of semidefinite matrix $\mathbf{S}$. Generally, convex transformation does not apply. However, since the uncertainties in $\mathbf{h}_s$ and $\mathbf{h}_e$ are constrained separately, we will show that the convex transformation preserves as in the case of perfect CSI.

Proposition 6.11. *Problem 6.3 is equivalent to Problem 6.12, which is given by*

Problem 6.12.

$$\max_{\hat{\mathbf{S}} \succeq 0, t \geq 0} \min_{\mathbf{h}_s \in \mathcal{H}_s} t + \mathbf{h}_s^\dagger \hat{\mathbf{S}} \mathbf{h}_s \quad (6.41)$$

$$\text{s.t.} \quad t + \mathbf{h}_e^\dagger \hat{\mathbf{S}} \mathbf{h}_e \leq 1, \forall \mathbf{h}_e \in \mathcal{H}_e \quad (6.42)$$

$$\text{tr}(\hat{\mathbf{S}}) - Pt \leq 0 \quad (6.43)$$

$$\mathbf{h}_p^\dagger \hat{\mathbf{S}} \mathbf{h}_p - Qt \leq 0, \forall \mathbf{h}_p \in \mathcal{H}_p, \quad (6.44)$$

and the optimal solution of Problem 6.3 is $\mathbf{S}^* = \hat{\mathbf{S}}^o/t^o$, where $(\hat{\mathbf{S}}^o, t^o)$ is the optimal solution of Problem 6.12.

Proof. We first present a lemma, which is needed for the proof of Proposition 6.11.

Lemma 6.13. At the optimum of Problem 6.12, $(\hat{\mathbf{S}}^o, t^o)$ must satisfy that $t^o + \max_{\mathbf{h}_e \in \mathcal{H}_e} \mathbf{h}_e^\dagger \hat{\mathbf{S}}^o \mathbf{h}_e = 1$.

Proof. First, note that (6.42) is equivalent to $t^o + \max_{\mathbf{h}_e \in \mathcal{H}_e} \mathbf{h}_e^\dagger \hat{\mathbf{S}}^o \mathbf{h}_e \leq 1$. The proof can then be easily shown by contradiction. If we have $t^o + \max_{\mathbf{h}_e \in \mathcal{H}_e} \mathbf{h}_e^\dagger \hat{\mathbf{S}}^o \mathbf{h}_e < 1$ at the optimum, then we can always find a $t = t^o + \Delta t, \Delta t \geq 0$ such that the objective value is increased and the constraints (6.42)-(6.44) are still satisfied. This contradicts the assumption that $(\hat{\mathbf{S}}^o, t^o)$ is the optimal solution. This completes the proof. $\square$

We denote the optimal objective values of Problem 6.3 and Problem 6.12 as f^* and f^o , respectively. The proof can be divided into two parts. First, we will show that Problem 6.12 can achieve an objective value of f^* , i.e., $f^* \leq f^o$. This can be easily verified by showing the pair $(\hat{\mathbf{S}} = \frac{\mathbf{S}^*}{1 + \max_{\mathbf{h}_e \in \mathcal{H}_e} \mathbf{h}_e^\dagger \mathbf{S}^* \mathbf{h}_e}, t = \frac{1}{1 + \max_{\mathbf{h}_e \in \mathcal{H}_e} \mathbf{h}_e^\dagger \mathbf{S}^* \mathbf{h}_e})$ is feasible for Problem 6.12.

Next, we will show that Problem 6.3 can also achieve an objective value of f^o , i.e., $f^* \geq f^o$. Since $(\hat{\mathbf{S}}^o, t^o)$ is the optimal solution of Problem 6.12, it is clear that

$\mathbf{S} = \hat{\mathbf{S}}^o/t^o$ is feasible for *Problem 6.3*. Then, by lemma 6.13, $f^o = t^o + \min_{\mathbf{h}_s \in \mathcal{H}_s} \mathbf{h}_s^\dagger \hat{\mathbf{S}}^o \mathbf{h}_s = \frac{1 + \min_{\mathbf{h}_s \in \mathcal{H}_s} \mathbf{h}_s^\dagger \hat{\mathbf{S}}^o/t^o \mathbf{h}_s}{1 + \max_{\mathbf{h}_e \in \mathcal{H}_e} \mathbf{h}_e^\dagger \hat{\mathbf{S}}^o/t^o \mathbf{h}_e}$ is achievable for *Problem 6.3*. Proposition 6.11 thus follows. $\square$

Problem 6.12 is a linear semi-infinite program, which can be transformed into an SDP by using the S-Procedure as in the previous two approaches.

Problem 6.14.

$$\max_{\hat{\mathbf{S}} \succeq 0, \tau, t, s, p, e \geq 0} \tau \quad (6.45)$$

$$\text{s.t.} \quad \text{tr}(\hat{\mathbf{S}}) - Pt \leq 0 \quad (6.46)$$

$$\begin{bmatrix} \hat{\mathbf{h}}_s^\dagger \hat{\mathbf{S}} \hat{\mathbf{h}}_s + t - \tau - s & \hat{\mathbf{h}}_s^\dagger \hat{\mathbf{S}} \\ \hat{\mathbf{S}} \hat{\mathbf{h}}_s & \hat{\mathbf{S}} + s \mathbf{W}_s \end{bmatrix} \succeq 0 \quad (6.47)$$

$$\begin{bmatrix} -\hat{\mathbf{h}}_p^\dagger \hat{\mathbf{S}} \hat{\mathbf{h}}_p + tQ - p & -\hat{\mathbf{h}}_p^\dagger \hat{\mathbf{S}} \\ -\hat{\mathbf{S}} \hat{\mathbf{h}}_p & -\hat{\mathbf{S}} + p \mathbf{W}_p \end{bmatrix} \succeq 0 \quad (6.48)$$

$$\begin{bmatrix} -\hat{\mathbf{h}}_e^\dagger \hat{\mathbf{S}} \hat{\mathbf{h}}_e - t + 1 - e & -\hat{\mathbf{h}}_e^\dagger \hat{\mathbf{S}} \\ -\hat{\mathbf{S}} \hat{\mathbf{h}}_e & -\hat{\mathbf{S}} + e \mathbf{W}_e \end{bmatrix} \succeq 0. \quad (6.49)$$

Compared to the Virtual CRN transformation, instead of solving a sequence of SDPs, this approach only requires to solve a single SDP, and hence the computational complexity is substantially reduced.

6.3 Suboptimal Solutions

Although the optimal solution can be computed by the numerical approaches proposed in the previous section, the structure of the optimal solution, whether being beamforming or spatial multiplexing, is not yet known. From the practical implementation point of view, beamforming is preferred since it greatly simplifies the code design and the scalar wiretap channel code can be used. Nevertheless, finding the exact robust solution under the beamforming constraint (i.e., $\text{rank}(\mathbf{S}) = 1$) may not be computationally

tractable and usually some approximations have to be involved¹⁰. Therefore, in this section, we present a few heuristic beamforming solutions, the performance of which will be evaluated in the next section.

Before we present the heuristic beamforming solutions, we first show how the secrecy rate is computed for a given feasible beamforming vector. Note that when a beamforming vector is chosen as $\mathbf{w}$, the secrecy rate becomes $\log_2 \frac{1 + \min_{\mathbf{h}_s \in \mathcal{H}_s} |\mathbf{w}^\dagger \mathbf{h}_s|^2}{1 + \max_{\mathbf{h}_e \in \mathcal{H}_e} |\mathbf{w}^\dagger \mathbf{h}_e|^2}$. According to the triangular inequality and the Cauchy-Schwarz inequality, we have

$$|\mathbf{w}^\dagger \mathbf{h}_s| = |\mathbf{w}^\dagger \hat{\mathbf{h}}_s + \mathbf{w}^\dagger \Delta \mathbf{h}_s| \quad (6.50)$$

$$\geq |\mathbf{w}^\dagger \hat{\mathbf{h}}_s| - |\mathbf{w}^\dagger \mathbf{W}_s^{-1/2} \mathbf{W}_s^{1/2} \Delta \mathbf{h}_s| \quad (6.51)$$

$$\geq |\mathbf{w}^\dagger \hat{\mathbf{h}}_s| - \|\mathbf{w}^\dagger \mathbf{W}_s^{-1/2}\| \|\mathbf{W}_s^{1/2} \Delta \mathbf{h}_s\| \quad (6.52)$$

$$\geq |\mathbf{w}^\dagger \hat{\mathbf{h}}_s| - \|\mathbf{w}^\dagger \mathbf{W}_s^{-1/2}\|. \quad (6.53)$$

The minimum is $\min_{\mathbf{h}_s \in \mathcal{H}_s} |\mathbf{w}^\dagger \mathbf{h}_s| = |\mathbf{w}^\dagger \hat{\mathbf{h}}_s| - \|\mathbf{w}^\dagger \mathbf{W}_s^{-1/2}\|$ and it is achieved when $\Delta \mathbf{h}_s = -\frac{\mathbf{W}_s^{-1} \mathbf{w}}{\|\mathbf{w}^\dagger \mathbf{W}_s^{-1/2}\|} \frac{\mathbf{w}^\dagger \hat{\mathbf{h}}_s}{|\mathbf{w}^\dagger \hat{\mathbf{h}}_s|}$. Similarly, we have $\max_{\mathbf{h}_e \in \mathcal{H}_e} |\mathbf{w}^\dagger \mathbf{h}_e| = |\mathbf{w}^\dagger \hat{\mathbf{h}}_e| + \|\mathbf{w}^\dagger \mathbf{W}_e^{-1/2}\|$. The secrecy rate based on the feasible beamforming vector $\mathbf{w}$ is given as

$$\log_2 \frac{1 + \left(|\mathbf{w}^\dagger \hat{\mathbf{h}}_s| - \|\mathbf{w}^\dagger \mathbf{W}_s^{-1/2}\| \right)^2}{1 + \left(|\mathbf{w}^\dagger \hat{\mathbf{h}}_e| + \|\mathbf{w}^\dagger \mathbf{W}_e^{-1/2}\| \right)^2}. \quad (6.54)$$

One common approach to tackle the untractable beamforming problem is to solve a relaxed problem (i.e., dropping the rank-one constraint) and then use randomization techniques to generate an approximate beamforming solution based on the relaxed one [204, 205]. This suggests that we may solve the original problem by *Problem 6.12* and then generate an approximate solution using some randomization techniques. However, due to the complex forms of the constraints in *Problem 6.12*, conventional

¹⁰It is pointed out that when the number of antennas is large, it is possible to find the transmit directions which are favorable towards the SU-Rx and at the same time are null to both the eavesdropper and primary channels even though there are uncertainties involved. Hence, simple beamforming strategy can be used.

randomization techniques do not apply, and it is also likely to be complex to develop a randomization technique that is suitable to our problem. Besides, it is still unknown whether such an approximation is tight or not for our problem. Therefore, in all the beamforming approaches that will be presented subsequently, we will first generate some feasible rank-relaxation solutions (i.e., without the rank-one constraint) and then simply take the principle eigenvector of each solution as the beamforming vector, which can be easily seen to be feasible.

1. *Beamforming by the Exact Robust Solution* (BERS): The first approach is quite straightforward. After obtaining the optimal transmit covariance matrix based on *Problem 6.12*, we simply choose its principle eigenvector as the beamforming vector and calculate the corresponding secrecy rate from (6.54).
2. *Beamforming by the Approximate Robust Solution* (BARS): In this approach, we first consider an approximate robust beamforming design problem based on slightly strengthened uncertainty sets and then obtain the rank-relaxation solution of this approximate robust design problem. Notice that

$$\left(|\mathbf{w}^\dagger \hat{\mathbf{h}}_s| - \|\mathbf{w}^\dagger \mathbf{W}_s^{-1/2}\| \right)^2 \quad (6.55)$$

$$= \mathbf{w}^\dagger \hat{\mathbf{h}}_s \hat{\mathbf{h}}_s^\dagger \mathbf{w} + \mathbf{w}^\dagger \mathbf{W}_s^{-1} \mathbf{w} - 2 \left| \mathbf{w}^\dagger \mathbf{W}_s^{-1/2} \mathbf{W}_s^{1/2} \hat{\mathbf{h}}_s \right| \|\mathbf{w}^\dagger \mathbf{W}_s^{-1/2}\| \quad (6.56)$$

$$\geq \mathbf{w}^\dagger \hat{\mathbf{h}}_s \hat{\mathbf{h}}_s^\dagger \mathbf{w} + \mathbf{w}^\dagger \mathbf{W}_s^{-1} \mathbf{w} - 2 \|\mathbf{w}^\dagger \mathbf{W}_s^{-1/2}\|^2 \left\| \mathbf{W}_s^{1/2} \hat{\mathbf{h}}_s \right\| \quad (6.57)$$

$$= \mathbf{w}^\dagger \mathbf{H}_s \mathbf{w}, \quad (6.58)$$

where $\mathbf{H}_s = \hat{\mathbf{h}}_s \hat{\mathbf{h}}_s^\dagger - \mathbf{W}_s^{-1}(1 + 2\|\mathbf{W}_s^{1/2} \hat{\mathbf{h}}_s\|)$. Hence, we have $\min_{\mathbf{h}_s \in \mathcal{H}_s} |\mathbf{w}^\dagger \mathbf{h}_s|^2 \geq \mathbf{w}^\dagger \mathbf{H}_s \mathbf{w}$. Note that for (6.57) to hold with equality, $\mathbf{W}_s^{-1/2} \mathbf{w}$ has to be linearly dependent on $\mathbf{W}_s^{1/2} \hat{\mathbf{h}}_s$. This condition may not be satisfied in the subsequent optimization w.r.t. $\mathbf{w}$. Hence, this minimum may not be achieved. Similarly, we also have $\max_{\mathbf{h}_e \in \mathcal{H}_e} |\mathbf{w}^\dagger \mathbf{h}_e|^2 \leq \mathbf{w}^\dagger \mathbf{H}_e \mathbf{w}$, where $\mathbf{H}_e = \hat{\mathbf{h}}_e \hat{\mathbf{h}}_e^\dagger + \mathbf{W}_e^{-1}(1 + 2\|\mathbf{W}_e^{1/2} \hat{\mathbf{h}}_e\|) \succ$

0. Therefore, an approximate robust design problem is given as

$$\max_{\mathbf{w}} \frac{1 + \mathbf{w}^\dagger \mathbf{H}_s \mathbf{w}}{1 + \mathbf{w}^\dagger \mathbf{H}_e \mathbf{w}} \quad (6.59)$$

$$\text{s.t.} \quad \|\mathbf{w}\|^2 \leq P \quad (6.60)$$

$$\mathbf{h}_p^\dagger \mathbf{w} \mathbf{w}^\dagger \mathbf{h}_p \leq Q, \forall \mathbf{h}_p \in \mathcal{H}_p. \quad (6.61)$$

Note that (6.59) is only a lower bound to the original objective function. Then, by rank-relaxation ($\mathbf{S} = \mathbf{w} \mathbf{w}^\dagger$) and SDP transformation as in Section 6.2.3, the above problem can be transformed as

$$\max_{\mathbf{S} \succeq 0, t \geq 0} t + \text{tr}(\mathbf{H}_s \hat{\mathbf{S}}) \quad (6.62)$$

$$\text{s.t.} \quad \text{tr}(\hat{\mathbf{S}}) \leq Pt \quad (6.63)$$

$$t + \text{tr}(\mathbf{H}_s \hat{\mathbf{S}}) = 1 \quad (6.64)$$

$$\begin{bmatrix} -\hat{\mathbf{h}}_p^\dagger \hat{\mathbf{S}} \hat{\mathbf{h}}_p + tQ - p & -\hat{\mathbf{h}}_p^\dagger \hat{\mathbf{S}} \\ -\hat{\mathbf{S}} \hat{\mathbf{h}}_p & -\hat{\mathbf{S}} + p \mathbf{W}_p \end{bmatrix} \succeq 0. \quad (6.65)$$

Finally, the beamforming vector is chosen as the principle eigenvector of $\hat{\mathbf{S}}^*/t^*$, where $(\hat{\mathbf{S}}^*, t^*)$ is the optimal solution of the above problem.

3. *Beamforming by the Partially Robust Solution (BPRS)*: Since we consider that both the SU-Rx and the ED-Rx are the secondary users of the CRN, it is natural to assume that the quality of the channel estimates for the secondary and eavesdropper channels are much better than that of the primary channel. In this approach, we simply ignore the channel uncertainties in $\mathbf{h}_s$ and $\mathbf{h}_e$ and choose the beamforming vector as the principle eigenvector of the optimal transmit covariance matrix based on $(\hat{\mathbf{h}}_s, \hat{\mathbf{h}}_e, \mathbf{h}_p)$. Mathematically, this corresponds to solving

the following problem,

$$\max_{\mathbf{S} \succeq 0} \frac{1 + \hat{\mathbf{h}}_s^\dagger \mathbf{S} \hat{\mathbf{h}}_s}{1 + \hat{\mathbf{h}}_e^\dagger \mathbf{S} \hat{\mathbf{h}}_e} \quad (6.66)$$

$$\text{s.t.} \quad \text{tr}(\mathbf{S}) \leq P \quad (6.67)$$

$$\mathbf{h}_p^\dagger \mathbf{S} \mathbf{h}_p \leq Q, \forall \mathbf{h}_p \in \mathcal{H}_p, \quad (6.68)$$

which can be recast as the following SDP by the approach presented in Section 6.2.3,

$$\max_{\mathbf{S} \succeq 0, t \geq 0} t + \hat{\mathbf{h}}_s^\dagger \hat{\mathbf{S}} \hat{\mathbf{h}}_s \quad (6.69)$$

$$\text{s.t.} \quad \text{tr}(\hat{\mathbf{S}}) \leq tP \quad (6.70)$$

$$\hat{\mathbf{h}}_e^\dagger \hat{\mathbf{S}} \hat{\mathbf{h}}_e + t = 1 \quad (6.71)$$

$$\begin{bmatrix} -\hat{\mathbf{h}}_p^\dagger \hat{\mathbf{S}} \hat{\mathbf{h}}_p + tQ - p & -\hat{\mathbf{h}}_p^\dagger \hat{\mathbf{S}} \\ -\hat{\mathbf{S}} \hat{\mathbf{h}}_p & -\hat{\mathbf{S}} + p\mathbf{W}_p \end{bmatrix} \succeq 0. \quad (6.72)$$

6.4 Numerical Results and Discussions

In this section, we evaluate the performance of the proposed algorithms via computer simulations. Each entry of the channel vectors $\hat{\mathbf{h}}_s$, $\hat{\mathbf{h}}_e$ and $\hat{\mathbf{h}}_p$ is i.i.d. as $\mathcal{CN}(0, 1)$. For simplicity, the uncertainty sets of all channels are assumed to be norm-bounded, i.e., $\mathbf{W}_s = \frac{1}{\epsilon_s} I$, $\mathbf{W}_p = \frac{1}{\epsilon_p} I$, $\mathbf{W}_e = \frac{1}{\epsilon_e} I$, where $(\epsilon_s, \epsilon_e, \epsilon_p)$ specifies the size of each uncertainty region, which is a measure of the quality of the channel estimations. Smaller values of ϵ imply better CSI knowledge at the SU-Tx. Monte Carlo simulations with 1000 randomly generated channel-triplets $(\hat{\mathbf{h}}_s, \hat{\mathbf{h}}_p, \hat{\mathbf{h}}_e)$ are performed and the average achievable secrecy rates are plotted. The transmit power and interference temperature limit are defined in dB w.r.t. the noise power. The basic Matlab code for the simulation can be found in Appendix H.

We first consider a secure MISO CRN with $N = 4$ transmit antennas and the PU-Rx

needs to be protected at the interference temperature limit of $Q = -10$ dB. In Fig. 6.3, the secrecy rates achieved under different levels of channel uncertainties, as indicated by the triplet $(\epsilon_s, \epsilon_e, \epsilon_p)$, are plotted versus the transmit power level P . It is observed that

Figure 6.3: Achievable secrecy rate vs transmit power with $N = 4$ antennas at $Q = -10$ dB for different levels of channel uncertainties.

the secrecy rates obtained by the two approaches, namely, ACRN transformation and SDP transformation, coincide perfectly since they are both optimal approaches. It is also observed that higher secrecy rate can be achieved when the uncertainty regions are smaller. This can be explained by the fact that more accurate CSI allows the SU-Tx to better direct its antenna beams towards the directions that are favorable to maximize its secrecy rate while avoiding harmful interference to the PU-Rx. Furthermore, we can also see that the secrecy rate becomes saturated at lower transmit power level when the uncertainty sets are larger. This is reasonable since injecting power into the channel does not necessarily help to increase the secrecy rate when the SU-Tx is less informed of the exact directions of the receivers.

In Fig. 6.4, the achievable secrecy rate for a $N = 4$ transmit antenna MISO CR at

the transmit power limit $P = 15$ dB is plotted against various interference temperature limits. The secrecy rates are also evaluated at different levels of channel uncertainties.

Figure 6.4: Achievable secrecy rate vs interference power with $N = 4$ antennas at $P = 15$ dB for different levels of channel uncertainties.

Similarly, it is also observed that higher secrecy rates can be achieved with the increased accuracy in the CSI. We can also see that as the interference power constraint relaxes, the increase in secrecy rates is higher when there are uncertainties in the CSI.

Figure 6.5 shows the secrecy rate achieved with the use of different number of antennas at $P = 20$ dB when the level of uncertainty is $(10^{-3}, 10^{-3}, 10^{-2})$. We can observe that the secrecy rates are increased substantially with the use of multiple antennas. This demonstrates the effectiveness of multiple antennas in achieving simultaneous secure, robust and cognitive transmission.

Figure 6.6 plots the secrecy rate of both the optimal and three suboptimal solutions achieved using $N = 3$ antennas against various interference temperature limits at the transmit power $P = 15$ dB. For each evaluated Q value, we consider two different sets of uncertainty regions: (i) $(10^{-3}, 10^{-3}, 10^{-2})$ and (ii) $(10^{-2}, 10^{-2}, 10^{-1})$. It is observed

Figure 6.5: Achievable secrecy rate vs number of transmit antennas at $P = 20$ dB and uncertainty level $(10^{-3}, 10^{-3}, 10^{-2})$.

that BERS is very close to the optimal solution for almost all the cases. This implies that beamforming along the principle eigenvector of the optimal transmit covariance only suffers marginal rate loss, if any, which is favorable since beamforming is simpler to implement than spatial multiplexing. Furthermore, we can see that BPRS can also achieve close-to-optimal secrecy rate for the given uncertainty sets, which means that ignoring the uncertainty in the secondary and eavesdropper channels does not degrade the performance too much. Since it is practically reasonable to have good estimates of these two channels, BPRS is also a good choice since it is less complex than the optimal SDP approach and BERS. Lastly, BARS seems not to be an effective solution, which reveals that the techniques used in approximating the secrecy rate function significantly enlarge the uncertainty regions.

Remark. The computational complexities of various proposed approaches will be briefly discussed here. Since all the proposed optimal and suboptimal approaches are based on SDP, the computational complexity can be computed following the discussion in

Figure 6.6: Achievable secrecy rate vs interference temperature limit at $P = 15$ dB and uncertainty levels (i) $(10^{-3}, 10^{-3}, 10^{-2})$ and (ii) $(10^{-2}, 10^{-2}, 10^{-1})$.

Section 5.2.3. Note that since the computational complexity depends significantly on the number and size of variables and constraints as seen from (5.37), we summarize such information in Table 6.1. Generally speaking, the fewer the number of variables and constraints, the less the complexity. For the optimal approaches, the SDP approach is almost of the same complexity as the ACRN at each given q . However, since the ACRN has to solve a sequence of SDPs, which takes $\left\lceil \log_c \left(\frac{\varepsilon}{q} \right) \right\rceil$ iterations to terminate, the overall complexity of the ACRN is significantly higher than the optimal SDP one. The BERS has the same complexity as that of the optimal SDP since they solve the same optimization problem. The BARS and BPRS approaches are of the same complexity and they are simpler than the others since they have the fewest variables and SDP constraints. To have an quantitative idea of the complexity of various proposed schemes, we can convert the proposed schemes into the standard form as in (5.35)-(5.36), we summarize the corresponding number of variables and size of SDP constraints in Table 6.2. Despite the differences in variables and constraints, from (5.37) with some

simplifications, the arithmetic complexity of all the proposed optimal and suboptimal schemes can be found to be of the order of $\mathcal{O}(N^{6.5})$.

	Number of Variables		Number of Constraints	
	complex semidefinite of size $N \times N$	positive scalar	complex semidefinite of size $(N + 1) \times (N + 1)$	real scalar
SDP	1	5	3	1
ACRN (at each q)	1	4	3	1
BERS	1	5	3	1
BARS	1	1	1	2
BPRS	1	1	1	2

Table 6.1: Complexity Comparison of Various Approaches

	Number of Real Variables	Size of Real SDP Constraints
SDP	$N^2 + 5$	3 of size $2(N + 1)$ 6 of size 1
ACRN (at each q)	$N^2 + 4$	3 of size $2(N + 1)$ 5 of size 1
BERS	$N^2 + 5$	3 of size $2(N + 1)$ 6 of size 1
BARS	$N^2 + 1$	1 of size $2(N + 1)$ 3 of size 1
BPRS	$N^2 + 1$	1 of size $2(N + 1)$ 3 of size 1

Table 6.2: Number of Variables and Size of Constraints in Standard Form

6.5 Conclusions

In this chapter, we have addressed the optimal robust transmitter design problem for the secure MISO CRN where the SU-Tx does not have perfect CSI of all the channels but only knows the associated uncertainty sets. Such a problem has been formulated as a maximin non-convex semi-infinite optimization problem to maximize the achievable secrecy rate for the SU such that the interference received at the PU-Rx does not

exceed the predefined threshold for all the possible channel realizations within the uncertainty regions. We have proposed two approaches to solve the problem. In the first approach, we relate the original problem with the optimal robust transmitter design problem in the ACRN with two PUs where all the relevant channels are subject to uncertainty, and solve it by exploring the relationship between these two networks. The second approach effectively recasts the original problem as a single SDP by exploring its inherent convexity. Finally, some heuristic beamforming solutions for the ease of implementation have been presented and their performance has been evaluated via simulations.

Chapter 7

Conclusions and Future Work

7.1 Conclusions

The OSA and the spectrum sharing represent the most basic model of operating a CRN. In either of these two models, resource allocation in a CRN has to balance the tradeoff between optimizing the SU's own performance and most importantly, maintaining sufficient protection to the PUs. In this thesis, two resource allocation problems have been identified and studied, namely, sensing-access design in the OSA model, and secure transmission in the spectrum sharing model.

The sensing-access design involves different considerations under different multi-channel sensing approaches. We have first addressed the design in the parallel channel sensing where multiple channels can be sensed simultaneously. We have investigated the sensing design which specifies the optimal time duration for sensing, and the access design which specifies the optimal power allocation upon transmission to maximize the sum throughput of an SU under two types of sum transmit power constraints (i.e., average and peak transmit power constraints) and the probability of detection constraint on each channel. The design has been formulated as an optimization problem. In particular, we have found that the optimal power allocation has a water-filling form and the optimal water level for a particular channel is shown to be independent of the

status of the PUs on other channels under the average sum transmit power constraint; whereas it is dependent under the peak sum transmit power constraint. The optimal sensing time can be determined through exhaustive search in general settings while in the numerical results provided, unique optimal sensing time is observed and can be determined with more efficient search algorithm. We have then studied the design in the sequential channel sensing where an SU can sequentially sense the channels one at a time. In this case, the primary channel occupancy and the secondary channel fading information is revealed sequentially. The objective is to dynamically design the sensing strategy that determines when to stop sensing and start transmission, the access strategy that specifies the transmit power level upon transmission, and the sensing order that tells the SU which channel to sense next if the current channel is given up for transmission, such that the energy efficiency of the sequential channel sensing process is maximized and the PU on each channel is sufficiently protected under a fixed probability of detection constraint. The design has been formulated as a finite-horizon stochastic sequential decision-making problem. An algorithm has been proposed to compute the optimal strategies numerically. Besides, it has been found analytically that the optimal sensing strategy has a threshold structure, which indicates that the SU should stop sensing and start transmission if the current channel condition is good enough; the optimal access strategy has a water-filling structure with the water level determined by the long-term energy efficiency and the perceived spectrum opportunity of the transmission channel; and the optimal sensing order will choose the channel to be sensed as the one with maximum expected future net reward among the set of remaining channels. Numerical results have shown that the energy efficiency improves and the optimal sensing time reduces as the number of channels that the SU is allowed to sense increases.

The secure transmission in the spectrum sharing model has been addressed from the information-theoretic perspective for the secure MISO CR channel. The secrecy

rate, which measures the rate at which the information can be reliably transmitted from the SU-Tx to the SU-Rx but is kept secret from the ED-Rx, at the same time the interference power received at the PU-Rx is restricted, has been of interest. We have considered both the cases that the SU-Tx has the perfect and imperfect knowledge of the secondary channel, the eavesdropper channel and the primary channel. In particular, when the CSI is perfectly known at the SU-Tx, the maximum secrecy rate, i.e., secrecy capacity, has been characterized in terms of a nonconvex optimization problem of the transmit covariance matrix. In the case of imperfect CSI when the SU-Tx only knows the uncertainty sets where the actual CSI is contained, the worst-case secrecy rate under Gaussian signaling without preprocessing of information has been characterized in terms of a maximin non-convex semi-infinite optimization problem. Under both cases of CSI, we have proposed two numerical approaches to compute the optimal transmit covariance matrix and the corresponding secrecy capacity/rate. Moreover, when CSI is perfectly known, beamforming has been shown to be the optimal transmission strategy. Furthermore, we have also proposed a few beamforming solutions to trade off between secrecy rate and computational complexity. Numerical results have shown that it is effective to use multiple antennas to preserve information confidentiality as well as to protect the PU-Rx.

7.2 Future Work

In all the work that we have addressed, the CRN only consists of a single pair of SU-Tx and SU-Rx. In the OSA model, while the single-user model simplifies the analysis and allows us to concentrate on the basic sensing-access tradeoff, it is only an abstraction of the multi-user scenario where a single pair of SUs is granted exclusive right to sense and access the spectrum either through centralized control or contention on a common control channel. The multi-user scenario, where multiple SUs can sense the channels simultaneously and decide whether to access or not distributively, cannot be addressed

under the current studies. Such designs are generally more challenging since it has to take into consideration the collision between SUs, (e.g., multiple SUs may access the same set of available channels identified by spectrum sensing), and the aggregate interference to the PUs. This is even more complicated when sequential channel sensing is deployed. The design of sensing order is of great importance. Intuitively, it should be designed as different as possible from other SUs to avoid the simultaneous sensing and subsequent access over the same channel. On the other hand, it should also try to sense the good channel first to avoid it being claimed by other SUs during the earlier sensing stage. Game theory could be a potential mathematical tool to model such kind of design, and has already been applied to study various distributed resource allocation problems in cognitive radio networks [206]. However, more sophisticated mathematical models beyond game theory that can capture various considerations and tradeoffs described above should be further explored to facilitate the sensing-access design in the multi-user scenario. In the spectrum sharing model, the multiuser version of this basic secure CR channel can be further extended to the multiple access channel, broadcast channel or interference channel. Their relationship with the corresponding channel models in the conventional CRNs could be explored. Robust design for such channel models can also be investigated in the future.

Another possible extension that is worth investigating is to address the transmission of delay-sensitive traffic over time-varying channels for an SU in the OSA model, which is in general extremely challenging. Such designs are usually modeled as the framework of sequential decision-make process, and have been studied intensively for non-CR networks in [207–210]. However, besides the difficulty due to time-varying channel condition as in the conventional non-CRNs, the availability of the channels depends on the PUs' activities and are also time-varying. If an SU with a limited energy budget wants to deliver a fixed amount of data before a given deadline, the sensing-access decision should balance the tradeoff between gaining immediate access and waiting for

future access. The former may help to empty the queue of data sooner. The latter may possibly find a better channel that may deliver more data using the same amount of energy but also have the risk of failing to transmit all the data within the given deadline due to the unavailability of the channels or worse channel conditions. Therefore, the design that can best balance such a tradeoff should be carefully investigated.

List of Publications

Journal papers

1. Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, “How much time is needed for wideband spectrum sensing?” *IEEE Trans. Wireless Commun.*, vol. 8, no. 11, pp. 5466–5471, Nov. 2009.
2. Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, “Secure communication over MISO cognitive radio channels,” *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.
3. Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, “Secure communication in multi-antenna cognitive radio networks with imperfect channel state information,” *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683–1693, Apr. 2011.
4. Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, “Energy-efficient design of sequential channel sensing in cognitive radio networks: Optimal sensing strategy, power allocation, and sensing order,” *IEEE J. Sel. Areas Commun.*, vol. 29, no. 8, pp. 1648–1659, Sep. 2011.

Conference papers

1. Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, “Sensing-throughput tradeoff for cognitive radio networks: A multiple-channel scenario,” in *Proc. IEEE Int. Symp. Personal, Indoor and Mobile Radio Commun. (PIMRC’09)*, Sep. 2009, pp. 1257–1261.
2. Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, “Achieving cognitive and secure transmissions using multiple antennas,” in *Proc. IEEE Int. Symp. Personal, Indoor and Mobile Radio Commun. (PIMRC’09)*, Sep. 2009, pp. 1–5.
3. Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, “Achieving robust, secure and cognitive transmissions using multiple antennas,” in *Proc. IEEE Int. Conf. Commun. (ICC’10)*, May 2010, pp. 1–5.

Bibliography

- [1] “Spectrum policy task force,” Federal Communications Commission, Rep. ET Docket No. 02-135, Nov. 2002.
- [2] Q. Zhao and B. M. Sadler, “A survey of dynamic spectrum access,” *IEEE Signal Process. Mag.*, vol. 24, no. 3, pp. 79–89, May 2007.
- [3] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, “Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey,” *Elsevier Comput. Netw.*, vol. 50, no. 13, pp. 2127–2159, Sep. 2006.
- [4] Y.-C. Liang, K. Chen, Y. Li, and P. Mahonen, “Cognitive radio networking and communications: An overview,” *IEEE Trans. Veh. Technol.*, vol. 60, no. 7, pp. 3386–3407, Sep. 2011.
- [5] “United States frequency allocations: The radio spectrum,” National Telecommunications and Information Administration of United States, Oct. 2003. [Online]. Available: <http://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf>
- [6] “Singapore spectrum allocation chart,” Infocomm Development Authority of Singapore. [Online]. Available: http://www.ida.gov.sg/doc/Policies%20and%20Regulation/Policies_and_Regulation_Level2/20060421164253/SpectrumChart.pdf
- [7] T. Taher, R. Bacchus, K. Zdunek, and D. Roberson, “Long-term spectral occupancy findings in Chicago,” in *IEEE Symp. New Frontiers in Dynamic Spectrum Access Netw. (DySPAN’11)*, May 2011, pp. 100–107.
- [8] M. Islam, C. L. Koh, S. W. Oh, X. Qing, Y. Y. Lai, C. Wang, Y.-C. Liang, B. E. Toh, F. Chin, G. L. Tan, and W. Toh, “Spectrum survey in Singapore: Occupancy measurements and analyses,” in *Proc. IEEE Int. Conf. on Cognitive Radio Oriented Wireless Netw. and Commun. (CrownCom’08)*, May 2008, pp. 1–7.
- [9] M. Wellens, J. Wu, and P. Mahonen, “Evaluation of spectrum occupancy in indoor and outdoor scenario in the context of cognitive radio,” in *Proc. IEEE Int. Conf. Cognitive Radio Oriented Wireless Netw. and Commun. (CrownCom’07)*, Aug. 2007, pp. 420–427.

- [10] R. Chiang, G. Rowe, and K. Sowerby, "A quantitative analysis of spectral occupancy measurements for cognitive radio," in *Proc. IEEE Veh. Technol. Conf. (VTC'07-Spring)*, Apr. 2007, pp. 3016–3020.
- [11] S. Yin, D. Chen, Q. Zhang, M. Liu, and S. Li, "Mining spectrum usage data: A large-scale spectrum measurement study," *IEEE Trans. Mobile Comput.*, vol. PP, no. 99, pp. 1–14, 2011.
- [12] I. Akyildiz, W.-Y. Lee, M. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 40–48, Apr. 2008.
- [13] T. A. Weiss and F. K. Jondral, "Spectrum pooling: An innovative strategy for the enhancement of spectrum efficiency," *IEEE Commun. Mag.*, vol. 42, no. 3, pp. S8–S14, Mar. 2004.
- [14] S. K. Jayaweera and T. Li, "Dynamic spectrum leasing in cognitive radio networks via primary-secondary user power control games," *IEEE Trans. Wireless Commun.*, vol. 8, no. 6, pp. 3300–3310, Jun. 2009.
- [15] K. Shin, H. Kim, A. Min, and A. Kumar, "Cognitive radios for dynamic spectrum access: From concept to reality," *IEEE Wireless Commun. Mag.*, vol. 17, no. 6, pp. 64–74, Dec. 2010.
- [16] R. Etkin, A. Parekh, and D. Tse, "Spectrum sharing for unlicensed bands," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 3, pp. 517–528, Apr. 2007.
- [17] Z.-Q. Luo and S. Zhang, "Dynamic spectrum management: Complexity and duality," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 57–73, Feb. 2008.
- [18] L. H. Grokop and D. N. C. Tse, "Spectrum sharing between wireless networks," *IEEE/ACM Trans. Netw.*, vol. 18, no. 5, pp. 1401–1412, Oct. 2010.
- [19] C. W. Tan, S. Friedland, and S. H. Low, "Spectrum management in multiuser cognitive wireless networks: Optimality and algorithm," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 2, pp. 421–430, Feb. 2011.
- [20] J. Mitola and G. Q. Maguire, "Cognitive radio: Making software radios more personal," *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13–18, Aug. 1999.
- [21] J. Mitola, "Cognitive radio: An integrated agent architecture for software defined radio," Ph.D. dissertation, Royal Institute of Technology, 2000.
- [22] "Notice of proposed rulemaking and order," Federal Communications Commission, Rep. ET Docket No. 03-322, Dec. 2003.
- [23] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

- [24] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proc. IEEE*, vol. 97, no. 5, pp. 894–914, May 2009.
- [25] J. Mitola, *Software Radios: Wireless Architecture for the 21st Century*. New York: Wiley, 2000.
- [26] "Notice of proposed rulemaking," Federal Communications Commission, Rep. ET Docket No. 00-402, Nov. 2000.
- [27] "Notice of proposed rulemaking," Federal Communications Commission, Rep. ET Docket No. 04-113, May 2004.
- [28] "Second memorandum opinion and order," Federal Communications Commission, Rep. ET Docket No. 10-174, Sep. 2010.
- [29] "Connecting America: The national broadband plan," Federal Communications Commission, Tech. Rep., Mar. 2010.
- [30] "Digital dividend review: A statement on our approach to awarding the digital dividend," Office of Communications, Tech. Rep., Dec. 2007.
- [31] "White space technology trials," Infocomm Development Authority of Singapore, 2011. [Online]. Available: <http://www.ida.gov.sg/Policies%20and%20Regulation/20100730141139.aspx>
- [32] C. Cordeiro, K. Challapali, D. Birru, and N. Sai Shankar, "IEEE 802.22: The first worldwide wireless standard based on cognitive radios," in *Proc. IEEE Int. Symp. New Frontiers in Dynamic Spectrum Access Netw. (DySPAN'05)*, Nov. 2005, pp. 328–337.
- [33] Y.-C. Liang, A. Hoang, and H.-H. Chen, "Cognitive radio on TV bands: A new approach to provide wireless connectivity for rural areas," *IEEE Wireless Commun. Mag.*, vol. 15, no. 3, pp. 16–22, Jun. 2008.
- [34] *IEEE Standard for Information Technology–Telecommunications and information exchange between systems Wireless Regional Area Networks (WRAN)–Specific requirements Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands*, IEEE Std 802.22, Jul. 2011.
- [35] J. Wang, M. S. Song, S. Santhiveeran, K. Lim, G. Ko, K. Kim, S. H. Hwang, M. Ghosh, V. Gaddam, and K. Challapali, "First cognitive radio networking standard for personal/portable devices in TV white spaces," in *Proc. IEEE Int. Symp. New Frontiers in Dynamic Spectrum Access Netw. (DySPAN'10)*, Apr. 2010, pp. 1–12.
- [36] *ECMA-392: MAC and PHY for Operation in TV White Space*, Ecma International Std., Rev. 1st, Dec. 2009. [Online]. Available: <http://www.ecma-international.org/publications/standards/Ecma-392.htm>

- [37] S. Filin, H. Harada, H. Murakami, and K. Ishizu, "International standardization of cognitive radio systems," *IEEE Commun. Mag.*, vol. 49, no. 3, pp. 82–89, Mar. 2011.
- [38] R. Zhang, Y.-C. Liang, and S. Cui, "Dynamic resource allocation in cognitive radio networks," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 102–114, May 2010.
- [39] X. Kang, Y.-C. Liang, H. K. Garg, and L. Zhang, "Sensing-based spectrum sharing in cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 8, pp. 4649–4654, Oct. 2009.
- [40] M. G. Khoshkholgh, K. Navaie, and H. Yanikomeroglu, "Access strategies for spectrum sharing in fading environment: Overlay, underlay, and mixed," *IEEE Trans. Mobile Comput.*, vol. 9, no. 12, pp. 1780–1793, Dec. 2010.
- [41] S. Stotas and A. Nallanathan, "Optimal sensing time and power allocation in multiband cognitive radio networks," *IEEE Trans. Commun.*, vol. 59, no. 1, pp. 226–235, Jan. 2011.
- [42] S. Srinivasa and S. Jafar, "Soft sensing and optimal power control for cognitive radio," *IEEE Trans. Wireless Commun.*, vol. 9, no. 12, pp. 3638–3649, Dec. 2010.
- [43] V. Asghari and S. Aissa, "Adaptive rate and power transmission in spectrum-sharing systems," *IEEE Trans. Wireless Commun.*, vol. 9, no. 10, pp. 3272–3280, Oct. 2010.
- [44] D. Gurney, G. Buchwald, L. Ecklund, S. L. Kuffner, and J. Grosspietsch, "Geolocation database techniques for incumbent protection in the TV white space," in *Proc. IEEE Symp. New Frontiers in Dynamic Spectrum Access Netw. (DySPAN'08)*, Oct. 2008, pp. 1–9.
- [45] Z. Quan, S. Cui, H. V. Poor, and A. H. Sayed, "Collaborative wideband sensing for cognitive radios," *IEEE Signal Process. Mag.*, vol. 25, no. 6, pp. 60–73, Nov. 2008.
- [46] T. Yücek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 1, pp. 116–130, First Quarter 2009.
- [47] J. Ma, G. Li, and B. H. Juang, "Signal processing in cognitive radio," *Proc. IEEE*, vol. 97, no. 5, pp. 805–823, May 2009.
- [48] K. B. Letaief and W. Zhang, "Cooperative communications for cognitive radio networks," *Proc. IEEE*, vol. 97, no. 5, pp. 878–893, May 2009.
- [49] Y. Zeng, Y.-C. Liang, A. T. Hoang, and R. Zhang, "A review on spectrum sensing for cognitive radio: Challenges and solutions," *EURASIP J. Advances in Signal Process.*, vol. 2010, no. 381465, pp. 1–15, 2010.

- [50] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Elsevier Physical Commun.*, vol. 4, no. 1, pp. 40–62, Mar. 2011.
- [51] S. M. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory*, ser. Prentice-Hall Signal Processing. PTR Prentice Hall, 1998, vol. 2.
- [52] G. Ko, A. Franklin, S.-J. You, J.-S. Pak, M.-S. Song, and C.-J. Kim, "Channel management in IEEE 802.22 WRAN systems," *IEEE Commun. Mag.*, vol. 48, no. 9, pp. 88–94, Sep. 2010.
- [53] R. Zhang and Y.-C. Liang, "Exploiting multi-antennas for opportunistic spectrum sharing in cognitive radio networks," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 88–102, Jan. 2008.
- [54] —, "Exploiting hidden power-feedback loops for cognitive radio," in *Proc. IEEE Symp. New Frontiers in Dynamic Spectrum Access Netw. (DySPAN'08)*, Oct. 2008, pp. 1–5.
- [55] F. Gao, X. Wang, R. Zhang, and Y.-C. Liang, "Optimal design of learning based MIMO cognitive radio systems," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT'09)*, Jun.-Jul. 2009, pp. 2537–2541.
- [56] F. Gao, R. Zhang, Y.-C. Liang, and X. Wang, "Multi-antenna cognitive radio systems: Environmental learning and channel training," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Process. (ICASSP'09)*, Apr. 2009, pp. 2329–2332.
- [57] R. Zhang, F. Gao, and Y.-C. Liang, "Cognitive beamforming made practical: Effective interference channel and learning-throughput tradeoff," *IEEE Trans. Commun.*, vol. 58, no. 2, pp. 706–718, Feb. 2010.
- [58] I. Bajaj and Y. Gong, "Cross-channel estimation using supervised probing and sensing in cognitive radio networks," in *Proc. IEEE Int Conf. Communications (ICC'11)*, Jun. 2011, pp. 1–5.
- [59] Y.-C. Liang, Y. Zeng, E. C. Y. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1326–1337, Apr. 2008.
- [60] Y. Liang, H. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Commun. and Inf. Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.
- [61] D. P. Bertsekas, *Dynamic Programming and Optimal Control*, 2nd ed. Athena Scientific, 2000, vol. 1.
- [62] S. Boyd, L. E. Ghaoui, E. Feron, and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory*. Society for Industrial and Applied Mathematics, 1994.

- [63] R. Tandra, A. Sahai, and S. M. Mishra, "What is a spectrum hole and what does it take to recognize one?" *Proc. IEEE*, vol. 97, no. 5, pp. 824–848, May 2009.
- [64] B. Wild and K. Ramchandran, "Detecting primary receivers for cognitive radio applications," in *Proc. Int. Symp. New Frontiers in Dynamic Spectrum Access Netw. (DySPAN'05)*, Nov. 2005, pp. 124–130.
- [65] A. Ghasemi and E. S. Sousa, "Spectrum sensing in cognitive radio networks: Requirements, challenges and design trade-offs," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 32–39, Apr. 2008.
- [66] R. Tandra and A. Sahai, "SNR walls for signal detection," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 4–17, Feb. 2008.
- [67] G. Zhao, G. Y. Li, C. Yang, and J. Ma, "Proactive detection of spectrum holes in cognitive radio," in *Proc. IEEE Int. Conf. Communications (ICC '09)*, Jun. 2009, pp. 1–5.
- [68] G. Zhao, G. Y. Li, and C. Yang, "Proactive detection of spectrum opportunities in primary systems with power control," *IEEE Trans. Wireless Commun.*, vol. 8, no. 9, pp. 4815–4823, Sep. 2009.
- [69] R. Zhang, "On active learning and supervised transmission of spectrum sharing based cognitive radios by exploiting hidden primary radio feedback," *IEEE Trans. Commun.*, vol. 58, no. 10, pp. 2960–2970, Oct. 2010.
- [70] Y. Che, R. Zhang, and Y. Gong, "Opportunistic spectrum access for cognitive radio in the presence of reactive primary users," in *Proc. IEEE Int. Conf. Commun. (ICC'11)*, Jun. 2011, pp. 1–5.
- [71] S. Huang, X. Liu, and Z. Ding, "Decentralized cognitive radio control based on inference from primary link control information," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 2, pp. 394–406, Feb. 2011.
- [72] K. Eswaran, M. Gastpar, and K. Ramchandran, "Cognitive radio through primary control feedback," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 2, pp. 384–393, Feb. 2011.
- [73] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proc. IEEE*, vol. 55, no. 4, pp. 523–531, Apr. 1967.
- [74] F. F. Digham, M.-S. Alouini, and M. K. Simon, "On the energy detection of unknown signals over fading channels," *IEEE Trans. Commun.*, vol. 55, no. 1, pp. 21–24, Jan. 2007.
- [75] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*, ser. Prentice-Hall Signal Processing. Prentice Hall, 1993, vol. 1.

- [76] A. Sahai, N. Hoven, and R. Tandra, "Some fundamental limits on cognitive radio," in *Proc. Allerton Conf. on Commun., Control, and Comput.*, Oct. 2004, pp. 1–11.
- [77] D. Cabric, S. M. Mishra, and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Proc. Asilomar Conf. Signals, Systems and Computers*, vol. 1, Nov. 2004, pp. 772–776.
- [78] W. A. Gardner, "Signal interception: A unifying theoretical framework for feature detection," *IEEE Trans. Commun.*, vol. 36, no. 8, pp. 897–906, Aug. 1988.
- [79] —, "Exploitation of spectral redundancy in cyclostationary signals," *IEEE Signal Process. Mag.*, vol. 8, no. 2, pp. 14–36, Apr. 1991.
- [80] S. Enserink and D. Cochran, "A cyclostationary feature detector," in *Proc. IEEE Asilomar Conf. on Signals, Systems, and Computers*, Oct. 1994, pp. 806–810.
- [81] A. Sahai and D. Cabric, "Spectrum sensing: Fundamental limits and practical challenges," in *Int. Symp. New Frontiers in Dynamic Spectrum Access Netw. (DySPAN'05)*, Nov. 2005, tutorial.
- [82] N. S. Shankar, C. Cordeiro, and K. Challapali, "Spectrum agile radios: Utilization and sensing architectures," in *Proc. IEEE Int. Symp. New Frontiers in Dynamic Spectrum Access Netw. (DySPAN'05)*, Nov. 2005, pp. 160–169.
- [83] M. Ghozzi, F. Marx, M. Dohler, and J. Palicot, "Cyclostationarity-based test for detection of vacant frequency bands," in *Proc. IEEE Cognitive Radio Oriented Wireless Netw. and Commun. Conf. (CrownCom'06)*, Jun. 2006, pp. 1–5.
- [84] A. V. Dandawate and G. B. Giannakis, "Statistical tests for presence of cyclostationarity," *IEEE Trans. Signal Process.*, vol. 42, no. 9, pp. 2355–2369, Sep. 1994.
- [85] R. Tandra and A. Sahai, "SNR walls for feature detectors," in *Proc. IEEE Int. Symp. New Frontiers in Dynamic Spectrum Access Netw. (DySPAN '07)*, Apr. 2007, pp. 559–570.
- [86] Y. Zeng and Y.-C. Liang, "Spectrum-sensing algorithms for cognitive radio based on statistical covariances," *IEEE Trans. Veh. Technol.*, vol. 58, no. 4, pp. 1804–1815, May 2009.
- [87] —, "Eigenvalue based spectrum sensing algorithms for cognitive radio," *IEEE Trans. Commun.*, vol. 57, no. 6, pp. 1784–1793, Jun. 2009.
- [88] Y. Zeng, C. L. Koh, and Y.-C. Liang, "Maximum eigenvalue detection: Theory and application," in *Proc. IEEE Int. Conf. Communications (ICC '08)*, May 2008, pp. 4160–4164.

- [89] A. Kortun, T. Ratnarajah, M. Sellathurai, C. Zhong, and C. B. Papadias, "On the performance of eigenvalue-based cooperative spectrum sensing for cognitive radio," *IEEE J. Sel. Topics Signal Process.*, vol. 5, no. 1, pp. 49–55, Feb. 2011.
- [90] Z. Tian and G. B. Giannakis, "A wavelet approach to wideband spectrum sensing for cognitive radios," in *Proc. IEEE Int. Conf. on Cognitive Radio Oriented Wireless Netw. and Commun. (CrownCom'06)*, 2006, pp. 1–5.
- [91] D. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.
- [92] Z. Tian and G. B. Giannakis, "Compressed sensing for wideband cognitive radios," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Process. (ICASSP '07)*, vol. 4, 2007, pp. IV–1357 – IV–1360.
- [93] Y. L. Polo, Y. Wang, A. Pandharipande, and G. Leus, "Compressive wide-band spectrum sensing," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Process. (ICASSP'09)*, 2009, pp. 2337–2340.
- [94] S.-J. Kim and G. B. Giannakis, "Sequential and cooperative sensing for multi-channel cognitive radios," *IEEE Trans. Signal Process.*, vol. 58, no. 8, pp. 4239–4253, Aug. 2010.
- [95] Y. Xin, H. Zhang, and S. Rangarajan, "SSCT: A simple sequential spectrum sensing scheme for cognitive radio," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM'09)*, 2009, pp. 1–6.
- [96] L. Lai, Y. Fan, and H. V. Poor, "Quickest detection in cognitive radio: A sequential change detection framework," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM'08)*, 2008, pp. 1–5.
- [97] Q. Zhao and J. Ye, "Quickest detection in multiple on-off processes," *IEEE Trans. Signal Process.*, vol. 58, no. 12, pp. 5994–6006, Dec. 2010.
- [98] H. Li, "Restless watchdog: Selective quickest spectrum sensing in multichannel cognitive radio systems," *EURASIP J. Advances in Signal Process.*, vol. 2009, no. 417457, pp. 1–12, 2009.
- [99] H. V. Poor and O. Hadjiladis, *Quickest Detection*. Cambridge University Press, 2009.
- [100] A. Domenico, E. Strinati, and M.-G. D. Benedetto, "A survey on MAC strategies for cognitive radio networks," *IEEE Commun. Surveys Tuts.*, vol. PP, no. 99, pp. 1–24, 2010.
- [101] Z. Quan, S. Cui, A. H. Sayed, and H. V. Poor, "Optimal multiband joint detection for spectrum sensing in cognitive radio networks," *IEEE Trans. Signal Process.*, vol. 57, no. 3, pp. 1128–1140, Mar. 2009.

- [102] J. Jia, Q. Zhang, and X. Shen, "HC-MAC: A hardware-constrained cognitive MAC for efficient spectrum management," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 106–117, Jan. 2008.
- [103] T. Shu and M. Krunz, "Throughput-efficient sequential channel sensing and probing in cognitive radio networks under sensing errors," in *Proc. ACM Int. Conf. Mob. Comput. and Networking (MobiCom'09)*, Sep. 2009, pp. 37–48.
- [104] H. Jiang, L. Lai, R. Fan, and H. V. Poor, "Optimal selection of channel sensing order in cognitive radio," *IEEE Trans. Wireless Commun.*, vol. 8, no. 1, pp. 297–307, Jan. 2009.
- [105] N. B. Chang and M. Liu, "Optimal channel probing and transmission scheduling for opportunistic spectrum access," *IEEE/ACM Trans. Netw.*, vol. 17, no. 6, pp. 1805–1818, Dec. 2009.
- [106] H. T. Cheng and W. Zhuang, "Simple channel sensing order in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 676–688, Apr. 2011.
- [107] H. Kim and K. G. Shin, "Fast discovery of spectrum opportunities in cognitive radio networks," in *Proc. IEEE Symp. New Frontiers in Dynamic Spectrum Access Netw. (DySPAN'08)*, Oct. 2008, pp. 1–12.
- [108] —, "Efficient discovery of spectrum opportunities with MAC-layer sensing in cognitive radio networks," *IEEE Trans. Mobile Comput.*, vol. 7, no. 5, pp. 533–545, May 2008.
- [109] Q. Zhao, L. Tong, A. Swami, and Y. Chen, "Decentralized cognitive MAC for opportunistic spectrum access in ad hoc networks: A POMDP framework," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 3, pp. 589–600, Apr. 2007.
- [110] Y. Chen, Q. Zhao, and A. Swami, "Joint design and separation principle for opportunistic spectrum access in the presence of sensing errors," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 2053–2071, May 2008.
- [111] Q. Zhao, B. Krishnamachari, and K. Liu, "On myopic sensing for multi-channel opportunistic access: Structure, optimality, and performance," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 5431–5440, Dec. 2008.
- [112] Y. Chen, Q. Zhao, and A. Swami, "Distributed spectrum sensing and access in cognitive radio networks with energy constraint," *IEEE Trans. Signal Process.*, vol. 57, no. 2, pp. 783–797, Feb. 2009.
- [113] A. T. Hoang, Y.-C. Liang, D. Wong, Y. Zeng, and R. Zhang, "Opportunistic spectrum access for energy-constrained cognitive radios," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1206–1211, Mar. 2009.
- [114] S. Gong, P. Wang, W. Liu, and W. Yuan, "Maximize secondary user throughput via optimal sensing in multi-channel cognitive radio networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM'10)*, Dec. 2010, pp. 1–5.

- [115] S. Huang, X. Liu, and Z. Ding, "Opportunistic spectrum access in cognitive radio networks," in *Proc. IEEE Int. Conf. Computer Communications (INFOCOM'08)*, 2008, pp. 1427–1435.
- [116] ———, "Optimal transmission strategies for dynamic spectrum access in cognitive radio networks," *IEEE Trans. Mobile Comput.*, vol. 8, no. 12, pp. 1636–1648, Dec. 2009.
- [117] Q. Zhao, S. Geirhofer, L. Tong, and B. M. Sadler, "Opportunistic spectrum access via periodic channel sensing," *IEEE Trans. Signal Process.*, vol. 56, no. 2, pp. 785–796, Feb. 2008.
- [118] S. Geirhofer, L. Tong, and B. M. Sadler, "Cognitive medium access: Constraining interference based on experimental models," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 95–105, Jan. 2008.
- [119] X. Li, Q. Zhao, X. Guan, and L. Tong, "Optimal cognitive access of markovian channels under tight collision constraints," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 746–756, Apr. 2011.
- [120] W.-Y. Lee and I. Akyildiz, "Optimal spectrum sensing framework for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 10, pp. 3845–3857, Oct. 2008.
- [121] Y. Pei, A. T. Hoang, and Y. C. Liang, "Sensing-throughput tradeoff in cognitive radio networks: How frequently should spectrum sensing be carried out?" in *Proc. IEEE Int. Symp. Personal, Indoor and Mobile Radio Commun. (PIMRC'07)*, Sep. 2007, pp. 1–5.
- [122] Z. Sun, G. J. Bradford, and J. N. Laneman, "Sequence detection algorithms for PHY-layer sensing in dynamic spectrum access networks," *IEEE J. Sel. Topics Signal Process.*, vol. 5, no. 1, pp. 97–109, Feb. 2011.
- [123] L. Lai, H. El Gamal, H. Jiang, and H. V. Poor, "Cognitive medium access: Exploration, exploitation, and competition," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 239–253, Feb. 2011.
- [124] M. Gastpar, "On capacity under receive and spatial spectrum-sharing constraints," *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 471–487, Feb. 2007.
- [125] L. Zhang, Y.-C. Liang, and Y. Xin, "Joint beamforming and power allocation for multiple access channels in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 38–51, Jan. 2008.
- [126] L. Zhang, Y. Xin, Y.-C. Liang, and H. V. Poor, "Cognitive multiple access channels: Optimal power allocation for weighted sum rate maximization," *IEEE Trans. Commun.*, vol. 57, no. 9, pp. 2754–2762, Sep. 2009.

- [127] L. Zhang, Y. Xin, and Y.-C. Liang, "Weighted sum rate optimization for cognitive radio MIMO broadcast channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 6, pp. 2950–2959, Jun. 2009.
- [128] K. T. Phan, S. A. Vorobyov, N. D. Sidiropoulos, and C. Tellambura, "Spectrum sharing in wireless networks via QoS-aware secondary multicast beamforming," *IEEE Trans. Signal Process.*, vol. 57, no. 6, pp. 2323–2335, Jun. 2009.
- [129] G. Scutari, D. Palomar, and S. Barbarossa, "Cognitive MIMO radio," *IEEE Signal Process. Mag.*, vol. 25, no. 6, pp. 46–59, Nov. 2008.
- [130] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the K-user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.
- [131] S. M. Perlaza, N. Fawaz, S. Lasaulce, and M. Debbah, "From spectrum pooling to space pooling: Opportunistic interference alignment in MIMO cognitive networks," *IEEE Trans. Signal Process.*, vol. 58, no. 7, pp. 3728–3741, Jul. 2010.
- [132] A. Ghasemi and E. S. Sousa, "Fundamental limits of spectrum-sharing in fading environments," *IEEE Trans. Wireless Commun.*, vol. 6, no. 2, pp. 649–658, Feb. 2007.
- [133] X. Kang, Y.-C. Liang, A. Nallanathan, H. K. Garg, and R. Zhang, "Optimal power allocation for fading channels in cognitive radio networks: Ergodic capacity and outage capacity," *IEEE Trans. Wireless Commun.*, vol. 8, no. 2, pp. 940–950, Feb. 2009.
- [134] L. Musavian and S. Aissa, "Capacity and power allocation for spectrum-sharing communications in fading channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 1, pp. 148–156, Jan. 2009.
- [135] —, "Fundamental capacity limits of cognitive radio in fading environments with imperfect channel information," *IEEE Trans. Commun.*, vol. 57, no. 11, pp. 3472–3480, Nov. 2009.
- [136] R. Zhang, S. Cui, and Y.-C. Liang, "On ergodic sum capacity of fading cognitive multiple-access and broadcast channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 11, pp. 5161–5177, Nov. 2009.
- [137] R. Zhang, "On peak versus average interference power constraints for protecting primary users in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 4, pp. 2112–2120, Apr. 2009.
- [138] L. Musavian and S. Aissa, "Capacity of spectrum-sharing channels with minimum-rate requirements," in *Proc. IEEE Int. Conf. Commun. (ICC '08)*, May 2008, pp. 4639–4643.

- [139] X. Kang, R. Zhang, Y.-C. Liang, and H. Garg, "Optimal power allocation strategies for fading cognitive radio channels with primary user outage constraint," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 2, pp. 374–383, Feb. 2011.
- [140] A. Goldsmith, S. A. Jafar, N. Jindal, and S. Vishwanath, "Capacity limits of MIMO channels," *IEEE J. Sel. Areas Commun.*, vol. 21, no. 5, pp. 684–702, Jun. 2003.
- [141] E. Visotsky and U. Madhow, "Space-time transmit precoding with imperfect feedback," *IEEE Trans. Inf. Theory*, vol. 47, no. 6, pp. 2632–2639, Sep. 2001.
- [142] S. A. Jafar and A. Goldsmith, "Transmitter optimization and optimality of beamforming for multiple antenna systems," *IEEE Trans. Wireless Commun.*, vol. 3, no. 4, pp. 1165–1175, Jul. 2004.
- [143] F. Rey, M. Lamarca, and G. Vazquez, "Robust power allocation algorithms for MIMO OFDM systems with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 53, no. 3, pp. 1070–1085, Mar. 2005.
- [144] X. Zhang, D. P. Palomar, and B. Ottersten, "Statistically robust design of linear MIMO transceivers," *IEEE Trans. Signal Process.*, vol. 56, no. 8, pp. 3678–3689, Aug. 2008.
- [145] K. Son, B. C. Jung, S. Chong, and D. K. Sung, "Power allocation for OFDM-based cognitive radio systems under outage constraints," in *Proc. IEEE Int Conf. Commun. (ICC'10)*, May 2010, pp. 1–5.
- [146] Y. J. Zhang and A. M. So, "Optimal spectrum sharing in MIMO cognitive radio networks via semidefinite programming," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 2, pp. 362–373, Feb. 2011.
- [147] A. Pascual-Iserte, D. P. Palomar, A. I. Perez-Neira, and M. A. Lagunas, "A robust maximin approach for MIMO communications with imperfect channel state information based on convex optimization," *IEEE Trans. Signal Process.*, vol. 54, no. 1, pp. 346–360, Jan. 2006.
- [148] A. Abdel-Samad, T. N. Davidson, and A. B. Gershman, "Robust transmit eigen beamforming based on imperfect channel state information," *IEEE Trans. Signal Process.*, vol. 54, no. 5, pp. 1596–1609, May 2006.
- [149] A. Wiesel, Y. C. Eldar, and S. Shamai, "Optimization of the MIMO compound capacity," *IEEE Trans. Wireless Commun.*, vol. 6, no. 3, pp. 1094–1101, Mar. 2007.
- [150] L. Zhang, Y.-C. Liang, Y. Xin, and H. V. Poor, "Robust cognitive beamforming with partial channel state information," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 4143–4153, Aug. 2009.

- [151] T. Al-Khasib, M. B. Shenouda, and L. Lampe, "Dynamic spectrum management for multiple-antenna cognitive radio systems: Designs with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 2850–2859, Sep. 2011.
- [152] J. Wang, G. Scutari, and D. P. Palomar, "Robust MIMO cognitive radio via game theory," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1183–1201, Mar. 2011.
- [153] K. Cumanan, R. Krishna, V. Sharma, and S. Lambotharan, "A robust beamforming based interference control technique and its performance for cognitive radios," in *Proc. Int. Symp. Commun. and Inf. Technol. (ISCIT'08)*, 2008, pp. 9–13.
- [154] G. Zheng, K.-K. Wong, and B. Ottersten, "Robust cognitive beamforming with bounded channel uncertainties," *IEEE Trans. Signal Process.*, vol. 57, no. 12, pp. 4871–4881, Dec. 2009.
- [155] E. Gharavol, Y.-C. Liang, and K. Mouthaan, "Robust downlink beamforming in multiuser MISO cognitive radio networks with imperfect channel-state information," *IEEE Trans. Veh. Technol.*, vol. 59, no. 6, pp. 2852–2860, Jul. 2010.
- [156] J. L. Burbank, "Security in cognitive radio networks: The required evolution in approaches to wireless network security," in *Proc. Int. Conf. Cognitive Radio Oriented Wireless Netw. and Commun. (CrownCom'08)*, May 2008, pp. 1–7.
- [157] G. Baldini, T. Sturman, A. Biswas, R. Leschhorn, G. Godor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Commun. Surveys Tuts.*, vol. PP, no. 99, pp. 1–25, 2011.
- [158] R. Chen and J.-M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in *Proc. IEEE Workshop Networking Technologies for Software Defined Radio Netw.*, Sep. 2006, pp. 110–119.
- [159] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 25–37, Jan. 2008.
- [160] S. Anand, Z. Jin, and K. P. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in *Proc. IEEE Symp. New Frontiers in Dynamic Spectrum Access Netw. (DySPAN'08)*, Oct. 2008, pp. 1–6.
- [161] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in *Proc. IEEE Int. Conf. Commun. (ICC'09)*, Jun. 2009, pp. 1–5.
- [162] C. Chen, H. Cheng, and Y.-D. Yao, "Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack," *IEEE Trans. Wireless Commun.*, vol. 10, no. 7, pp. 2135–2141, Jul. 2011.

- [163] 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.
- [164] —, "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.
- [165] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. IEEE Conf. Computer Commun. (INFOCOM'08)*, Apr. 2008, pp. 1876–1884.
- [166] K. Zeng, P. Paweczak, and D. Cabric, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Commun. Lett.*, vol. 14, no. 3, pp. 226–228, Mar. 2010.
- [167] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *IEEE Trans. Signal Process.*, vol. 59, no. 2, pp. 774–786, 2011.
- [168] P. Kaligineedi, M. Khabbazi, and V. K. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE Trans. Wireless Commun.*, vol. 9, no. 8, pp. 2488–2497, Aug. 2010.
- [169] H. Li and Z. Han, "Catch me if you can: An abnormality detection approach for collaborative spectrum sensing in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3554–3565, Nov. 2010.
- [170] A. Wyner, "The wire-tap channel," *The Bell Systems Technical J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [171] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [172] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
- [173] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
- [174] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.
- [175] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
- [176] T. Liu and S. Shamai(Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

- [177] R. Bustin, R. Liu, H. V. Poor, and S. Shamai(Shitz), "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," *EURASIP J. Wirelss Commun. and Networking*, vol. 2009, no. 370970, pp. 1–8, 2009.
- [178] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
- [179] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. on Inf. Theory (ISIT'07)*, Jun. 2007, pp. 2466–2470.
- [180] R. Liu and H. V. Poor, "Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1235–1249, Mar. 2009.
- [181] —, "Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1235–1249, Mar. 2009.
- [182] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.
- [183] Y. Liang, H. V. Poor, and S. Shamai(Shitz), "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.
- [184] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.
- [185] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York, NY, USA: Wiley-Interscience, 1991.
- [186] G. B. Thomas, *Thomas' Calculus*, eleven ed. Boston, USA: Pearson Addison Wesley, 2005.
- [187] S. Cui, A. Goldsmith, and A. Bahai, "Energy-constrained modulation optimization," *IEEE Trans. Wireless Commun.*, vol. 4, no. 5, pp. 2349–2360, Sep. 2005.
- [188] G. Miao, N. Himayat, Y. G. Li, and A. Swami, "Cross-layer optimization for energy-efficient wireless communications: A survey," *Wireless Commun. Mob. Comput.*, vol. 9, no. 4, pp. 529–542, Apr. 2009.
- [189] D. Kadhimi, S. Gong, W. Xia, W. Liu, and W. Cheng, "Power efficiency maximization in cognitive radio networks," in *Proc. IEEE Wireless Commun. and Networking Conf. (WCNC'09)*, Apr. 2009, pp. 1–6.
- [190] L. Li, X. Zhou, H. Xu, Y. G. Li, D. Wang, and A. Soong, "Energy-efficient transmission in cognitive radio networks," in *Proc. IEEE Consumer Commun. and Networking Conf. (CCNC'10)*, Jan. 2010, pp. 1–5.

- [191] M. Sniedovich, *Dynamic Programming*. N.Y. Marcel Dekker, 1992.
- [192] E. Jorswieck, H. Boche, and S. Naik, "Energy-aware utility regions: Multiple access pareto boundary," *IEEE Trans. Wireless Commun.*, vol. 9, no. 7, pp. 2216–2226, Jul. 2010.
- [193] C. Saraydar, N. Mandayam, and D. Goodman, "Efficient power control via pricing in wireless data networks," *IEEE Trans. Commun.*, vol. 50, no. 2, pp. 291–303, Feb. 2002.
- [194] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.
- [195] T. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Prentice Hall PTR, 2002.
- [196] Y. Liang and H. V. Poor, "Secure communication over fading channels," in *Proc. 44th Annu. Allerton Conf. on Commun., Control and Comput.*, Sep. 2006, pp. 817–823.
- [197] H. Wiengarten, Y. Steinberg, and S. Shamai(Shitz), "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936–3964, Sep. 2006.
- [198] J. F. Sturm, "Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones," *Optimization Methods and Softw.*, vol. 11, no. 1, pp. 625–653, 1999.
- [199] L. Zhang, Y.-C. Liang, Y. Pei, and R. Zhang, "Robust beamforming design: From cognitive radio MISO channels to secrecy MISO channels," in *Proc. IEEE Global TeleCommun. Conf. (GLOBECOM'09)*, Dec. 2009, pp. 1–5.
- [200] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," *IEEE Trans. Commun.*, vol. 58, no. 6, pp. 1877–1886, Jun. 2010.
- [201] A. Ben-Tal and A. Nemirovski, *Lectures on Modern Convex Optimization: Analysis, Algorithms, and Engineering Applications*. Society for Industrial and Applied Mathematics, 2001.
- [202] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wiretap channels," in *Proc. 45th Annu. Allerton Conf. on Commun., Control and Comput.*, Sep. 2007, pp. 136–143.
- [203] Z.-Q. Luo, J. F. Sturm, and S. Zhang, "Multivariate nonnegative quadratic mappings," *SIAM J. Optim.*, vol. 14, no. 4, pp. 1140–1162, Apr. 2004.
- [204] N. D. Sidiropoulos, T. N. Davidson, and Z.-Q. Luo, "Transmit beamforming for physical-layer multicasting," *IEEE Trans. Signal Process.*, vol. 54, no. 6, pp. 2239–2251, Jun. 2006.

- [205] Z.-Q. Luo, W.-K. Ma, A.-C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.
- [206] B. Wang, Y. Wu, and K. Liu, "Game theory for cognitive radio networks: An overview," *Elsevier Comput. Netw.*, vol. 54, no. 14, pp. 2537–2561, Oct. 2010.
- [207] R. Negi and J. M. Cioffi, "Delay-constrained capacity with causal feedback," *IEEE Trans. Inf. Theory*, vol. 48, no. 9, pp. 2478–2494, Sep. 2002.
- [208] R. A. Berry and R. G. Gallager, "Communication over fading channels with delay constraints," *IEEE Trans. Inf. Theory*, vol. 48, no. 5, pp. 1135–1149, May 2002.
- [209] A. Fu, E. Modiano, and J. N. Tsitsiklis, "Optimal transmission scheduling over a fading channel with energy and deadline constraints," *IEEE Trans. Wireless Commun.*, vol. 5, no. 3, pp. 630–641, Mar. 2006.
- [210] J. Chen and K.-K. Wong, "Communication with causal CSI and controlled information outage," *IEEE Trans. Wireless Commun.*, vol. 8, no. 5, pp. 2221–2229, May 2009.

Appendices

Appendix A

Proof of Proposition 3.1

Proof. The proof can be shown by induction. Denote A_K as the left-hand side of the constraint (3.8), i.e., $A_K = \sum_{m=1}^{2^K-1} \mathcal{P}_{s,m} \sum_{k \in \Phi_m} \mathbb{E}\{p_k\}$. Firstly, when $K = 1$, it is clear that $A_1 = \mathcal{P}_{a,1} \mathbb{E}\{p_1\}$. Next, when $K = n$, we assume that A_n can be simplified to $A_n = \sum_{k=1}^n \mathcal{P}_{a,k} \mathbb{E}\{p_k\}$. Then we will proceed to verify that $A_{n+1} = \sum_{k=1}^{n+1} \mathcal{P}_{a,k} \mathbb{E}\{p_k\}$ when $K = n+1$. The number of scenarios arisen due to the introduction of the $(n+1)$ th channel can be characterized into three categories: 1) When the $(n+1)$ th channel is active, the other n channel activities remain the same; 2) When the $(n+1)$ th channel is not active, the other n channel activities remain the same; 3) When the $(n+1)$ th channel is active, all the other n channels are not active. Noted that A_n excludes the scenario when all channels are turned off, so we have to include the additional case 3) in the representation of A_{n+1} .

Thus, A_{n+1} can be expressed as

$$\begin{aligned}
 A_{n+1} &= \mathcal{P}_{a,n+1} \sum_{m=1}^{2^n-1} \mathcal{P}_{s,m} \left(\sum_{k \in \Phi_m} \mathbb{E}\{p_k\} + \mathbb{E}\{p_{n+1}\} \right) + (1 - \mathcal{P}_{a,n+1}) \sum_{m=1}^{2^n-1} \mathcal{P}_{s,m} \left(\sum_{k \in \Phi_m} \mathbb{E}\{p_k\} \right) \\
 &\quad + \mathcal{P}_{a,n+1} \left(1 - \sum_{m=1}^{2^n-1} \mathcal{P}_{s,m} \right) \mathbb{E}\{p_{n+1}\} \\
 &= \mathcal{P}_{a,n+1} A_n + \mathcal{P}_{a,n+1} \mathbb{E}\{p_{n+1}\} \sum_{m=1}^{2^n-1} \mathcal{P}_{s,m} + (1 - \mathcal{P}_{a,n+1}) A_n
 \end{aligned}$$

$$\begin{aligned}
& + \left(1 - \sum_{m=1}^{2^n-1} \mathcal{P}_{s,m}\right) \mathcal{P}_{a,n+1} \mathbb{E}\{p_{n+1}\} \\
= & A_n + \mathcal{P}_{a,n+1} \mathbb{E}\{p_{n+1}\} = \sum_{k=1}^{n+1} \mathcal{P}_{a,k} \mathbb{E}\{p_k\}.
\end{aligned}$$

The objective function can also be verified in the same way. □

Appendix B

Proof of (5.16)

With $\mathbf{S} = P\mathbf{v}\mathbf{v}^\dagger$, the transmitter design problem for the conventional MISO CR channel is simplified as

$$\max_{\mathbf{v}} \quad \log_2 (1 + P|\mathbf{h}_s^\dagger \mathbf{v}|^2) \quad (\text{B.1})$$

$$\text{s.t.} \quad \|\mathbf{v}\|^2 \leq 1 \quad (\text{B.2})$$

$$|\mathbf{h}_p^\dagger \mathbf{v}|^2 \leq Q/P. \quad (\text{B.3})$$

Note that the objective function (B.1) remains invariant if $\mathbf{h}_s$ undergoes an arbitrary phase rotation. Thus, without loss of generality, we can assume $\text{Im}(\mathbf{h}_p^\dagger \mathbf{h}_s) = 0$ and $\text{Re}(\mathbf{h}_p^\dagger \mathbf{h}_s) \geq 0$. If we denote $\phi = \arccos(\check{\mathbf{h}}_p^\dagger \mathbf{h}_s / \|\mathbf{h}_s\|)$, then we have $(\check{\mathbf{h}}_p^\perp)^\dagger \mathbf{h}_s = \|\mathbf{h}_p^\perp\| = \|\mathbf{h}_s\| \sin \phi$. As a result, (5.15) can be simplified as

$$(\alpha_{CR}, \beta_{CR}) = \begin{cases} (\cos \phi, \sin \phi), & Q \geq P(\|\mathbf{h}_p\| \cos \phi)^2, \\ (\lambda, \sqrt{1 - \lambda^2}), & \text{otherwise.} \end{cases} \quad (\text{B.4})$$

Then the optimal beamforming vector can be expressed as (5.16) by substituting $\check{\mathbf{h}}_p = \frac{\mathbf{h}_s - \mathbf{h}_p^\perp}{\check{\mathbf{h}}_p^\dagger \mathbf{h}_s}$ into (5.14).

Appendix C

Proof of (5.18)

Firstly, we will show that the optimal beamforming vector is of the form $\mathbf{v} = \alpha \check{\mathbf{h}}_e + \beta \check{\mathbf{h}}_e^\perp$, where α and β are complex-valued weights. Since the optimal transmit covariance matrix is of the form $\mathbf{S} = P\mathbf{v}\mathbf{v}^\dagger$, the secrecy-capacity achieving design is reduced to the following problem

$$\max_{\|\mathbf{v}\|=1} \frac{1 + P|\mathbf{h}_s^\dagger \mathbf{v}|^2}{1 + P|\mathbf{h}_e^\dagger \mathbf{v}|^2}. \quad (\text{C.1})$$

Let the optimal beamforming vector be $\mathbf{v} = \alpha \check{\mathbf{h}}_e + \beta \check{\mathbf{g}}$, where $\check{\mathbf{g}}$ can be any unit-norm vector other than $\check{\mathbf{h}}_e^\perp$ that is orthogonal to $\check{\mathbf{h}}_e$, i.e., $\check{\mathbf{g}}^\dagger \check{\mathbf{h}}_e = 0$. Since $\mathbf{h}_e^\dagger \mathbf{v} = \alpha \|\mathbf{h}_e\|$ and $|\mathbf{h}_s^\dagger \check{\mathbf{h}}_e^\perp| \geq |\mathbf{h}_s^\dagger \check{\mathbf{g}}|$, it can then be seen that replacing $\check{\mathbf{g}}$ with $\check{\mathbf{h}}_e^\perp$ does not increase the transmit power and the received signal-to-noise ratio (SNR) $|\mathbf{h}_e^\dagger \mathbf{v}|^2$ at the eavesdropper, but always increases the SNR $|\mathbf{h}_s^\dagger \mathbf{v}|^2$ at the SU-Rx. It can thus be concluded that the optimal beamforming vector is of the form $\mathbf{v} = \alpha \check{\mathbf{h}}_e + \beta \check{\mathbf{h}}_e^\perp$, where $|\alpha|^2 + |\beta|^2 = 1$.

Secondly, we will show that α and β are real-valued numbers. Without loss of generality, we assume that $\text{Im}(\mathbf{h}_e^\dagger \mathbf{h}_s) = 0$ and $\text{Re}(\mathbf{h}_e^\dagger \mathbf{h}_s) \geq 0$. Denote $\psi = \arccos\left(\frac{\check{\mathbf{h}}_e^\dagger \mathbf{h}_s}{\|\mathbf{h}_s\|}\right)$, then we have $(\check{\mathbf{h}}_e^\perp)^\dagger \mathbf{h}_s = \|\mathbf{h}_e^\perp\| = \|\mathbf{h}_s\| \sin \psi$ and

$$\frac{1 + P|\mathbf{h}_s^\dagger \mathbf{v}|^2}{1 + P|\mathbf{h}_e^\dagger \mathbf{v}|^2} = \frac{1 + P\|\mathbf{h}_s\|^2 |\alpha \cos \psi + \beta \sin \psi|^2}{1 + P\|\mathbf{h}_e\|^2 |\alpha|^2} \quad (\text{C.2})$$

$$\leq \frac{1 + P\|\mathbf{h}_s\|^2(|\alpha| \cos \psi + |\beta| \sin \psi)^2}{1 + P\|\mathbf{h}_e\|^2|\alpha|^2}, \quad (\text{C.3})$$

where (C.3) is obtained from the triangle inequality, with the equality achieved when α and β have the same phase. Since $\mathbf{v}$ can be rotated by an arbitrary phase angle, we can assume α is of nonnegative real value, and hence also β .

Thirdly, we will compute the values of α and β . Since $\alpha^2 + \beta^2 = 1$, α and β can be expressed in terms of a single variable. We denote $\theta = \arctan \frac{\beta}{\alpha}$, then we have $\alpha = \cos \theta$ and $\beta = \sin \theta$. Then (C.1) becomes

$$\max_{\psi \leq \theta \leq \frac{\pi}{2}} h(\theta) \triangleq \frac{1 + P\|\mathbf{h}_s\|^2 \cos^2(\theta - \psi)}{1 + P\|\mathbf{h}_e\|^2 \cos^2 \theta}, \quad (\text{C.4})$$

where the constraint on θ is due to the fact that $\theta, \psi \in [0, \pi/2]$ and that it is always beneficial to choose $\theta = \psi + \Delta$ instead of $\theta = \psi - \Delta$ where $\Delta \in [0, \psi]$ since cosine function is decreasing in $[0, \pi/2]$. The optimal θ^* to maximize $h(\theta)$ resides on either the point $\frac{d(h(\theta))}{d\theta} = 0$ or the boundary points. The derivative of $h(\theta)$ can be obtained as

$$\frac{d(h(\theta))}{d\theta} = \frac{P(a \sin 2\theta + b \cos 2\theta - c)}{(1 + P\|\mathbf{h}_e\|^2 \cos^2 \theta)^2}, \quad (\text{C.5})$$

where

$$\begin{aligned} a &= \|\mathbf{h}_e\|^2 + \frac{P}{2}\|\mathbf{h}_s\|^2\|\mathbf{h}_e\|^2 - \|\mathbf{h}_s\|^2 \cos 2\psi \\ &\quad - \frac{P}{2}\|\mathbf{h}_s\|^2\|\mathbf{h}_e\|^2 \cos 2\psi \end{aligned} \quad (\text{C.6})$$

$$b = \|\mathbf{h}_s\|^2 \sin 2\psi + \frac{P}{2}\|\mathbf{h}_s\|^2\|\mathbf{h}_e\|^2 \sin 2\psi \quad (\text{C.7})$$

$$c = -\frac{P}{2}\|\mathbf{h}_s\|^2\|\mathbf{h}_e\|^2 \sin 2\psi. \quad (\text{C.8})$$

Hence, we have $a \sin 2\theta + b \cos 2\theta = c$. Let $\cos 2\theta = \omega$, then $\sin 2\theta = \sqrt{1 - \omega^2}$ and we

have

$$a\sqrt{1-\omega^2} = c - b\omega. \quad (\text{C.9})$$

The solution of (C.9) can be found as

$$\omega^* = \left\{ \omega \mid \omega = \frac{bc \pm |a|\sqrt{a^2 + b^2 - c^2}}{a^2 + b^2}, \frac{c - b\omega}{a} \geq 0 \right\}. \quad (\text{C.10})$$

It can be verified that $a^2 + b^2 - c^2 \geq 0$ and hence the solution always exists. Therefore, the optimal θ^* is given by

$$\theta^* = \underset{\theta \in \{\psi, \frac{\pi}{2}, \frac{1}{2}\arccos(\omega^*)\}}{\operatorname{argmax}} h(\theta) \quad (\text{C.11})$$

and the optimal beamforming vector is obtained as $\mathbf{v}_{WT}(\mathbf{h}_s, \mathbf{h}_e) = \cos \theta^* \check{\mathbf{h}}_e + \sin \theta^* \check{\mathbf{h}}_e^\perp$.

Finally, $\mathbf{v}_{WT}(\mathbf{h}_s, \mathbf{h}_e)$ can be transformed in a similar way as the CR channel (See Appendix B) to $\mathbf{v}_{WT}(\mathbf{h}_s, \mathbf{h}_e) = \alpha_{WT} \check{\mathbf{h}}_s + \beta_{WT} \check{\mathbf{h}}_e^\perp$, where $(\alpha_{WT}, \beta_{WT}) = \left(\frac{\cos \theta^*}{\cos \psi}, \sin \theta^* - \cos \theta^* \tan \psi \right)$.

Appendix D

Proof of Concavity of $\mathcal{G}(q)$

The Lagrangian of *Problem 5.6* can be written as $\mathcal{L}(\mathbf{S}, \mu, \nu_p, \nu_e, q) = 1 + \mathbf{h}_s^\dagger \mathbf{S} \mathbf{h}_s + \mu(P - \text{tr}(\mathbf{S})) + \nu_p(Q - \mathbf{h}_p^\dagger \mathbf{S} \mathbf{h}_p) + \nu_e(q - \mathbf{h}_e^\dagger \mathbf{S} \mathbf{h}_e)$. Since *Problem 5.6* is a convex function, the duality gap is zero. Hence, we have $\mathcal{G}(q) = \min_{\mu, \nu_p, \nu_e \geq 0} \max_{\mathbf{S} \succeq 0} \mathcal{L}(\mathbf{S}, \mu, \nu_p, \nu_e, q)$. Assuming that $q_1, q_2 \geq 0$ and $0 \leq \xi \leq 1$, we have

$$\begin{aligned}
& \mathcal{G}(\xi q_1 + (1 - \xi)q_2) \\
&= \min_{\mu, \nu_p, \nu_e \geq 0} \max_{\mathbf{S} \succeq 0} \mathcal{L}(\mathbf{S}, \mu, \nu_p, \nu_e, \xi q_1 + (1 - \xi)q_2) \\
&= \min_{\mu, \nu_p, \nu_e \geq 0} \max_{\mathbf{S} \succeq 0} \xi \mathcal{L}(\mathbf{S}, \mu, \nu_p, \nu_e, q_1) + (1 - \xi) \mathcal{L}(\mathbf{S}, \mu, \nu_p, \nu_e, q_2) \\
&\geq \min_{\mu, \nu_p, \nu_e \geq 0} \max_{\mathbf{S} \succeq 0} \xi \mathcal{L}(\mathbf{S}, \mu, \nu_p, \nu_e, q_1) + \min_{\mu, \nu_p, \nu_e \geq 0} \max_{\mathbf{S} \succeq 0} (1 - \xi) \mathcal{L}(\mathbf{S}, \mu, \nu_p, \nu_e, q_2) \\
&= \xi \mathcal{G}(q_1) + (1 - \xi) \mathcal{G}(q_2). \tag{D.1}
\end{aligned}$$

Therefore, $\mathcal{G}(q)$ is a concave function by the definition in [194, p. 67].

Appendix E

Proof of Proposition 6.8

Proof. Assume that $\mathbf{S}^*$ is the optimal covariance matrix of *Problem 6.6* with $q = q^o$, where $\mathbf{S}^* \neq \mathbf{S}^o$. If $\min_{\mathbf{h}_s \in \mathcal{H}_s} \mathbf{h}_s^\dagger \mathbf{S}^* \mathbf{h}_s < \min_{\mathbf{h}_s \in \mathcal{H}_s} \mathbf{h}_s^\dagger \mathbf{S}^o \mathbf{h}_s$, $\mathbf{S}^o$ is a better solution for *Problem 6.6* since it satisfies all the constraints. This contradicts the assumption that $\mathbf{S}^*$ is the optimal solution for *Problem 6.6*. If $\min_{\mathbf{h}_s \in \mathcal{H}_s} \mathbf{h}_s^\dagger \mathbf{S}^* \mathbf{h}_s > \min_{\mathbf{h}_s \in \mathcal{H}_s} \mathbf{h}_s^\dagger \mathbf{S}^o \mathbf{h}_s$, then $\mathbf{S}^*$ is a better solution for *Problem 6.3* since $\max_{\mathbf{h}_e \in \mathcal{H}_e} \mathbf{h}_e^\dagger \mathbf{S}^* \mathbf{h}_e \leq q^o$. This contradicts the assumption that $\mathbf{S}^o$ is the optimal solution for *Problem 6.3*. Therefore, $\min_{\mathbf{h}_s \in \mathcal{H}_s} \mathbf{h}_s^\dagger \mathbf{S}^* \mathbf{h}_s = \min_{\mathbf{h}_s \in \mathcal{H}_s} \mathbf{h}_s^\dagger \mathbf{S}^o \mathbf{h}_s$ and $\mathbf{S}^* = \mathbf{S}^o$. $\square$

Appendix F

Proof of Proposition 6.9

Proof. The equivalency of the two problems can be shown via *Problem 6.6*. Denote the optimal objective values of *Problem 6.3* and *Problem 6.10* by f^o and $\tilde{f}$, respectively. The proof can be divided into two parts. First, we shall show that the optimal objective value of *Problem 6.3* can be achieved by *Problem 6.10*, i.e., $f^o \leq \tilde{f}$. Denote $t^o = \min_{\mathbf{h}_s \in \mathcal{H}_s} \mathbf{h}_s^\dagger \mathbf{S}^o \mathbf{h}_s$, then the maximum value of *Problem 6.3* is $f^o = (1 + t^o)/(1 + q^o)$. By Proposition 6.8, $\mathbf{S}^o$ is also optimal for *Problem 6.6* with $q = q^o$. Then, we have $\mathcal{G}(q^o) = t^o$. Therefore, f^o is achievable for *Problem 6.10*. Next, we shall show by contradiction that the maximum objective value of *Problem 6.10* can also be achieved by *Problem 6.3*, i.e., $f^o \geq \tilde{f}$. Denote the optimal solution of *Problem 6.10* by $\tilde{q}$ and the optimal solution of *Problem 6.6* with $q = \tilde{q}$ by $\tilde{\mathbf{S}}$. If $f^o < \tilde{f}$, then we have $f^o < \frac{1 + \min_{\mathbf{h}_s \in \mathcal{H}_s} \mathbf{h}_s^\dagger \tilde{\mathbf{S}} \mathbf{h}_s}{1 + \tilde{q}} \leq \frac{\min_{\mathbf{h}_s \in \mathcal{H}_s} (1 + \mathbf{h}_s^\dagger \tilde{\mathbf{S}} \mathbf{h}_s)}{\max_{\mathbf{h}_e \in \mathcal{H}_s} (1 + \mathbf{h}_e^\dagger \tilde{\mathbf{S}} \mathbf{h}_e)}$, which indicates that $\tilde{\mathbf{S}}$ is a better solution for *Problem 6.3* than $\mathbf{S}^o$. This contradicts the assumption that $\mathbf{S}^o$ is the optimal solution for *Problem 6.3*. Hence, we have $f^o \leq \tilde{f}$. The proof is thus completed by combining the two parts. $\square$

Appendix G

Proof of Quasiconcavity of (6.40)

Proof. We will first show that $\mathcal{G}(q)$ is a concave function. Note that *Problem 6.6* and *Problem 6.7* are equivalent with the same objective value, and strong duality holds for the convex *Problem 6.7*. Thus, we have

$$\mathcal{G}(q) = \min_{\Phi \succeq 0} \max_{(\mathbf{S}, t, s, p, e) \in \mathcal{F}} \mathcal{L}(\mathbf{S}, t, s, p, e, \Phi, q), \quad (\text{G.1})$$

where Φ is the lagrange multiplier associated with (6.39); $\mathcal{F}$ is the combined constraint set defined by (6.36), (6.37) and (6.38), i.e., $\mathcal{F} = \{\mathbf{S} \succeq 0, t, s, p, e \geq 0 | (6.36), (6.37), (6.38)\}$; and $\mathcal{L}(\mathbf{S}, t, s, p, e, \Phi, q)$ is the partial Lagrangian w.r.t. the constraint (6.39). Furthermore, denoting

$$\Phi = \begin{bmatrix} \phi_a & \Phi_{b,1 \times N} \\ \Phi_{b,1 \times N}^\dagger & \Phi_{c,N \times N} \end{bmatrix}, \quad (\text{G.2})$$

$$\mathbf{A}(\mathbf{S}, e) = \begin{bmatrix} -\hat{\mathbf{h}}_e^\dagger \mathbf{S} \hat{\mathbf{h}}_e - e & -\hat{\mathbf{h}}_e^\dagger \mathbf{S} \\ -\mathbf{S} \hat{\mathbf{h}}_e & -\mathbf{S} + e \mathbf{W}_e \end{bmatrix}, \quad (\text{G.3})$$

$$\mathbf{B}(q) = \begin{bmatrix} q & \mathbf{0}_{1 \times N} \\ \mathbf{0}_{N \times 1} & \mathbf{0}_{N \times N} \end{bmatrix}, \quad (\text{G.4})$$

we have

$$\mathcal{L}(\mathbf{S}, t, s, p, e, \mathbf{\Phi}, q) = t + \text{tr}(\mathbf{\Phi}(\mathbf{A}(\mathbf{S}, e) + \mathbf{B}(q))) = t + \text{tr}(\mathbf{\Phi}\mathbf{A}(\mathbf{S}, e)) + \phi_a q. \quad (\text{G.5})$$

Then, the concavity of $\mathcal{G}(q)$ will be shown by the definition of convexity. Suppose $q_1, q_2 \geq 0$. Then, for any $0 \leq \theta \leq 1$, we have

$$\begin{aligned} & \mathcal{G}(\theta q_1 + (1 - \theta)q_2) \\ &= \min_{\mathbf{\Phi} \succeq 0} \max_{(\mathbf{S}, t, s, p, e) \in \mathcal{F}} \mathcal{L}(\mathbf{S}, t, s, p, e, \mathbf{\Phi}, \theta q_1 + (1 - \theta)q_2) \\ &= \min_{\mathbf{\Phi} \succeq 0} \max_{(\mathbf{S}, t, s, p, e) \in \mathcal{F}} \theta \mathcal{L}(\mathbf{S}, t, s, p, e, \mathbf{\Phi}, q_1) + (1 - \theta) \mathcal{L}(\mathbf{S}, t, s, p, e, \mathbf{\Phi}, q_2) \\ &\geq \min_{\mathbf{\Phi} \succeq 0} \max_{(\mathbf{S}, t, s, p, e) \in \mathcal{F}} \theta \mathcal{L}(\mathbf{S}, t, s, p, e, \mathbf{\Phi}, q_1) + \min_{\mathbf{\Phi} \succeq 0} \max_{(\mathbf{S}, t, s, p, e) \in \mathcal{F}} (1 - \theta) \mathcal{L}(\mathbf{S}, t, s, p, e, \mathbf{\Phi}, q_2) \\ &= \theta \mathcal{G}(q_1) + (1 - \theta) \mathcal{G}(q_2). \end{aligned} \quad (\text{G.6})$$

Therefore, $\mathcal{G}(q)$ is a concave function of q . Furthermore, it can be easily shown that the superlevel set of (6.40) is concave. Therefore, by the definition of quasiconvexity, (6.40) is quasiconcave [194, p. 95]. $\square$

Appendix H

Sample Simulation Code

Chapter 3

```

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Settings                                                                 %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
M=3;                               % number of channels
SNR_P_dB = [ -12;-15; -20];        % primary user worst-ase SNR in dB
SNR_P= 10.^(SNR_P_dB./10);
BW = 6*10^6;                       % Bandwidth
T = 100*10^(-3);                   % Frame duration
P_d_exp=[0.9; 0.9; 0.9];           % Target Probability of detection
P_P = [0.2; 0.2;0.2];              % PU busy probability
gain=[1; 1; 1];                    % average channel gain
N=1;                                % noise power
P_tot_dB=[5:5:20];                 % transmit power in dB
P_tot=10.^(P_tot_dB./10);
delta = 10^(-6);                   % precision to 0.00001ms

Qinvpd=sqrt(2).*erfcinv(2.*P_d_exp); % Q^(-1)(Pd0)
alpha = sqrt(2.*SNR_P+1).*Qinvpd;
interval=[0:10^(-6):30*10^(-3)];   % Set of sensing time
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Compute optimal Solutions (Average Transmit Power)                     %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
for k=1:size(P_tot,2)
    for n=1:size(interval,2)
        %-----%
        % 1. Calculate P_{a_k} for a given sensing time
        P_1 = ( (1-P_P).*(1-erfc((alpha+ sqrt(interval(n).*BW).*SNR_P)./sqrt(2))./2) + P_P.*(1-P_d_exp));
        %-----%
        % 2. Find the optimal waterlevel for the given sensing time
        wlv=50;
        for m=1:10^8
            beta = expint(N./wlv./gain);
            gamma = exp(-N./wlv./gain);
            h = P_1*(wlv.*gamma -N./gain.*beta)-P_tot(k);          % function F for Rayleigh fading
            if abs(h)<delta
                C = 1/log(2) .* beta;
                break;
            end
            dh= P_1*gamma;      % first-order derivative of function F
            wlv = wlv - h/dh;
        end
    end
end

```

```

end
%-----%
% 3. Calculate the maximum capacity for the given sensing time
Throughput(n,k)=(T-interval(n))./T.* (C'*P_1);

end%interval
end%P_tot

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Plot Figure 3.3 (For average transmit Power) %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
figure(1);
for k=1:size(P_tot,2)
    plot(interval.*1000,Throughput(:,k));
    xlabel('Sensing time (ms)');
    ylabel('Total ergodic throughput of the secondary network bits/sec/Hz');
    grid on;
    hold all;
end
legend('P_{total}= 5 dB','P_{total}= 10 dB','P_{total}=15 dB','P_{total}=20 dB',4);
hold off;

```

Chapter 4

```

global N B sigma2 Gamma P_min P_max P_s P_c G LM T tau val_x prob_x omega ALPHA
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Settings %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
B = 6*10^6; % Bandwidth
N_0_2 = -204; % Noise PSD, N_0/2, in dBW
Nf = 10; % Noise figure, in dB
sigma2 = 10^(N_0_2/10)*2*B*10^(Nf/10);
% Noise Power, in Watt
BER = 10^(-5); % Bit error rate
Gamma = -log(5*BER)/1.5; % SNR gap to capacity
%-----%
d = 200; % Distance
%-----%
P_min = 1*10^(-3); % Maximum Transmit Power, in Watt
LM_dB = 10; % Link Margin in dB
LM = 10^(-LM_dB/10);
P_H0 = 0.8; % Probability of absence (idle) of PU channels (same across all channels)
T = 100*10^(-3); % Transmission time
%-----%

```

```

% Power Amplifier
PAPR_dB = 6;           % Peak to Average Ratio
PAPR = 10^(PAPR_dB/10);
DE = 0.35;             % Drain Efficiency
ALPHA = PAPR/DE;
%-----%
P_s  = 110*10^(-3);    % Sensing Power, in Watt
P_c  = 210*10^(-3);    % Circuit Power, in Watt
P_max = (10^(33/10)*10^(-3)-100*10^(-3))/ALPHA % Maximum Transmit Power, in Watt,
1W=30dBm=0dBW
%-----%
% SU Fading
val_SU_x  = [1:5];      % SU channel fading levels
val_x     = [0:5];      % 0 indicates primary channel is busy, others is val_SU_x
prob_SU_x = [0.64 0.23 0.09 0.03 0.01]; % probability of each fading levels
%-----%
% Sensing
Pd = 0.9;              % Target Probability of detection
fs = B;                % Sampling frequency
SNR_P_dB = -20;        % Worst-case PU SNR in dB
SNR_P = 10^(SNR_P_dB/10);
%-----%
NUMCH = [9:-2:1];      % Set of number of channels
Sen_Time = [0.1:1:35].* 10^(-3); % Set of Sensing time
opt_L = zeros(size(Sen_Time,2),size(NUMCH,2)); %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Compute optimal Solutions (Theoretical) (Theoretical) %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

for n = 1:size(NUMCH,2)
    N = NUMCH(n);      % Number of channels
    fc = 800*10^6 + [0 cumsum(B.*ones(1,N-1))]; % Carrier frequency
    G = (3*10^8./fc./4./pi./d).^2; % Propagation loss

    for k = 1:size(Sen_Time,2)
        tau = Sen_Time(k);
        % False alarm probability
        Pf = qfunc( sqrt(2*SNR_P+1)* qfuncinv(Pd) + sqrt(tau.*fs).*SNR_P );
        theta = P_H0 .*(1-Pf) + (1-P_H0).*(1-Pd);
        omega = P_H0 .*(1-Pf)./theta;
        prob_x = [1-theta theta.*prob_SU_x];
        %-----%
        % Bisection (Theorectic Calculation) %
    end
end

```

```

                                %-----%
                                [opt_L(k,n) temp] = func_opt_bisection;
                                end
                                end

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Plot Figure 4.4
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
figure(1);
legendtext = '';
for n = 1:size(NUMCH,2)
    plot(Sen_Time.*10^3, opt_L(:,n)./log(2)./B, '-');
    legendtext = strvcat(legendtext, ['N = ', num2str(NUMCH(n))]);
end
hold all;
xlabel('Sensing Time \tau (ms)');
ylabel('Energy Efficiency bits/Hz/Joule');
grid on;
legend(legendtext,1);

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Function Definition: func_opt_bisection
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Calculate the optimal lambda (L) using bisection over the parametric problem
function [opt_L opt_EJ] = func_opt_bisection
%-----%
% Bisection
%-----%
esp = 10^(-7); % tolerance
LB = 1*10^6; % lower bound
UB = 1*10^9; % upper bound
%-----%
while(1)
    L = (LB+UB)/2;
    temp_EJ = func_parametric_discrete(L);
    if abs(temp_EJ(1))<=esp
        opt_L=L;
        opt_EJ = temp_EJ;
        break;
    else
        if temp_EJ(1)<=0
            UB=L;
        else
            LB=L;
        end
    end
end

```



```

end
end
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Function Definition: func_parametric_disc
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
function [EJ] = func_parametric_discrete(L);
% Solve the parametric formulation for a given lambda (L) for the case of constant transmission time
global N B sigma2 Gamma P_min P_max P_s P_c G LM T tau val_x prob_x omega ALPHA
%-----%
% Calculate optimal Power and f_star (eq. (4.12))
val_u = zeros(size(val_x,2), N);
val_f_star = zeros(size(val_x,2), N);
for j = 2:size(val_x,2)
    val_u(j,:) = omega*B/L/ALPHA - Gamma*sigma2./G./LM./val_x(j);
    ind1 = find(val_u(j,:) <= P_min);
    val_u(j,ind1) = P_min;
    ind2 = find(val_u(j,:) >= P_max);
    val_u(j,ind2) = P_max;
    val_f_star(j,:) = omega.*T.*B.*log(1+val_x(j).*val_u(j,:)./(Gamma.*sigma2./G./LM))
L.*T.*(ALPHA.*val_u(j,:) + P_c);
end
%-----%
% Backward induction for DP
%-----%
EJ = -L*tau*P_s * ones(N,1);
%-----%
% Channel N: Calculate E[J_N]
%-----%
EJ(N) = EJ(N) + prob_x(2:size(val_x,2))*val_f_star(2:size(val_x,2),N);
%-----%
% Channel k = 1, ..., N-1: Calculate E[J_k]
%-----%
for k = [N-1:-1:1]
    temp = 0;
    for j = 2:size(val_x,2)
        if val_f_star(j,k) >= EJ(k+1)
            temp = temp + prob_x(j)*val_f_star(j,k);
        else
            temp = temp + prob_x(j)*EJ(k+1);
        end
    end
end

EJ(k) = EJ(k) + prob_x(1)*EJ(k+1)+ temp;

```

```
end
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

Chapter 5

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Settings
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
M = 3;          % Number of transmit antenna at SU-Tx
P_dB = [-5:5:25]; % Transmit power limit (dB)
Q_dB = -20;      % Interference temperature limit (dB)
P = 10.^(P_dB./10);
Q = 10.^(Q_dB./10);
NRUN = 10000;    % number of simulations
%-----
--%
SC_CR_SDP = zeros(size(P_dB,2),1); % Secrecy Capacity computed with SDP
SC_CR_VCRN = zeros(size(P_dB,2),1); % Secrecy Capacity computed with ACRN
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Monte-Carlo Simulation
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
for np=1:size(P_dB,2)
    for nRun = 1:NRUN
        %-----%
        hs = 1/sqrt(2).*(randn(M,1)+i.*randn(M,1)); % channel from SU-Tx to SU-Rx
        he = 1/sqrt(2).*(randn(M,1)+i.*randn(M,1)); % channel from SU-Tx to ED
        hp = 1/sqrt(2).*(randn(M,1)+i.*randn(M,1)); % channel from SU-Tx to PU
        %-----%
        % 1. SDP Transformation
        [Cap1 S_SC_CR] = SCCRSDP(hs,he,hp,P(np),Q);
        SC_CR_SDP(np)=SC_CR_SDP(np)+log2(Cap1);
        %-----%
        % 2. ACRN Transformation
        [Cap] = CRSC_VCR(hs,he,hp,P(np),Q);
        SC_CR_VCRN(np)=SC_CR_VCRN(np)+log2(Cap);
        %-----%
    end
end

figure(1)
plot(P_dB,SC_CR_SDP./NRUN,'o-',P_dB,SC_CR_VCRN./NRUN,'*-');
legend('Secure CR (SDP)','Secure CR (ACRN)',4)
```

```

ylabel('Secrecy Capacity');
xlabel('Transmit Power P(dB)')
grid on;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Function Definitions: SCCRSDP
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
function [C S] = SCCRSDP(hs,he,hp,P,Q)
% SDP Transformation: Solve Problem 5.4 using SeDuMi
% Transform it into Standard Primal Form that can be solved by SeDuMi
% min c'x
% st. Ax=b
% x in K

% C: Secrecy capacity (without log2)
% S: transmit covariance matrix

M = size(hs,1);
Hs=hs*hs';
He=he*he';
Hp=hp*hp';

c = -[1; 0; 0; vec(Hs')];
A1 = [-P 1 0; -Q 0 1; 1 0 0];
A2 = [vec(eye(M)) vec(Hp.') vec(He.')]';
A=[A1 A2];
b=[0;0;1];

K.l = [3]; % Number of nonnegative variables
K.s = [M]; % Dimension of positive semidefinit matrix
K.xcomplex=[];
K.scomplex = 1;
K.ycomplex=[1:3];

pars.fid = 0;
[x,y,info]=sedumi(A,b,c,K,pars);

St=mat(x(4:end));
S=St/x(1);
C = real(-c'*x);

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Function Definitions: CRSC_VCR
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
function [C] = CRSC_VCR(hs,he,hp,P,Q)
% ACRN Transformation: Solve Problem 5.8 using Golden Section Search

rmin = 0; % r>=0
rmax = 10^(20/10); % 20dB ([*]:adjust)
d = (sqrt(5)-1)/2; % Golden section number
esp = 10^(-6); % tolerance

```

```

r1=d*rmin+(1-d)*rmax;
r2=d*rmax+(1-d)*rmin;
[g1]=CRmPUSDP(hs,[hp he],P,[Q;r1]);
[g2]=CRmPUSDP(hs,[hp he],P,[Q;r2]);

while(1)
    if g1/(1+r1) > g2/(1+r2)
        rmax=r2;
        r2=r1;
        r1=d*rmin+(1-d)*rmax;
        g2=g1;
        [g1]=CRmPUSDP(hs,[hp he],P,[Q;r1]);
    else
        rmin=r1;
        r1=r2;
        g1=g2;
        r2=d*rmax+(1-d)*rmin;
        [g2]=CRmPUSDP(hs,[hp he],P,[Q;r2]);
    end

    if abs(rmax-rmin)<=esp
        break;
    end
end
C = g1/(1+r1);

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Function Definitions: CRmPUSDP
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
function [C]=CRmPUSDP(h,g,P,Q)
% Solve Problem 5.8 using Algorithm 4 with Sedumi
% Transform the problem into the standard dual form

% h: MISO channel from SU-TX to SU-RX (column vector)
% g(:,n): MISO channel from SU-Tx to nth PU (column vector)
% P: transmit power
% Q(n): interference power limit of nth PU (column vector)
% C: Capacity w/o log2

M = size(h,1); % number of transmit antennas at SU-TX
N = size(g,2); % number of PUs

%% objective
b=-[P;Q]; %(["-" sign]: standard dual form in Sedumi: max obj)

%% nonnegative lagrange multipliers
c = sparse(N+1,1); %zeros(N+1,1);
At = -speye(N+1);

K.l = [N+1];
K.xcomplex=[];

```

```

%%% positive semidefinite cone
% [*]: sedumi restricts  $\text{mat}(c - A^T y) + \text{mat}(c - A^T y)' \succeq 0$ 
% let  $c - A^T y = \text{diag} + 2 * \text{triu}(:, 1)$ 

H = h*h';
Hd = spdiags(diag(H),0,M,M); % diag(diag(H))
Hut = sparse(triu(H,1)); % take the upper triangular of H, without the diagonal
c=[c;vec(-Hd-2*Hut)];

At2 = -vec(speye(M));
for n=1:N
    G = g(:,n)*g(:,n)';
    Gd = spdiags(diag(G),0,M,M); % diag(diag(H))
    Gut = sparse(triu(G,1)); % take the upper triangular of H, without the diagonal
    At2=[At2 -vec(Gd+2*Gut)];
end
At=[At;At2];
K.s=[M];
K.scomplex=1;
K.ycomplex=[]; % real lagrange multipliers

[x,y,info]=sedumi(At,b,c,K);

C=1-b.*y;

```

Chapter 6

```

%% Settings
M = 4; % number of transmit antennas at SU-Tx

Ws = 1/(1*10^(-3))*eye(M); % uncertainty in hs
Wp = 1/(1*10^(-3))*eye(M); % uncertainty in hp
We = 1/(1*10^(-3))*eye(M); % uncertainty in he

P_dB = [0:4:20]; % transmit power limit
Q_dB = -10; % interference threshold
P = 10.^(P_dB./10);
Q = 10.^(Q_dB./10);

nRun = 1000;

Cap_SDP = zeros(size(P_dB,2),1);
Cap_ACRN = zeros(size(P_dB,2),1);

%% Simulations

```

```

for nP = 1:size(P,2)
    for nr = 1:nRun

        % iid Rayleigh fading channel
        hs0 = 1/sqrt(2).*(randn(M,1)+ 1i.* randn(M,1)); % mean channel from SU-Tx to SU-Rx
        he0 = 1/sqrt(2).*(randn(M,1)+ 1i.* randn(M,1)); % mean channel from SU-Tx to ED
        hp0 = 1/sqrt(2).*(randn(M,1)+ 1i.* randn(M,1)); % mean channel from SU-Tx to PU

        %-----%
        % SDP Transformation
        %-----%
        [C S_opt] = RSCRN_SDP(hs0, hp0, he0,P(nP), Q, Ws, Wp, We);
        Cap_SDP(nP) = Cap_SDP(nP) + log2(C);
        %-----%
        % ACRN Transformation
        %-----%
        [C S_opt] = RSCRN_VCRN(hs0, hp0, he0,P(nP), Q, Ws, Wp, We);
        Cap_ACRN(nP) = Cap_ACRN(nP) + log2(C);

    end
end

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Plot
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
figure(1);
plot(P_dB, Cap_SDP./nRun, '-s', P_dB, Cap_ACRN./nRun, '-o');
legend('SDP Transformation', 'ACRN Transformation', 2);
xlabel('Transmit Power P (dB)')
ylabel('Achievable Secrecy Rate (bps/Hz)')
grid on

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Function Definition: RSCRN_SDP
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
function [C S] = RSCRN_SDP(hs0, hp0, he0,P, Q, Ws, Wp, We)
% SDP Transformation
% Solve Problem 6.14 using the Yalmip interface that uses SeduMi as the
% solver
% C: secrecy rate w.o. log2
% St: transmit covariance matrix

M = size(hs0,1);

tau = sdpvar(1,1);
t = sdpvar(1,1);
s = sdpvar(1,1);
p = sdpvar(1,1);
e = sdpvar(1,1);
St = sdpvar(M,M,'hermitian','complex');

```

```

F = [tau>=0, t>=0, s>=0, p>=0, e>=0, St>=0, trace(St)-P*t<=0];
F = [F, [ -hp0'*St*hp0 + t*Q-p      -hp0'*St ;      -St*hp0      -St+p*Wp] >=0];
F = [F, [ hs0'*St*hs0 + t-tau-s      hs0'*St ;      St*hs0      St+s*Ws] >=0];
F = [F, [ -he0'*St*he0 - t+1-e      -he0'*St ;      -St*he0      -St+e*We] >=0];

ops = sdpsettings('solver','sedumi','verbose',0);
solvesdp(F, -tau,ops);

C = double(tau);
S = double(St/t);

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Function Definition: RSCRN_SDP
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
function [Cap S_opt] = RSCRN_VCRN(hs0, hp0, he0,P, Q1, Ws, Wp, We)
% ACRN Transformation
% Solve Problem 6.10 using Golden Section Search
rmin = 0;
rmax = 10^(20/10);
d = (sqrt(5)-1)/2; % golden section number
esp = 10^(-6);

r1=d*rmin+(1-d)*rmax;
r2=d*rmax+(1-d)*rmin;
[g1 S1]=F_RCRN(hs0, hp0, he0,P, Q1, r1, Ws, Wp, We);
[g2 S2]=F_RCRN(hs0, hp0, he0,P, Q1, r2, Ws, Wp, We);

while(1)
    if g1/(1+r1) > g2/(1+r2)
        rmax=r2;
        r2=r1;
        r1=d*rmin+(1-d)*rmax;
        g2=g1;
        [g1 S1]=F_RCRN(hs0, hp0, he0,P, Q1, r1, Ws, Wp, We);
    else
        rmin=r1;
        r1=r2;
        g1=g2;
        r2=d*rmax+(1-d)*rmin;
        [g2 S2]=F_RCRN(hs0, hp0, he0,P, Q1, r2, Ws, Wp, We);
    end

    if abs(rmax-rmin)<=esp
        break;
    end
end

Cap = g1/(1+r1);
S_opt = S1;

```

```

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Function Definition: F_RSCRN
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
function [C St] = F_RSCRN(hs0, hp0, he0,P, Q1, Q2, Ws, Wp, We)
% Solve Problem 6.7 in Yalmip
% C: capacity w.o. log2
% St: transmit covariance matrix

M = size(hs0,1);

t = sdpvar(1,1);
s = sdpvar(1,1);
p = sdpvar(1,1);
e = sdpvar(1,1);
S = sdpvar(M,M,'hermitian','complex');

F = [S>=0, t>=0, s>=0, p>=0, e>=0, trace(S)-P<=0];
F = [F, [ hs0'*S*hs0-t-s      hs0'*S;    S*hs0    S+s*Ws] >=0];
F = [F, [ -hp0'*S*hp0+Q1-p    -hp0'*S;    -S*hp0    -S+p*Wp] >=0];
F = [F, [ -he0'*S*he0+Q2-e    -he0'*S;    -S*he0    -S+e*We] >=0];

ops = sdpsettings('solver','sedumi','verbose',0);
solvesdp(F,-t,ops);

C = 1+double(t);
St = double(S);

```