ABSTRACT

Title of dissertation: GAME-THEORETIC STRATEGIES FOR DYNAMIC BEHAVIOR IN COGNITIVE RADIO NETWORKS

Yongle Wu, Doctor of Philosophy, 2010

Dissertation directed by: Professor K. J. Ray Liu
Department of Electrical and Computer Engineering

Cognitive radio technology is a new revolutionary communication paradigm which allows flexible access to spectrum resources and leads to efficient spectrum sharing. Recent studies have shown that cognitive radio is a promising approach to improve efficiency of spectrum utilization, because wireless users are capable of accessing the spectrum in an intelligent and adaptive manner. The theory of cognitive radio is however still immature to fully understand its broader impacts on the design of future wireless networks. This dissertation contributes to the advancement of cognitive radio technology by analyzing wireless users' interaction in a network and developing game-theoretic frameworks to suppress selfish and malicious behaviors, with the goal to improve system performance by stimulating selfish users and enhance network security against malicious users.

We first develop a cheat-proof repeated spectrum sharing game, which provides the incentive for selfish users to cooperate with each other and reveal their private information truthfully. We propose specific cooperation rules based on the maximum

total throughput and proportional fairness criteria, and investigate the impact of spectrum sensing duration on system performance.

We also consider the situation where a group of selfish users collude for higher payoffs. We propose a novel multi-winner spectrum auction framework which did not exist in auction literature, and develop collusion-resistant auction mechanisms to suppress collusive behavior. In addition, we apply the semi-definite programming relaxation to significantly reduce the complexity of algorithms.

When malicious users are taken into consideration, we apply game-theoretic tools to suppress potential malicious behavior in cognitive radio networks. Specifically, we model the anti-jamming defense as a zero-sum game, and derive the optimal strategy for secondary users to execute in face of jamming threats. Moreover, we propose learning schemes for secondary users to gain knowledge of adversaries.

Finally, we consider security countermeasures against eavesdroppers, and propose a cooperative paradigm that primary users improve secrecy with the help of trustworthy secondary users. We derive the achievable pair of primary users' secrecy rate and secondary users' transmission rate under various circumstances, and model the interaction between primary users and secondary users as a Stackelberg game.

GAME-THEORETIC STRATEGIES FOR DYNAMIC BEHAVIOR IN COGNITIVE RADIO NETWORKS

by

Yongle Wu

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2010

Advisory Committee:
Professor K. J. Ray Liu, Chair/Advisor
Professor Min Wu
Professor Mark A. Shayman
Professor T. Charles Clancy
Professor Lawrence C. Washington

Dedication

To my family.

Acknowledgments

I owe my deepest gratitude to my advisor, Professor K. J. Ray Liu, without whom this dissertation would not have been possible. With his great enthusiasm and forward-thinking vision, Dr. Liu has been my inspiration for conducting cutting-edge research on wireless communications over the past few years. Dr. Liu spared no effort in helping me for both professional advancement and personal development, and he was always available whenever I needed his advice. I am extremely grateful to Dr. Liu for his support, guidance, encouragement, patience, and understanding in various aspects.

I would like to thank other members in my dissertation committee. Special thanks are due to Professor T. Charles Clancy for his collaboration and enormous help that led to fruitful research results. I would also like to thank Professor Min Wu not only for serving on the committee but also for her continuous support and kind guidance. I am also grateful to Professor Mark A. Shayman and Professor Lawrence C. Washington for their time and effort serving on my committee.

I would like to thank every member in our Signals and Information group for their friendship, encouragement, and help. I have learned a lot from each one of them, and for that I am deeply grateful. My special thanks go to Dr. Beibei Wang, Mr. Yan Chen, Dr. Ahmed Sadek, and Dr. Wan-Yi Lin for our research discussions that were all inspiring for me.

I would like to thank Professor André L. Tits, Professor Alexander Barg, Professor Peter Cramton, and other faculty members in University of Maryland. I learned a lot from their lectures and benefited even more from their great help and wise advice. I also want to thank other friends for the wonderful time we spent together.

Finally, I would like to thank my entire family— my parents, my grandparents, and my wife, for their endless support and love. Without them, I would not have been able to accomplish this achievement. I dedicate this dissertation to them.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Motivation

With the emergence of new wireless applications and devices, the last decade has witnessed a dramatic increase in the demand for radio spectrum, which has forced the government agencies such as Federal Communications Commission (FCC) to review their policies [1]. The traditional rigid allocation policies by FCC have severely hindered the efficient utilization of scarce spectrum. Hence, dynamic spectrum access, with the aid of cognitive radio technology [2], has become a promising approach by breaking the paradigm and enabling wireless devices to utilize the spectrum adaptively and efficiently.

Depending on the regulation of spectrum bands in which they operate, cognitive radio networks can be roughly classified into three categories. The first one is the open sharing in the unlicensed band on which nobody owns the exclusive right. For instance, the industrial, scientific, and medical (ISM) radio band, in which WLAN networks, bluetooth systems, cordless phones, and other novel wireless devices coexist, demonstrates success and importance of open sharing. Nevertheless, unlicensed sharing without regulation usually leads to the overuse of the time/frequency/power units, and in order to avoid such inefficient usage, as suggested in [3], basic open access protocols/etiquettes have to be set by either government or industry standardization. In [4], spectrum sharing in the unlicensed band with time-invariant flat-fading channels was formed into a repeated game and the Pareto optimal frontier was obtained. In [5], iterative waterfilling power allocation was proposed for Gaussian interference channels with frequency-selective fading, and some practical difficulties the method were circumvented in [6] by exchanging "interference price" which took mutual interference into consideration.

The second category "the opportunistic dynamic spectrum access" has received more research interest. In this case, licensed spectrum bands are owned by legacy spectrum holders (a.k.a "primary users"), but unlicensed users (a.k.a "secondary users") are allowed to access the bands as long as they do not interfere with primary users. Secondary users have to frequently sense the radio environment to detect the presence of primary users. Whenever finding a spectrum opportunity when the primary user is absent, secondary users are allowed to occupy the spectrum; but they must immediately vacate the band when the primary user appears. There were a lot of works on the opportunistic dynamic spectrum access. To name a few, in [7], three ways to sense the presence of primary users, including matched filtering, energy detection, and feature detection, have been investigated. [8] showed that the detection time could be reduced and spectrum agility could be enhanced through user cooperation in spectrum sensing. The authors in [9] proposed a primary prioritized Markov dynamic spectrum access scheme to optimally coordinate secondary users' spectrum access.

The last category, sometimes known as the "negotiation-based dynamic spectrum access", has been intensively studied, too. This kind of the cognitive radio network also operates in the licensed band, but different from the previous approach, there is some cooperation between primary users and secondary users such that spectrum opportunities are announced by primary users rather than discovered by secondary users. Since primary users have the incentive to trade their temporarily unused bands for monetary gains and secondary users want to lease some bands for data transmission, they may negotiate the price for a short-term lease. For example, [10] proposed a real-time spectrum auction framework where secondary users submitted their price-demand curves and the primary user employed revenue-maximizing auction clearing algorithms. In [11], distributed ascending clock auction schemes were proposed for multimedia streaming over cognitive radio networks. In [12], double auction mechanisms were used to efficiently allocate spectrum resources when there were not only multiple secondary users but also multiple primary users.

A notable difference of a cognitive radio network from traditional wireless networks is that users need to be aware of the dynamic environment and adaptively adjust their operating parameters based on the interactions with the environment and other users in the network. Traditional spectrum sharing and management approaches, however, generally assume that all network users cooperate unconditionally in a static environment, and thus they are not applicable to a cognitive radio network. In a cognitive radio network, users are intelligent and have the ability to observe, learn, and act to optimize their performance. If they do not serve a common goal or belong to a single authority, fully cooperative behaviors cannot be taken for granted. Instead, users will only aim at maximizing their own payoffs. Therefore, game theory [13] has naturally become an important tool that is ideal and essential in studying, modeling, and analyzing the cognitive interaction process, and designing efficient, self-enforcing, distributed and scalable algorithms for cognitive radio networks [14].

The importance of studying cognitive radio networks in a game-theoretic framework is multi-fold. First, by modeling dynamic spectrum sharing among network users (primary and secondary users) as games, network users' behaviors and actions can be analyzed in a formalized game structure, by which the theoretical achievements in game theory can be fully utilized. Second, game theory equips us with various optimality criteria for the spectrum sharing problem. To be specific, the optimization of spectrum usage is generally a multi-objective optimization problem, which is very difficult to analyze and solve. Game theory provides us with well-defined equilibrium criteria to measure game optimality under various game settings. Third, non-cooperative game theory, one of the most important branches of game theory, enables us to derive efficient distributed approaches for dynamic spectrum sharing using only local information. Such approaches become highly desirable when centralized control is not available or flexible self-organized approaches are necessary.

Although existing dynamic spectrum access schemes based on game theory have successfully enhanced spectrum efficiency, some critical challenges have not been fully addressed or understood. First, cooperation is usually helpful, but seems incompatible with players' selfish nature. Hence, enforcing cooperation in the network consisting of selfish players is important. Second, many of the existing papers do not consider the situation when selfish players reveal false private information in order to achieve higher payoffs. Since a lot of games rely on private information revealed by individuals, cheat-proof strategies are necessary to guarantee that the network runs in good shape. Third, the collusive behavior of selfish users, which is a prevalent threat to efficient spectrum utilization but has been generally overlooked, has to be taken into consideration. Driven by their pursuit of higher payoffs, a clique of players may cheat together and take away profits that should have been credited to other players, which makes collusion-resistant strategies important.

Moreover, most of existing works have not taken security issues into consideration, which may lead to a severe loss when a malicious user shows up. A malicious user, who may be an enemy in the context of military communications or a business rival in the context of civilian communications, aims at maximizing the damage that he/she causes. In fact, cognitive radio networks are extremely vulnerable to malicious attacks for the following reasons. First, secondary users do not own the spectrum, and hence their opportunistic access cannot be enforced by law from adversaries. Second, highly dynamic spectrum availability and often distributed network structures make it difficult to implement effective security countermeasures. Third, as cognitive radio networks benefit from technology evolution to be capable of utilizing spectrum adaptively and intelligently, the same technologies can also be exploited by malicious attackers to launch more complicated and unpredictable attacks with even greater damage. Therefore, ensuring security is of critical importance to the successful deployment of cognitive radio networks. However, it was not until recent years that security issues began to receive research interest. For instance, in [15], the primary user emulation attack was described and a transmitter verification scheme was proposed to distinguish a primary user from other sources; the authors of [16] discussed the attack where malicious users attempted to mislead the learning process of secondary users; denial-of-service attacks were considered and potential protection remedies were discussed in [17]; in [18], a malicious user reporting false sensing results would be found and excluded from the collaborative spectrum sensing when the calculated "suspicious" level was high.

In a nutshell, cognitive radio is a promising and revolutionary communication paradigm that enables more efficient and intelligent usage of the spectrum resources, but its successful deployment is loomed by selfish users and threatened by potential malicious users. Therefore, in this dissertation, we want to develop a game-theoretic framework for cognitive radio networks to suppress selfish and malicious behaviors, in order to make the network more efficient and robust.

1.2 Dissertation Outline

From the discussion above, cognitive radio technology is a new communication paradigm, which allows wireless users to share the spectrum in an adaptive and intelligent manner, and improves the efficiency of spectrum utilization. This dissertation develops game-theoretic frameworks to suppress selfish and malicious behaviors in cognitive radio networks with the goal to improve system performance and enhance network security. The rest of the dissertation is organized as follows.

1.2.1 An Overview of Game Theory (Chapter 2)

Since game theory has been recognized as an important tool in studying, modeling, and analyzing the cognitive interaction process, in this chapter, we present an overview of the most fundamental concepts of game theory and explain in detail how these concepts can be leveraged in designing spectrum sharing protocols, with an emphasis on state-of-the-art research contributions in cognitive radio networking. We hope this will aid the design of efficient, self-enforcing, and distributed spectrum sharing schemes in future wireless networks [14].

1.2.2 Cheat-Proof Open Spectrum Sharing (Chapter 3)

In a cognitive radio network, wireless users usually compete with each other for spectrum resources, and have no incentive to cooperate with each other. They may even exchange false private information in order to get more access to the spectrum. To combat such selfish behavior, we propose a repeated spectrum sharing game with cheat-proof strategies. By using the punishment-based repeated game, users get the incentive to share the spectrum in a cooperative way; through mechanism-design-based and statistics-based approaches, user honesty is further enforced. We propose specific cooperation rules based on the maximum total throughput and proportional fairness criteria. Simulation results show that the proposed scheme can greatly improve the spectrum efficiency by alleviating mutual interference [19].

1.2.3 Collusion-Resistant Spectrum Auction (Chapter 4)

It is also of interest to know what happens when a group of selfish users collude for higher payoffs. In this chapter, we focus on the collusion-resistant strategy in the setting of a spectrum market. Because spectrum resources are interference-limited rather than quantity-limited, we present a novel multi-winner spectrum auction game not existing in auction literature in order to accommodate this special feature in wireless communications. As secondary users may be selfish in nature and tend to be dishonest in pursuit of higher profits, we develop effective mechanisms to suppress their dishonest/collusive behaviors when secondary users distort their valuations about spectrum resources and interference relationships. Moreover, the semi-definite programming (SDP) relaxation is applied to significantly reduce the complexity [20].

1.2.4 Anti-Jamming Zero-Sum Game (Chapter 5)

We apply game-theoretic tools to suppress potential malicious behavior in cognitive radio networks. In this chapter, we focus on defending against the jamming attack, one of the major threats to cognitive radio networks. We investigate the situation where a secondary user can access only one channel at a time and hop among different channels, and model it as an anti-jamming game. We derive the defense strategy through the Markov decision process approach, and then propose two learning schemes to gain knowledge of adversaries. In addition, we extend to the scenario where secondary users can access all available channels simultaneously, and redefine the anti-jamming game with randomized power allocation as the defense strategy. We derive the Nash equilibrium for this Colonel Blotto game which minimizes the worst-case damage [21].

1.2.5 Anti-Eavesdropping Information Secrecy Game (Chapter 6)

Besides the jamming attack, eavesdropping is another serious concern for network security. In this chapter, we propose a new cooperative paradigm in cognitive radio networks that primary users improve secrecy with the help of trustworthy secondary users, in the presence of an intelligent and passive eavesdropper attempting to decode primary users' messages. We derive the achievable pair of primary users' secrecy rate and secondary users' transmission rate under various circumstances, and model the interaction between primary users and secondary users as a Stackelberg game. Moreover, based on a 2-D representation of how achievable rates depend on power-level regions, we apply equilibrium analysis to understand the optimal strategy of primary and secondary users [22].

Chapter 2

Game Theory in Cognitive Radio Networks: An Overview

Game theory [13] is a mathematical tool that analyzes the strategic interactions among multiple decision makers. Its history dates back to the publication of the 1944 book *Theory of Games and Economic Behavior* by J. von Neumann and O. Morgenstern, which included the method for finding mutually consistent solutions for two-person zero-sum games and laid the foundation of game theory. During the late 1940s, cooperative game theory had come into being, which analyzes optimal strategies for groups of individuals, assuming that they can enforce collaboration between them so as to jointly improve their positions in a game. In early 1950s, J. Nash developed a new criterion, known as Nash equilibrium, to characterize mutually consistent strategies of players. This concept is more general than the criterion proposed by von Neumann and Morgenstern, since it is applicable to non-zero-sum games, and marks a quantum leap forward in the development of non-cooperative game theory. During the 1950s, many important concepts of game theory were developed, such as the concepts of the core, the extensive form games, repeated games, and the Shapley value. Refinement of Nash equilibriums and the concepts of complete information and Bayesian games were proposed in the 1960s. Application of game theory to biology, i.e., the evolutionary game theory, was introduced by J. M. Smith in the 1970s, during which time, the concepts of correlated equilibrium and common knowledge were introduced by R. Aumann. Starting from the 1960s, game theorists have started to investigate a new branch of game theory, mechanism design theory, focusing on the solution concepts for a class of private information games. In nowadays, game theory has been widely recognized as an important tool in many fields, such as social sciences, biology, engineering, political science, international relations, and computer science, for understanding cooperation and conflict between individuals. In this chapter, we will present a brief overview on fundamental game theory and how game theory has been applied to various aspects of cognitive radio networks.

2.1 Non-Cooperative Games and Nash Equilibrium

The majority of games applied to cognitive radio networks belong to the category of non-cooperative games, since usually in cognitive radio networks users have no incentive to cooperate with each other but instead aim at maximizing their own payoffs. A strategic game $\langle N, (A_i), (u_i) \rangle$ consists of three components: a set of *players*, denoted by N; a set of *actions*, denoted by A_i for player i; and *payoff functions*, denoted by $u_i : A \to \mathbb{R}$ for player i, where $A = \times_{i \in N} A_i$ is the action set of all players. For cognitive radio networks, players of the game may be secondary users, primary users, and even malicious users; for example, a game can be played between one secondary user and another secondary user, between a primary user and a secondary user, between a secondary user and a malicious users, or between two groups of users. Usually, the possible actions include sensing the spectrum, allocating power, choosing spectrum bands, deciding ways of accessing spectrum and so on, and depend on the specific application. Payoff functions can be chosen as channel capacity, achievable throughput, quality-of-service (QoS) measures, monetary gains, other user-defined metrics, or a combination of them. Note that one player's payoff depends on not only his/her own action, but also other players' actions, and hence there is a strategic interaction between players.

Nash equilibrium is the key concept to understand non-cooperative game theory, which, informally speaking, is an equilibrium where everyone plays the best strategy when taking decision-making of others into account, i.e., $a^\star$ is a Nash equilibrium if for every player $i \in N$,

$$u_i(a_i^\star, a_{-i}^\star) \geq u_i(a_i, a_{-i}^\star),\ \forall a_i \in A_i, \tag{2.1}$$

where a_i denotes the strategy of player i and a_{-i} is a common notation in game theory representing the strategies of all players other than player i. Therefore, Nash equilibrium predicts the outcome of a game when all players are rational. Depending on whether players choose a single action or randomize over a set of actions according to some probability distribution, an equilibrium can be classified as the *pure-strategy* Nash equilibrium or the *mixed-strategy* Nash equilibrium.

For a given game, it is natural to ask questions such as "Does a Nash equilibrium exist?", "Is it unique?", "If there are multiple equilibria, which one(s) are the best?", "How can a system reach the equilibrium from scratch?", and "Can we go beyond the Nash equilibrium?". These questions have been addressed in game theory, and are also of critical importance in equilibrium analysis and performance enhancement of cognitive radio games, after a specific cognitive radio application scenario is modeled as a game.

Based on the fixed point theorem, the existence of a Nash equilibrium is quite general. It is well-known that every finite strategic game has a mixed-strategy Nash equilibrium, and many games with a compact and convex action set have a pure-strategy Nash equilibrium, as long as the payoff functions are continuous and quasi-concave. The uniqueness of the equilibrium, however, has to be analyzed on a case-by-case basis, unless the game presents some special structures.

When there are multiple equilibria, we want to choose the optimal one(s) in some sense. Because game theory essentially solves a multi-objective optimization problem, it is not straightforward to define the optimality in such scenarios. One way is to compare the weighted sum of the individual payoffs, which reduces the multi-dimension problem into a one-dimension one; a more popular alternative is the Pareto optimality, which, informally speaking, is a point at which no single player can improve his/her own payoff without hurting any other player. Specifically, let $\mathbf{u}$ be a vector composed of payoffs in one particular game outcome. Then, $\mathbf{u}$ is *Pareto efficient* if there is no $\mathbf{u}'$ of another game outcome for which $u'_i > u_i$ for all $i \in N$; $\mathbf{u}$ is *strongly Pareto efficient* if there is no $\mathbf{u}'$ for which $u'_i \geq u_i$ for all $i \in N$ and $u'_i > u_i$ for some $i \in N$. The *Pareto frontier* is defined as the set of all $\mathbf{u}$ that are Pareto efficient. Besides the Pareto criterion which mainly focuses on efficiency, other criteria may also be employed to select a desirable Nash equilibrium, taking robustness into consideration. For instance, in a sequential game, incredible threats about consequential actions or implausible beliefs of other players may result in unreasonable outcomes that should be excluded. This process is known as the "equilibrium refinement" in game theory.

The remaining two questions, namely, "How can a system reach the equilibrium from scratch?" and "Can we go beyond the Nash equilibrium?", are of particular interest in cognitive radio networks. A cognitive radio network often has no pre-existing infrastructure, and wireless users may lack the global information to predict the equilibrium directly. Instead, they may need to start from an arbitrary strategy and update their strategies according to certain rules, which hopefully will converge to the equilibrium. Hence, a distributed implementation is preferred. Moreover, the goal of cognitive radio networks is to improve the efficiency of spectrum utilization, but a Nash equilibrium often suffers from excessive competition among selfish players in a non-cooperative game. Since the Nash equilibrium may be inefficient, researchers are eager to know if there are some way to improve the system performance. In what follows, we will address these two questions in cognitive radio context.

2.1.1 Distributed Implementation

When a game has certain structures, its Nash equilibrium is unique and convergence to the equilibrium is guaranteed. Two such examples are potential games [23] and standard functions [24].

A game $\langle N, (A_i), (u_i) \rangle$ is called a *potential game* if there is a potential function

$P : A \to \mathbb{R}$ such that

$$P(a_i, a_{-i}) - P(a'_i, a_{-i}) = u_i(a_i, a_{-i}) - u_i(a'_i, a_{-i}) \tag{2.2}$$

for any $i \in N, a \in A$, and $a'_i \in A_i$. Thanks to the potential function, every single player's individual interest is "aligned" with the group's interest, and hence each player choosing a "better" strategy given all other players' current strategies will necessarily lead to improvement in the value of potential function. A potential game in which all players take better strategies sequentially will terminate in finite steps to the Nash equilibrium that maximizes the potential function. Certain conditions have been known to prove a game to be a potential game or guide the design of a potential game; one example is that different users' payoffs have certain symmetric properties.

The concept of potential games was first applied to cognitive radio networks in [25] and has been widely employed since then. For instance, in the waveform selection game [26], players distributively choose their signature waveforms to reduce correlation, and the payoff function is defined as a function of signal-to-interference-and-noise ratio (SINR) minus some cost associated with the selected waveform. A power control game [26] is similar except that the action space consists of all possible power levels and the cost is associated with power levels. In a channel allocation game [27], a player's strategy is to select a channel from multiple channels for transmission, and players in the same band interfere with each other. In order to reduce mutual interference, the payoff function is constructed as the total interference not only caused by other players but also causing to other players, which satisfies the symmetric condition of potential games.

The concept of standard functions is first introduced to aid power control in cellular networks. A positive and monotonic function $f(x)$ is a *standard function* if it satisfies the scalability condition

$$\alpha f(x) > f(\alpha x), \; \forall \alpha > 1. \tag{2.3}$$

It is known that if the best response strategy is a standard function of the variable that represents the user's action, then the non-cooperative game has a unique equilibrium [28], and moreover, the equilibrium can be obtained through iterative updates until convergence.

The idea of standard function has been applied, for example, in [29] which considers a cooperative cognitive radio network. Secondary users serve as cooperative relays for primary users, so that they can have the opportunity to access the wireless channel. Secondary users target at maximizing the utility defined as a function of their achievable rate minus the payment, by selecting the proper payment in the non-cooperative game. By proving the best response payment is a standard function, it is shown that the non-cooperative payment selection game has a unique equilibrium.

Potential games and standard functions are two families of games that ensure convergence of iterative procedures and enable the distributed implementation of the algorithm. For other games, usually there is no universal approach to prove convergence, but it is possible to analyze on a case-by-case basis. For instance, the authors of [30] show that the iterative waterfilling algorithm will converge under certain conditions by proving that the distributed updating function is a contraction map. In [31], convergence is discussed for a game where farsighted players use iterative waterfilling according to their prediction of other players' strategy, instead of updating the strategy myopically in each iteration.

2.1.2 Performance Enhancement

From a network designer's point of view, he/she would like to have a satisfying social welfare, which can be defined as maximizing the sum of all users' payoffs; however, due to the selfish nature of users and excessive competition, usually the game outcome is much inefficient than the social optimum. In order to study the optimality of the non-cooperative game outcomes, *price of anarchy* is an important measure, which is the difference or ratio between a Nash equilibrium and the social optimum that can be achieved when a central authority is available. Since the Nash equilibrium is not always satisfying due to inefficiency, sometimes people want to improve the system performance by reducing competition and/or introducing cooperation. We discuss three kinds of approaches applied to cognitive radio networks, namely, pricing, repeated games, and correlated equilibrium.

To improve the efficiency, pricing can be introduced when designing the non-cooperative game, since selfish network users will be guided to a more efficient operating point [28]. Intuitively, pricing can be viewed as the cost of the services or resources a network user receives, or the cost of harm the user imposes on other users, in terms of performance degradation, revenue deduction, or interference. As selfish users only optimize their own performance, their aggressive behavior will degrade the performance or QoS of all the other users in the network, and hence deteriorate the system efficiency. By adopting an efficient pricing mechanism, selfish users will be aware of the inefficiency, and encouraged to compete for the network resources more moderately and efficiently. This brings more benefits for all users and a higher revenue for the entire network.

Linear pricing which increases monotonically with the transmit power of a user has been widely adopted, because of its implementation simplicity and a reasonable physical meaning. In [32], for example, the service provider charges each user a certain amount of payment for each unit of the transmitting power on the uplink channel in wide-band cognitive radio networks for revenue maximization, while ensuring incentive compatibility for the users. In [33], the authors further point out that most existing pricing techniques, e.g., a linear pricing function with a fixed pricing factor for all users, can usually improve the equilibrium by pushing it closer to the Pareto optimal frontier. However, they may not be Pareto optimal, and not suitable for distributed implementation, as they require global information. Therefore, a user-dependent linear pricing function which drives the equilibrium closer to the Pareto optimal frontier is proposed in [33], through analysis of the Karush-Kuhn-Tucker conditions.

More sophisticated pricing functions (e.g., nonlinear functions) can also be used, according to the specific problem setting and requirements. In an underlay spectrum sharing problem [34] where secondary users transmit in the licensed spectrum concurrently with primary users, secondary users' transmission is constrained by the interference temperature limit. An exponential penalty of excessive interference is introduced as a pricing factor, and efficient secondary spectrum sharing will be achieved, with sufficient protection for primary transmission. In the spectrum sharing problem considered in [35], each wireless transmitter selects a single channel from multiple available channels and decides transmission power. To mitigate the effects of interference externality, users should exchange information that can reflect interference levels. Such information is defined by the so-called interference "price", which essentially indicates the marginal loss/increase in each user's payoff if the received interference is increased/decreased by one unit. It is shown [35] that the proposed algorithm considering interference price always outperforms the heuristic algorithm where each user only picks the best channel without exchanging interference prices, and the iterative water-filling algorithm where users do not exchange any information.

The second approach is to use the repeated game modeling. Because wireless users coexist in the same network for quite a long time, the spectrum sharing game will be played for multiple times. In order to model and analyze long-term interactions among players, the repeated game model is used. A *repeated game* is a special form of an extensive-form game in which each stage is a repetition of the same strategic-form game. The number of rounds may be finite or infinite, but usually the infinite case is more interesting. Because players care about not only the current payoff but also the future payoffs, and a player's current behavior can affect the other players' future behavior, cooperation and mutual trust among players can be established. The most popular repeated game is the δ-discounted infinitely repeated game, where the payoff function for player i is defined as the discounted average of immediate payoffs from each round of the repeated game, i.e.,

$$\bar{u}_i(a^1, a^2, \ldots, a^t, \ldots) = (1-\delta)\sum_{t=1}^{\infty} \delta^{t-1} u_i(a^t), \tag{2.4}$$

where a^t is actions taken at time t, and δ is the discount factor that measures how much the players value the future payoff over the current payoff. The larger the value is, the more patient the players are.

In order to stimulate cooperation among selfish players, the so-called "grim trigger" strategy is a common approach. In the beginning, all players are in the cooperative stage, and they continue to cooperate with each other until someone deviates from cooperation. Then, the game jumps to the punishment stage where the deviating player will be punished by other peers, and there will be no cooperation forever. A less harsh alternative, also known as the "punish-and-forgive" strategy, is similar except for the limited punishment where deviation is forgiven and cooperation resumes after long enough punishment. Because cooperation is often more beneficial, the threat of punishment will prevent players from deviation, and hence cooperation is maintained. This is formally established by *folk theorems* [13], a family of theorems characterizing equilibria in repeated games, although the statement of a folk theorem varies slightly depending on the type of the equilibrium (the Nash equilibrium or the subgame perfect equilibrium), the length of punishment (grim-trigger or punish-and-forgive), the punishment payoff (the Nash threat or the minmax threat), and the criterion of the infinitely repeated game (δ-discounted or others).

Other than the grim trigger strategy and the punish-and-forgive strategy, "tit-for-tat" and "fictitious play" are also popular strategies in a repeated game. Both of them involve learning from opponents. When using the "tit-for-tat" strategy, a player chooses an action based on the outcome of the very last stage of the game, for example, he/she decides to cooperate only when all the other players cooperated in the last time. If the "fictitious play" strategy is used, a player learns the empirical frequency of each action of the other players from all history outcomes, and then chooses the best strategy accordingly assuming the opponents are playing stationary strategies.

Examples of cooperation enforcement and adaptive learning in repeated games can be found in context of cognitive radio networks. For instance, it is shown in [4] that any achievable rate in a Gaussian interference channel, in which multiple unlicensed users share the same band, can be obtained by piece-wise constant power allocations in that band with the number of segments at most twice of the number of users. The paper also shows that only the pure-strategy Nash equilibria exist, and under certain circumstances, spreading power evenly over the whole band is the unique Nash equilibrium that is often inefficient. Then, a set of Pareto optimal operating points are made possible by repeated game modeling and punishment-based strategies.

The last approach that we discuss is the *correlated equilibrium.* In deriving the Nash equilibrium of a game, players are assumed to take their strategies independent of the others' decisions. When they no longer do so, for instance, following the recommendation of a third party, the efficiency of the game outcome can be significantly improved. Correlated equilibrium is a more general equilibrium concept than the Nash equilibrium, where players can observe the value of a public signal and choose their actions accordingly. When no player would deviate from the recommended strategy, given that the others also adopt the recommendation, the resulting outcome of the game is a correlated equilibrium.

In order to adjust their strategies and converge to the set of correlated equilibria, players can track a set of "regret" values for strategy updates [36]. The regret value is defined as

$$\mathcal{R}_i^T(a_i, a_i') = \max\{\frac{1}{T}\sum_{t\leq T}[u_i^t(a_i', a_{-i}) - u_i^t(a_i, a_{-i})], 0\}, \tag{2.5}$$

where $u_i^t(a_i', a_{-i})$ represents the payoff of player i at time t by taking action a_i' against the other players taking action a_{-i}. Therefore, the regret value characterizes the average payoff that player i would have obtained, if he/she had adopted action a_i' every time in the past instead of action a_i. If the regret value is smaller than 0, meaning adopting action a_i brings a higher average payoff, then there will be no regret, and thus the regret value is lower bounded by 0. According to the regret value, players can update their strategies by adjusting the probability of taking different actions. For player i who takes action a_i^t at time t, the probability of taking action a_i at time $t+1$ is updated by

$$p_i^{t+1}(a_i) = \begin{cases} \frac{1}{\mu}\mathcal{R}_i^t(a_i^t, a_i) & \text{if } a_i \neq a_i^t, \\ 1 - \sum_{a_i' \neq a_i} p_i^{t+1}(a_i') & \text{if } a_i = a_i^t, \end{cases} \tag{2.6}$$

with μ being a large enough parameter that adjusts the learning rate. If all players learn their strategies according to (2.6), as time goes to infinity, their strategies will converge to the set of correlated equilibria almost surely [36].

The concept of correlated equilibrium and regret learning has been used to design dynamic spectrum access protocols [37], where a group of secondary users compete for the access of spectrum white space. Users' utility function is defined as the average throughput and an additional term representing performance degradation due to excess access and collisions. Since the common history observed by all users can serve as a natural coordination device, users can pick their actions based on the observation about the past actions and payoff values, and achieve better coordination with a higher performance.

2.2 Economic Games and Auctions

As game theory studies interaction between rational and intelligent players, it can be applied to the economic world to deal with how people interact with each other in the market. The marriage of game theory and economic models yields interesting games and fruitful theoretic results in microeconomics and auction theory. On one hand, they can be regarded as applied branches of game theory which builds on top of key game-theoretic concepts such as rationality and equilibria. Often, players are sellers and buyers in the market (e.g., firms, individuals, and so on), payoff functions are defined as the utility or revenue that players want to maximize, and equilibrium strategies are of considerable interest. On the other hand, they are distinguished from fundamental game theory, not only because additional market constraints such as supply and demand curves and auction rules give insight on market structures, but also because they are fully-developed with their own research concerns. Hence, we make a separate section to address those economic games, so as to respect the distinction of these games and to highlight their intensive use in cognitive radio networks.

The application of games in economy into cognitive radio networks has the following reasons. First, economic models are suitable for the scenario of the secondary spectrum market where primary users are allowed to sell unused spectrum rights to secondary users. Primary users, as sellers, have the incentive to trade temporarily unused spectrum for monetary gains, while secondary users, as buyers, may want to pay for spectrum resources for data transmissions. The deal is made through pricing, auctions, or other means. Second, these games in economy do not confine themselves to the scenario with explicit buyers and sellers, and the ideas behind can be extended to some cognitive radio scenarios other than secondary spectrum markets. One example is that the Stackelberg game, originally describing an economic model, has been generalized to a strategic game consisting of a leader and a follower. Third, as cognitive radio goes far beyond technology and its success will highly rely on the combination of technology, policy, and markets, it is of extreme importance to understand cognitive radio networks from the economic perspective and develop effective procedures (e.g., auction mechanisms) to regulate the spectrum market.

2.2.1 Oligopolistic Competition

When the market is fully competitive, the market equilibrium is the intersection of the demand curve and the supply curve; the other extreme is monopoly, when only one firm controls all over the market of one product. Lying between the full competition and no competition (monopoly), oligopoly is more complicated and interesting, which is defined as a market with only a few firms and with substantial barriers to entry in economics. Because the number of firms is limited, each one can influence the price and hence affect other firms; for example, their strategies are to decide the quantity or price of goods supplied to the market. The interaction and competition between different firms can be well modelled by game theory, and several models have been proposed long before. These models share common attributes including price-quantity relations, profit-maximizing goals, and the first-order optimality, but they are different in actions (quantities vs. prices), structures (simultaneous moves vs. sequential moves), or forms (competition vs. cooperation).

In the *Cournot game*, oligopoly firms choose their quantities independently and simultaneously. Because the market price depends on the total quantity of the product, each firm's action directly affects others' profits. Assume the cost is associated with the production quantity, the payoff function of each firm is revenue minus cost. Hence, the equilibrium of this game is the solution to a set of equations derived from the first-order condition that maximizes the payoff of each firm.

In the *Bertrand game*, firms also decide their actions independently and simultaneously, but their decisions are prices rather than quantities, and their produce capacity is unlimited. Although it looks like the Cournot game, the outcome is significantly different. Since the firm with the lower price will occupy the entire market, firms will try to reduce their price until hitting the bottom line with zero profit. Hence, the equilibrium of this game is trivial. A modification of the game is to assume each firm produces a somewhat differentiated product. The demand function of one particular product is a decreasing function of its price but often an increasing function of prices of alternating products from other providers. With the model established, the payoffs can be written down explicitly, and the equilibrium price can be found through the first-order conditions that maximize the profit.

In the *Stackelberg game*, firms still choose their quantities as in the Cournot game, but the two firms make decisions sequentially rather than simultaneously. The firm that moves first is called the *leader*, and the other is called the *follower*. Because the follower takes action after the leader announces his/her production quantity, the best response of the follower would depend on the leader's action. Predicting that the follower will choose the best response corresponding to each possible action of the leader, the leader can maximize the profit by choosing a proper action. This process is known as the *backward induction*. If the leader chooses the Cournot equilibrium quantity, the best response of the follower will also be the Cournot equilibrium quantity. This implies that the leader guarantees at least the Cournot payoff, and takes an advantage from the asymmetric structure.

In the *Cartel maintenance game*, things are quite different because firms no longer compete with each other but cooperate with each other. In general, they can reduce the output, which leads to higher prices and higher profits for each firm. One example is the Organization of the Petroleum Exporting Countries (OPEC) that manipulates the stability of international oil price. In order to enforce cooperation among selfish firms, the Cartel maintenance can be modelled as a repeated game. From the firms' perspective, cooperation in the form of Cartel reduces competition and improves their profits, but in reality, it is harmful to economic systems and hence is forbidden by antitrust laws in many countries.

In what follows, we will show some examples on how these microeconomic concepts inspire research in cognitive radio networks. Depending on the assumptions and structures of spectrum markets, different models can be applied.

The spectrum market in [38] consists of one primary user and multiple secondary users who compete for spectrum resources. This is essentially a Cournot game, but the players in the game are buyers instead of sellers in the original setting. In this game, secondary user i requests a quantity q_i for the allocated spectrum size, and the price is determined by an inverse supply function

$$\mathcal{S}^{-1}\left(\sum_{i\in N} q_i\right) = c_1 + c_2\left(\sum_{i\in N} q_i\right)^{c_3}, \tag{2.7}$$

where c_1, c_2, c_3 are non-negative constants and $c_3 \geq 1$. Then, the payoff is defined as

$$u_i(q_i) = u_i^0 q_i - q_i\left(c_1 + c_2\left(\sum_{j\in N} q_j\right)^{c_3}\right), \tag{2.8}$$

where u_i^0 is the effective revenue per unit bandwidth for user i, and the equilibrium follows from the first-order condition.

Another spectrum market proposed in [39] consists of multiple competing primary users and one secondary user network. This game falls into the category of Bertrand games, as primary users adjust the price of spectrum resources. The authors adopt a linear demand function

$$\mathcal{D}(p) = \frac{(1+(N-2)\nu)(u_i^0 - p_i) - \nu \sum_{i \neq j}(u_j^0 - p_j)}{(1-\nu)(1+(N-1)\nu)}, \tag{2.9}$$

where p_i and q_i are the price and quantity purchased from primary user i, u_i^0 is the effective revenue per unit bandwidth, and the parameter $\nu(-1 \leq \nu \leq 1)$ reflects the cross elasticity of demand among different spectrum resources. Specifically, $\nu > 0$ implies substitute products, that is, one spectrum band can be used in place of another, while $\nu < 0$ implies complementary products, that is, one band has to be used together with another (like uplink and downlink). The value of ν measures the degrees of substitution or complement. In this model, the revenue is defined as the sum of monetary gains collected from the secondary network and the transmission gains of primary services, whereas the cost is defined as the performance loss to primary services due to spectrum transactions. Then, the equilibrium pricing is derived from the first-order condition.

The structure of spectrum markets could be more complicated. For instance, [40] proposes a hierarchical model in which there are two levels of markets: in the upper level, a few wireless service providers buy some spectrum bands from spectrum holders, and in the lower level, they sell these bands to end users. Wireless service providers are the players in this game who not only decide the quantity bought from spectrum holders but also the price charged to end users, and therefore, it is actually a combination of the Cournot game in the upper level and the Bertrand game in the lower level. The two levels are coupled in that the quantity sold to end users cannot exceed the quantity bought from license holders. The authors discuss four possible cases in the lower-level game due to quantity limitation, and conclude that only one equilibrium exists in the whole game. Another hierarchical market is proposed in [41] which considers both channel allocation and power allocation. In this model, the spectrum holder takes control of the upper-level market and hence the market fits in the monopoly model. In the lower-level game, service providers adjust the price of resources in the market, but the demand from end users comes from the equilibrium of a non-cooperative power-control game.

Just like other non-cooperative games, the Nash equilibria in these games are often inefficient due to competition among players. The price of anarchy for the proposed spectrum market has been analyzed through theoretical derivation or demonstrated by simulation results in [38] [39] and [40]. In addition, [39] [42] shows that the efficiency can be improved by enforcing cooperation among users, that is, establishing a Cartel.

In game models, it is common to assume all players have full knowledge about each other. However, it is not always true in realistic setting such as in a cognitive radio network. For instance, one player may know nothing about other players' profits or current strategies. Therefore, to make those games implementable in spectrum markets, it is crucial to involve learning processes. The learning processes in [38] [39] [40] and [41] can be roughly classified into two categories. When the information of strategies is available, players always update their strategies with the best response against other players' current strategies

$$a_i(t+1) = B(a_{-i}(t)), \tag{2.10}$$

where action a may refer to the quantity or the price depending on the market model, and $B(\cdot)$ is the best response. When only local information is available, a gradient-based update rule can be applied, i.e.,

$$a_i(t+1) = a_i(t) + \varepsilon \frac{\partial u_i(a(t))}{\partial a_i}, \tag{2.11}$$

where ε is the learning rate and the partial derivative can be approximated by local observations. The convergence of the learning process has been analyzed using the Jacobian matrix, e.g., see [39].

Although originally a game between two firms of the same product, the Stackelberg game in a broad sense can refer to any two-stage game where one player moves after the other has made a decision. The problem can be formulated as

$$\begin{aligned} &\max_{a_1 \in A_1, a_2 \in A_2} u_1(a_1, a_2), \\ &\text{s.t. } a_2 \in \arg\max_{a_2' \in A_2} u_2(a_1, a_2'). \end{aligned} \tag{2.12}$$

Similar to the Stackelberg game in an oligopoly market, the general Stackelberg game can also be solved using the backward induction. In [43], the Stackelberg game is employed to model and analyze the cooperation between a primary user and several secondary users where the primary user trade some spectrum usage to some secondary users for cooperative communications. Specifically, the primary user can choose to transmit the entire time slot on its own, or choose to ask for secondary users' cooperation by dividing one time slot to three fractions with two parameters

$\tau_1, \tau_2 (0 \leq \tau_1, \tau_2 \leq 1)$. In the first $(1 - \tau_1)$ fraction of the slot, the primary transmitter sends data to secondary users, and then they form a distributive antenna array and cooperatively transmit information to the primary receiver in the following $\tau_1 \tau_2$ fraction of the slot. As rewards, the secondary users involved in the cooperative communications are granted with the spectrum rights in the rest $\tau_1(1 - \tau_2)$ fraction of the slot. The primary user chooses the strategy including τ_1, τ_2, and the set of secondary users for cooperation, and then the selected secondary users will choose powers for transmission according to the primary user's strategy. As the leader of the game, the primary user is aware of secondary users' best response to any given strategy, and hence is able to choose the optimal strategy that maximizes the payoff. The cooperation structure in [29] is similar, where the major difference is that the secondary users pay for spectrum opportunities in addition to cooperative transmissions for the primary user. The implementation protocol and utility functions change, but the underlying Stackelberg game remains the same.

2.2.2 Auction Games

Auction theory [44] is an applied branch of game theory which analyzes interactions in auction markets and researches the game-theoretic properties of auction markets. An auction, conducted by an *auctioneer*, is a process of buying and selling products by eliciting *bids* from potential buyers (i.e., *bidders*) and deciding the auction outcome based on the bids and auction rules. The rules of auction, or *auction mechanisms*, determine whom the goods are allocated to (i.e., the allocation rule) and how much price they have to pay (i.e., the payment rule).

As efficient and important means of resource allocation, auctions have quite a long history and have been widely used for a variety of objects, including antiques, real properties, bonds, spectrum resources, and so on. For example, the Federal Communications Commission (FCC) has used auctions to award spectrum since 1994, and the United States 700 MHz FCC wireless spectrum auction held in 2008, also known as Auction 73, generated 19.1 billion dollars in revenue by selling licenses in the 698–806 MHz band [45]. The spectrum allocation problem in cognitive radio networks, although micro-scaled and short-termed compared with the FCC auctions, can also be settled by auctions.

Auctions are used precisely because the seller is uncertain about the values that bidders attach to the product. Depending on the scenario, the values of different bidders to the same product may be independent (the *private values* model) or dependent (the *interdependent values* model). Almost all the existing literature on auctions in cognitive radio networks assumes private values. Moreover, if the distribution of values is identical to all bidders, the bidders are *symmetric*. Last, it is common to assume a *risk neutral* model, where the bidders only care about the expected payoff, regardless of the variance (risk) of the payoff.

The well-known four basic forms of auctions are: *English auction*, a sequential auction where price increases round by round from a low starting price until only one bidder is left, who wins the product and pays his/her bid; *Dutch auction*, a sequential auction where price decreases round by round from a high starting price until one bidder accepts the price, who wins the product and pays the price at acceptance; *Second-price (sealed-bid) auction*, an auction where each bidder submits a bid in a sealed envelope simultaneously, and the highest bidder wins the product with payment equal to the second highest bid; *First-price (sealed-bid) auction*, an auction where each bidder submits a bid in a sealed envelope simultaneously, and the highest bidder wins the product with payment equal to his/her own bid.

Interestingly, the four simple auctions, albeit quite different at first glance, are indeed equivalent in some sense under certain conditions. The main idea was established in the seminal work [46] by William Vickrey, a Nobel laureate in Economics. In a nutshell, the Dutch auction is equivalent to the first-price sealed-bid auction, because for every strategy in the first-price auction, there is an equivalent strategy in the Dutch auction, and vice versa; the English auction is equivalent to the second-price sealed-bid auction under the private values model; and all four auctions yield the same expected revenue of the seller, given symmetric and risk-neutral bidders and private values. Thanks to the equivalence under mild conditions, it will suffice to study or adopt only one kind of auction out of the four basic forms. Usually, the second-price auction is a favorite candidate, because the procedure is simple, and more importantly, the mechanism makes bidders bid their true values in a self-enforced manner. Mathematically, in a second-price auction, bidder i whose value of the product is v_i submits a sealed bid b_i to the auctioneer. Then, the winner of the auction is $\arg\max_{j\in N} b_j$, and payoffs are

$$u_i = \begin{cases} v_i - \max_{j\neq i} b_j, & \text{if } i = \arg\max_{j\in N} b_j; \\ 0, & \text{otherwise.} \end{cases} \tag{2.13}$$

In a second-price sealed-bid auction, it is a weakly dominant strategy to bid truthfully, i.e., $b_i = v_i$ for all $i \in N$.

The seller plays a passive role in the auctions so far, because his/her benefit has not been taken into consideration. When the seller wants to design an auction game that has the Nash equilibrium with the highest possible expected revenue, it is called the *optimal auction* [47]. Assume that all bidders' values of the product are drawn from i. i. d. random variables with the same probability distribution, whose probability density function and probability distribution function are denoted by $f(v)$ and $F(v)$, respectively. Then, an optimal auction may be constructed by adding a *reserve price* on top of a second-price auction. In this case, the seller reserves the right not to sell the product to any bidder if the highest bid is lower than the reserve price $b_0 = T^{-1}(v_0)$, where v_0 is the seller's value of the product, and $T^{-1}(\cdot)$ is the inverse function of $T(v) = v - \frac{1-F(v)}{f(v)}$. In addition, setting a reserve price is also an effective measure against *bidding ring collusion*, where some or even all of the bidders collude not to overbid each other and hence the price is kept low.

An auction becomes more involved when more than one item are simultaneously sold and bidders bid for "packages" of products instead of individual products. This is known as the *combinatorial auction* [48]. The second-price mechanism can be generalized to the Vickrey-Clarke-Groves (VCG) mechanism, which maintains the incentive to bid truthfully. The basic idea is that the allocation of products maximizes the social welfare and each winner in the auction pays the opportunity cost that their presence introduces to all the other bidders.

Beyond the basic types of auctions, there are other forms of auctions such as the clock auction, the proxy auction, the double auction, and so on. Furthermore, there are a lot of practical concerns and variants in the real-world auctions. We will not go into the details of these issues; instead, we will focus on the auction games in cognitive radio networks in what follows.

In [49], SINR auctions and power auction mechanisms are studied subjected to a constraint on the accumulated interference power, or the so-called "interference temperature", at a measurement point, which must be below the tolerable amount of the primary system. In this auction game, the resource to sell is not the spectrum band; instead, users compete for the portion of interference that they may cause to the primary system, because the interference is the "limited resources" in this auction. Another kind of auctions has been used in [50], where spectrum sensing effort, rather than monetary payment, is the price to pay for the spectrum opportunities. The auction still follows the form of first-price and second-price sealed-bid auctions.

In the auction framework proposed in [10], users bid for a fraction of the band and the auction outcome has to satisfy the interference constraint. In this auction, each user has a piece-wise linear demand curve, and it is assumed that all users reveal demand curves to the auctioneer truthfully. Because the corresponding revenue is a piece-wise quadratic function, the auctioneer can find the revenue-maximizing point under the constraint that the allocation is conflict-free.

The cheat-proof property is a major concern in auction design, and we have mentioned that the VCG mechanism is capable of enforcing truth-telling. However, the VCG mechanism sometimes suffers from high complexity and vulnerability to collusive attacks. In [51] and [52], system efficiency is traded for low complexity using the greedy algorithm, while the authors carefully design the mechanism to guarantee that truth-telling is still a dominant strategy in this auction game.

When there are multiple sellers who also compete in selling the spectrum, the scenario can be modeled as a double auction. A truth-telling enforced double auction mechanism has been proposed in [53], and an anti-collusion double auction mechanism has been developed in [12] where history observations are employed to estimate users' private values.

2.2.3 Mechanism Design

Auction is one of the many possible ways of selling products. If striping off any particular selling format (e.g., an auction format), we arrive at a fundamental question: what is the best way to allocate a product? This generalized allocation problem falls into the category of *mechanism design*, a field of game theory on a class of private information games. The 2007 Nobel Memorial Prize in Economic Sciences was awarded to Leonid Hurwicz, Eric Maskin, and Roger Myerson as the founders of mechanism design theory.

The distinguishing feature of mechanism design is that the game structure is "designed" by a game designer called a "*principal*" who wants to choose a mechanism for his/her own interest. Like in an auction, the players, called the "*agents*", hold some information that is not known by the others, and the principal asks the agents for some *messages* (like the bids in an auction) to elicit the private information. Hence, this is a game of incomplete information where each agent's private information, formally known as the "*type*", is denoted by θ_i, a value drawn from a set

Θ_i, for $i \in N$. Based on the messages from agents, the principal makes an allocation *decision* $d \in D$, where D is the set of all potential decisions on how resources are allocated. Because agents are not necessarily honest, incentives have to be given in terms of monetary gains, known as *transfers*. The transfer may be negative values (as if paying tax) or positive values (as if receiving compensation). Then, agent i's utility is the benefit from the decision d plus a transfer, i.e., $u_i = v_i(d, \theta_i) + t_i$, which may provide agents with incentives to reveal the information truthfully. In summary, the basic insight of mechanism design is that both resource constraints and incentive constraints are coequally considered in an allocation problem with private information [54].

For a given mechanism, the agents' strategy is mapping the individual type to a message, i.e., $m : \Theta_i \rightarrow M_i$, being aware that their own utilities depend on all the reported messages. Because there are unlimited possibilities of choosing message spaces and allocation functions, analyzing the equilibrium and designing the mechanism seem to be extremely challenging. However, thanks to the equivalence established in the *revelation principle* [55], we can restrict attention to only *"direct" mechanisms* in which the message space coincides with the type space, i.e., $M_i = \Theta_i$, and all agents will truthfully announce their types.

In [56], mechanism design has been applied to multimedia resource allocation problems in cognitive radio networks. For the multimedia transmission, the utility function is defined as the expected distortion reduction resulting from using the channels. Since the system designer wants to maximize the system utility, mechanism-based resource allocation is used to enforce users to represent their private parameters truthfully. A cheat-proof strategy for open spectrum sharing has been proposed based on the Bayesian mechanism design [57]. In this work, a co-operative sharing is maintained by repeated game modeling, and users share the spectrum based on their channel state information. In order to provide users an incentive to reveal their private information honestly, mechanism design has been employed to determine proper transfer functions.

2.3 Cooperative Games

In cognitive radio network, sometimes it is possible that users cooperate with each other. We discuss two important types of cooperative spectrum sharing games, bargaining games and coalitional games, where network users have an agreement on how to fairly and efficiently share the available spectrum resources.

2.3.1 Bargaining Games

The bargaining game is one interesting kind of cooperative games in which individuals have the opportunity to reach a mutually beneficial agreement. In this game, individual players have conflicts of interest, and no agreement may be imposed on any individual without his/her approval. Despite there are other models such as the strategic approach, we will focus on Nash's axiomatic model which has been established in Nash's seminal paper [58], because it has been widely applied to cognitive radio networks.

For convenience, we consider the two-player bargaining game $N = \{1, 2\}$, which can be extended to more players straightforwardly. For a certain agreement, player 1 receives utility u_1 and player 2 receives utility u_2. If players fail to reach any agreement, they receive utilities u_1^0 and u_2^0, respectively. The set of all possible utility pairs is the feasible set denoted by U.

A set of axioms [59] imposed on the bargaining solution $(u_1^*, u_2^*) = f(U, u_1^0, u_2^0)$ are listed as follows: (1) *Individual Rationality.* $u_1^* > u_1^0$ and $u_2^* > u_2^0$. (2) *Feasibility.* $(u_1^*, u_2^*) \in U$. (3) *Pareto Efficiency.* If $(u_1, u_2), (u_1', u_2') \in U$, $u_1 < u_1'$, and $u_2 < u_2'$, then $f(U, u_1^0, u_2^0) \neq (u_1, u_2)$. (4) *Symmetry.* Suppose a bargaining problem is symmetric, i.e., $(u_1, u_2) \in S \iff (u_2, u_1) \in S$ and $u_1^0 = u_2^0$. Then, $u_1^* = u_2^*$. (5) *Independence of Irrelevant Alternatives.* If $(u_1^*, u_2^*) \in U' \subset U$, then $f(U', u_1^0, u_2^0) = f(U, u_1^0, u_2^0) = (u_1^*, u_2^*)$. (6) *Independence of Linear Transformations.* Let U' be obtained from U by the linear transformation $u_1' = c_1 u_1 + c_2$ and $u_2' = c_3 u_2 + c_4$ with $c_1, c_3 > 0$. Then, $f(U', c_1 u_1^0 + c_2, c_3 u_2^0 + c_4) = (c_1 u_1^* + c_2, c_3 u_2^* + c_4)$.

There is a unique bargaining solution satisfying all the axioms above, which is called the *Nash bargaining solution* (NBS), given by

$$(u_1^*, u_2^*) = \underset{(u_1,u_2)\in U, u_1 > u_1^0, u_2 > u_2^0}{\operatorname{argmax}} (u_1 - u_1^0)(u_2 - u_2^0). \tag{2.14}$$

When there are more than two players, the NBS has a generalized form,

$$\underset{(u_1,u_2,\ldots)\in U,\ u_k > u_k^0, \forall k \in N}{\operatorname{argmax}} \prod_{k\in N} \left(u_k - u_k^0\right). \tag{2.15}$$

When $u_k^0 = 0, \forall k \in N$, the NBS coincides with the proportional fairness resource allocation criterion. This suggests that the NBS achieves some degree of fairness among cooperative players through bargaining. In [60], the NBS is directly applied to allocate frequency-time units in an efficient and fair way, after a learning process is first applied to find the payoffs with disagreement.

The symmetry axiom implies that all players are equal in the bargaining game; however, sometimes it is not true because some players have priority over others. To accommodate this situation, a variant of the NBS is to offset the disagreement point to some other payoff vectors that implicitly incorporate the asymmetry among players. An alternative approach is to modify the objective function to $\prod_{k \in N} (u_k - u_k^0)^{w_k}$ with weights w_k reflecting the priority of players. For instance, in the power allocation game consisting of primary users and secondary users [61], different values of u_k^0 are set to primary users and secondary users because primary users have the priority to use spectrum resources in cognitive radio networks. In [62] with heterogenous wireless users, the disagreement point in the NBS objective function is replaced by the threat made by individual players.

Moreover, finding the NBS needs global information which is not always available. A distributed implementation is proposed in [63] where users adapt their spectrum assignment to approximate the optimal assignment through bargaining within local groups. Although not explicitly stated, it actually falls into the category of the NBS, because the objective is to maximize the total logarithmic user throughput which is equivalent to maximizing the product of user payoffs. In this work, neighboring players adjust spectrum band assignment for better system performance through one-to-one or one-to-many bargaining. In addition, a theoretic lower bound is derived to guide the bargaining process.

A similar approach is conducted in [64] which iteratively updates the power allocation strategy using only local information. In this game, players allocate power to channels and their payoffs are the corresponding capacity. Given the assumption that players far away from each other have negligible interference, from a particular player's perspective, the global objective is detached to two parts: the product of faraway players' payoffs and the product of neighboring players' payoffs. Because the player's power allocation strategy only affects the second term, maximizing the second term is equivalent to maximizing the global objective. Each player sequentially adjusts the strategy, and it is proved that the iterative process is convergent. Although it is not sure whether it converges to the NBS, simulation results show that the convergence point is close to the true NBS.

2.3.2 Coalitional Games

The coalitional game is another type of cooperative game. It describes how a set of players can cooperate with others by forming cooperating groups and thus improve their payoff in a game.

A coalition S is a nonempty subset of N, the set of all players. Since the players in coalition S have agreed to cooperate together, they can be viewed as one entity and is associated with a *value* $v(S)$ which represents the worth of coalition S. Then, a coalitional game is determined by N and $v(S)$. When the value $v(S)$ is the total payoff that can be distributed in any way among the members of S, e.g., using an appropriate fairness rule, this kind of coalitional games is known as games *with transferrable payoff*. However, in some coalitional games, rigid restrictions exist on the allocation of the payoff. These games fall into the other category known as games *without transferrable payoff*.

In coalitional games with or without transferrable payoff values, the value of a coalition S only depends on the members of S, while not affected by how the players outside coalition S are partitioned. We call these coalition games are in *characteristic function form*. Sometimes, the value of S is also affected by how the players in $N \setminus S$ are partitioned into various coalitions, and we call those coalitional games are of the *partition function form* [65].

In characteristic function form coalitional games, often cooperation by forming larger coalitions is beneficial for players in terms of a higher payoff. This property is referred to as *superadditivity*. For instance in games with transferrable payoff, superadditivity means

$$v\left(S_1 \bigcup S_2\right) \geq v(S_1) + v(S_2),\ \forall S_1, S_2 \subset N,\ S_1 \bigcap S_2 = \emptyset. \tag{2.16}$$

Therefore, forming larger coalitions from disjoint smaller coalitions can bring at least a payoff that can be obtained from the disjoint coalitions individually. Due to this property, it is always beneficial for players in a superadditive game to form a coalition that contains all the players, i.e., the *grand coalition*.

As the grand coalition provides the highest total payoff for the players, it is the optimal solution that is preferred by rational players. Naturally, one may wonder: is the grand coalition always achievable and stable? To answer this question, the *core* [13] of the coalitional game is defined as the set of feasible payoff profiles,

$$\mathbb{C} = \left\{ (x_i) : \sum_{i \in N} x_i = v(N), \text{ and} \sum_{i \in S} x_i \geq v(S),\ \forall S \subseteq N \right\}. \tag{2.17}$$

The idea behind the core is similar to that behind a Nash equilibrium of a non-cooperative game: a strategy profile where no player would deviate unilaterally to obtain a higher payoff. In a coalitional game, no coalition $S \subset N$ has an incentive to reject the proposed payoff profile in the core, deviate from the grand coalition, and form coalition S instead. As long as one can find a payoff allocation (x_i) that lies in the core, the grand coalition is a stable and optimal solution for the coalitional game.

It can be seen that the core is the set of payoff profiles that satisfy a system of weak linear inequalities, and thus is closed and convex. The existence of the core depends on the feasibility of the linear program and is related to the *balanced* property of a game. A coalitional game with transferrable payoff is called *balanced* if and only if the following inequality,

$$\sum_{S \subseteq N} \lambda_S v(S) \leq v(N), \tag{2.18}$$

holds for all non-negative weight collections $\lambda = (\lambda_S)_{S \subseteq N}$, where the collection $(\lambda_S)_{S \in \mathcal{S}}$ of numbers in $[0, 1]$ denotes a balanced collection of weights, and the sum of λ_S over all the coalitions that contain player i is $\sum_{S \supseteq i} \lambda_S = 1$. It is known that a coalitional game with transferrable payoff has a nonempty core if and only if it is balanced.

If the balanced property of a game does not hold, the core will be empty, and one will have trouble in finding a suitable solution of a coalitional game. Thus, an alternative solution concept that always exists in a coalitional game is in need. Shapley proposed a solution concept, known as the *Shapley value* ψ, to assign a unique payoff value to each player in the game. Similar to the NBS, it also takes the axiomatic approach. The axioms are: (1) *Symmetry.* If player i and player j are interchangeable in v, i.e., $v(S \bigcup \{i\}) = v(S \bigcup \{j\})$ for every coalition S that does not contain player i or j, then $\psi_i(v) = \psi_j(v)$. (2) *Dummy player.* If player i is a dummy in v, i.e., $v(S) = v(S \bigcup \{i\})$ for every coalition S, then $\psi_i(v) = 0$. (3) *Additivity.* For any two games u and v, define the game $u + v$ by $(u + v)(S) = u(S) + v(S)$, then $\psi_i(u + v) = \psi_i(u) + \psi_i(v)$, for all $i \in N$. (4) *Efficiency.* $\sum_{i \in N} \psi_i(v) = v(N)$. The Shapley value is the only solution that satisfies all the above axioms, and it has the following form,

$$\psi_i(v) = \sum_{S \subseteq |N| \setminus \{i\}} \frac{|S|!(|N| - |S| - 1)!}{|N|!} [v(S \cup \{i\}) - v(S)], \qquad (2.19)$$

which can be interpreted as the expected marginal contribution of player i when joining the grand coalition.

In a cognitive radio network, cooperation among rational users can generally improve the network performance due to the multiuser diversity and spatial diversity in a wireless environment. Thus, coalitional game theory has been used to study user cooperation and design optimal, fair, and efficient collaboration strategies. In [66], spectrum sharing through receiver cooperation is studied under a coalitional game framework. The authors model the receiver cooperation in a Gaussian interference channel as a coalitional game with transferrable payoff, where the value of the game is defined as the sum-rate achieved by jointly decoding all users in the coalition. It is shown that the grand coalition that maximizes the sum-rate is stable, and the rate allocation to members of a coalition is solved by a bargaining game modeling. Receiver cooperation by forming a linear multiuser detector is modeled as a game without transferrable payoff, where the payoff of each player is the received SINR. At high SINR regime, the grand coalition is proved to be stable and sum-rate maximizing. The work in [67] has modeled cooperative spectrum sensing among secondary users as a coalition game without transferrable payoff, and a distributed algorithm is proposed for coalition formation through merge and split. It is shown that the secondary users can self-organize into disjoint independent coalitions, and the detection probability is maximized while maintaining a certain false alarm level.

2.4 Stochastic Games

We have discussed various games, but generally speaking, players are assumed to face the same stage game at each time, meaning the game and the players' strategies are not depending on the current state of the network. However, this is not true for a cognitive radio network where the spectrum opportunities and the surrounding radio environment keep changing over time. In order to study the cooperation and competition behaviors of cognitive users in a dynamic environment, the theory of stochastic games might be a better fit.

A stochastic game [68] is an extension of Markov decision process (MDP) [69] by considering the interactive competition among different agents. In a stochastic game, there is a set of states, denoted by $\mathcal{S}$, and a collection of action sets, $A_1, \cdots, A_{|N|}$, one for each player in the game. The game is played in a sequence of stages. At the beginning of each stage the game is in a certain state. After the players select and execute their actions, the game then moves to a new random state with some transition probability determined by the current state and actions from all players: $T : \mathcal{S} \times A_1 \times \cdots \times A_{|N|} \mapsto PD(\mathcal{S})$. Meanwhile, at each stage each player receives a payoff $u_i : \mathcal{S} \times A_1 \times \cdots \times A_{|N|} \mapsto \mathbb{R}$, which also depends on the current state and all the chosen actions. The game is played continually for a number of stages, and each player attempts to maximize an objective function. Like in the repeated game, the overall payoff function is defined as the expected sum of discounted intermediate payoffs.

The solution, also called a *policy* of a stochastic game is defined as a probability distribution over the action set at any state, $\pi_i : \mathcal{S} \to PD(A_i)$, for all $i \in N$. Given the current state s^t at time t, if player i's policy π_i^t at time t is independent of the states and actions in all previous time slots, the policy π_i is said to be *Markov*. If the policy is further independent of time, it is said to be *stationary*.

The stationary policy of the players in a stochastic game, i.e., their optimal strategies, can be obtained by value iteration according to Bellman's optimality condition. For example, in a two-player stochastic game with opposite objectives, let us denote $V(s)$ as the expected reward (of player 1) for the optimal policy starting from state s, and $Q(s, a_1, a_2)$ as the expected reward of player 1 for taking action a_1 against player 2 who takes action a_2 from state s and continuing optimally thereafter [70]. Then, the optimal strategy for player 1 can be obtained from the following iterations,

$$V(s) = \max_{\pi} \min_{a_2 \in A_2} \sum_{a_1 \in A_1} Q(s, a_1, a_2)\pi_{a_1}, \tag{2.20}$$

$$Q(s,a_1,a_2) = u_1(s,a_1,a_2) + \delta \sum_{s' \in \mathcal{S}} T(s,a_1,a_2,s')V(s'), \tag{2.21}$$

where π_{a_1} denotes player 1's strategy profile, and $T(s,a_1,a_2,s')$ denotes the transition probability from state s to s' when player 1 takes a_1 and player 2 takes a_2.

Cognitive attackers may exist in a cognitive radio network, who can adapt their attacking strategy to the time-varying spectrum opportunities and secondary users' strategy. To alleviate the damage caused by cognitive attackers, a dynamic security mechanism is investigated in [71] by a stochastic game modeling. The state of the anti-jamming game includes the spectrum availability, channel quality, and the status of jammed channels observed at the current time slot. The action of the secondary users reflects how many channels they should reserve for transmitting control and data messages and how to switch between the different channels. Since secondary users and attackers have opposite objectives, the anti-jamming game is a zero-sum game, and the optimal policy of secondary users is obtained by the minimax-Q learning algorithm based on (2.20) and (2.21).

In [72], stochastic games are used for spectrum auctions. At each time slot, a central spectrum moderator auctions the currently available spectrum resources, and a set of secondary users strategically bid for the resources. As secondary users need to cope with uncertainties from both the environment (e.g., channel availability and quality variations, packet arrivals from the source) and interactions with the other secondary users (e.g., resource allocation from the auction), the state of the stochastic game is composed of the buffer state and channel state, where the buffer state is dependent on the current spectrum allocation status. The transition probability of the game can be derived, since the packet arrival is assumed to be a Poisson process and the channel state transition is modeled as a Markov chain. Strategic secondary users want to maximize the number of transmitted packets by choosing the optimal bidding strategy. To this end, an interactive learning algorithm is proposed, where the high dimensional state space is decomposed and reduced to a simpler expression, based on the conjecture from previous spectrum allocations, and state transition probabilities are further estimated using past observations on transitions between different states. In this way, secondary users can approximate the future reward and approach the optimal policy through iterations.

Chapter 3

Cheat-Proof Repeated Open Spectrum Sharing Games

As discussed in Chapter 1 and 2, cognitive radio technology has become a promising approach by breaking the paradigm and enabling wireless devices to utilize the spectrum adaptively and efficiently, and game theory is a proper and flexible tool to analyze the interactions among selfish users. Because unlicensed sharing without regulation usually leads to overuse of time/frequency/power units, or the so-called "tragedy of the commons" phenomenon [73], in this chapter, we focus on developing spectrum access schemes for open spectrum bands to improve the efficiency of spectrum utilization.

Although existing dynamic spectrum access schemes based on game theory have successfully enhanced spectrum efficiency, in order to achieve more flexible spectrum access in long-run scenarios, some basic questions still remain unanswered. First, the spectrum environment is constantly changing and there is no central authority to coordinate the spectrum access of different users. Thus, the spectrum access scheme should be able to distributively adapt to the spectrum dynamics, e.g., channel variations, with only local observations. Moreover, users competing for the open spectrum may have no incentive to cooperate with each other, and they may even exchange false private information about their channel conditions in order to get more access to the spectrum. Therefore, cheat-proof spectrum sharing schemes should be developed to maintain the efficiency of the spectrum usage.

In this chapter we propose a cheat-proof etiquette for unlicensed spectrum sharing by modeling the distributed spectrum access as a repeated game. In the proposed game, punishment will be triggered if any user deviates from cooperation, and hence users are enforced to access the spectrum cooperatively. We propose two sharing rules based on the maximum total throughput and proportional fairness criteria, respectively; accordingly, two cheat-proof strategies are developed: one provides players with the incentive to be honest based on mechanism design theory [55], and the other makes cheating nearly unprofitable by statistical approaches. Therefore, the competing users are enforced to cooperate with each other honestly. Simulation results show that the proposed scheme can greatly improve the efficiency of spectrum utilization under mutual interference.

3.1 System Model

We consider a situation where K groups of unlicensed users coexist in the same area and compete for the same unlicensed spectrum band, as shown in Fig. 3.1. The users within the same group attempt to communicate with each other, whose usage of the spectrum will introduce interference to other groups. For simplicity, we assume that each group consists of a single transmitter-receiver pair, and that all the pairs are fully loaded, i.e., they always have data to transmit. At time slot n, all pairs are trying to occupy the spectrum, and the received signal at the ith

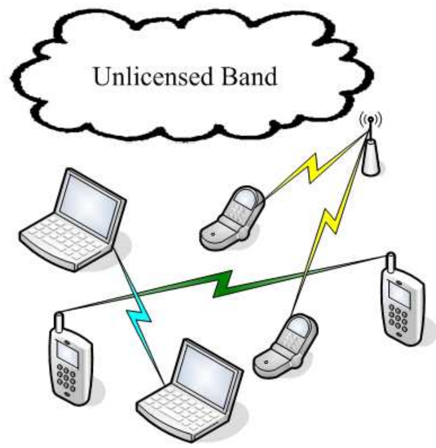


Figure 3.1: Illustration of open spectrum sharing.

receiver $y_i[n]$ can be expressed as

$$y_i[n] = \sum_{j=1}^{K} h_{ji}[n]x_j[n] + w_i[n],\ i = 1, 2, \ldots, K, \tag{3.1}$$

where $x_j[n]$ is the transmitted information of the jth pair, $h_{ji}[n](j = 1, 2, \ldots, K; i = 1, 2, \ldots, K)$ represents the channel gain from the jth transmitter to the ith receiver, and $w_i[n]$ is the white noise at the ith receiver. In the rest of the chapter, the time index n will be omitted wherever no ambiguity is caused. We assume the channels are Rayleigh fading, i.e., $h_{ji} \sim \mathcal{CN}(0, \sigma_{ji}^2)$, and distinct h_{ji}'s are statistically independent. The channels are assumed to remain constant during one time slot, and change independently from slot to slot. The noise is independently identically distributed (i.i.d.) with $w_i \sim \mathcal{CN}(0, N_0)$, where N_0 is the noise power. Limited by the instrumental capability, the transmission power of the ith user cannot exceed his/her own peak power constraint P_i^M, i.e., $|x_i[n]|^2 \leq P_i^M$ at any time slot n.

Usually, there is no powerful central unit to coordinate the spectrum access in the unlicensed band, and different coexisting systems do not share a common goal to help each other voluntarily. It is reasonable to assume that each transmitter-receiver pair is selfish: pursuing higher self-interest is the only goal for the wireless users. Such selfish behaviors can be well analyzed by game theory. Therefore, we can model the open spectrum sharing problem as a game specified in Table 3.1.

Table 3.1: The game model of open spectrum sharing.

Players	The K transmitter-receiver pairs
Actions	Each player can choose the transmission power level p_i in $[0, P_i^M]$
Payoffs	$R_i(p_1, p_2, \dots, p_K)$, the gain of transmission achieved by the ith player.

In general, the gain of transmission $R_i(p_1, p_2, \dots, p_K)$ is a non-negative increasing function of data throughput which depends on all players' power levels. For simplicity, we assume that all the players share the same valuation model that the gain of transmission equals data throughput, which can be easily extended to cases with different valuation models. The averaged payoff of the ith player can be approximated by

$$R_i(p_1, p_2, \dots, p_K) = \log_2\left(1 + \frac{p_i|h_{ii}|^2}{N_0 + \sum_{j \neq i} p_j |h_{ji}|^2}\right), \tag{3.2}$$

when mutual interference is treated as Gaussian noise, e.g., when the code division multiple access (CDMA) technique is employed.

3.2 Repeated Spectrum Sharing Game

In this section, we find the equilibria of the proposed spectrum sharing game. We assume that all the players are selfish and none is malicious. In other words, players aim to maximize their own interest, but will not harm others at their own cost. Because all the selfish players try to access the unlicensed spectrum as much as possible, severe competition often leads to strong mutual interference and low spectrum efficiency. However, since wireless systems coexist over a long period of time, the spectrum sharing game will be played for multiple times, in which the undue competition could be resolved by mutual trust and cooperation. We propose a punishment-based repeated game to boost cooperation among competing players.

3.2.1 One-shot game

First, we look into the one-shot game where players are myopic and only care for the current payoff. The Nash equilibrium of the game is a vector of power levels $(p_1^\star, p_2^\star, \ldots, p_K^\star)$ from which no individual would have the incentive to deviate. Proposition 1 implies that every transmitter will use the peak power level at the equilibrium.

Proposition 1 *The unique Nash equilibrium for this game is* $\left(P_1^M, P_2^M, \ldots, P_K^M\right)$.

Proof: First, we show that $\left(P_1^M, P_2^M, \ldots, P_K^M\right)$ is a Nash equilibrium. According to the definition of the payoff (3.2), when $p_1, p_2, \ldots, p_{i-1}, p_{i+1}, \ldots, p_K$ are fixed, and hence the interference power is fixed, the ith player's payoff $R_i(p_1, p_2, \ldots, p_K)$ grows as the power level p_i increases. Therefore, for any player i, deviating from P_i^M to any lower value will decrease the payoff, which makes $\left(P_1^M, P_2^M, \ldots, P_K^M\right)$ a Nash equilibrium.

Then, we show by contradiction that no other equilibria exist. Assume that $(p_1^\star, p_2^\star, \ldots, p_K^\star)$ is any equilibrium other than $\left(P_1^M, P_2^M, \ldots, P_K^M\right)$, which means at least one entry is different, say $p_i^\star \neq P_i^M$. However, this player can always be better off by deviating from $p_i^\star$ to P_i^M, which violates the definition of a Nash equilibrium.

$\blacksquare$

When channel states are fixed, substituting the equilibrium strategy $p_i = P_i^M$ for all i into (3.2) yields

$$R_i^S(h_{1i}, h_{2i}, \ldots, h_{Ki}) = \log_2 \left(1 + \frac{P_i^M |h_{ii}|^2}{N_0 + \sum_{j \neq i} P_j^M |h_{ji}|^2}\right), \tag{3.3}$$

where the superscript 'S' stands for "selfish". This is indeed the only possible outcome of the one-shot game with selfish players. Furthermore, when channel fading is taken into account, the expected payoff can be calculated by averaging over all channel realizations,

$$r_i^S = E_{\{h_{ji}, j=1,\ldots,K\}} \left[R_i^S(h_{1i}, h_{2i}, \ldots, h_{Ki})\right]. \tag{3.4}$$

In this chapter, the payoff represented by upper-case letters is the utility under a specific channel realization, whereas the payoff in lower-case letters is the utility averaged over all channel realizations.

Proposition 1 implies that the common open spectrum is excessively exploited owing to lack of cooperation among selfish players. In order to maximize their own payoffs, all the players always occupy the spectrum with maximum transmission power, which, in turn, makes everyone suffer from strong mutual interference. If players can somehow share the spectrum in a more cooperative and regulated fashion, everyone will be better off because interference has been greatly reduced. Since spectrum sharing lasts over quite a long period of time, it can be seen as a game played for numerous rounds, in which cooperation is made possible by established individual reputation and mutual trust.

3.2.2 Repeated game

In open spectrum sharing, players cannot be "forced" to cooperate with each other; instead, they must be self-enforced to participate in cooperation. We propose a punishment-based repeated game to provide players with the incentive for cooperation.

As introduced in Chapter 2, the payoff of a repeated game is defined as the sum of discounted payoffs discounted over time,

$$U_i = (1-\delta)\sum_{n=0}^{+\infty} \delta^n R_i[n], \tag{3.5}$$

where $R_i[n]$ is player i's immediate payoff at the nth time slot, and $\delta\,(0 < \delta < 1)$ is the discount factor. When δ is closer to 1, the player is more patient. Because players value not only the current payoff but also rewards in the future, they have to constrain behavior in the present to keep a good credit history; otherwise, a bad reputation may cost even more in the future.

In general, if players do not cooperate with each other, the only reasonable choice is the one-shot game Nash equilibrium with the expected payoff r_i^S given in (3.4). However, if all the players follow some predetermined rules to share the spectrum, higher expected one-slot payoffs r_i^C ('C' stands for "cooperation") may be achieved, i.e., $r_i^C > r_i^S$ for $i = 1, 2, \ldots, K$. For example, the cooperation rule may require only several players access the spectrum simultaneously, and hence mutual interference is greatly reduced. Nevertheless, without any commitment, selfish players always want to deviate from cooperation. One player can take advantage of others by transmitting in the time slots which he/she is not supposed to, and the instantaneous payoff at one specific slot is a random variable denoted by R_i^D ('D' stands for "deviation").

Although it is not a stable equilibrium in the one-shot game, cooperation is an equilibrium in the repeated game enforced by the threat of punishment. Specifically, every player states the threat to others: if anyone deviates from cooperation, there will be no more cooperation forever. Such a threat, also known as the "trigger" punishment [13], deters deviation and helps maintain cooperation. For example, assume that player i hesitates whether to deviate or not. Denote the discounted payoff with deviation as U_i^D, and that without deviation as U_i^C. Proposition 2 shows that the payoffs strongly converge to constants regardless of the channel realizations. Then, for the sake of the player's own benefit, it is better not to deviate as long as $r_i^C > r_i^S$.

Proposition 2 *As $\delta \to 1$, U_i^D converges to r_i^S almost surely, and U_i^C converges to r_i^C almost surely.*

Proof: First, we show that as $\delta \to 1$, the discounted payoff defined in (3.5) is asymptotically equivalent to the average of the one-time payoffs. By switching the order of operations, we have

$$\begin{aligned}\lim_{\delta\to 1} U_i &= \lim_{\delta\to 1}\lim_{N\to+\infty}\frac{1-\delta}{1-\delta^{N+1}}\sum_{n=0}^{N}\delta^n R_i[n]\\ &= \lim_{N\to+\infty}\sum_{n=0}^{N}\left(\lim_{\delta\to 1}\frac{\delta^n-\delta^{n+1}}{1-\delta^{N+1}}\right)R_i[n]\\ &= \lim_{N\to+\infty}\frac{1}{N+1}\sum_{n=0}^{N}R_i[n],\end{aligned} \tag{3.6}$$

where the last equality holds according to L'hospital's rule.

Assume that player i deviates at time slot T_0. Then, the payoffs $\{R_i[n], n = 0, 1, \ldots, T_0-1\}$ are i.i.d. random variables with mean r_i^C, whose randomness comes from the i.i.d. channel variations. Similarly, the payoffs $\{R_i[n], n = T_0{+}1, T_0{+}2, \ldots\}$ are i.i.d. random variables with mean r_i^S. Deviating only affects the payoff at time slot T_0. According to the strong law of large numbers [74], the payoff U_i^D converges to its mean r_i^S almost surely. On the other hand, if no deviation ever happens, the repeated game always stays in the cooperative stage. By using the same argument, U_i^C converges to r_i^C almost surely. ■

Because selfish players always choose the strategy that maximizes their own payoffs, they will keep cooperation if $U_i^C(= r_i^C) > U_i^D(= r_i^S)$, that is, all players are self-enforced to cooperate in the repeated spectrum sharing game because of punishment after any deviation.

Nevertheless, such a harsh threat is neither efficient nor necessary. Note that not only the deviating player gets punished, but the other "good" players also suffer from the punishment. For example, if one player deviates by mistake or punishment is triggered by mistake, there will be no cooperation due to punishment, which results in lower efficiency for all players. We have to review the purpose of the punishment. The aim of punishment is more like "preventing" the deviating behaviors from happening rather than punishing for revenge after deviation. As long as the punishment is long enough to negate the reward from a one-time deviation, no player has an incentive to deviate. The new strategy, called "punish-and-forgive", is stated as follows: the game starts from the cooperative stage, and will stay in the cooperative stage until some deviation happens. Then, the game jumps into the punishment stage for the next $T-1$ time slots before the misbehavior is forgiven and cooperation resumes from the Tth time slot. T is called the duration of punishment. In the cooperative stage, every player shares the spectrum in a cooperative way according to their agreement; while in the punishment stage, players occupy the spectrum non-cooperatively as they would do in the one-shot game. Using folk theorems we have introduced in Chapter 2, we show that cooperation is a subgame perfect equilibrium that ensures the Nash optimality for subgames starting from any round of the whole game.

Proposition 3 *Provided $r_i^C > r_i^S$ for all $i = 1, 2, \ldots, K$, there is $\bar{\delta} < 1$, such that for a sufficiently large discount factor $\delta > \bar{\delta}$, the game has a subgame perfect equilibrium with discounted utility r_i^C, if all players adopt the "punish-and-forgive" strategy.*

The parameter T can be determined by analyzing the incentive of the players. For example, we investigate under what condition player i will lose the motivation to deviate at time slot T_0. Although cooperation guarantees an average payoff r_i^C at each time slot, the worst-case instantaneous payoff could be 0. On the contrary, deviation will boost the instantaneous payoff at that slot. Assume the maximal profit obtained from deviation is $\overline{R_i^D}$. If player i chooses to deviate, punishment stage will last for the next $T-1$ slots; otherwise, cooperation will always be maintained. Thus, the expected payoffs with and without deviation are bounded by

$$u_i^D \triangleq E[U_i^D] \leq (1-\delta) \cdot \left(\sum_{n=0}^{T_0-1} \delta^n r_i^C + \delta^{T_0} \overline{R_i^D} + \sum_{n=T_0+1}^{T_0+T-1} \delta^n r_i^S + \sum_{n=T_0+T}^{+\infty} \delta^n r_i^C \right), \tag{3.7}$$

and

$$u_i^C \triangleq E[U_i^C] \geq (1-\delta) \cdot \left(\sum_{n=0}^{T_0-1} \delta^n r_i^C + 0 + \sum_{n=T_0+1}^{+\infty} \delta^n r_i^C \right), \tag{3.8}$$

respectively. In order to deter players from deviating, T should be large enough such that $u_i^C > u_i^D$ for all $i = 1, 2, \ldots, K$, i.e.,

$$T > \max_i \frac{\log \left(\delta - \frac{(1-\delta)\overline{R_i^D}}{r_i^C - r_i^S} \right)}{\log \delta}, \tag{3.9}$$

which can be further approximated by

$$T > \max_i \frac{\overline{R_i^D}}{r_i^C - r_i^S} + 1, \tag{3.10}$$

by L'Hopital's rule when δ is close to 1. If the tendency to deviate is stronger (i.e., $\overline{R_i^D}/(r_i^C - r_i^S)$ is larger), the punishment should be harsher (longer duration of punishment) to prevent the deviating behavior.

3.3 Cooperation with Optimal Detection Duration

In this section, we will discuss the specific design of the cooperation rules for spectrum sharing, as well as the method to detect deviation. When designing the rules, we assume that players can exchange information over a common control channel. Based on the information, each individual can independently determine who is eligible to transmit in the current time slot according to the cooperation rule, and thus the proposed scheme does not require a central management unit.

Cooperative spectrum sharing can be designed in the following way: in one time slot, only a few players with small mutual interference can access the spectrum simultaneously. In the extreme case, only one player is allowed to occupy the spectrum at one time slot, and the mutual interference can be completely prevented. We consider such orthogonal channel allocation because it is simple and requires only a little overhead.

The slot structure for the spectrum sharing is shown in Fig. 3.2. Every slot is divided into three phases: in the first phase, each player broadcasts information to others, such as channel gains; in the second phase, each player collects all the necessary information and decides whether to access the spectrum or not, according to the cooperation rule; then the eligible player will occupy the spectrum in the third phase of the slot. If the channel does not change too rapidly, the length of a slot can be designed long enough to make the overhead (the first and second phases) negligible. Since it is necessary to detect the potential deviating behavior and punish correspondingly, the eligible player cannot transmit all the time during the third phase. Instead, the player has to suspend his/her own transmission sometimes and listens to the channel to catch the deviators. The eligible player transmits and detects during the third phase: a portion of time is reserved for detection, while the rest can be used for transmission. When to perform detection during the slot is kept secret by individuals; otherwise, the other players may take advantage by

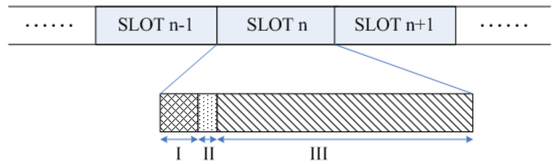


Figure 3.2: Proposed slot structure for spectrum sharing. Phase I: exchange information; phase II: make decision; phase III: transmit and detect.

deviating when the detector is not operating. Finally, if detection shows someone is deviating, an alert message will be delivered in the first phase of the next time slot.

3.3.1 Cooperation Criteria

There are numerous cooperation rules to decide which players can have exclusive priority to access the channel, such as the time division multiple access (TDMA). Out of many possible choices, the cooperation rules must be reasonable and optimal under some criteria, such as the maximum total throughput criterion [75] and the proportional fairness criterion [76].

Given a cooperation rule d, player i would have an expected discounted payoff r_i^{Cd}. Denote $\mathbb{D}$ as the set of all possible cooperation rules. The maximum total throughput criterion aims to improve the overall system performance by maximizing the sum of individual payoffs,

$$d_{\text{MAX}} = \operatorname*{argmax}_{d \in \mathbb{D}} \sum_{i=1}^{K} r_i^{Cd}, \tag{3.11}$$

whereas the proportional fairness criterion is known to maximize their product,

$$d_{\mathrm{PF}} = \underset{d \in \mathbb{D}}{\operatorname{argmax}} \prod_{i=1}^{K} r_i^{Cd}. \tag{3.12}$$

The rule based on the maximum total throughput criterion (MTT) is quite straightforward. In order to maximize the total throughput, each time slot should be assigned to the player that makes best use of it. Denote $g_i[n] = P_i^M |h_{ii}[n]|^2$ as the instantaneous received signal power of the ith player at time slot n, and $\{g_i[n]\}$ are i.i.d. exponentially-distributed random variables with mean $P_i^M \sigma_{ii}^2$ according to the assumption about $\{h_{ii}[n]\}$. The allocation rule is to assign the channel to the player with the highest instantaneous received signal power, i.e.,

$$d_1(g_1, g_2, \ldots, g_K) = \underset{i}{\operatorname{argmax}}\, g_i. \tag{3.13}$$

Since only the information of the current time slot is necessary and the same rule applies to every time slot, the time index n has been omitted. The expected payoff is

$$r_i^{C1} = \int_0^{+\infty} \log_2 \left(1 + \frac{g_i}{N_0}\right) \Pr(g_i > max_{j \neq i} g_j) f(g_i) \mathrm{d}g_i, \tag{3.14}$$

where $f(g_i) = \frac{1}{P_i^M \sigma_{ii}^2} \exp(-\frac{g_i}{P_i^M \sigma_{ii}^2})$ is the probability density function of the random variable g_i, and $\Pr(\cdot)$ denotes the probability that the statement within the parenthesis holds true.

The maximum total throughput criterion is optimal from the system designer's perspective; however, in a heterogeneous situation where some players always have better channels than others, the players under poor channel conditions may have little chance to access the spectrum. To address the fairness problem, another rule is proposed which allocates the spectrum according to the normalized channel gain $\bar{g}_i = g_i/E[g_i]$ instead of the absolute values,

$$d_2(\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_K) = \underset{i}{\operatorname{argmax}}\, \bar{g}_i. \tag{3.15}$$

Note that all $\{\bar{g}_i, i = 1, 2, \ldots, K\}$ are exponentially-distributed random variables with mean 1, the symmetry of which implies that every player will have an equal chance $(1/K)$ to access the spectrum.

Proposition 4 *The closed-form payoff with the proposed rule (3.15) used can be shown as follows*

$$r_i^{C2} = \int_0^{+\infty} \log_2 \left(1 + \frac{P_i^M \sigma_{ii}^2 \bar{g}}{N_0}\right) \exp(-\bar{g}) \left(1 - \exp(-\bar{g})\right)^{K-1} \mathrm{d}\bar{g}. \tag{3.16}$$

Proof: The probability distribution function of each $\bar{g}_i$ is $F(\bar{g}_i) = 1 - \exp(-\bar{g}_i)$. Using order statistics [77], we can write the distribution function of $\max\{\bar{g}_i, i = 1, 2, \ldots, K\}$ as $F_{\mathrm{M}}(\bar{g}) = (1 - \exp(-\bar{g}))^K$. Since each player can be the one with the largest $\bar{g}_i$ with probability $1/K$ due to symmetry, the expected payoff is

$$r_i^{C2} = \int_0^{+\infty} \log_2 \left(1 + \frac{P_i^M \sigma_{ii}^2 \bar{g}}{N_0}\right) \frac{1}{K}\, \mathrm{d}F_{\mathrm{M}}(\bar{g}). \tag{3.17}$$

Substituting $F_{\mathrm{M}}(\bar{g})$ yields the form of the payoff in (3.16). ■

The proposed rule (3.15) can be seen as an approximation to the proportional fairness criterion (3.12). g_i can be decomposed into a fixed component $E[g_i]$ and a fading component $\bar{g}_i$. When the channel is constant without fading, i.e., $g_i = E[g_i]$, the proportional fairness problem becomes

$$\begin{aligned} \max_{\{\omega_i\}} \; & \prod_{i=1}^{K} \omega_i \log_2 \left(1 + \frac{E[g_i]}{N_0}\right) \\ \text{s.t.} \; & \sum_{i=1}^{K} \omega_i \leq 1, \end{aligned} \tag{3.18}$$

where ω_i is the probability that the ith player should occupy the channel. The optimal solution is $\omega_i = 1/K$ for any i, which means an equal share is proportionally fair. On the other hand, when only the fading part is considered, since $\bar{g}_i$ is completely symmetric for all players, assigning resources to the player with the largest $\bar{g}_i$ will maximize the product of payoffs. The two aspects suggest that rule (3.15) is a good approximation which requires only the information of the current time slot, and we will refer to it as the APF. In addition, it can be extended to a more general case which allocates the band according to weighted normalized channel gain $\pi_i \bar{g}_i$, where π_i is a weight factor reflecting a player's priority for heterogeneous applications.

3.3.2 Optimal detection

The punishment-based spectrum sharing game can provide all players with the incentive to obey the rules, since deviation is deterred by the threat of punishment. Detection of the deviating behavior is necessary to ensure the threat to be credible; otherwise, selfish players will tend to deviate knowing their misbehavior will not be caught. Because only one player can occupy the spectrum at one time slot according to the proposed cooperation rules, if that player finds that any other player is deviating, the system will be alerted into the punishment phase. There are several ways to detect whether the spectrum resources are occupied by others, e.g., an energy detector [78].

The detectors are generally imperfect, and some detection errors are inevitable. There is the possibility that the detector believes someone else is using the channel although in fact nobody is. Triggering the game into punishment phase by mistake, this false alarm event reduces the system efficiency, and hence the probability of false alarm should be kept as low as possible. Generally speaking, the performance of the detector can be improved by increasing the detection time. Nevertheless, the player cannot transmit and detect at the same time because one cannot easily distinguish one's own signal from other players' signal in the same spectrum. Therefore, there is a tradeoff between transmission and detection: the more time one spends on the detection, the less time one reserves for data transmission.

Assume all the other parameters have been fixed, such as the length of one time slot. Then, the question is how much time in a slot should be used for detection. Let α denote the ratio of time for detection, T_s the length of one slot, W_s the bandwidth, and assume an energy detector with a threshold λ is used, then the false alarm probability is [78]

$$\xi(\alpha) = \frac{\Gamma(\alpha T_s W_s, \alpha\lambda/2)}{\Gamma(\alpha T_s W_s)}, \tag{3.19}$$

where $\Gamma(\cdot)$ and $\Gamma(\cdot,\cdot)$ are the gamma function and incomplete gamma function, respectively.

We have shown that the expected discounted payoff u_i equals r_i^C without considering the detection error. When the imperfect detector is taken into account, the modified discounted payoff, denoted by $\check{u}_i(\alpha)$, will depend on α. The expected throughput from the current time slot is $(1-\alpha)r_i^C$, since only the remaining $(1-\alpha)$ part of the duration can be employed for transmission. The system will jump into the punishment stage with probability $\xi(\alpha)$ due to the false alarm event, and stay in the cooperative stage with probability $1 - \xi(\alpha)$. If the system stays in the cooperative stage, the expected payoff in the future is $\check{u}_i(\alpha)$ discounted by one time unit; otherwise, the expected throughput in each time slot is r_i^S until cooperation resumes from the Tth slot, which yields the payoff $\check{u}_i(\alpha)$ discounted by T time units. Overall, the modified discount utility should satisfy the following equation,

$$\begin{aligned}\check{u}_i(\alpha) =& (1-\delta)(1-\alpha)r_i^C + (1-\xi(\alpha))\delta\check{u}_i(\alpha) \\ &+\xi(\alpha)\left((1-\delta)\sum_{n=1}^{T-1}\delta^n r_i^S + \delta^T\check{u}_i(\alpha)\right),\end{aligned} \tag{3.20}$$

from which $\check{u}_i(\alpha)$ can be solved as

$$\check{u}_i(\alpha) = \frac{(1-\delta)(1-\alpha)r_i^C + (\delta-\delta^T)\xi(\alpha)r_i^S}{1-\delta+(\delta-\delta^T)\xi(\alpha)}. \tag{3.21}$$

Note that the discounted payoff $\check{u}_i(\alpha)$ is a convex combination of $(1-\alpha)r_i^C$ and r_i^S, and thus $r_i^S < \check{u}_i(\alpha) < r_i^C$ for all $0 < \alpha < 1 - r_i^S/r_i^C$. Therefore, the imperfect detector will reduce the utility from r_i^C to a smaller value $\check{u}_i(\alpha)$. However, $\check{u}_i(\alpha)$ is always larger than r_i^S, which means that the players still have the incentive to join in this repeated game and cooperate.

Similar to [42], the optimal α^* that maximizes the modified discounted payoff (3.21) can be found by the first-order condition

$$\frac{\partial \check{u}_i(\alpha)}{\partial \alpha} = 0. \tag{3.22}$$

Or equivalently, α^* is the solution to the following equation

$$(1-\delta+(\delta-\delta^T))r_i^C + ((1-\alpha)r_i^C - r_i^S)(\delta-\delta^T)\frac{\xi'(\alpha)}{\xi(\alpha)} = 0, \tag{3.23}$$

where $\xi'(\alpha)$ is the derivative of $\xi(\alpha)$ with respect to α. Note that by replacing r_i^C

with $\check{u}_i(\alpha^*)$, the impact of imperfect detection is incorporated into the game, and requires no further considerations.

3.4 Cheat-Proof Strategies

The repeated game discussed so far is based on the assumption of complete and perfect information. Nevertheless, information, such as the power constraints and channel gains, is actually private information of each individual player, and thus there is no guarantee that players will reveal their private information honestly to others. If cheating is profitable, selfish players will cheat in order to get a higher payoff. As the proposed cooperation rules always favor the player with good channel conditions, selfish players will tend to exaggerate their situations in order to acquire more opportunities to occupy the spectrum. Therefore, enforcing truth-telling is a crucial problem, since distorted information would undermine the repeated game.

In [4], a delicate scheme is designed to testify whether the information provided by an individual player has been revealed honestly. However, the method is complex and difficult to implement, especially under time-varying channels. In our proposed allocation rules, much easier strategies can be employed to induce truth-telling. When the MTT rule is used for spectrum sharing, we design a mechanism to make players self-enforced to reveal their true private information, and when the APF rule is adopted, a scheme based on statistical properties is proposed to discourage players from cheating.

3.4.1 Mechanism-design-based strategy

Since the MTT sharing rule assigns the spectrum resources to the player who claims the highest instantaneous received signal power, players tend to exaggerate their claimed values. To circumvent the difficulty to tell whether the exchanged information has been distorted or not, a better way is to make players self-enforced to tell the truth.

Mechanism design is employed to provide players with incentives to be honest. To be specific, the players claiming high values are asked to pay a tax, and the amount of the tax will increase as the claimed value increases, whereas the players reporting low values will get some monetary compensation. Because players care for not only the gain of data transmission but also their monetary balance, the overall payoff is gain of transmission plus the transfer (tax or compensation). In other words, after introducing transfer functions, the spectrum sharing game actually becomes a new game with original payoffs replaced by the overall payoffs. By appropriately designing the transfer function, the players can get the highest payoff only when they claim their true private values.

In the game, the private information $\{g_1, g_2, \ldots, g_K\}$ has to be exchanged among players. Assume at one time slot, $\{\tilde{g}_1, \tilde{g}_2, \ldots, \tilde{g}_K\}$ is a realization of the random variables $\{g_1, g_2, \ldots, g_K\}$. Observing his/her own private information, the ith player will claim $\hat{g}_i$ to others, which may not be necessarily the same as the true value $\tilde{g}_i$. All the players claim the information simultaneously. Since $\{\hat{g}_1, \hat{g}_2, \ldots, \hat{g}_K\}$ is common knowledge but $\{\tilde{g}_1, \tilde{g}_2, \ldots, \tilde{g}_K\}$ is not, the allocation decision and transfer calculation have to be based on the claimed rather than the true values. In the MTT spectrum sharing game, the player with index $d_1(\hat{g}_1, \hat{g}_2, \ldots, \hat{g}_K)$ defined in (3.13) can access the channel, and thus data throughput at the current time slot can be written in a compact form

$$R_i(\tilde{g}_i, d_1(\hat{g}_1, \hat{g}_2, \ldots, \hat{g}_K)) = \begin{cases} \log_2(1 + \frac{\tilde{g}_i}{N_0}) & \text{if } d_1(\hat{g}_1, \hat{g}_2, \ldots, \hat{g}_K) = i; \\ 0 & \text{otherwise.} \end{cases} \tag{3.24}$$

The transfer of the ith player in the proposed cheat-proof strategy is defined as

$$t_i(\hat{g}_1, \hat{g}_2, \ldots, \hat{g}_K) \triangleq \Phi_i(\hat{g}_i) - \frac{1}{K-1} \sum_{j=1, j \neq i}^{K} \Phi_j(\hat{g}_j), \tag{3.25}$$

where

$$\Phi_i(\hat{g}_i) \triangleq E\left[\sum_{j=1, j \neq i}^{K} R_j(g_j, d_1(g_1, g_2, \ldots, g_K)) \middle| g_i = \hat{g}_i \right]. \tag{3.26}$$

Note the expectation is taken over all realizations of $\{g_1, g_2, \ldots, g_K\}$ except g_i, since the player has no knowledge about others of the current time slot when deciding what to claim. $\Phi_i(\hat{g}_i)$ is the sum of all other players' expected data throughput given that player i claims a value $\hat{g}_i$. Intuitively, if user i claims a higher $\hat{g}_i$, he/she will gain a greater chance to access the spectrum, and all the other players will have a smaller spectrum share. However, higher payment may negate the additional gain from more spectrum access through bragging the channel gain. On the contrary, if claiming a smaller $\hat{g}_i$, user i will receive some compensation at the cost of less chance to occupy the spectrum. Therefore, it is an equilibrium that each user reports his/her true private information. A rigorous proof is provided in Proposition 5.

Proposition 5 *In the proposed mechanism, it is an equilibrium that each player reports his/her true private information, i.e.,* $\hat{g}_i = \tilde{g}_i$, $i = 1, 2, \ldots, K$.

Proof: To prove the equilibrium, it suffices to show that for any $i \in \{1, 2, \ldots, K\}$, if all players except player i reveal their private information without distortion, the best response of player i is also to report the true private information. Without loss of generality, we assume player 2 through player K report true values $\hat{g}_i = \tilde{g}_i$, $i = 2, 3, \ldots, K$.

Then, the expected overall payoff of player 1 is the expected data throughput plus the transfer. The expectation is taken over all realizations of $\{g_2, g_3, \ldots, g_K\}$ throughout the proof. When claiming $\hat{g}_1$, player 1 gets the expected overall payoff

$$\begin{aligned} r_1^t(\hat{g}_1) &\triangleq E\left[R_1(\tilde{g}_1, d_1(\hat{g}_1, g_2, \ldots, g_K)\right] + t_1(\hat{g}_1, \hat{g}_2, \ldots, \hat{g}_K) \\ &= E\left[R_1(\tilde{g}_1, d_1(\hat{g}_1, g_2, \ldots, g_K) + \sum_{j=2}^{K} R_j(g_j, d_1(\hat{g}_1, g_2, \ldots, g_K))\right] - \frac{1}{K-1} \sum_{j=2}^{K} \Phi_j(\hat{g}_j). \end{aligned} \tag{3.27}$$

From analysis of incentive compatibility, player 1 will claim a distorted value $\hat{g}_1$ instead of $\tilde{g}_1$ if and only if reporting $\hat{g}_1$ results in a higher payoff, i.e., $r_1^t(\tilde{g}_1) < r_1^t(\hat{g}_1)$, or equivalently,

$$\begin{aligned} &E\left[R_1(\tilde{g}_1, d_1(\tilde{g}_1, g_2, \ldots, g_K) + \sum_{j=2}^{K} R_j(g_j, d_1(\tilde{g}_1, g_2, \ldots, g_K))\right] < \\ &E\left[R_1(\tilde{g}_1, d_1(\hat{g}_1, g_2, \ldots, g_K) + \sum_{j=2}^{K} R_j(g_j, d_1(\hat{g}_1, g_2, \ldots, g_K))\right]. \end{aligned} \tag{3.28}$$

Note that the MTT rule maximizes the total throughput, that is, for any realization of $\{g_2, g_3, \ldots, g_K\}$, $\sum_{i=1}^{K} R_i(\tilde{g}_i, d_1(\tilde{g}_1, \tilde{g}_2, \ldots, \tilde{g}_K)) > \sum_{i=1}^{K} R_i(\tilde{g}_i, d^o)$ for any other possible allocation strategy d^o. After taking the expectation, we have

$$\begin{aligned} &E\left[R_1(\tilde{g}_1, d(\tilde{g}_1, g_2, \ldots, g_K) + \sum_{j=2}^{K} R_j(g_j, d(\tilde{g}_1, g_2, \ldots, g_K))\right] > \\ &E\left[R_1(\tilde{g}_1, d^o) + \sum_{j=2}^{K} R_j(g_j, d^o)\right] \quad \text{for any } d^o, \end{aligned} \tag{3.29}$$

which contradicts (3.28). Therefore, player 1 is self-enforced to report the true value, i.e., $\hat{g}_1 = \tilde{g}_1$. Hence, in the equilibrium, all players will reveal their true private information. $\blacksquare$

Proposition 5 proves that by adopting the proposed mechanism-based strategy with transfer function defined in (3.25), every player gets the incentive to reveal true private information to others. For the homogenous case where $P_i^M = P$, $h_{ii} \sim \mathcal{CN}(0,1)$ for all i, the transfer function can be further simplified into the following form by order statistics

$$t_i(\hat{g}_1, \hat{g}_2, \ldots, \hat{g}_K) = \sum_{j=1}^{K} \int_{\hat{g}_i/P}^{\hat{g}_j/P} \log_2\left(1 + \frac{Pg}{N_0}\right) \exp(-g) \left(1 - \exp(-g)\right)^{K-2} \mathrm{d}g. \quad (3.30)$$

Moreover, with the proposed transfer functions, all players' payment/income adds up to 0 at any time slot:

$$\sum_{i=1}^{K} t_i(\hat{g}_1, \hat{g}_2, \ldots, \hat{g}_K) = \sum_{i=1}^{K} \left(\Phi_i(\hat{g}_i) - \frac{1}{K-1} \sum_{j=1, j\neq i}^{K} \Phi_j(\hat{g}_j) \right) = 0. \quad (3.31)$$

It means that the monetary transfer is exchanged only within the community of cooperative players without either surplus or deficit at any time. This property is very suitable for the open spectrum sharing scenario. Vickrey-Clark-Groves (VCG) mechanism [46], another well-known mechanism, can also enforce truth-telling, but it cannot keep the budget balanced. If the VCG mechanism is used, at each slot some players will have to pay a third party outside the community (e.g., a spectrum manager), which goes against the intention of the unlicensed band. Furthermore, paying for the band may make players less willing to access the spectrum. Despite that the VCG mechanism is a good choice for auctions in licensed spectrum, for the unlicensed band, as our goal is increasing spectrum efficiency and enforcing truth-telling rather than making money out of the spectrum resources, the proposed mechanism is more appropriate.

3.4.2 Statistics-based strategy

For the APF rule, every player reports the normalized channel gain, and the player with the highest reported value will get access to the spectrum. Since the normalized gains are all exponentially distributed with mean 1, if the true values are reported, the symmetry will result in an equal share of the time slots in the long run, i.e., each player will have $1/K$ fractional access to the spectrum.

If player i occupies the spectrum more than $(1/K + \varepsilon)$ of the total time, where ε is a pre-determined threshold, it is highly possible that he/she may have cheated. Consequently, the selfish players, in order not to be caught as a cheater, can only access up to $(1/K+\varepsilon)$ of all the time slots even if they distort their private information. Thus, the statistics-based cheat-proof strategy for the APF spectrum sharing rule can be designed as follows. Everyone keeps a record of the spectral usage in the past. If any player is found to overuse the spectrum, i.e., transmitting for more than $(1/K + \varepsilon)$ of the entire time, that player will be marked as a cheater and get punished. In this way, the profit of cheating, defined as the ratio of the extra usage over the normal usage, is greatly limited.

Proposition 6 *The profit of cheating is bounded when the statistics-based strategy is employed; furthermore, the profit approaches* 0 *as* $n \to \infty$.

Proof: The worst case is that the cheater gets exactly $(1/K+\varepsilon)$ portion of resources without being caught. The profit of cheating is at most $\frac{\varepsilon}{1/K} = K\varepsilon$, which is bounded.

Moreover, the threshold ε can shrink with time; to make it explicit, we use $\varepsilon[n]$ to denote the threshold at slot n. At one time slot, the event that a particular player accesses the spectrum is a Bernoulli distributed random variable with mean $1/K$. Then, the n-slot averaged access rate of a player is the average of n i.i.d. Bernoulli random variables, since the channel fading is independent from slot to slot. According to the central limit theorem [74], the average access rate converges in distribution to a Gaussian random variable with mean $1/K$, whose variance decays with rate $\frac{1}{n}$. To keep the same false alarm rate, $\varepsilon[n]$ can be chosen to decrease with rate $\frac{1}{\sqrt{n}}$. Then, the upper bound of the cheating profit $K\varepsilon[n]$ will decay to 0 as $n \to \infty$. ■

Therefore, we can conclude from the proposition that the benefit to the cheater, or equivalently speaking, the harm to the others, is quite limited. As a result, this statistics-based strategy is cheat-proof.

3.5 Simulation Studies

In this section, we conducted numerical simulations to evaluate the proposed spectrum sharing game with cheat-proof strategies.

We first look into the simplest case with two players ($K = 2$) to get some insight. We assume the two players are homogeneous with $P_1^M = P_2^M = P$, $\{h_{11}, h_{22}\} \sim \mathcal{CN}(0, 1)$, and $\{h_{12}, h_{21}\} \sim \mathcal{CN}(0, \gamma)$, where $\gamma = E[|h_{12}|^2]/E[|h_{11}|^2]$ reflects the relative strength of interference over the desired signal powers, and we call it the interference level. The prerequisite for the players to join the game is that each individual can obtain more profit by cooperation ($r_i^C > r_i^S$); however, cooperation is unnecessary in the extreme case when there is no mutual interference ($\gamma = 0$). Therefore, we want to know under what interference level γ the proposed cooperation is profitable. Fig. 3.3 shows the cooperation payoff r_i^C and non-cooperation payoff r_i^S versus γ when the averaged SNR $= P/N_0 = 15dB$. Since the two rules are equivalent in the homogeneous case, only the MTT rule is demonstrated. Under cooperative spectrum sharing, since only one player gets the transmission opportunity in each time slot, the expected payoff is independent of the strength of interference, and thus is a horizontal line in the figure. The non-cooperation payoff drops significantly as interference strength increases. From the figure, we can see that the payoff of cooperation is larger than that of non-cooperative for a wide range of the interference level ($\gamma > 0.15$). Therefore, the proposed cooperation is profitable for medium to high interference environment, which is typical for an urban area with high user density.

In Fig. 3.4, we illustrate the idea of the punishment-based repeated game. Assume player 1 deviates from cooperation at slot 150, and the duration of the punishment stage is $T = 150$. According to the "punish-and-forgive" strategy, the game will stay in the punishment stage from time slot 151 to 300. The figure shows an averaged result over 100 independent runs. We can see that although the player gets a high payoff at time slot 150 by deviation, the temporary profit will be negated in the punishment stage. Hence, considering the consequence of deviation, players have no incentive to deviate.

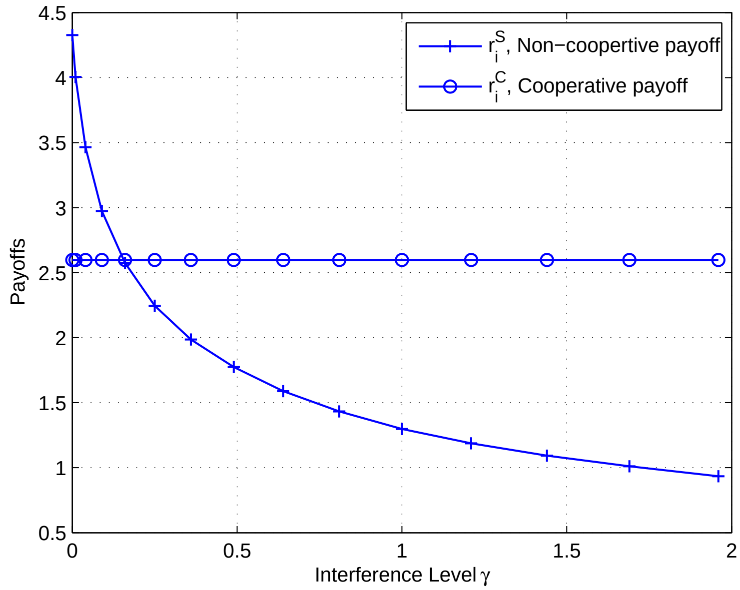


Figure 3.3: Comparison of payoffs when the players share the spectrum either cooperatively or non-cooperatively.

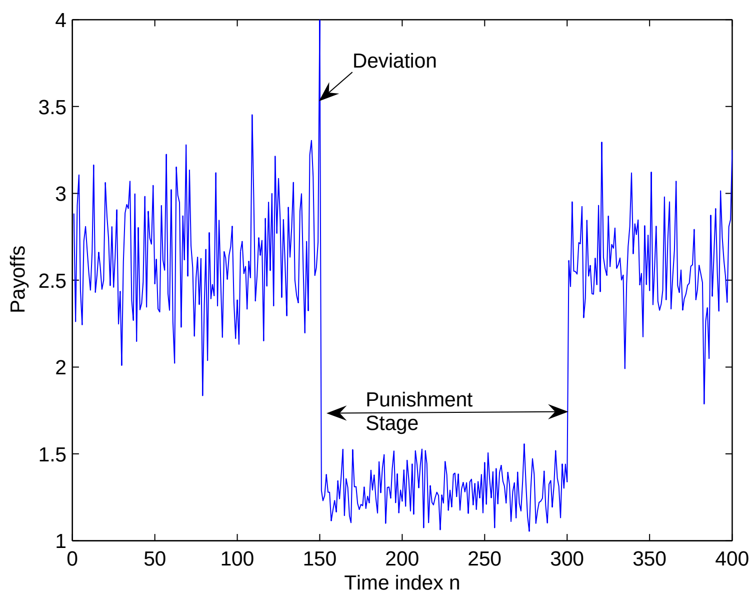


Figure 3.4: Illustration of the punishment-based repeated game.

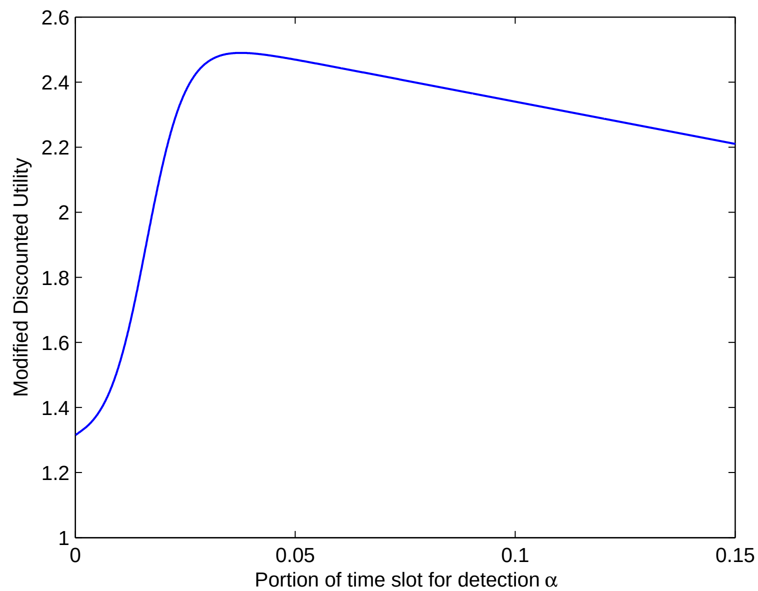


Figure 3.5: Effect of detection duration on the discounted utility.

Now, we take imperfect detection into consideration. Fig. 3.5 shows how a player's discount utility $\check{u}(\alpha)$ is affected by α when an energy detector with a fixed detection threshold is employed. We can see that when the detection time is short, the utility is quite low due to the high false alarm rate. On the other hand, when the detection time is too long, a significant portion of the transmission opportunity is wasted. Therefore, α should be carefully designed to achieve the optimal tradeoff that maximizes the utility.

Next, we show the payoffs of proposed cooperation rules in a heterogeneous environment. By heterogeneity, we mean that different players may differ in power constraints, averaged direct-channel gains $\{h_{ii}, i = 1, 2, \ldots, K\}$, averaged cross-channel gains $\{h_{ij}, i \neq j\}$, or combination of them. Here we only illustrate the results when the power constraints are different, since other types of asymmetry have similar results. In the simulation, we fix the power constraint of player 1, and increase P_2^M, the power constraint of player 2. The payoffs with the MTT and APF rules are demonstrated in Fig. 3.6, where '1' and '2' refer to the payoffs of player 1 and player 2, respectively. As benchmarks, the payoffs without cooperation and payoffs using the max-min fairness criterion (another resource allocation criterion sacrificing efficiency for absolute fairness, see [79]) are provided, denoted by "NOC" and "MMF", respectively. Since player 2 has more power to transmit data, he/she can be seen as a strong player in this heterogeneous environment. As seen from the figure, both the MTT and APF rules outperform the non-cooperation case, which means players have the incentive to cooperate no matter which rule is used. Furthermore, the MTT rule favors the strong player in order to maximize the system efficiency, and the APF rule achieves a tradeoff between efficiency and fairness. The MMF curves show that the strong user is inhibited in order to reach the absolute fairness, which might conflict with selfish users' interest.

We also conduct simulations for spectrum sharing with more than two users. In Fig. 3.7, the cooperation gain, characterized by the ratio of r_i^C/r_i^S, is plotted versus the number of the players K. We assume a homogeneous environment with a fixed interference level $\gamma = 1$. Since the allocation rules can reap multiuser diversity gains, the cooperation gain increases as more players are involved in the sharing game.

Finally, we examine the proposed mechanism-design-based cheat-proof strategy. We assume a 3-user spectrum sharing game with the MTT rule. At one specific

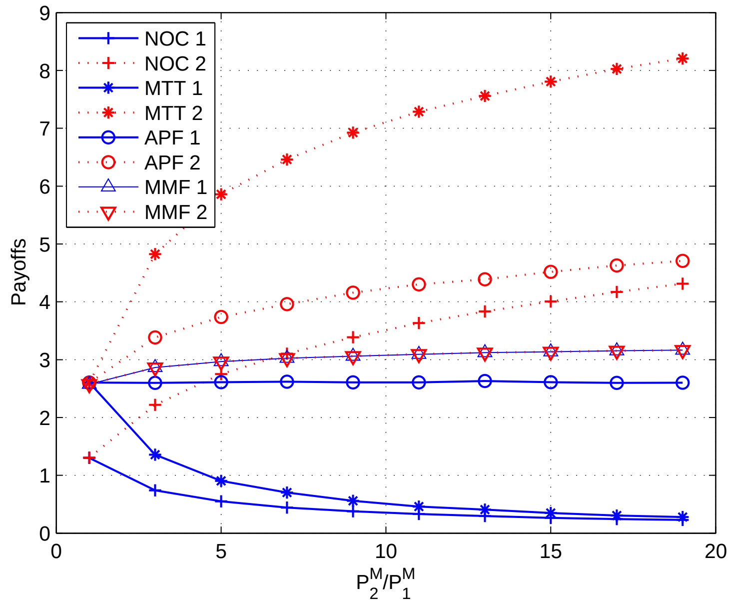


Figure 3.6: The payoffs under a heterogeneous setting with different cooperation rules.

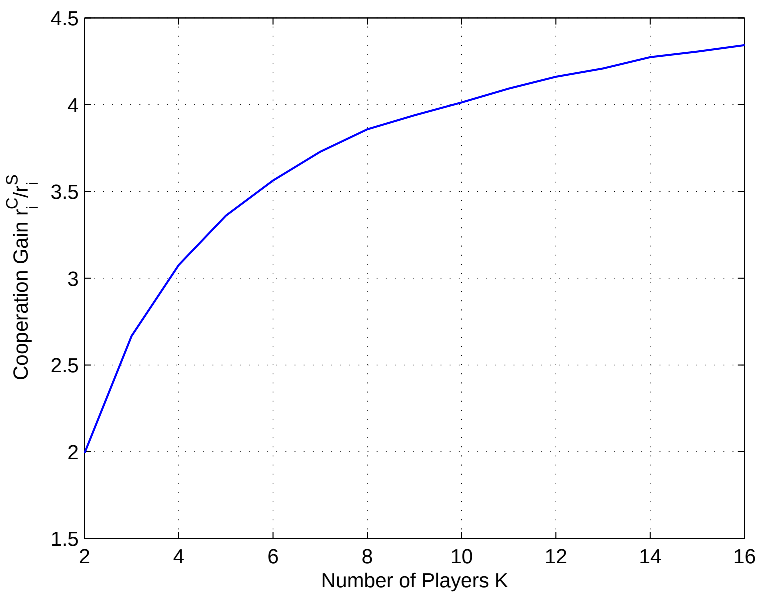


Figure 3.7: The cooperation gain in a K-player spectrum sharing game.

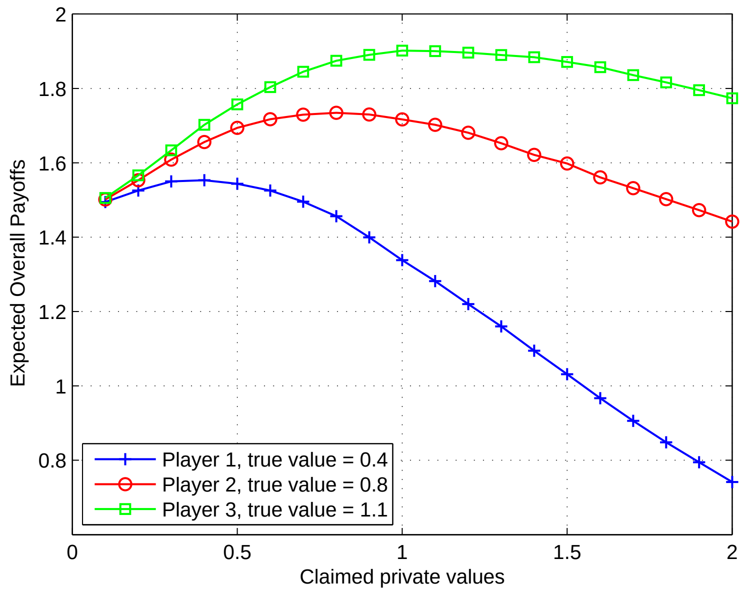


Figure 3.8: The expected overall payoffs versus different claimed values.

time slot, for example, the true private values are $\tilde{g}_1 = 0.4$, $\tilde{g}_2 = 0.8$, and $\tilde{g}_3 = 1.1$. In Fig. 3.8, the expected overall payoffs (throughput plus transfer) versus the claimed values are shown for each player, given the other two are honest. From the figure, we see that the payoff is maximized only if the player honestly claims his/her true information. Therefore, players are self-enforced to tell the truth with the proposed mechanism.

Chapter 4

A Scalable Collusion-Resistant Multi-Winner Spectrum Auction

In the previous chapter, we investigate on selfish behavior in open spectrum sharing and develop cheat-proof strategy to prevent a single player from lying about his/her private value. It is also of interest to know what happens when a group of selfish users collude for higher payoffs. In this chapter, we focus on the collusion-resistant strategy in the setting of a spectrum market, where spectrum opportunities are *announced* by primary users rather than *discovered* by secondary users. Since primary users have the incentive to trade their temporarily unused bands for monetary gains and secondary users want to lease some bands for data transmission, they may negotiate the price for a short-term lease. There have been a lot of previous efforts studying dynamic spectrum access via pricing and auction mechanisms, and some of them have been introduced in Chapter 1. Although existing schemes have enhanced spectrum allocation efficiency through market mechanisms, some critical challenges still remain unanswered.

First, in most of the current auctions, one licensed band (or a collection of multiple bands) is awarded to a unique winner just like traditional auctions studied by economists [44]. However, the spectrum resource is quite different from other commodities in that it is *interference-limited* rather than *quantity-limited*, because it is reusable by wireless users geographically far apart. In this case, allowing multiple winners to lease the band is an option consented by everyone: primary users get higher revenue, secondary users get more chances to access the spectrum, and spectrum usage efficiency gets boosted as well from the system designer's perspective. To the best of our knowledge, such an auction does not exist in the literature, and we coin the name *multi-winner auction* to highlight the special features of the new auction game, in which auction outcomes (e.g., the number of winners) highly depend on the geographical locations of the wireless users.

Second, although a few papers (e.g., [49][10]) have discussed spectrum auctions under interference constraints, most of them are based on the assumption that secondary users are truth-tellers, that is, they will honestly reveal their private information such as the valuations and interference relationships. However, since secondary users are selfish by nature, they may misrepresent their private information in order for a higher payoff. Therefore, proper mechanisms have to be developed to provide incentives to reveal true private information. Although the Vickrey-Clarke-Groves (VCG) mechanism is a possible choice enforcing that users bid their true valuations [48], it is also well-known to suffer from several drawbacks such as low revenue [80][81]. As auction rules significantly impact bidding strategies, it is of essential importance to develop new auction mechanisms to overcome the disadvantages.

Third, mechanisms to be developed should take into consideration the collusive behavior of selfish users, which is a prevalent threat to efficient spectrum utilization but has been generally overlooked [12]. Driven by their pursuit of higher payoffs, a clique of secondary users may cheat together, and sometimes they may even have a more facilitated way to exchange information for collusion if they belong to the same service provider. Furthermore, awarding the same band to multiple buyers simultaneously under interference constraints, the multi-winner auction makes possible new kinds of collusion. Therefore, effective countermeasures have to be developed against them.

Last but not least, it is much more meaningful to show the proposed scheme can be applied in practice, where complexity issues come into the spotlight: the mechanism should be easy to implement, and it should be scalable when more and more users are incorporated into the auction game. However, the optimal resource allocation that maximizes the system utility in the auction is an NP-complete problem [82] whose exact solution needs a processing time increasing exponentially with the size of the problem, and hence the computational complexity becomes too formidable to be practical when the number of users is large. By applying the semi-definite programming (SDP) relaxation [83] to the original problem, a tight upper bound can be obtained in polynomial time.

4.1 System Model

We consider a cognitive radio network where N secondary users coexist with M primary users, and primary users seek to lease their unused bands to secondary users for monetary gains. We model it as an auction where the sellers are the primary users, the buyers are the secondary users, and the auctioneer is a spectrum broker who helps coordinate the auction. Assume there is a common channel to exchange necessary information and a central bank to circulate money in the community. For simplicity, we assume each primary user owns one band exclusively, and each secondary user needs only one band. In this chapter, we first consider the auction with a single band ($M = 1$), and later extend it to the multi-band auction.

The system designer determines a fixed leasing period T according to channel dynamics and overhead considerations, that is, the duration should be short enough to make spectrum access flexible but not too short since the overhead of the auction would become problematic. At the beginning of each leasing period, if a primary user decides not to use his/her own licensed band for the next duration of T, he/she will notify the spectrum broker of the intention to sell the spectrum rights. Meanwhile, the potential buyers simultaneously submit their sealed bids $\mathbf{b} = [b_1, b_2, \ldots, b_N]^T$ to the spectrum broker, where b_i is the bid made by user i. According to the bids and channel availability, the broker decides both the allocation $\mathbf{x} = [x_1, x_2, \ldots, x_N]^T$ and the prices $\mathbf{p} = [p_1, p_2, \ldots, p_N]^T$, where $x_i = 1$ means secondary user i wins some band, $x_i = 0$ otherwise, and p_i is the price of the band for the ith secondary user. Alternatively, we can define the set of winners as $W \subseteq \{1, 2, \ldots, N\}$, where $i \in W$ if and only if $x_i = 1$. Assume user i gains value v_i from transmitting information in the leased band, his/her reward is

$$r_i = v_i x_i - p_i, \; i = 1, 2, \ldots, N. \tag{4.1}$$

Given all users' valuations $\mathbf{v} = [v_1, v_2, \ldots, v_N]^T$, the system utility, or the *social welfare* can be represented by

$$U_{\mathbf{v}}(\mathbf{x}) = \sum_{i=1}^{N} v_i x_i = \sum_{i \in W} v_i. \tag{4.2}$$

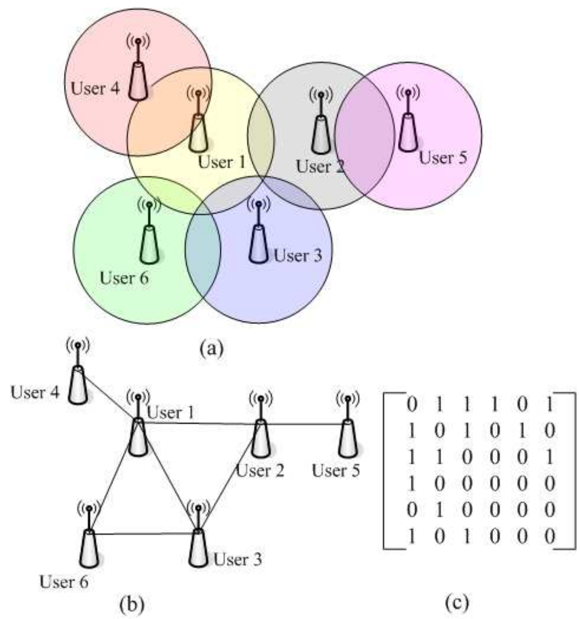


Figure 4.1: Illustration of the interference structure in a cognitive spectrum auction. (a) physical model; (b) graph representation; (c) matrix representation.

Since the proposed multi-winner auction awards the band simultaneously to several secondary users according to their mutual interference, interference plays an important role in the auction. We first use the well-known protocol interference model [84], where mutual interference in Fig. 4.1 (a) where $N = 6$ secondary cognitive base stations compete for the spectrum lease can be well captured by a conflict graph (Fig. 4.1 (b)), or equivalently, by an $N \times N$ adjacency matrix $\mathbf{C}$ (Fig. 4.1 (c)). By collecting reports from secondary users about their locations or their neighbors, the spectrum broker keeps the matrix $\mathbf{C}$ updated, even if the interference constraints change from time to time because of the slow movement of secondary users. When $C_{ij} = 1$, user i and user j cannot access the same band simultaneously, and if they do, neither of them gains due to collision. Therefore, the interference constraint is

$x_i + x_j \leq 1$ if $C_{ij} = 1$.

Our method can be extended to the physical physical model [85] as well, which describes interference in a more accurate but more complicated way. In this model, only transmissions with the received signal-to-interference-and-noise ratio (SINR) exceeding some threshold β are considered successful, i.e., $g_{ii}P / \left(\sum_{j \neq i} g_{ji} P x_j + Z_i\right) \geq \beta$, where g_{ji} represents the channel gain from jth user's transmitter to ith user's receiver, Z_i is the noise at receiver i, and we assume all users use the same power P. By neglecting the noise term when interference is the dominant factor in the system, the condition for simultaneous transmissions when no individual is impaired by mutual interference can be further reduced to $\sum_{j=1}^{N} \alpha_{ji} x_j \leq 0$ if $x_i = 1$, where we define $\alpha_{ii} = -1$ and $\alpha_{ji} = \beta g_{ji}/g_{ii}, i \neq j$.

Notations: $\mathbf{A} \in \mathbb{M}^{m \times n}$ means $\mathbf{A}$ is a matrix with dimension $m \times n$, and $\mathbf{b} \in \mathbb{M}^{m \times 1}$ indicates $\mathbf{b}$ is a column vector with length m. Denote their entries as A_{ij} and b_i, respectively. The trace of a matrix $\mathbf{A}$ is denoted by $\mathrm{tr}(\mathbf{A})$, and its rank is denoted by $\mathrm{rank}(\mathbf{A})$. The 2-norm of a vector $\mathbf{b}$ is denoted by $|\mathbf{b}|_2$. The all-zero, all-one, and identity matrices are denoted by $\mathbf{O}$, $\mathbf{1}$, and $\mathbf{I}$, respectively, and their dimensions are given in the subscript when there is room for confusion. The Kronecker product of two matrices $\mathbf{A}$ and $\mathbf{B}$ is denoted by $\mathbf{A} \otimes \mathbf{B}$. $\mathbf{S} \in \mathbb{S}^n$ means $\mathbf{S}$ is an $n \times n$ real symmetric matrix, and $\mathbf{S} \succeq \mathbf{O}$ implies $\mathbf{S}$ is positive semi-definite. Denote $\mathbf{b}_{-i} = [b_1, b_2, \ldots, b_{i-1}, b_{i+1}, \ldots, b_m]^T$ as a new vector with the ith entry of $\mathbf{b}$ excluded. Similarly, if W is a set of indices, $\mathbf{b}_{-W}$ implies all the entries whose indices fall in W are removed. $|W|$ denotes the cardinality of a set W. For two sets W_1 and W_2, the set difference is defined as $W_1 \setminus W_2 = \{x | x \in W_1 \text{ and } x \notin W_2\}$.

4.2 Collusion and Drawbacks of the VCG mechanism

Defining rules for winner determination and price determination, mechanism design plays an important role in an auction, since it greatly affects the auction outcome as well as user behavior. For example, the widely employed VCG mechanism, as discussed in Chapter 2, ensures the maximum system utility and enforces that all buyers bid their true valuations in the absence of collusion, i.e., $b_i = v_i$ $(i = 1, 2, \ldots, N)$, and could be applied to the multi-winner auction; However, serious drawbacks make the VCG mechanism less attractive, and it is necessary to develop suitable mechanisms for the multi-winner auction. In this section, we present its drawbacks and emerging kinds of collusion through specific examples in cognitive spectrum auctions.

In Fig. 4.2, several network topologies with user values are given, and the VCG auction outcome (x_i and p_i) has been calculated and listed in tables. First, the seller's revenue may be low. As in Case (a) with the VCG prices, the total payment collected by the primary user is $p_2 + p_3 + p_4 = 6$, which is quite low compared to the system utility. Furthermore, there is no guarantee that the primary user's revenue is bounded away from zero. In some unfavorable cases, for example, $v_1 = v_2 = v_3 = v_4 = 10$, the primary user sells the spectrum for nothing according to the VCG price.

Second, the losers may take advantage of the VCG pricing by colluding. For example, in Case (b), secondary user 1 gets the spectrum lease, and user 2, 3, 4 are the losers in the VCG auction. However, if colluding and misrepresenting their

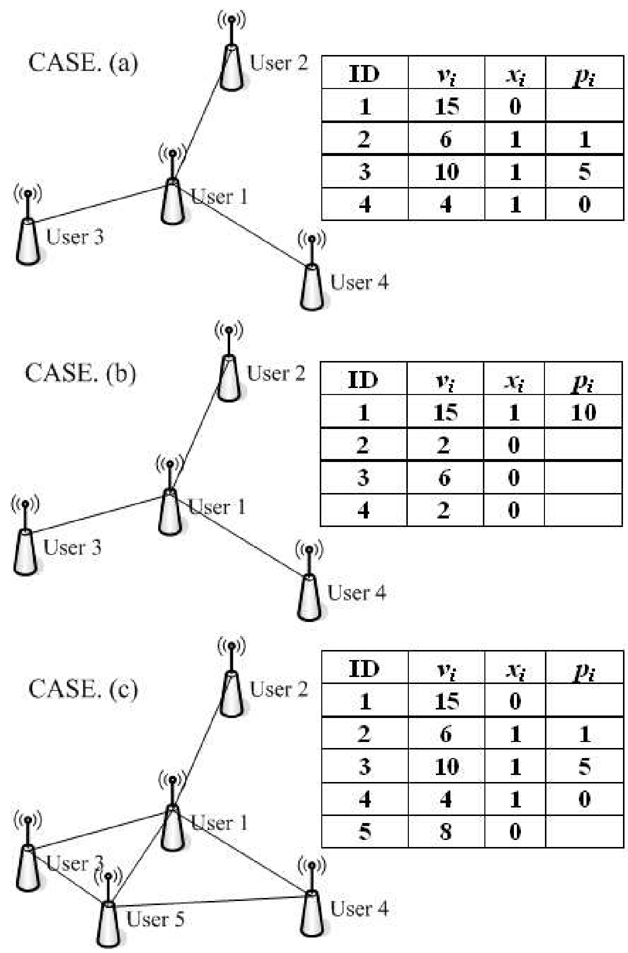


Figure 4.2: Different network topologies with the VCG mechanism employed.

valuations, they may become winners instead. For instance, they may collude to mimic Case (a) by claiming the same valuations as in Case (a), whose outcome is favorable since all colluders gain positive rewards, i.e., $r_2 = v_2 - p_2 = 1$, $r_3 = 1$, and $r_4 = 2$, respectively. The system efficiency is degraded because the spectrum resources are not assigned to the users who value them most. We name this kind of collusion as *loser collusion*.

Third, colluders may extract some profits from the seller by sublease collusion. In this Case (c), user 3 and user 4 may now collude with user 5 by subleasing the band at price $p_5 = 7$, and the income is split between them as 6 and 1. Then, both user 3 and 4 make extra profit by subleasing the band at higher prices than their leasing prices, and user 5 also benefits from subleasing since the reward is $v_5 - p_5 = 1$. Such collusion impairs the spectrum efficiency as well as the primary user's revenue, and we name it *sublease collusion*.

In addition to these two kinds of collusion, *kick-out collusion* is another possible collusion form when a group of users reveal wrong interference relation with others. For example, when several users belonging to the same group of interests, they may kick out a winner by saying they have mutual interference, and welcome their ally to join in the winner set instead.

4.3 One-Band Multi-Winner Auction

In this section, we develop suitable mechanisms for the multi-winner auction which guarantee system efficiency, yield high revenue, prevent potential collusion, and are of low complexity.

4.3.1 The Optimal Allocation

Because the goal of dynamic spectrum access is to improve the efficiency of spectrum utilization, the auction mechanisms should be designed such that the social welfare is maximized, that is, the band is awarded to the secondary users who value them most.

In a cognitive spectrum auction, only those without mutual interference can be awarded the band simultaneously, and we group them together as *virtual bidders*, whose valuations equal the sum of the individual valuations. Take Fig. 4.1 for example, there are seventeen virtual bidders, such as $\{1\}$, $\{1,5\}$, $\{4,5,6\}$ and so on; on the other hand, combinations like $\{1,3\}$ and $\{2,5,6\}$ are not virtual bidders due to interference. In order to achieve full efficiency, the virtual bidder with the highest bid will win the band. It is unnecessary to list all virtual bidders explicitly; instead, the optimal allocation $\mathbf{x}$ can be determined by the following N-variable binary integer programming (BIP) problem,

$$\begin{aligned} U^*_{\mathbf{v}} = & \max_{\mathbf{x}\in\{0,1\}^N} \sum_{i=1}^{N} v_i x_i, \\ & \text{s.t.} \ \ x_i + x_j \leq 1, \ \forall i,j \text{ if } C_{ij} = 1, \ \text{(interference constraints)} \end{aligned} \tag{4.3}$$

where interference constraints require that secondary users with mutual interference should not be assigned the band simultaneously.

4.3.2 Collusion-Resistant Pricing Strategies

After introducing the concept of virtual bidders, the multi-winner spectrum auction becomes similar to the single-winner auction, and hence it is possible to employ the second-price strategy which enforces truthful bidding. By applying the second-price mechanism to the auction consisting of virtual bidders, the virtual bidder with the highest bid wins the band (ties are broken randomly if two virtual bidders have the same valuation), and pays the highest bid made by the virtual bidder only consisting of losers. This can be done by solving two optimal allocation problems in succession. First, we solve (4.3) to determine the set of winners W, or the virtual winner. Then, we remove all the winners W from the system, and solve the optimization problem again to calculate the maximum utility, denoted by $U^*_{\mathbf{v}_{-W}}$, which is the amount of money that the virtual winner has to pay.

We have to point out that the new pricing strategy sacrifices the enforcement of truth-telling a little bit for higher revenue and more robustness against collusion; however, since the proposed pricing strategy is quite similar to the second-price mechanism where users bid their true valuations, we expect users will not shade their bids too much from their true valuations. Thus, we neglect the difference between b_i and v_i in the following analysis to focus on revenue and robustness aspects of the new mechanisms.

The remaining problem is splitting the payment $U^*_{\mathbf{v}_{-W}}$ among the secondary users within the virtual winner. This is quite similar to a Nash bargaining game [13] where each selfish player proposes his/her own payment during a bargaining process such that the total payment equals $U^*_{\mathbf{v}_{-W}}$, and it is well-known that the Nash bargaining solution (NBS), which maximizes the product of individual payoffs, is an equilibrium [13]. In the proposed auction, no individual bargaining is necessary; instead, the spectrum broker directly sets the NBS prices for each winner, and everyone is ready to accept them since they are equilibrium prices. The pricing strategy is the solution to the following optimization problem,

$$\begin{aligned} &\max_{\{p_i \in [0, v_i],\, i \in W\}} \prod_{i \in W} (v_i - p_i), \\ &\text{s.t.} \ \sum_{i \in W} p_i = U^*_{\mathbf{v}_{-W}}. \end{aligned} \tag{4.4}$$

Proposition 7 *User i has to pay the price $p_i = \max\{v_i - \rho, 0\}$, for $i \in W$, where ρ is chosen such that $\sum_{i \in W} p_i = U^*_{\mathbf{v}_{-W}}$. In particular, if $\hat{p}_i \triangleq v_i - \frac{U^*_{\mathbf{v}} - U^*_{\mathbf{v}_{-W}}}{|W|} \geq 0$ for any i, $p_i = \hat{p}_i$ will be the solution.*

Proposition 7 can be proved using the Lagrangian method and the KarushKuhnTucker (KKT) condition, the detail of which can be found in [20]. It implies that the payment is split in such a way that the profits are shared among the winners as equally as possible. Different from the VCG pricing strategy which sometimes may yield low revenue or even zero revenue, such a pricing strategy always guarantees that the seller receives revenue as much as $U^*_{\mathbf{v}_{-W}}$. Moreover, if some losers collude to beat the winners by raising their bids, they will have to pay more than $U^*_{\mathbf{v}_{-W}}$; however, the payment is already beyond what the band is actually worth to them, and as a result, loser collusion is completely eliminated. Nevertheless, users can still benefit from the sublease collusion, and hence we call the pricing strategy in (4.4) the *partially collusion-resistant pricing strategy.*

In order to find a *fully collusion-resistant pricing strategy*, we have to analyze how sublease collusion takes place, and add more constraints accordingly. It happens when a subset of the winners $W_C \subseteq W$ subleases the band to a subset of the losers $L_C \subseteq L$, where $L = \{1, 2, \ldots, N\} \setminus W$ denotes the set of all losers. The necessary condition for the sublease collusion is $\sum_{i \in W_C} p_i < \sum_{i \in L_C} v_i$, so that they can find a sublease price in between acceptable to both parties. Given any colluding-winner subset $W_C \subseteq W$, the potential users who may be interested in subleasing the band should have no mutual interference with the remaining winners $W \setminus W_C$; otherwise, the band turns out to be unusable. Denote the set of all such potential users by $L(W \setminus W_C)$, i.e., $L(W \setminus W_C) \triangleq \{i \in L | C_{ij} = 0, \forall j \in W \setminus W_C\}$. Therefore, as long as prices are set such that $\sum_{i \in W_C} p_i \geq \max_{L_C \in L(W \setminus W_C)} \sum_{i \in L_C} v_i$, there will be no sublease collusion. Note that $\max_{L_C \in L(W \setminus W_C)} \sum_{i \in L_C} v_i$ is the maximum system utility $U^*_{\mathbf{v}_{L(W \setminus W_C)}}$ which can be obtained by solving the optimal allocation problem within the user set $L(W \setminus W_C)$, thus the optimum collusion-resistant pricing strategy is the solution to the following problem,

$$\begin{aligned} &\max_{\{p_i \in [0, v_i],\, i \in W\}} \prod_{i \in W} (v_i - p_i), \\ &\text{s.t.} \sum_{i \in W_C} p_i \geq U^*_{\mathbf{v}_{L(W \setminus W_C)}}, \forall W_C \subseteq W. \end{aligned} \tag{4.5}$$

When $W_C = W$, the constraint reduces to $\sum_{i \in W} p_i \geq U^*_{\mathbf{v}_{-W}}$, which incorporates the constraint in (4.4) as a special case. There are $2^{|W|} - 1$ constraints in total because each of them corresponds to a subset $W_C \subseteq W$ except $W_C = \emptyset$. From another perspective, this actually takes into consideration of virtual bidders consisting of both winners and losers, in contrast to the previous pricing strategy where only those consisting of losers are considered.

4.3.3 Interference Matrix Disclosure

So far, our auction mechanism is based on the assumption that the underlying interference matrix $\mathbf{C}$ reflects the true mutual interference relationships between secondary users. However, since $\mathbf{C}$ comes from secondary users' own reports, it is quite possible that the selfish users manipulate this information just as what they may do with their bids. If cheating could help a loser become a winner, or help a winner pay less, the selfish users would have incentives to do so, which would compromise the efficiency of the spectrum auction. Also, the cheating behavior may happen individually or in a collusive way. Therefore, we have to carefully consider whether they have such an incentive to deviate, and if so, how to fix the potential problem.

In order to obtain the matrix $\mathbf{C}$, the spectrum broker has to collect information from secondary users. Secondary users may report their locations in terms of coordinates, and the spectrum broker calculates the matrix according to their distances. In this way, secondary users do not have much freedom to fake an interference relationship in favor of themselves. Alternatively, secondary users may directly inform the spectrum broker about who are their neighbors, and hence they are able to manipulate the matrix, either by concealing an existing interference relationship or by fabricating an interference relationship that actually does not exist.

When secondary users have little information about others, they will misrepresent the interference relationships only if they do not get punished, even in the worst case. Assume user j lies about C_{jk}. When users j and k do not mutually interfere, i.e., $C_{jk} = 0$, but user j claims $\hat{C}_{jk} = 1$, he/she may lose an opportunity of being a winner since an extra interference constraint is added; on the other hand, if $C_{jk} = 1$ but user j claims $\hat{C}_{jk} = 0$, user j may end up winning the band together with user k, but the band cannot be used at all due to strong interference. In short, the worst-case analysis suggests secondary users have no incentive to cheat whenever information is limited.

When secondary users somehow have more information about others, they may distort the information in a more intelligent way, that is, they can choose when to cheat and how to cheat. Nevertheless, by investigating whether user j is better off by misrepresenting C_{jk}, we show that truth-telling is an equilibrium from which no individual would have the incentive to deviate unilaterally. We discuss all possible situations in what follows.

1. Under the condition that user j is supposed to be a loser.

   1a. Claim $\hat{C}_{jk} = 1$ against the truth $C_{jk} = 0$. By doing this, user j actually introduces an additional interference constraint to himself/herself, but since user j is already a loser, nothing would change.

   1b. Claim $\hat{C}_{jk} = 0$ against the truth $C_{jk} = 1$. Removing a constraint possibly helps user j to become a winner, but in the case, user k is also one of the winners. Then, user j has to pay a band that turns out to be unusable due to strong mutual interference with user k. This is unacceptable to user j.

2. Under the condition that user j is supposed to be a winner.

2a. Claim $\hat{C}_{jk} = 0$ against the truth $C_{jk} = 1$. If user j is the only one among the winners that has interference with user k, it would take user k into the winner set, which would in turn make user j suffer from mutual interference.

2b. Claim $\hat{C}_{jk} = 1$ against the truth $C_{jk} = 0$. If user k is not a winner, doing this would change nothing. If user k is indeed a winner, user j takes the risk of throwing himself/herself out of the winner set. Even if user j has enough information to secure he/she can still be a winner, kicking out user k does not necessarily make user j pay less.

Similar analysis can be applied to the situation where a group of secondary users are able to distort the information collusively, and we find that kick-out collusion is the only way that colluders gain an advantage. If channels are symmetric, i.e., $C_{jk} = C_{kj}$ always holds, we can apply the following conservative rule: the spectrum broker sets C_{jk} to 1 only when both users j and k confirm they have mutual interference. Colluding users cannot unilaterally fabricate an interference relationship to an innocent user who is honest, and they will lose their incentives to cheat because their efforts are in vain.

4.3.4 Complexity Issues

We have to examine the complexity of the proposed mechanism to see whether it is scalable when more users are involved in the auction game. Since the fully collusion-resistant pricing is a convex optimization problem when linear inequality constraints are known, they can be efficiently solved by numerical methods such as the interior point method [86]. However, one optimal allocation problem has to be solved to find the set of winners W, and another $2^{|W|}-1$ problems have to be solved to obtain $U^*_{\mathbf{v}_{L(W \setminus W_C)}}$ used in the constraints. Unfortunately, the optimal allocation problem can be seen as the maximal weighted independent set problem [87] in graph theory, which is known to be NP-complete in general, even for the simplest case with $v_i = 1$ for all i [82]. As the computational complexity becomes formidable when the number of users N is large, the proposed auction mechanism seems unscalable. Therefore, near-optimal approximations with polynomial complexity are of great interest.

Proposition 8 *Define* $\boldsymbol{\mu}_{\mathbf{v}} = [\sqrt{v_1}, \sqrt{v_2}, \ldots, \sqrt{v_N}]^T$*, the optimal allocation problem (4.3) with* $\mathbf{x}^*$ *as its optimizer is equivalent to the following optimization problem,*

$$
\begin{aligned}
\widetilde{U}^*_{\mathbf{v}} = &\max_{\mathbf{y}} \left(\boldsymbol{\mu}_{\mathbf{v}}^T \mathbf{y}\right)^2, \\
\text{s.t.} \quad & y_i y_j = 0, \ \forall i, j \text{ if } C_{ij} = 1, \\
& |\mathbf{y}|_2 = 1,
\end{aligned}
\tag{4.6}
$$

whose optimizer $\mathbf{y}^*$ *is given by* $y_i^* = c\sqrt{v_i}x_i^*$ *where* c *is a normalization constant such that* $|\mathbf{y}^*|_2 = 1$.

According to Proposition 8 whose proof can be found in [20], the optimal allocation is no longer an integer programming problem, but still difficult to solve because of the non-convex feasible set. To make it numerically solvable in polynomial time, the SDP relaxation can be applied, which enlarges the feasible set to a cone of positive semi-definite matrices (which is a convex set) by removing some constraints [83]. To this end, let $\mathbf{S} = \mathbf{y}\mathbf{y}^T$, i.e., $S_{ij} = y_i y_j$. The objective function in (4.6) becomes $\boldsymbol{\mu}_{\mathbf{v}}^T \mathbf{S} \boldsymbol{\mu}_{\mathbf{v}}$, and the two constraints turn out to be $S_{ij} = 0, \ \forall i, j$ if $C_{ij} = 1$

and $\mathrm{tr}(\mathbf{S}) = 1$, respectively. The problem has to be optimized over $\{\mathbf{S} \in \mathbb{S}^N | \mathbf{S} = \mathbf{y}\mathbf{y}^T, \mathbf{y} \in \mathbb{M}^{N\times 1}\}$, or equivalently, $\{\mathbf{S} \in \mathbb{S}^N | \mathbf{S} \succeq \mathbf{O},\ \mathrm{rank}(\mathbf{S}) = 1\}$. Discarding the rank requirement while only keeping the positive semi-definite constraint, we arrive at the following convex optimization problem,

$$\begin{aligned} \vartheta(\mathbf{C}, \mathbf{v}) = &\max_{\mathbf{S}\succeq\mathbf{O}}\ \boldsymbol{\mu}_{\mathbf{v}}^T \mathbf{S} \boldsymbol{\mu}_{\mathbf{v}} \\ \text{s.t.}\ \ &\mathrm{tr}(\mathbf{S}) = 1, \\ &S_{ij} = 0,\ \forall i, j \text{ if } C_{ij} = 1, \end{aligned} \tag{4.7}$$

which is also known as the *theta number* [88] in graph theory.

With the feasible set enlarged by relaxing a constraint to its necessary condition, the new optimization problem provides an upper bound to the original one: if the optimizer $\mathbf{S}^*$ can be decomposed as $\mathbf{S}^* = \mathbf{y}^*\mathbf{y}^{*T}$ which means $\mathbf{S}^*$ falls into the original feasible set, $\mathbf{y}^*$ will be the exact solution to (4.6); otherwise, $\vartheta(\mathbf{C}, \mathbf{v})$ is an upper bound that is unattainable. Fortunately, we verify by simulation that the near-optimal algorithm with relaxation performs well: in our problem setting, it gives the exact solution most of the time ($> 90\%$), and even for those unattainable cases, the bound is considerably tight since the average gap is within 5%.

4.3.5 Physical Interference Model

In this subsection, we extend our auction mechanism to the situation where the physical model is employed to describe mutual interference. Now, the optimal allocation becomes social welfare maximization under physical interference constraints,

$$
\begin{aligned}
U_{\mathbf{v}}^* = \max_{\mathbf{x}\in\{0,1\}^N} & \sum_{i=1}^{N} v_i x_i, \\
\text{s.t.} \quad \sum_{j=1}^{N} & \alpha_{ji} x_j \leq 0, \text{ if } x_i = 1.
\end{aligned}
\tag{4.8}
$$

Recall that those α's have been defined as $\alpha_{ii} = -1$ and $\alpha_{ji} = \beta g_{ji}/g_{ii}, i \neq j$, which basically depend on channel gains. Thus, the optimal allocation remains much the same except that protocol interference constraints are replaced by physical interference constraints. Pricing strategies are similar, too.

Nevertheless, the SDP relaxation is a bit difficult because the constraints are much more complicated than constraints exerted by the protocol model. First, we replace the constraint "$\sum_{j=1}^{N} \alpha_{ji} x_j \leq 0$ if $x_i = 1$" by an equivalent but compact form $x_i \left(\sum_{j=1}^{N} \alpha_{ji} x_j\right) \leq 0$, because x_i is a binary integer variable. Then, we can apply similar approaches, i.e., $y_i = c\sqrt{v_i} x_i$ and $S_{ji} = y_j y_i$, and finally get the following relaxed optimization problem,

$$
\begin{aligned}
& \max_{\mathbf{S}\succeq\mathbf{O}} \boldsymbol{\mu}_{\mathbf{v}}^T \mathbf{S} \boldsymbol{\mu}_{\mathbf{v}} \\
& \text{s.t.} \quad \operatorname{tr}(\mathbf{S}) = 1, \\
& \qquad S_{ji} = 0, \ \forall i, j \text{ if } \alpha_{ji} > 1, \\
& \qquad \sum_{j=1}^{N} \frac{\alpha_{ji}}{\sqrt{v_j v_i}} S_{ji} \leq 0, \ i = 1, 2, \ldots, N.
\end{aligned}
\tag{4.9}
$$

Note that when $\alpha_{ji} > 1$, i.e., user j has strong interference on user i, user i cannot transmit simultaneously with user j, because if $x_i = x_j = 1$, we have $\sum_{j=1}^{N} \alpha_{ji} x_j \geq \alpha_{ji} x_j + \alpha_{ii} x_i = \alpha_{ji} - 1 > 0$ which will violate the constraint. Hence, the corresponding constraint is quite similar to that under the protocol model. Moreover, compared with (4.7), the SDP relaxation under the physical model (4.9) incorporates additional constraints reflecting the accumulation of interference power.

4.4 Multi-Band Multi-Winner Auction

In this section, we study the case when M primary users want to lease their unused bands or a single primary user divides the band into M sub-bands for lease. In other words, there are M bands ($M > 1$) available for secondary users to lease.

Since usually there are a lot of secondary users competing for the spectrum resources, it is unfair if some users can access several bands while others are starved. In addition, if each secondary user is equipped with a single radio, the physical limitation will make it impossible to access several bands simultaneously. Therefore, we require each user should lease at most one band, and we further assume secondary users do not care which band they get, i.e., any band's value is v_i to user i.

Extending the one-band auction to a more general multi-band one, we have to find the counterpart of the auction mechanism including the optimal allocation and pricing strategies. As there are M sets of winners $W^1, W^2, \ldots, W^M$, we define M vectors $\mathbf{x}^1, \mathbf{x}^2, \ldots, \mathbf{x}^M$ correspondingly, where $x_i^m = 1$ indicates user i wins the mth band. Including the additional constraint that each user cannot lease more than one band, we have the M-band optimal allocation as follows,

$$
\begin{aligned}
U^*_{\mathbf{v}} = &\max_{\mathbf{x}^1,\mathbf{x}^2,\ldots,\mathbf{x}^M} \sum_{m=1}^{M}\sum_{i=1}^{N} v_i x_i^m, \\
\text{s.t.}\ \ & x_i^m + x_j^m \le 1,\ \forall i,j \text{ if } C_{ij}=1, \forall m, \\
& \sum_{m=1}^{M} x_i^m \le 1,\ \forall i, \\
& x_i^m = 0 \text{ or } 1, i=1,2,\ldots,N; m=1,2,\ldots,M.
\end{aligned}
\tag{4.10}
$$

In the multi-band auction, the set of losers becomes $L = \{1,2,\ldots,N\} \setminus \bigcup_{j=1}^{M} W^j$ instead. Similar to the single-band partially collusion-resistant pricing strategy, the winners of the mth band have to pay the highest rejected bid from the losers, and the payment is split according to the NBS equilibrium,

$$
\begin{aligned}
&\max_{\{p_i\in[0,v_i],\, i\in W^m\}} \prod_{i\in W^m} (v_i - p_i), \\
&\text{s.t.}\ \ \sum_{i\in W^m} p_i = U^*_{\mathbf{v}_{-\left(\cup_{j=1}^{M} W^j\right)}}.
\end{aligned}
\tag{4.11}
$$

The single-band fully collusion-resistant pricing strategy can be generalized too; for instance, the prices for the mth band are determined by

$$
\begin{aligned}
&\max_{\{p_i\in[0,v_i],\, i\in W^m\}} \prod_{i\in W^m} (v_i - p_i), \\
&\text{s.t.}\ \ \sum_{i\in W_C} p_i \ge U^*_{\mathbf{v}_{L(W^m\setminus W_C)}}, \forall W_C \subseteq W^m.
\end{aligned}
\tag{4.12}
$$

When $M=1$, the two pricing strategies reduce to the single-band case.

It is not difficult to convert the multi-band auction to an equivalent single-band auction with MN bidders, and the SDP relaxation can be directly applied. However, Proposition 9 provides a better solution which takes advantage of the symmetric structure of the problem. As the new optimization problem is optimized over two symmetric matrices $\mathbf{S}_D, \mathbf{S}_F \in \mathbb{S}^N$, the total number of degrees of freedom is $N(N+1)$, which is significantly smaller than that of direct relaxation $\frac{1}{2}MN(MN+1)$. Roughly speaking, degrees of freedom, as an important factor affecting the computational complexity, are reduced from $O(M^2N^2)$ to $O(N^2)$. The proof of Proposition 9 can be found in [20].

Proposition 9 *The multi-band optimal allocation (4.10) can be relaxed by the following optimization problem,*

$$\begin{aligned}
&\max_{\mathbf{S}_D,\mathbf{S}_F} \boldsymbol{\mu}_{\mathbf{v}}^T(\mathbf{S}_D + (M-1)\mathbf{S}_F)\boldsymbol{\mu}_{\mathbf{v}} \\
&\ s.t.\ \ tr(\mathbf{S}_D) = 1, (S_D)_{ij} = 0,\ \forall i,j\ \ if\ C_{ij} = 1, \\
&\qquad\ (S_F)_{ii} = 0,\ \forall i, \\
&\qquad\ \mathbf{S}_D \succeq \mathbf{O},\ \mathbf{S}_D - \mathbf{S}_F \succeq \mathbf{O}, \mathbf{S}_D + (M-1)\mathbf{S}_F \succeq \mathbf{O}.
\end{aligned} \tag{4.13}$$

4.5 Simulation Studies

In this section, we evaluate the performance of the proposed collusion-resistant multi-winner spectrum auction mechanisms by computer experiments. Consider a $1000 \times 1000\,\mathrm{m}^2$ area, in which N secondary users are uniformly distributed. Assume each secondary user is a cognitive base station with R_I-meter coverage radius, and according to the protocol model, two users at least $2R_I$ meters away can share the same band without mutual interference. We use two values for R_I: $R_I = 150$ for a light-interference network, and $R_I = 350$ for a heavy-interference network. The valuations of different users $\{v_1, v_2, \ldots, v_N\}$ are assumed to be i.i.d. random variables uniformly distributed in $[20, 30]$.

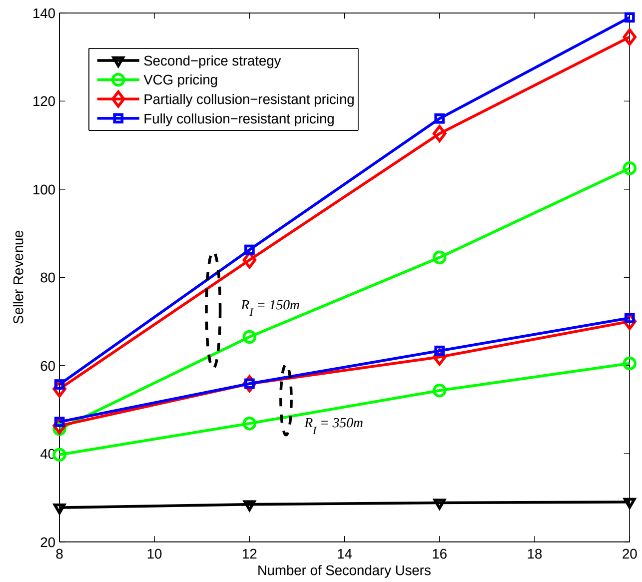


Figure 4.3: Seller's revenue when different auction mechanisms are employed.

We consider the one-band auction, i.e., $M = 1$. Fig. 4.3 shows the seller's revenue versus the number of secondary users when different auction mechanisms are employed. The result is averaged over 100 independent runs, in which the locations and valuations of the N secondary users are generated randomly with uniform distribution. As shown in the figure, directly applying the second-price scheme under-utilizes spectrum resources, and the VCG mechanism also suffers from low revenue. The proposed collusion-resistant methods, however, significantly improve the primary user's revenue, e.g., nearly 15% increase compared to the VCG outcome when $R_I = 350$, and 30% increase when $R_I = 150$. This means the proposed algorithms have better performance when more secondary users are admitted to lease the band simultaneously.

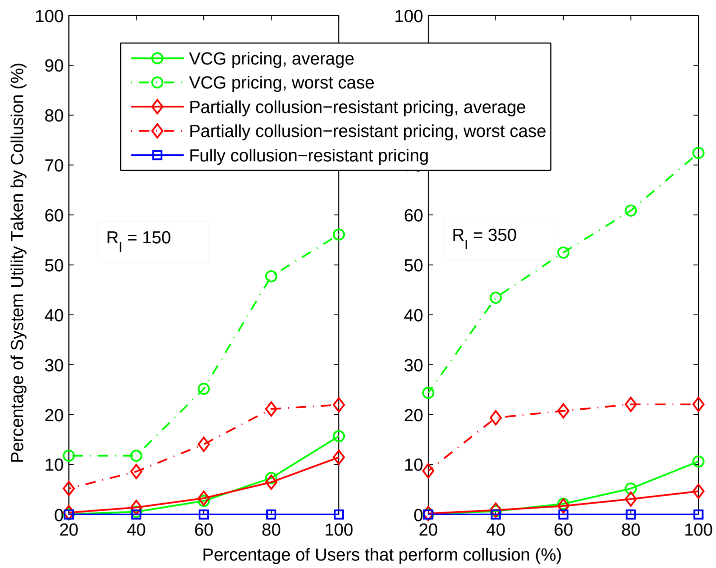


Figure 4.4: Normalized collusion gains under different auction mechanisms versus the percentage of colluders in a spectrum auction with $N = 20$ secondary users.

Moreover, the proposed auction mechanisms can effectively combat user collusion. We use the percentage of the system utility taken away by colluders to represent the vulnerability to sublease colluding attacks. Fig. 4.4 demonstrates the results from 100 independent runs. For example, when $R_I = 150$ and there are 20% colluders, colluders may steal away up to 10% of the system utility with the VCG pricing mechanism, and much more profits could be taken away by colluders if more secondary users become colluders. To protect the primary user's benefit, collusion-resistant mechanisms can be applied. As show in the figure, the partially collusion-resistant pricing strategy may be not as good as the VCG mechanism on average under some circumstances because it cannot completely remove sublease collusion, but it makes the worst-case colluding gains drop considerably; for instance, when $R_I = 150$ and all users are able to collude, more than half of the system utility could be taken away if the VCG pricing is used, but only 22% with the partially collusion-resistant pricing method. The fully collusion-resistant pricing strategy, as expected, completely eliminates collusion, and hence is an ideal choice when there is a risk of sublease collusion.

The performance of the near-optimal algorithm is presented in Fig. 4.5. As shown by the simulation results, the near-optimal algorithm can yield the exact solution in more than 90% of the total runs. Even for those that the near-optimal algorithm fails to return the exact solution, it can still yield a tight upper bound with the average difference less than 5%; to show the robustness of the algorithm, we further provide the 90% confidence intervals (i.e., the range that 90% of the data fall in), which show that the gap between the near-optimal solution and the exact solution is within 10%.

Finally, we show the reduction of complexity in terms of the processing time when optimization is done in MATLAB. In Fig. 4.6, the processing time of solving the optimal allocation problem is compared with that of solving the near-optimal allocation problem in 100 independent runs, when $R_I = 350$ and the number of users is N =20, 30, and 40, respectively. With N increasing, the time to find the optimal solution increases dramatically, whereas the time to find an near-optimal solution using the SDP relaxation only increases slightly. Moreover, the processing time of the optimal algorithm fluctuates considerably in different realizations, but the processing time with the SDP relaxation shows small variation.

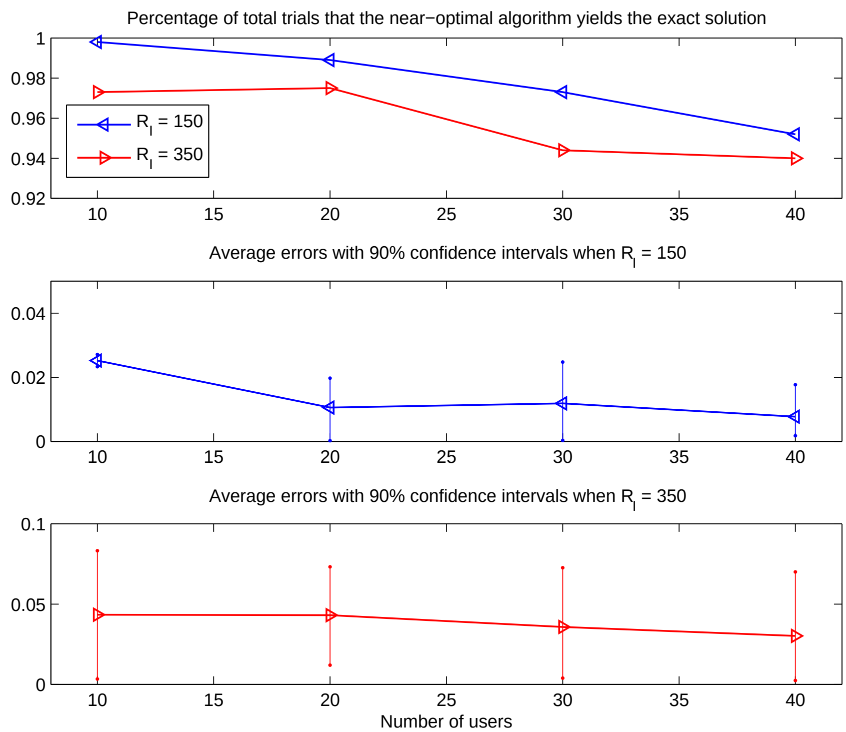


Figure 4.5: The percentage of total trials that the near-optimal algorithm yields the exact solution (upper), and the average gap with 90% confidence intervals between the near-optimal solution and the exact solution for those failed trials (middle and lower, for $R_I = 150$ and 350, respectively).

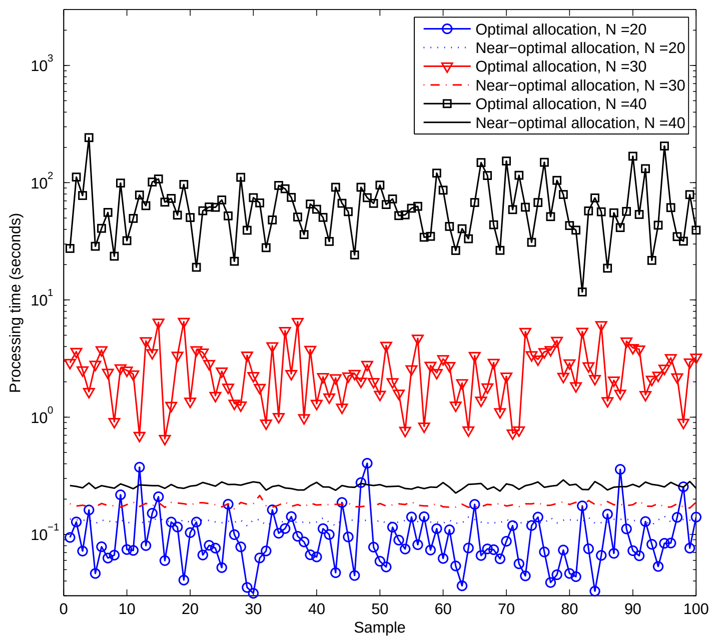


Figure 4.6: Sampled processing time of the optimal allocation and the near-optimal allocation with the SDP relaxation.

Chapter 5

Anti-Jamming Games in Multi-Channel Cognitive Radio Networks

In previous chapters, we have shown how to apply game-theoretic tools to suppress the selfish behavior in cognitive radio networks consisting of selfish users. However, as we pointed out in Chapter 1, security issues are very important to the deployment of cognitive radio networks which are extremely vulnerable to malicious attacks. In this chapter, we mainly focus on jamming attacks, one of the major threats to cognitive radio networks, where several malicious attackers intend to interrupt the communications of a secondary user by injecting interference. Because cognitive radio technology enables flexible access to different channels, secondary users are able to transmit information over multiple channels, and may exploit such flexibility as a way to hide from attackers. On the other hand, attackers are also intelligent such that they can come up with efficient attack strategies. Therefore, this scenario is modeled as a *zero-sum anti-jamming game*, in which the two players, namely, secondary users and attackers, have opposite objectives.

There have been quite a few papers on jamming attacks in wireless ad hoc networks, such as [89] and [90]. A jamming game with transmission costs was formulated in [89], and the blocking probability was analyzed for different kinds of attack strategies and defense strategies in [90]. However, the problem becomes more complicated in a cognitive radio network where primary users' access has to be taken into consideration.

In the context of cognitive radio networks, channel hopping was considered as a defense strategy in [91] which derived the Nash equilibrium in a one shot game and applied this equilibrium strategy to a multi-stage game. However, this is different from our approaches. In our work, we explicitly model transitions in time as Markov chains, take the cost and damage into account in addition to communication gains, and further develop a learning process to estimate unknown parameters.

5.1 System Model

We consider the situation where a secondary user (e.g., a base station for a secondary network) opportunistically accesses the spectrum bands. Assume there are M licensed channels in total, each licensed channel is time-slotted, and the access pattern of primary users can be characterized by an ON-OFF model [92]. As shown in Fig. 5.1, one channel can either be busy (ON) or idle (OFF) in one time slot, and the state can be switched from ON to OFF (or from OFF to ON) with a transition probability α (or β). We assume all channels share the same model and parameters, but different channels are used by different primary users whose accesses are independent. In order to avoid interference to primary users, a secondary user has to synchronize with the primary network and detect the presence of the primary user at the beginning of each time slot. It is only when the primary user is absent that the secondary user is allowed to access the channel, which is also known as the "listen-before-talk" rule. Meanwhile, there are m malicious attackers intending to

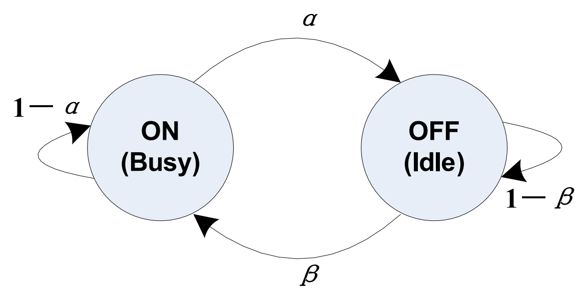


Figure 5.1: An ON-OFF model for primary users' spectrum usage.

jam the secondary user's communications, and they coordinate with each other to maximize the damage.

With attackers jamming interference into spectrum bands, it is possible that the signal-to-interference-and-noise ratio (SINR) at the secondary user's receiver will be dragged down, and when the SINR drops below a certain threshold β, the communication fails (e.g., packets cannot be decoded correctly). We assume that a secondary user has a power constraint p^B, and an attacker has a power constraint i^B. All channel gains are assumed to be 1 because they can be absorbed into the power constraint term. Furthermore, it is of interest to consider the case that the attacker is stronger than the secondary user, and we limit ourselves to the case $p^B \leq \beta i^B$. For example, when both users allocate all power to the same band, the secondary user always fails to communicate due to the poor SINR $p^B/(i^B + \sigma^2) < \beta$.

In different application scenarios, secondary users may have different capabilities. For example, a secondary user may be equipped with a single radio or multiple radios. Attackers are assumed to be comparable with the secondary user, that is, equipped with a single radio in the first case, and with multiple radios in the second case. In order to improve throughput, in the single-radio case, it is best for the secondary user to pour all power to a single band, and channel hopping is the defense strategy. For the multi-radio case, the secondary user could allocate power to several bands, and the defense can be fortified via optimal power allocation. In this attack-and-defense game, attack and defense should be randomized; otherwise, a fixed pattern of one player will be taken advantage of by the other player.

5.2 Channel Hopping Anti-Jamming Games

When the secondary user is equipped with a single radio, he/she can only sense and access one channel at one time slot, and could hop among multiple channels to make it difficult for attackers to find. Meanwhile, attackers search over multiple channels in order to catch and jam the secondary user.

5.2.1 Game Formation

A secondary user receives a communication gain R whenever there is a successful transmission. The cost associated with channel hopping is denoted by C, and a significant loss L is occurred when jammed, since normal communication is interrupted and considerable effort is needed to reestablish the link. At the end of each time slot, the secondary user decides either to *stay* or to *hop* for the next time slot, based on the observation of the current and past slots. The secondary user receives an immediate payoff $U(n)$ in the nth time slot, which is the communication gain minus the cost and damage. Because an employed strategy not only affects the current state but also has impact on the future, the payoff of this game $\overline{U}$, which the secondary user wants to maximize but malicious attackers want to minimize, is a δ-discounted sum of payoffs,

$$\overline{U} = \sum_{n=1}^{\infty} \delta^n U(n). \tag{5.1}$$

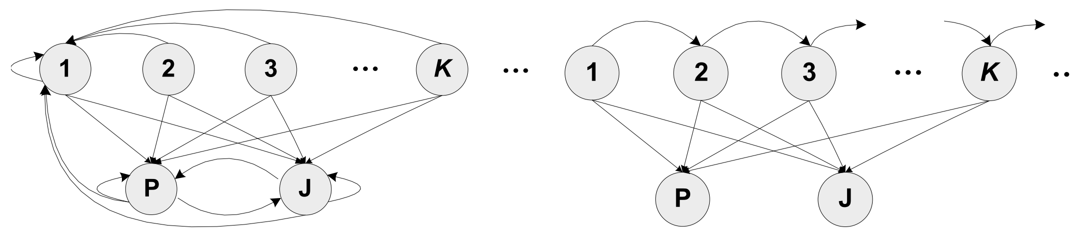
For this game, it is desirable to know what could be possible attack strategies and what should be the optimal defense strategy. However, an attack-and-defense problem is often like an arms race: when an attacker updates the attack strategy, it is possible for the defender to come up with a new defense strategy that best defeats the new attack strategy, and vice versa. We focus on the "first round", that is, what is the best attack strategy when there is no defense at all, and then what is the optimal defense strategy against such an attack strategy.

Without considering the jamming threats, the secondary user tends to stay in a fallow licensed channel as long as possible until the primary user reappears, in order to avoid the hopping cost. Then, from attackers' perspective, they want to find and jam the secondary user as soon as possible. It is inefficient if several malicious attackers tune their radios to the same channel to detect the secondary user, and they should coordinate not to overlap, detecting m channels in each time slot. A random scanning attack strategy performs best to find the secondary user remaining in an unknown channel, that is, attackers coordinately tune their radios randomly to m undetected channels in each time slot, until this process starts over when either all channels have been sensed or the secondary user has been found and jammed. Since attackers start a new random scanning cycle after a successful jamming, the secondary user has no clue about which channel will be detected by attackers next.

We assume attackers stick to this random scanning strategy and derive the optimal strategy that a secondary user should adopt. In the presence of attackers, the longer the secondary user stays in a channel, the higher the risk of exposure to attackers. As a result, proactive hopping to another channel may help to hide from attackers. With the random scanning attack strategy, the anti-jamming game boils down to a Markov decision process (MDP).

5.2.2 Markov Models

At the end of the nth time slot, the secondary user observes the state of the current time slot S_n, and chooses an action a_n, that is, whether to tune the radio to a new channel or not, which takes effect at the beginning of the next time slot. To set a clear distinction, states are denoted by upper-case letters while actions are denoted by lower-case letters. If the primary user occupied the channel or the secondary user was jammed in the nth time slot, denoted by $S_n = P$ and $S_n = J$, respectively, the secondary user has to hop to a new channel, i.e., $a_n = h$; otherwise, the secondary user has transmitted a packet successfully in the time slot, and possible actions are 'to hop' ($a_n = h$) and 'to stay' ($a_n = s$). If this is the Kth consecutive slot with successful transmission in the same channel, the state is denoted by $S_n = K$. For brevity, we will drop the time index n wherever there is no room for ambiguity. The



(a) Transition of states when taking the action *'hop'*.

(b) Transition of states when taking the action *'stay'*.

Figure 5.2: Markov chains of state transitions when different actions are taken.

immediate payoff function depends on both the state and the action, i.e.,

$$U(S,a)=\begin{cases} R, & \text{if } S\in\{1,2,3,\ldots,\}, a=s;\\ R-C, & \text{if } S\in\{1,2,3,\ldots,\}, a=h;\\ -L-C, & \text{if } S=J;\\ -C, & \text{if } S=P. \end{cases} \tag{5.2}$$

The transition of states can be described by Markov chains, as shown in Fig. 5.2, where transition probabilities depend on which action has been taken. Hence, we use $p(S'|S,h)$ and $p(S'|S,s)$ to represent the transition probability from an old state S to a new state S' when taking action h and action s, respectively.

If the secondary user hops to a new channel, transition probabilities do not depend on the old state, and furthermore, the only possible new states are P (the new channel is occupied by the primary user), J (transmission in the new channel is detected by an attacker), and 1 (successful transmission begins in the new channel). When the total number of channels M is large, i.e., $M \gg 1$, we can assume that the probability of primary user's presence in the new channel equals the steady-state probability of the ON-OFF model in Fig. 5.1, neglecting the case that the secondary user hops back to some channel in very short time, and we have

$$p(P|S,h) = \frac{\beta}{\alpha+\beta} \triangleq \gamma,\ \forall S \in \{P, J, 1, 2, 3, \ldots, \}. \tag{5.3}$$

Provided that the new channel is available, the secondary user will be jammed with the probability m/M, since each attacker detects one channel without overlapping. As a result, transition probabilities are

$$\begin{aligned} p(J|S,h) &= (1-\gamma)\frac{m}{M},\ \forall S \in \{P, J, 1, 2, 3, \ldots, \}; \\ p(1|S,h) &= (1-\gamma)\frac{M-m}{M},\ \forall S \in \{P, J, 1, 2, 3, \ldots, \}. \end{aligned} \tag{5.4}$$

On the other hand, if the secondary user stays in the same channel, the primary user may reclaim the channel with probability β given by the ON-OFF model. With the primary user absent, the state will go to J if the transmission is jammed, and will increase by 1 otherwise. Note that s is not a feasible action when the state is in J or P. At state K, only $\max(M-Km, 0)$ channels have yet been detected by attackers, but another m channels will be detected in the upcoming time slot; therefore, the probability of jamming conditioned on the absence of a primary user is given by

$$f_J(K) = \begin{cases} \frac{m}{M-Km}, & \text{if } K < \frac{M}{m} - 1; \\ 1, & \text{otherwise.} \end{cases} \tag{5.5}$$

To sum up, transition probabilities associated with action s are as follows: $\forall K \in \{1, 2, 3, \ldots\}$,

$$\begin{aligned} p(P|K,s) &= \beta, \\ p(J|K,s) &= (1-\beta) f_J(K), \\ p(K+1|K,s) &= (1-\beta)(1-f_J(K)). \end{aligned} \tag{5.6}$$

5.2.3 Markov Decision Process

If the secondary user stays in the same channel for too long, he/she will eventually be found by an attacker, as it can be seen from (5.5) and (5.6) that $p(K+1|K,s) = 0$ if $K > M/m - 1$. Therefore, we can limit the state S to a finite set $\{P, J, 1, 2, 3, \ldots, \bar{K}\}$, where $\bar{K} = \lfloor M/m - 1 \rfloor$ and the floor function $\lfloor x \rfloor$ returns the largest integer not greater than x.

An MDP consists of four important components, namely, a finite set of states, a finite set of actions, transition probabilities, and immediate payoffs. As we have already specified all of them, the defense problem is modeled by an MDP, and the optimal defense strategy can be obtained by solving the MDP.

For an MDP, a *policy* is defined as a mapping from a state to an action, i.e., $\pi : S_n \to a_n$. In other words, a policy π specifies an action $\pi(S)$ to take whenever the user is in state S. Among all possible policies, the optimal policy is the one that maximizes the expected total discounted payoffs. The value of a state S is defined as the highest expected payoff given the MDP starts from state S, i.e.,

$$V^*(S) = \max_{\pi} E\left(\sum_{n=1}^{\infty} \delta^n U(n) \middle| S_1 = S \right), \tag{5.7}$$

where the optimal policy is the optimizer π^*. It is also the optimal defense strategy that the secondary user should adopt since it maximizes the expected payoff. For example, when the secondary user observes the state is S, the action $\pi^*(S)$ should be taken in order to maximize the payoff.

An important but straightforward idea is that after a first move the remaining part of an optimal policy should still be optimal. Hence, the first move should maximize the sum of immediate payoff and expected payoff conditioned on the current action. This is the well-known Bellman equation [69],

$$
\begin{aligned}
Q(S,a) &= U(S,a) + \delta \sum_{S'} p(S'|S,a) V^*(S'), \\
V^*(S) &= \max_{a \in \{h,s\}} Q(S,a).
\end{aligned}
\tag{5.8}
$$

The values of states can be calculated from a standard procedure called *value iteration* [69], which updates the value of every state iteratively according to the Bellman equation, and this iteration is guaranteed to converge to the true value of states. The specific algorithm is summarized in Table 5.1. After obtaining these values, the optimal policy $\pi^*(S)$ is the maximizer to the Bellman equation (5.8).

Table 5.1: Value iteration of the MDP.

Initialize $V(S)$ arbitrarily. Set a small ε as the stopping criterion.
For $n = 1, 2, 3, \dots$
For every state $S \in \{P, J, 1, 2, 3, \dots, \bar{K}\}$
$Q(S,a) = U(S,a) + \delta \sum_{S'} p(S'\|S,a) V_n(S'),\ a \in \{s,h\}$
$V_{n+1}(S) = \max\left(Q(S,h), Q(S,s)\right)$.
End For
If $\|V_{n+1}(S) - V_n(S)\| < \varepsilon$ for all states
The outer loop is terminated.
End if
End For
Return $V_n(S)$ as the value of states.

As seen from (5.3) and (5.4), the transition probabilities associated with action h are independent of the old state. Thanks to the special feature of the MDP, its solution has a simple structure stated in Proposition 10.

Proposition 10 *The optimal policy can be characterized by a single number* $K^* \in$

$\{0, 1, \ldots, \bar{K}\}$, *i.e.*,

$$a^* = \pi^*(S) = \begin{cases} s, & \text{if } S \le K^*; \\ h, & \text{otherwise.} \end{cases} \tag{5.9}$$

Proof: Using transition probabilities (5.3) (5.4) and the definition of $Q(S, a)$ in (5.8), it is easy to show that $Q(1, h) = Q(2, h) = \cdots = Q(\bar{K}, h) \triangleq Q$, and $Q(J, h) = Q - R - L$, $Q(P, h) = Q - R$. Since h is the only action for states J and P, we have $V^*(J) = Q(J, h)$ and $V^*(P) = Q(P, h)$.

According to (5.6) and (5.8), $Q(\bar{K}, s) - Q(\bar{K} - 1, s) = \delta(1 - \beta)(1 - f_J(\bar{K} - 1))(V^*(J) - V^*(\bar{K}))$. Notice that $V^*(\bar{K}) = \max(Q(\bar{K}, h), Q(\bar{K}, s)) \ge Q(\bar{K}, h) = Q > V^*(J)$, and all the other factors are positive. Hence, $Q(\bar{K}, s) < Q(\bar{K} - 1, s)$ and $V^*(\bar{K}) = \max(Q(\bar{K}, h), Q(\bar{K}, s)) \le \max(Q(\bar{K} - 1, h), Q(\bar{K} - 1, s)) = V^*(\bar{K} - 1)$.

Similarly, we can show $Q(\bar{K} - 1, s) - Q(\bar{K} - 2, s) = \delta(1 - \beta)[(f_J(\bar{K} - 1) - f_J(\bar{K} - 2))(V^*(J) - V^*(\bar{K} - 1)) + (1 - f_J(\bar{K} - 1))(V^*(\bar{K}) - V^*(\bar{K} - 1))] < 0$, and $V^*(\bar{K} - 1) \le V^*(\bar{K} - 2)$ follows. The process can go all the way up to $K = 1$, leading to a conclusion that $Q(K, s)$ is a strictly decreasing function of $K \in \{1, 2, \ldots, \bar{K}\}$.

Notice that the optimal action at state K is s if $Q(K, s) \ge Q(K, h)$, and h if $Q(K, s) < Q(K, h)$. Since $Q(K, s)$ is decreasing and $Q(K, h)$ is a constant Q, there must exist a $K^* \in \{1, 2, \ldots, \bar{K} - 1\}$ such that $Q(K^*, s) \ge Q > Q(K^* + 1, s)$ except two extreme cases. One is $Q(\bar{K}, s) \ge Q$ where $K^* = \bar{K}$, and the other is $Q(1, s) < Q$ where we can simply set $K^* = 0$ in (5.9). This concludes the proof. ■

Intuitively, since the probability of being jammed increases when the secondary user stays in the same channel for a longer time, K^* will be the critical state beyond which the damage overwhelms the hopping cost. If the secondary user stays in the same channel for a short period ($\leq K^*$ time slots), he/she should stay to exploit more; otherwise, he/she should proactively hop to another channel since the risk of being jammed becomes significant. The exact value of K^*, however, has to be solved using the approach in Table 5.1.

5.2.4 The Learning Process

The MDP-based optimal strategy requires perfect knowledge. However, in practice, the information is generally not directly available, since the secondary user cannot expect reliable information from adversaries. Both overestimating and underestimating the threat may result in inappropriate degrees of protection. In the following, we propose two learning schemes for the secondary user to learn from environment, the maximum likelihood estimation (MLE) and Q-learning [93].

For the MLE-based learning, the secondary user has to first go through a learning process to obtain estimates of the parameters, such as the number of attackers m. After the learning period, the secondary user gains knowledge of the environment, and updates the critical state K^* accordingly. During the learning period, the secondary user simply sets a value $\hat{K}^*$ as an initial guess of the optimal critical state K^*, and follows the strategy (5.9) with $\hat{K}^*$. This guess needs not to be accurate, as the goal is merely to observe transitions during the learning period that can be used for estimation of parameters.

With full history available including states and actions, the secondary user is able to count the occurrences of transitions given either action. For example, the notation $N^{(h)}_{S,S'}$ gives the total number of transitions from S to S' with action h taken, whereas $N^{(s)}_{S,S'}$ is the total number of transitions with action s taken. We define $K_L \triangleq \max\{K : N^{(s)}_{K,K+1} > 0\}$, $\mathbb{H} \triangleq \{P, J, K_L + 1\}$, and $\mathbb{S} \triangleq \{1, 2, \ldots, K_L\}$. Given the sequence of transitions in history, the likelihood that such a sequence has occurred can be written as a product over all feasible transition tuples $(S, a, S') \in \{P, J, 1, 2, 3, \ldots, K_L + 1\} \times \{s, h\} \times \{P, J, 1, 2, 3, \ldots, K_L + 1\}$,

$$\Lambda = \prod_{(S,a,S') \,:\, p(S'|S,a)>0} \left(p(S'|S, a)\right)^{N^{(a)}_{S,S'}}. \tag{5.10}$$

Moreover, if we define $\rho \triangleq m/M$ and relax it to any real number, Proposition 11 gives the MLE of the parameters β, γ, and ρ. After the learning period, the secondary user rounds $M \cdot \rho_{\mathrm{ML}}$ to the nearest integer as an estimate of m, and calculate the optimal strategy using the MDP approach.

Proposition 11 *Given $N^{(h)}_{S,S'}$, $S \in \mathbb{H}$ and $N^{(s)}_{S,S'}$, $S \in \mathbb{S}$ counted from history of transitions, the MLE of primary users' parameters are*

$$\beta_{ML} = \frac{\sum_{K\in\mathbb{S}} N^{(s)}_{K,P}}{\sum_{K\in\mathbb{S}} \left(N^{(s)}_{K,P} + N^{(s)}_{K,J} + N^{(s)}_{K,K+1}\right)}, \tag{5.11}$$

$$\gamma_{ML} = \frac{\sum_{S\in\mathbb{H}} N^{(h)}_{S,P}}{\sum_{S\in\mathbb{H}} \left(N^{(h)}_{S,P} + N^{(h)}_{S,J} + N^{(h)}_{S,1}\right)}, \tag{5.12}$$

and the MLE of attackers' parameters ρ_{ML} is the unique root within an interval $(0, 1/(K_L + 1))$ of the following $(K_L + 1)$-order polynomial of ρ,

$$\frac{1}{\rho}\left(\sum_{S\in\mathbb{H}} N^{(h)}_{S,J} + \sum_{K\in\mathbb{S}} N^{(s)}_{K,J}\right) = \sum_{K\in\mathbb{S}} \frac{N^{(s)}_{K,P}}{\frac{1}{K} - \rho} + \frac{N^{(s)}_{K_L,K_L+1}}{\frac{1}{K_L+1} - \rho}. \tag{5.13}$$

The outline of proof is as follows. First, we show that the likelihood of the observed sequence of transitions can be decoupled into a product of three terms, and each term only contains one unknown parameter. By taking derivative of their logarithms, we obtain the closed-form solution in the Proposition. Finally, we have to show that out of multiple roots of (5.13), there is a unique one in the feasible interval that guarantees a positive likelihood. Details can be found in [21].

An alternative approach is to learn the optimal policy without explicitly knowing the model, which is known as Q-learning in the reinforcement learning literature. The intuition behind Q-learning is to approximate the unknown transition probability in (5.8) by the empirical distribution of states that have been reached as the game unfolds. Specifically, (5.8) is replaced by an iterative process

$$\begin{aligned} Q_n(S,a) &= (1-\mu_n)Q_{n-1}(S,a) + \mu_n(U(S,a)+\delta V_n(S')), \\ V_{n+1}(S) &= \max_{a\in\{h,s\}} Q_n(S,a), \end{aligned} \tag{5.14}$$

where the Q-value of a state-action pair (S,a) is updated based on the observed new state S', the frequency of which represents the empirical distribution of the transition from state S with action a. μ_n is the learning rate decreasing in time, and we set

$$\mu_n = \frac{1}{1 + \text{number of updates for } Q(S,a)}, \tag{5.15}$$

which results in a proved convergence.

Proposition 12 *Q-learning converges to the optimal policy with probability 1, provided that each state-action pair is encountered infinitively, and the learning rate obeys* $0 \le \mu_n < 1$, $\sum_{n=1}^{+\infty} \mu_n = \infty$, *and* $\sum_{n=1}^{+\infty} \mu_n^2 < \infty$.

One may choose $a_n = \pi(S_n)$, but the problem is $\pi(S)$ during learning may not be the true optimal policy, and always following $a_n = \pi(S_n)$ may enhance the false impression and prevent the truth from being discovered. Thus, the secondary user should deviate from $\pi(S_n)$ with a small probability η to exploit the state-action pairs that have been rarely visited.

5.3 Power Allocation Anti-Jamming Games

In this section, we extend the anti-jamming game to the scenario where a secondary user is equipped with multiple radios and is able to access all the available channels simultaneously with a limited power budget. Each attacker is also assumed to be able to inject interference to all channels, and thus all attackers can be viewed as a single attacker whose power budget is the sum of individual budgets.

5.3.1 Game Reformulation

In this case, the defense strategy is not to hop between channels, but to randomly allocate power in different channels. Whether the attackers can successfully jam communications in one particular channel will depend on how much power the secondary user and attackers allocate on that channel. Therefore, we have to redefine the game to reflect the changes.

The secondary user still adopts the "listen-before-talk" rule, that is, sensing for spectrum opportunities at the beginning of a time slot. Recall that transmitters have power constraints. On finding M_0 available channels out of the M total channels, the secondary user allocates power p_k to the kth available channel such that $\sum_{k=1}^{M_0} p_k = p^B$. At the same time, the attacker injects i_k to the kth available channel such that $\sum_{k=1}^{M_0} i_k = i^B$. The power allocation vectors $\mathbf{p} = (p_1, p_2, \ldots, p_{M_0})$ and $\mathbf{i} = (i_1, i_2, \ldots, i_{M_0})$ are actions. If the received SINR exceeds the minimum requirement β, i.e.,

$$\frac{p_k}{i_k + \sigma_k^2} \geq \beta, \tag{5.16}$$

packets can be transmitted successfully on that channel. σ_k^2 is the noise variance of channel k, which we assume is the same for all channels, i.e., $\sigma_k^2 = \sigma^2$. Because each successful transmission yields a communication gain R, the secondary user's payoff is defined as the number of successful transmissions, i.e.,

$$U(\mathbf{p}, \mathbf{i}) = \sum_{k=1}^{M_0} \mathbf{1}\left(\frac{p_k}{i_k + \sigma^2} \geq \beta\right), \tag{5.17}$$

where $\mathbf{1}(\cdot)$ is the indicator function. Attackers' payoff is the opposite. In order to hide the allocation strategy from attackers, the secondary user has to randomize the power allocation, and the strategy is characterized by a probability distribution function $F(\mathbf{p})$. Similarly, attackers will employ a random strategy characterized by $H(\mathbf{i})$. The expected payoff is to average (5.17) over the distribution of $F(\mathbf{p})$ and $H(\mathbf{i})$, i.e., $\bar{U}(F(\mathbf{p}), H(\mathbf{i})) = \iint U(\mathbf{p}, \mathbf{i})\, \mathrm{d}F(\mathbf{p})\, \mathrm{d}H(\mathbf{i})$.

Different from the single-radio case, we do not need to consider the arms race in this multi-radio case. Assuming perfect knowledge, we are able to derive the Nash equilibrium of this game, which is the best response given the other player sticks to the equilibrium strategy. Furthermore, since it is a zero-sum game, the Nash equilibrium $(F^*(\mathbf{p}), H^*(\mathbf{i}))$ also provides the minimax strategy [13] such that $F^*(\mathbf{p})$ is a maximizer to $\min_H \bar{U}(F(\mathbf{p}), H(\mathbf{i}))$. This property is of great interest. If capable of learning the secondary user's strategy $F(\mathbf{p})$, attackers can always come up with a strategy $H(\mathbf{i})$ tailored to $F(\mathbf{p})$, which minimizes the secondary user's expected payoff and maximizes the damage. Therefore, the secondary user should choose the strategy $F^*(\mathbf{p})$ to maximize the worst-case expected payoff.

To simplify the game, we define $j_k = \beta(i_k + \sigma^2)$ with the constraint $\sum_{k=1}^{M_0} j_k = \beta(i^B + M_0\sigma^2) \triangleq j^B$. Then, the condition of a successful transmission becomes $p_k \geq j_k$. This game falls into the category of Colonel Blotto games where two opponents distribute limited resources over a number of battlefields with a payoff equal to the sum of outcomes from individual battlefields [94]. However, the difference is that j_k has to be lower bounded by $\beta\sigma^2$, since attackers only have control over the i_k part. In this new game, the attackers' strategy is also given by a joint distribution function, denoted by $G(\mathbf{j})$.

5.3.2 Nash Equilibrium

We first derive the necessary condition of the Nash equilibrium (NE) in terms of marginal distribution functions $F_1(p_1), F_2(p_2), \ldots, F_{M_0}(p_{M_0})$, $G_1(j_1), \ldots, G_{M_0}(j_{M_0})$. Notice that the probability of a successful transmission is $Pr(p_k \geq j_k) = G_k(p_k)$, and the payoff of the secondary user is $\sum_{k=1}^{M_0} G_k(p_k)$ when he/she fixes the power allocation as $(p_1, p_2, \ldots, p_{M_0})$. When the player employs a randomized strategy, the expected payoff becomes

$$\sum_{k=1}^{M_0} \int_0^{\infty} G_k(p_k) \mathrm{d}F_k(p_k), \tag{5.18}$$

and the necessary condition of the total power constraint becomes

$$p^B = E\left(\sum_{k=1}^{M_0} p_k\right) = \sum_{k=1}^{M_0} \int_0^{\infty} p_k \mathrm{d}F_k(p_k). \tag{5.19}$$

If we introduce a Lagrangian multiplier λ_P, the optimization problem of the secondary user can be formulated as

$$\max_{\{F_k(p_k)\}} \sum_{k=1}^{M_0} \int_0^{\infty} (G_k(p_k) - \lambda_P p_k)\, \mathrm{d}F_k(p_k) + \lambda_P p^B. \tag{5.20}$$

Similarly, we can derive the optimization problem for attackers who attempt to maximize $\sum_{k=1}^{M_0} \mathbf{1}(p_k < j_k)$. As shown later in Proposition 13, at the equilibrium the amount of power allocated in the kth channel p_k is a random variable with a discrete part at 0 and a continuous part elsewhere. Hence, the event $p_k = j_k$ happens with probability 0, and $Pr(p_k < j_k) = Pr(p_k \leq j_k) = F_k(j_k)$. Therefore, from the attackers' point of view, the optimization problem is

$$\max_{\{G_k(j_k)\}} \sum_{k=1}^{M_0} \int_{\beta\sigma^2}^{\infty} (F_k(j_k) - \lambda_J j_k)\, \mathrm{d}G_k(j_k) + \lambda_J j^B, \tag{5.21}$$

where λ_J is the Lagrangian multiplier for attackers.

For the secondary user, he/she can either decide not to access channel k (i.e., $p_k = 0$) or decide to access that channel with some power lower bounded by $\underline{p}_k$ and upper bounded by $\bar{p}_k$ (i.e., $p_k \in [\underline{p}_k, \bar{p}_k]$). Apparently, $\underline{p}_k \geq \beta\sigma^2$, because if p_k is chosen in the open interval $(0, \beta\sigma^2)$, the secondary user will always fail in that channel, and it is better not to allocate power at all. When the equilibrium strategy is a mixed strategy over the domain $0 \cup [\underline{p}_k, \bar{p}_k]$, according to game theory, the player must be indifferent among these values [13], namely, $G_k(p_k) - \lambda_P p_k = constant$ for $p \in 0 \cup [\underline{p}_k, \bar{p}_k]$. In particular, since $G_k(0) = 0$, we can further have

$$G_k(p_k) - \lambda_P p_k = 0, \text{ for } p_k \in 0 \cup [\underline{p}_k, \bar{p}_k]. \tag{5.22}$$

The similar argument can be applied to attackers who allocate power $j_k \in [\underline{j}_k, \bar{j}_k]$

and has to be indifferent among the values, namely,

$$F_k(j_k) - \lambda_J j_k = constant, \text{ for } j_k \in [\underline{j}_k, \bar{j}_k]. \tag{5.23}$$

Proposition 13 *For the NE strategy, bounds are determined as* $\bar{p}_k = \bar{j}_k = \min(\frac{1}{\lambda_P}, \frac{1}{\lambda_J})$, *and* $\underline{p}_k = \underline{j}_k = \beta\sigma^2$. *Moreover,* $Pr(j_k = \beta\sigma^2) = \lambda_P\beta\sigma^2$, *and* $Pr(p_k = \beta\sigma^2) = 0$*; the probability distribution function* $F_k(p_k)$ *is continuous in the range* $(\beta\sigma^2, \bar{p}_k]$*, and so is* $G_k(j_k)$.

Proof: According to the definition of the NE, no single player can be better off by deviating unilaterally from the NE strategy. In what follows, we give a proof mainly by contradiction.

From optimization problems (5.20) and (5.21), it is clear that $p_k \leq 1/\lambda_P$ and $j_k \leq 1/\lambda_J$ have to be satisfied to avoid negative payoffs. $\bar{p}_k = \bar{j}_k$ can be proved by contradiction. If $\bar{p}_k \neq \bar{j}_k$, say $\bar{p}_k < \bar{j}_k$, attackers are better off by moving $\bar{j}_k$ to $(\bar{p}_k + \bar{j}_k)/2$, as $F_k(\bar{j}_k) - \lambda_J\bar{j}_k = 1 - \lambda_J\bar{j}_k < 1 - \lambda_J(\bar{p}_k + \bar{j}_k)/2 = F_k\left((\bar{p}_k + \bar{j}_k)/2\right) - \lambda_J(\bar{p}_k + \bar{j}_k)/2$. The analysis is similar for the case $\bar{p}_k > \bar{j}_k$.

Next, we prove $\underline{p}_k = \underline{j}_k$ by contradiction. If $\underline{p}_k \neq \underline{j}_k$, say $\underline{p}_k < \underline{j}_k$, the secondary user is better off by moving $(\underline{p}_k + \underline{j}_k)/2$ to $\underline{p}_k$, since power can be saved without affecting the winning probability. The analysis is similar for the case $\underline{p}_k > \underline{j}_k$. According to (5.22), $Pr(j_k = \underline{j}_k) = G(\underline{j}_k) = \lambda_P\underline{j}_k$. Because $p_k \geq \underline{j}_k$ always holds for $p_k \in [\underline{p}_k, \bar{p}_k]$, by contradiction, if $\underline{j}_k > \beta\sigma^2$, attackers will be better off by moving $\underline{j}_k$ to $\beta\sigma^2$. Therefore, $\underline{p}_k = \underline{j}_k = \beta\sigma^2$, and $Pr(j_k = \beta\sigma^2) = \lambda_P\beta\sigma^2$.

Then, if $Pr(p_k = \beta\sigma^2) > 0$, attackers can change the probability mass from $\beta\sigma^2$ to $\beta\sigma^2 + \epsilon$ where ϵ is an arbitrary small number, and can increase the jamming probability by $\lambda_P \beta\sigma^2 \cdot Pr(p_k = \beta\sigma^2)$ with only negligible power increase. This cannot be an NE, and as a result, $Pr(p_k = \beta\sigma^2) = 0$.

Finally, we show that $F_k(p_k)$ cannot have discontinuous points in the interval $(\beta\sigma^2, \bar{p}_k]$. By contradiction, assume there is at least one discontinuous point, denoted by p^o, and thus $Pr(p_k = p^o) > 0$. Then, attackers can move the neighborhood $(p^o - \epsilon, p^o)$ to $(p^o, p^o + \epsilon)$ to increase the jamming probability by $Pr(p_k = p^o) \cdot Pr(j_k \in (p^o - \epsilon, p^o))$ with only negligible power increase when ϵ is an arbitrary small number. Similar arguments can be made to prove $G_k(j_k)$ cannot have discontinuous points in the interval $(\beta\sigma^2, \bar{j}_k]$ either. This concludes the proof. ■

Based on Proposition 13 and necessary conditions (5.22)(5.23), in Proposition 14, we derive the marginal distribution of the NE.

Proposition 14 *Under the condition $p^B \leq \beta i^B$, there exists a unique Nash equilibrium whose marginal distributions for the secondary user and attackers are given by*

$$F_k^*(p_k) = \begin{cases} 0, & p_k < 0, \\ 1 - \lambda_J/\lambda_P + \lambda_J \beta\sigma^2, & p_k \in [0, \beta\sigma^2), \\ 1 - \lambda_J/\lambda_P + \lambda_J p_k, & p_k \in [\beta\sigma^2, 1/\lambda_P], \end{cases} \tag{5.24}$$

and

$$H_k^*(i_k) = \begin{cases} 0, & i_k < 0, \\ \lambda_P \beta(\sigma^2 + i_k), & i_k \in [0, 1/(\beta\lambda_P) - \sigma^2], \end{cases} \tag{5.25}$$

where $\lambda_J = M_0 p^B / ((j^B)^2 - \beta^2 {M_0}^2 \sigma^4 + j^B \sqrt{(j^B)^2 - \beta^2 {M_0}^2 \sigma^4})$ and $\lambda_P = M_0/(j^B + \sqrt{(j^B)^2 - \beta^2 {M_0}^2 \sigma^4})$.

Proof: Define $\bar{p}_k = \bar{j}_k = \min(1/\lambda_P, 1/\lambda_J) \triangleq \bar{p}$ which is independent on k. According to Proposition 13, $F_k(p_k)$ is continuous in the interval $[\beta\sigma^2, \bar{p}]$, and therefore, we can take the derivative of (5.23)

$$\mathrm{d}F_k(x) = \lambda_J \mathrm{d}x,\ x \in [\beta\sigma^2, \bar{p}], \tag{5.26}$$

and substitute it to the power constraint (5.19),

$$p^B = \sum_{k=1}^{M_0} \int_0^{\bar{p}} p_k \mathrm{d}F_k(p_k) = M_0 \int_{\beta\sigma^2}^{\bar{p}} \lambda_J p_k \mathrm{d}p_k = \frac{M_0}{2} \lambda_J (\bar{p}^2 - \beta^2\sigma^4). \tag{5.27}$$

Similar derivation can be applied to attackers' power constraint except that $G_k(j_k)$ is discontinuous at $j_k = \beta\sigma^2$,

$$j^B = M_0 \left(\beta\sigma^2(\lambda_P \beta\sigma^2) + \frac{1}{2}\lambda_P(\bar{p}^2 - \beta^2\sigma^4) \right). \tag{5.28}$$

If $1/\lambda_P \leq 1/\lambda_J$, then $\bar{p} = 1/\lambda_P$ and (5.28) becomes a quadratic equation of the variable $1/\lambda_P$, two roots of which are given by

$$\left(\frac{1}{\lambda_P} \right)_{1,2} = \frac{1}{M_0} \left(j^B \pm \sqrt{(j^B)^2 - \beta^2 {M_0}^2 \sigma^4} \right). \tag{5.29}$$

However, only the root with the plus sign is valid since the other root is smaller than $\beta\sigma^2$. Then, $1/\lambda_J$ can be solved from (5.27) accordingly,

$$\frac{1}{\lambda_J} = \frac{(j^B)^2 - \beta^2 {M_0}^2 \sigma^4 + j^B \sqrt{(j^B)^2 - \beta^2 {M_0}^2 \sigma^4}}{M_0 p^B}. \tag{5.30}$$

When the condition $p^B \leq \beta i^B$ holds, it is easy to verify that $1/\lambda_P \leq 1/\lambda_J$.

The pair of Lagrangian multipliers have been uniquely determined by (5.29) and (5.30). Since at least one mixed-strategy NE exists in a game [13], we can safely draw a conclusion that this characterizes the unique NE in the anti-jamming game. With parameters known, it is straightforward to write down the marginal distribution. For instance, according to (5.22),

$$G_k(j_k) = \begin{cases} 0, & j_k < \beta\sigma^2, \\ \lambda_P j_k, & j_k \in [\beta\sigma^2, 1/\lambda_P], \end{cases} \tag{5.31}$$

which can be further mapped back to the original domain $H_k(i_k)$ (5.25) using $j_k = \beta(i_k + \sigma^2)$. Similarly, marginal distribution $F_k(p_k)$ given by (5.24) can be derived from (5.26). ■

So far, we have known the existence of the NE and the formula of marginal distribution functions; however, it still remains a question to find the specific NE strategy determined by the joint probability distribution function. We have followed the procedure in [94] to construct one kind of joint distribution that matches desired marginal distribution and meets the total power restriction. With this procedure, we can finally characterize the NE strategy for the anti-jamming game.

5.4 Simulation Studies

In this section, we present some simulation results to evaluate the proposed defense strategies against jamming attacks. We first consider the scenario with the single-radio secondary user, whose defense strategy is proactive hopping among multiple channels. In the simulation, we fix a set of parameters to gain some insight of the defense strategy. The parameters are as follows: the communication gain $R = 5$, the hopping cost $C = 1$, the total number of channels $M = 60$, the discount factor $\delta = 0.95$, and the primary users' access pattern $\beta = 0.01, \gamma = 0.1$.

We show the critical state K^* obtained from the value iteration of the MDP,

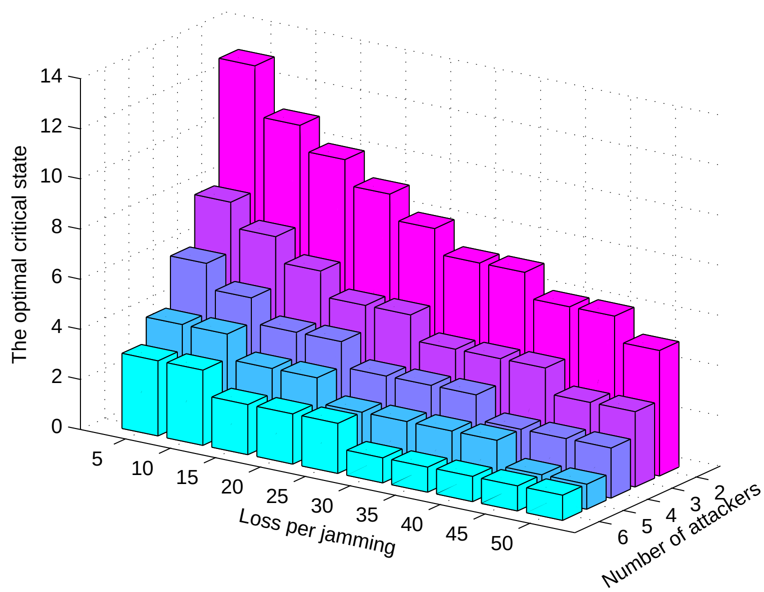


Figure 5.3: The critical state K^* with different attack strengths and damages.

when we change the value of damage L and the number of attackers m. We assume that the secondary user has perfect knowledge of the environment. As shown in Fig. 5.3, if the damage from each jamming L is fixed, say $L = 10$ for example, the critical state K^* decreases from 11 to 3 when the number of attackers m increases from 2 to 6. Similarly, when the number of attackers m is fixed, the critical state K^* also decreases as the value of L increases. The reason is that the secondary user should proactively hop more frequently (i.e., K^* is smaller) to avoid being jammed when the threat from attackers are more stronger (more attackers and/or more severe damage if jammed).

In Fig. 5.4, we present the damage caused by attackers when the number of attackers varies, in terms of percentages of payoff loss compared with a network without malicious attackers. The damage L is set to 20 in this simulation. Besides the optimal strategy (5.9), another two naive strategies are simulated and compared. We first consider the case where attackers stick to the "random scanning" attack strategy, against which the defense strategy has been derived using the MDP approach. If the "always hopping" strategy is employed, the secondary user will hop every time slot; if the "staying whenever possible" strategy is adopted, the secondary user will always stay in the channel unless the primary user reclaims the channel or the channel is jammed by attackers. When the number of attackers is small, it is better to stay than to hop, but when the number of attackers is large, hopping outperforms staying. The optimal strategy, however, beats both naive strategies in the entire range, as shown by the smaller decrease in payoffs in the figure.

Moreover, we want to show how the defense strategy performs if attackers adopt other strategies. One possible strategy for attackers is to randomly select m bands to detect but the selection is independent from slot to slot. This differs from the random scanning strategy in which the selection of channels depends on the past, and we refer to this strategy as "random jamming". In Fig. 5.4, the percentage of payoff decrease is also provided for the three defense strategies and the "random jamming" attack strategy. It can be seen that for all three defense strategies considered, attackers will prefer the random scanning strategy which results in more damage to the secondary user, and the difference becomes significant when the secondary user tends to remain in the same band. From the secondary user's perspective, although the "staying whenever possible" strategy slightly outperforms the MDP strategy when attackers adopt the random jamming strategy, the MDP

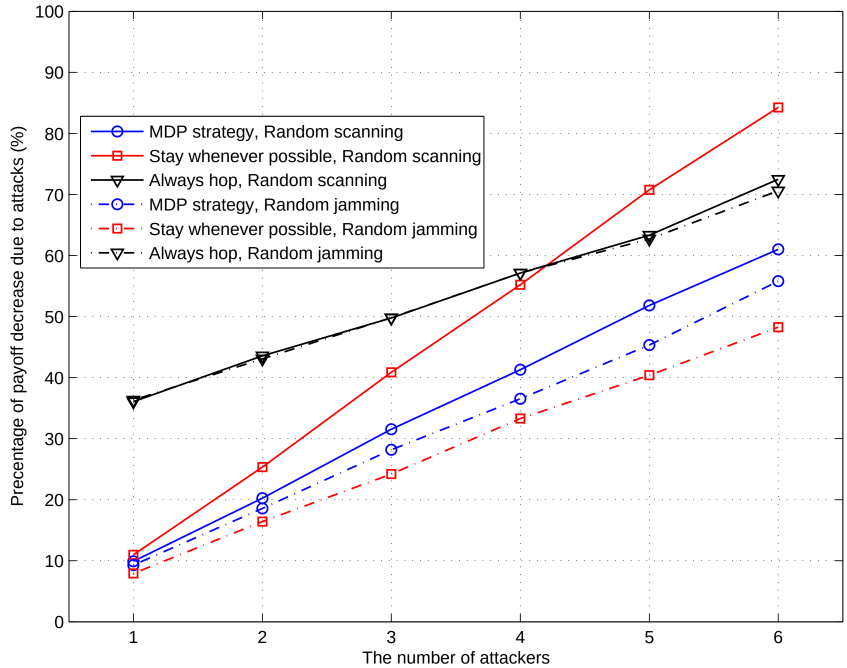


Figure 5.4: The percentage of payoff decrease due to jamming attacks with different numbers of attackers.

strategy should be used because it suffers from smaller worst-case damage.

We evaluate the MLE learning algorithm by showing the variance of estimation errors $M\rho_{\mathrm{ML}} - m$ from 100 independent simulation runs with certain lengths of learning period. The learning curves are plotted in the upper figure of Fig. 5.5. As the learning period lengthens, the variance decreases which means a more accurate estimate. The accuracy degrades slightly when there are more attackers in the network. Recall that the last step of learning is rounding $M\rho_{\mathrm{ML}}$ to the nearest integer, which could further reduce the estimation errors. In the lower figure of Fig. 5.5, we show the percentage of trials that the estimated number of attackers is exactly the true value. From the figure, we can see the percentage of exact estimation

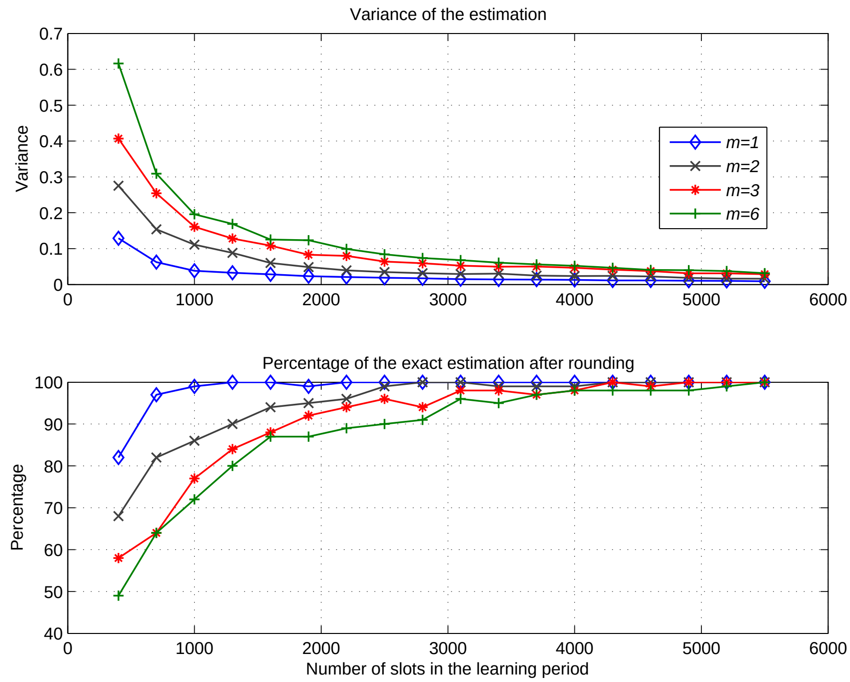


Figure 5.5: Learning curves of the MLE learning process.

grows fast and approaches to one hundred percent with increasing learning periods.

The anti-jamming game with the multi-radio secondary user who employs randomized power allocation strategy is also presented. In order to show that for the secondary user, the NE strategy is a minimax strategy such that the worst possible damage is minimized, we have run simulations with two other possible strategies considered: one decides the number of channels to access according to the NE strategy but allocates power equally, and the other allocates power based on a naive assumption that the jammer would inject equal interference to each channel. They are referred to as "NE-referred equal power allocation" and "naive power allocation", respectively. Fig. 5.6 provides the average number of channels that meet the SINR requirement when the secondary user adopts these strategies.

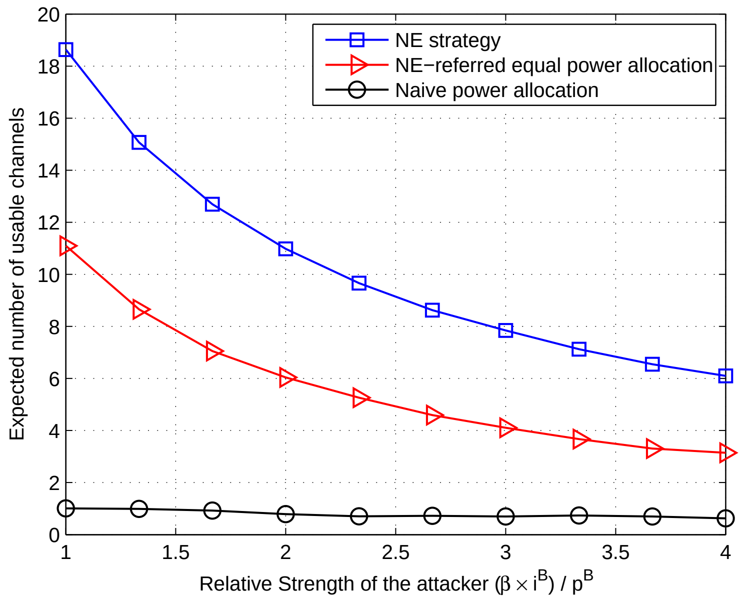


Figure 5.6: The average number of channels that meet the SINR requirement when different strategies are adopted by the secondary user.

When attackers are more powerful with a higher interference budget i^B, fewer usable channels can be expected for all three strategies. However, it is clear that the NE strategy performs much better than the other two strategies, and the secondary user has to choose it as the optimal power allocation strategy against malicious jamming attacks.

Chapter 6

An Information Secrecy Game in Cognitive Radio Networks

In the previous chapter, we discussed one particular threat from malicious users — the jamming attack, and developed a game-theoretic framework for jamming mitigation. As there are various kinds of attacks, in this chapter, we consider one primary-user-oriented attack — a passive but *intelligent* eavesdropper [95] who knows all channel state information (CSI) and codebooks. This malicious attacker eavesdrops upon the communications of primary users and attempts to decode some confidential messages.

In face of security threats, primary users may seek help from trustworthy secondary users, if such cooperation could potentially improve the secrecy level; in return, secondary users are granted spectrum opportunities for their own transmission. In order to know the maximal data rate that can be adopted by primary users without leaking any confidential information to the eavesdropper, we will investigate the information theoretic secrecy [96] in this cooperative cognitive radio network with an eavesdropper.

The concept of information theoretic secrecy dates back to Wyner's seminal paper [96]. In that work, the secrecy capacity of a wire-tap channel was studied, where a single source-destination communication was eavesdropped on via a degraded channel, that is, when the eavesdropper observed a degraded version of the signal received by the intended receiver. Later, this formulation was generalized to non-degraded broadcast channels with confidential information in [97], and Gaussian wire-tap channels were completely understood in [98]. Assume the transmitter encoded a confidential message w into a codeword x^n for broadcasting, and the intended receiver and the eavesdropper received noisy versions y^n and z^n, respectively. The level of ignorance that the eavesdropper had with respect to w given observation z^n, i.e., the conditional entropy $\frac{1}{n}h(w|z^n)$, was defined as the *equivocation rate*. When the equivocation rate was (asymptotically) equal to the information rate of the message w, the eavesdropper hardly knew anything about the message, and this was known as *perfect secrecy*. Just like the definition of channel capacity, a rate was *achievable* if there existed a coding scheme guaranteeing an arbitrarily small error probability for sufficiently long codewords, and the *secrecy capacity* was the maximum achievable rate with perfect secrecy. For Gaussian wire-tap channels, the secrecy capacity was the difference of mutual information of two channels, i.e., $C_S = \max\{I(X;Y) - I(X;Z), 0\}$, and stochastic encoding could achieve perfect secrecy [98].

Building on these fundamental ideas, information theoretic secrecy has gained a renewed research interest in recent years, thanks to fast developing wireless communications technologies. In this chapter, we study the information theoretic secrecy in a cognitive radio network. We model and analyze the achievable secrecy for a primary user, when secondary users potentially help to defeat eavesdropping while acquiring spectrum opportunities. Moreover, we propose a game-theoretic framework to understand how primary and secondary users optimize their transmission power for higher data rates, and discuss the Nash equilibrium for this information secrecy game. Contributions are summarized as follows.

First, this work suggests a new cooperative paradigm for cognitive radio networks, where cooperative simultaneous transmissions yield mutual benefits in the presence of an eavesdropper. In traditional opportunistic spectrum access, primary users in general do not benefit from opening up the spectrum, and sometimes their performance may degrade due to occasional collisions caused by secondary users' imperfect spectrum sensing. Spectrum trading mechanisms do award primary users monetary profits, but primary users have to give up short-term spectrum rights. However, when information secrecy is a concern, primary users may benefit from simultaneous transmissions of secondary users who need spectrum opportunities. This lays the foundation of incentives to cooperate.

Second, the primary user's secrecy is analyzed using the information theoretic approach. Information theory has been applied to study cognitive radio networks, for example, see [99] and references therein. Our work extends [95] to the cognitive radio network scenario where secondary users serve as the helper; however, different from [95] in which the helper simply transmits interfering coded signals bearing no useful information, in our work, secondary users do transmit meaningful messages for their receivers to decode.

Third, we describe a procedure of cooperation where the primary user has the upper hand, and model the interaction between primary users and secondary users as a Stackelberg game. In the proposed game, the players choose power levels to maximize their payoffs, and we further show that payoff functions are piece-wise

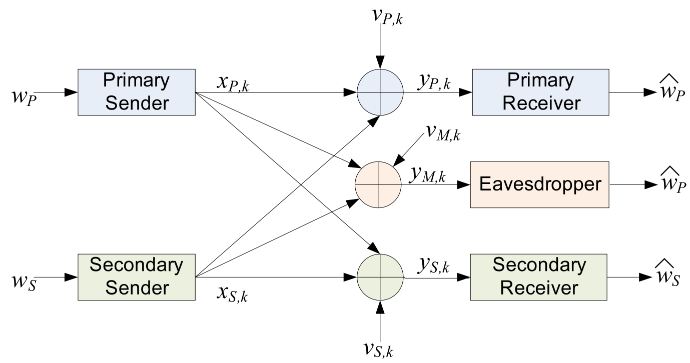


Figure 6.1: The model of a cognitive radio network with an eavesdropper.

defined so that the equilibrium can be easily found through a piece-by-piece search.

6.1 System Models

In this chapter, we consider a cognitive radio network consisting of a primary user, a trustworthy secondary user, and an eavesdropping malicious user who attempts to decode the primary user's message, as shown in Fig. 6.1. The primary user P wants to transmit some confidential messages from the transmitter to the receiver. The secondary user S also wants to transmit some messages from the transmitter to the receiver, but since he/she does not own the spectrum band, the transmission has to be approved by P when P is active. The malicious user M, attempting to decode P's message, is a passive eavesdropper with only a receiver. We further assume the malicious user is intelligent, in the sense that M knows P's and S's codebooks and all the CSI.

When P and S simultaneously transmit signals, denoted by $x_{P,k}$ and $x_{S,k}$ at time k, their receivers receives the superposition of signals from two transmitters,

$$\begin{aligned} y_{P,k} &= h_P x_{P,k} + h_{SP} x_{S,k} + v_{P,k}, \\ y_{S,k} &= h_S x_{S,k} + h_{PS} x_{P,k} + v_{S,k}. \end{aligned} \tag{6.1}$$

This can be viewed essentially as an interference channel [100], where h_P (or h_S) is the direct channel gain from P's (or S's) transmitter to the intended receiver, h_{SP} is the cross channel gain from S's transmitter to P's receiver, h_{PS} is from P's transmitter to S's receiver, and $v_{P,k}$ (or $v_{S,k}$) is the additive white Gaussian noise at P's (or S's) receiver. Similarly, the malicious user receives

$$y_{M,k} = h_{PM} x_{P,k} + h_{SM} x_{S,k} + v_{M,k}, \tag{6.2}$$

where h_{PM} (or h_{SM}) is the channel gain from P's (or S's) transmitter to the eavesdropping receiver, and $v_{M,k}$ is the Gaussian noise, too. For convenience, we assume all noises have unit variances, i.e., $v_{P,k}, v_{S,k}, v_{M,k} \sim \mathcal{N}(0,1)$. In addition, we define $g_P = |h_P|^2$, $g_S = |h_S|^2$, $g_{PS} = |h_{PS}|^2$, $g_{SP} = |h_{SP}|^2$, $g_{PM} = |h_{PM}|^2$, and $g_{SM} = |h_{SM}|^2$.

The primary user encodes a confidential message $w_P \in \mathcal{W}_P$ into a n-length block codeword $x_P^n = (x_{P,1}, x_{P,2}, \ldots, x_{P,n})$ with a rate Q_P, and the secondary user encodes a message $w_S \in \mathcal{W}_S$ (w_S is independent of w_P) into $x_S^n = (x_{S,1}, x_{S,2}, \ldots, x_{S,n})$ with a rate R_S. The size of codebook $\mathcal{W}_P$ is 2^{nQ_P}, and the size of $\mathcal{W}_S$ is 2^{nR_S}. Both transmitters are power constrained, i.e.,

$$p_P = \frac{1}{n}\sum_{k=1}^{n} |x_{P,k}|^2 \le p_P^M,\ p_S = \frac{1}{n}\sum_{k=1}^{n} |x_{S,k}|^2 \le p_S^M. \tag{6.3}$$

The primary user tries to recover w_P from observation, and the secondary user tries to recover w_S; an error is declared if recovered messages differ from original messages, $\hat{w}_P \neq w_P$ or $\hat{w}_S \neq w_S$. A joint encoding and decoding scheme of rate pair (Q_P, R_S) is desired such that Q_P can be made arbitrarily close to the equivocation rate $\frac{1}{n}h(w_P|y_M^n)$ and the average error probability can be made arbitrarily small, as long as n is sufficiently large. The achievable rate pair (Q_P, R_S) depends on power levels p_P and p_S.

When the secondary user is absent, the scenario reduces to the classical Gaussian wire-tap channel [98], the secrecy capacity of which is known as

$$C_P(p_P^M) = \left(\gamma(g_P p_P^M) - \gamma(g_{PM} p_P^M)\right)_+ , \tag{6.4}$$

where $\gamma(a) \triangleq \frac{1}{2}\log(1+a)$ and $(a)_+ \triangleq \max\{a, 0\}$. Note that the secrecy capacity is positive only if the eavesdropping channel has poorer quality, i.e., $g_{PM} < g_P$. With the help of a secondary user, the primary user may have a higher secrecy rate, which provides the incentive to share the spectrum band with the secondary user. The secondary user, on the other hand, is willing to join in cooperation because he/she needs such a spectrum opportunity to transmit information. This lays the incentive foundation of cooperation.

The potential cooperation can be established in the following procedure. The primary user first announces the power level p_P, and the secondary user responds by announcing his/her transmit power level p_S. Since the secrecy rate $C_P(p_P^M)$ is guaranteed without the secondary user's help, the primary user agrees to cooperate only when a higher secrecy rate is achievable. In this case, both users exchange necessary information (e.g., codebooks) and begin cooperative transmissions. Otherwise, the primary user rejects cooperation, and the secondary user is forbidden to use the spectrum band.

Since both users want to maximize rates of data transmission but the primary user has secrecy concerns, the primary user aims at maximizing the information secrecy rate Q_P and the secondary user aims at maximizing merely the information rate R_S. Moreover, because both users are able to manipulate transmit power levels for higher payoffs, this scenario forms a game where P and S are players, $p_P \in [0, p_P^M]$ and $p_S \in [0, p_S^M]$ are their actions, and achievable rates are their payoffs which depend on actions. We call it an *information secrecy game*, and will analyze it later.

6.2 Optimal Achievable Rates under Fixed Power

In this section, we derive the achievable rate pair (Q_P, R_S) for fixed power levels (p_P, p_S). We first describe the non-secrecy achievable rate region, and then show that the achievable secrecy rate is the difference between Pareto frontiers of two rate regions. Dividing the whole problem into four cases based on relative channel strengths, we further derive the specific expression for the optimal rate pair for each case under various conditions.

6.2.1 Pareto Frontiers of the Achievable Rate Region

We first consider the interference channel without secrecy concerns. Note that the primary user can transmit with a higher rate R_P because the secrecy is not taken into account for the moment. The primary user receives the superposition of two transmitted signals, and is only interested in recovering his/her own messages. Because the primary user and the secondary user cooperate with each other and share their codebooks, the primary user can apply a joint decoding to obtain both users' messages, and then simply ignores the secondary user's message. This constitutes a multiple-access channel (MAC) [100], whose capacity region is

$$\Re_P^{[\mathrm{MAC}]} = \left\{ (R_P, R_S) \left| \begin{array}{c} 0 \le R_P \le \gamma(g_P p_P); \\ 0 \le R_S \le \gamma(g_{SP} p_S); \\ R_P + R_S \le \gamma_P. \end{array} \right. \right\}, \tag{6.5}$$

where $\gamma_P \triangleq \gamma(g_P p_P + g_{SP} p_S)$. When a rate R_S is too high to decode, the primary user can still attempt to decode w_P by treating the secondary user's signal as noise. The achievable rate region for this separate decoding (SD) is

$$\Re_P^{[\mathrm{SD}]} = \left\{ (R_P, R_S) \left| \begin{array}{c} 0 \le R_P \le \gamma(\frac{g_P p_P}{1+g_{SP} p_S}); \\ R_S > \gamma(g_{SP} p_S). \end{array} \right. \right\}. \tag{6.6}$$

In sum, as long as the rate pair falls into either region, the primary user is able to recover the message of interest.

Similar arguments apply to the secondary user, and the two regions are written as

$$\Re_S^{[\mathrm{MAC}]} = \left\{ (R_P, R_S) \left| \begin{array}{c} 0 \le R_P \le \gamma(g_{PS} p_P); \\ 0 \le R_S \le \gamma(g_S p_S); \\ R_P + R_S \le \gamma_S. \end{array} \right. \right\}, \tag{6.7}$$

with $\gamma_S \triangleq \gamma(g_{PS} p_P + g_S p_S)$, and

$$\Re_S^{[\mathrm{SD}]} = \left\{ (R_P, R_S) \left| \begin{array}{c} R_P > \gamma(g_{PS} p_P); \\ 0 \le R_S \le \gamma(\frac{g_S p_S}{1+g_{PS} p_P}). \end{array} \right. \right\}. \tag{6.8}$$

Therefore, for any rate pair (R_P, R_S) inside the region

$$\Re^{[\mathrm{COOP}]} = \{\Re_P^{[\mathrm{MAC}]} \cup \Re_P^{[\mathrm{SD}]}\} \cap \{\Re_S^{[\mathrm{MAC}]} \cup \Re_S^{[\mathrm{SD}]}\}, \tag{6.9}$$

both users are able to recover their own messages by either joint decoding or separate decoding.

It is worth pointing out that (6.9) is not always the capacity of the interference channel, but (6.9) can be achievable by simple encoding and decoding operations. A straightforward enlargement of a non-convex rate region to its convex closure can be done by time sharing, but we have prove in [22] that time sharing will not help when secrecy is considered. Going beyond time sharing requires much more sophisticated coding methods, and hence we will focus on the principal achievable region (6.9).

From the eavesdropper's point of view, who is only interested in the primary user's message, the decodable rate pair also has to fall into either the MAC region,

$$\Re_M^{[\mathrm{MAC}]} = \left\{ (R_P, R_S) \left| \begin{array}{c} 0 \le R_P < \gamma(g_{PM} p_P); \\ 0 \le R_S < \gamma(g_{SM} p_S); \\ R_P + R_S < \gamma_M. \end{array} \right. \right\}, \tag{6.10}$$

where $\gamma_M \triangleq \gamma(g_{PM} p_P + g_{SM} p_S)$, or the separate decoding region,

$$\Re_M^{[\mathrm{SD}]} = \left\{ (R_P, R_S) \left| \begin{array}{c} 0 \le R_P < \gamma(\frac{g_{PM} p_P}{1+g_{SM} p_S}); \\ R_S > \gamma(g_{SM} p_S). \end{array} \right. \right\}. \tag{6.11}$$

In other words, correctly decoding messages with a rate pair outside the two regions is beyond the eavesdropper's capability.

Following [95], Proposition 15 provides a pair of achievable rates using stochastic encoding. Informally speaking, the primary user splits the total rate R_P into two parts, secret information Q_P and dummy information R_{PM}. The eavesdropper can only decode the dummy information at best. Details can be found in [22].

Proposition 15 *The rate pair* (Q_P, R_S) *is achievable if there exist rates* $R_P > R_{PM} > 0$ *such that*

$$\begin{cases} Q_P = R_P - R_{PM}, \\ (R_P, R_S) \in \Re^{[COOP]}, \\ (R_{PM}, R_S) \notin \{\Re_M^{[MAC]} \cup \Re_M^{[SD]}\}. \end{cases} \tag{6.12}$$

Note that the achievable rate pairs given by Proposition 15 are not unique in general, and we need to find the "optimal" one from all candidates. Because the primary user has higher priority than the secondary user, it is reasonable to satisfy the primary user first. Denote the set of all achievable rate pairs satisfying constraints (6.12) as $\Re^{[\mathrm{SEC}]}$, and the optimal secrecy rate of the primary user can be found as

$$Q_P^\star = \max\{Q_P \,\big|(Q_P, R_S) \in \Re^{[\mathrm{SEC}]}\}. \tag{6.13}$$

Given $Q_P^\star$ for the primary user, the secondary user achieves the rate

$$R_S^\star = \max\{R_S \,\big|(Q_P^\star, R_S) \in \Re^{[\mathrm{SEC}]}\}. \tag{6.14}$$

Given a rate R_S, maximizing Q_P means maximizing the difference between R_P and R_{PM} ($R_P > R_{PM}$) according to (6.12). It requires moving R_P upwards to the Pareto frontier of the region $\Re^{[\mathrm{COOP}]}$ and moving R_{PM} downwards to approach the frontier of $\{\Re_M^{[\mathrm{MAC}]} \cup \Re_M^{[\mathrm{SD}]}\}$. As a result, when the rate region is plotted in an R_P–R_S plane (R_S is the x-axis), $Q_P^\star$ can be viewed as the maximum vertical difference between these two frontiers, i.e., $Q_P^\star = \max_{R_S} Q_P(R_S)$, and

$$Q_P(R_S) = \left(f_C(R_S) - f_M(R_S)\right)_+, \tag{6.15}$$

where $f_M(R_S)$ denotes the frontier of $\{\Re_M^{[\mathrm{MAC}]} \cup \Re_M^{[\mathrm{SD}]}\}$, and $f_C(R_S)$ denotes the frontier of $\Re^{[\mathrm{COOP}]}$.

It is easy to characterize $f_M(R_S)$ as a function of R_S,

$$f_M(R_S) = \begin{cases} \gamma(g_{PM}p_P), \text{ if } 0 \le R_S < \gamma(\frac{g_{SM}p_S}{1+g_{PM}p_P}); \\ \gamma_M - R_S, \text{ if } \gamma(\frac{g_{SM}p_S}{1+g_{PM}p_P}) \le R_S < \gamma(g_{SM}p_S); \\ \gamma(\frac{g_{PM}p_P}{1+g_{SM}p_S}), \text{if } R_S \ge \gamma(g_{SM}p_S), \end{cases} \tag{6.16}$$

which is a linear function with $f_M'(R_S) = -1$ in the central segment, and keeps constant elsewhere. We use $f'(\cdot)$ to denote the right derivative of $f(\cdot)$ throughout the chapter. Similarly, the frontier of $\{\Re_P^{[\mathrm{MAC}]} \cup \Re_P^{[\mathrm{SD}]}\}$ is

$$f_P(R_S) = \begin{cases} \gamma(g_P p_P), \text{ if } 0 \le R_S < \gamma(\frac{g_{SP}p_S}{1+g_P p_P}); \\ \gamma_P - R_S, \text{ if } \gamma(\frac{g_{SP}p_S}{1+g_P p_P}) \le R_S < \gamma(g_{SP}p_S); \\ \gamma(\frac{g_P p_P}{1+g_{SP}p_S}), \text{if } R_S \ge \gamma(g_{SP}p_S), \end{cases} \tag{6.17}$$

and the frontier of $\{\Re_S^{[\mathrm{MAC}]} \cup \Re_S^{[\mathrm{SD}]}\}$ is

$$f_S(R_S) = \begin{cases} +\infty, \text{ if } 0 \le R_S \le \gamma(\frac{g_S p_S}{1+g_{PS}p_P}); \\ \gamma_S - R_S, \text{if } \gamma(\frac{g_S p_S}{1+g_{PS}p_P}) < R_S \le \gamma(g_S p_S); \\ 0, \quad \text{if } R_S > \gamma(g_S p_S). \end{cases} \tag{6.18}$$

Since $\Re^{[\mathrm{COOP}]}$ is the intersection of the two regions, $f_C(R_S)$ equals $\min(f_P(R_S), f_S(R_S))$, and its domain can be limited to $[0, \gamma(g_S p_S)]$ because $f_C(R_S) = 0$ when $R_S > \gamma(g_S p_S)$. It is easy to see that $f_C(R_S)$ is a non-increasing function with $f_C'(R_S) =$

0 or -1 except discontinuous points; however, its specific form depends heavily on the channel conditions. The results in [22] are summarized in Table 6.1, where there are four cases divided by channel conditions, and the closed-form frontiers are also provided. The segments that may be missing under certain conditions are marked by "if*". For all cases, $f_C(R_S)$ is a non-increasing function of R_S, and $f_C(R_S)$ is continuous within the interval $[0, \gamma(g_S p_S)]$ except a discontinuous point at $R_S = \gamma(\frac{g_S p_S}{1+g_{PS} p_P})$ in Case B and possibly Case D (when $p_S < (g_P/g_{PS} - 1)/g_{SP}$ or $p_S < p_P(g_P - g_{PS})/(g_S - g_{SP})$).

Table 6.1: Different cases and corresponding closed-form frontiers.

Case	Condition	Interpretation	Closed-form frontier $f_C(R_S)$
A	$g_P \le g_{PS}$ $g_S \le g_{SP}$	Strong interference	$\begin{cases} \gamma(g_P p_P), & \text{if } R_S \le \min(\gamma_P, \gamma_S) - \gamma(g_P p_P); \\ \min(\gamma_P, \gamma_S) - R_S, & \text{if* } R_S > \min(\gamma_P, \gamma_S) - \gamma(g_P p_P). \end{cases}$
B	$g_P > g_{PS}$ $g_S \le g_{SP}$	P is in the better position	$\begin{cases} \gamma(g_P p_P), & \text{if } R_S \le \min(\gamma(\frac{g_{SP} p_S}{1+g_P p_P}), \gamma(\frac{g_S p_S}{1+g_{PS} p_P})); \\ \gamma_P - R_S, & \text{if* } \gamma(\frac{g_{SP} p_S}{1+g_P p_P}) < R_S \le \gamma(\frac{g_S p_S}{1+g_{PS} p_P}); \\ \gamma_S - R_S, & \text{if } R_S > \gamma(\frac{g_S p_S}{1+g_{PS} p_P}). \end{cases}$
C	$g_P \le g_{PS}$ $g_S > g_{SP}$	S is in the better position	$\begin{cases} \gamma(g_P p_P), & \text{if } R_S < \gamma(\frac{g_{SP} p_S}{1+g_P p_P}); \\ \gamma_P - R_S, & \text{if } \gamma(\frac{g_{SP} p_S}{1+g_P p_P}) \le R_S < \gamma(g_{SP} p_S); \\ \gamma(\frac{g_P p_P}{1+g_{SP} p_S}), & \text{if } \gamma(g_{SP} p_S) \le R_S \le \gamma_S - \gamma(\frac{g_P p_P}{1+g_{SP} p_S}); \\ \gamma_S - R_S, & \text{if* } R_S > \gamma_S - \gamma(\frac{g_P p_P}{1+g_{SP} p_S}). \end{cases}$
D	$g_P > g_{PS}$ $g_S > g_{SP}$	Weak interference	$\begin{cases} \gamma(g_P p_P), & \text{if } R_S < \gamma(\frac{g_{SP} p_S}{1+g_P p_P}); \\ \gamma_P - R_S, & \text{if } \gamma(\frac{g_{SP} p_S}{1+g_P p_P}) \le R_S \\ & \quad \le \min(\gamma(g_{SP} p_S), \gamma(\frac{g_S p_S}{1+g_{PS} p_P})); \\ \gamma(\frac{g_P p_P}{1+g_{SP} p_S}), & \text{if* } \gamma(g_{SP} p_S) \le R_S \le \\ & \quad \max(\gamma(\frac{g_S p_S}{1+g_{PS} p_P}), \gamma_S - \gamma(\frac{g_P p_P}{1+g_{SP} p_S})); \\ \gamma_S - R_S, & \text{if } R_S > \\ & \quad \max(\gamma(\frac{g_S p_S}{1+g_{PS} p_P}), \gamma_S - \gamma(\frac{g_P p_P}{1+g_{SP} p_S})). \end{cases}$

Fig. 6.2 illustrates the secrecy rate by an example of Case A, where the frontiers $f_M(R_S), f_P(R_S), f_S(R_S)$, and $f_C(R_S)$ are plotted. The shaded regions are $\Re^{[\mathrm{COOP}]}$

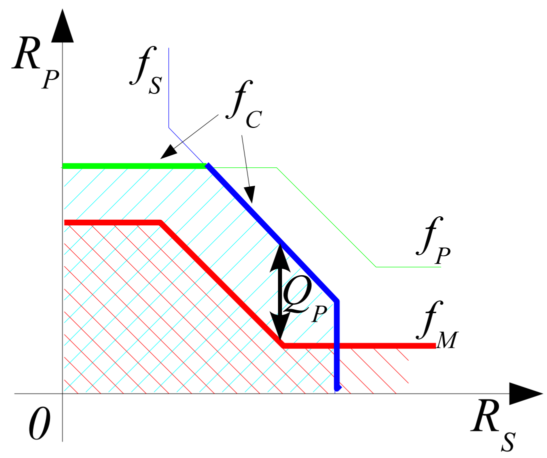


Figure 6.2: Illustration of Pareto frontiers and the achievable secrecy rate.

and $\{\Re_M^{[\mathrm{MAC}]} \cup \Re_M^{[\mathrm{SD}]}\}$. Then, the gap between the two Pareto frontiers in bold lines is the secrecy rate achievable by stochastic coding.

6.2.2 Optimal Rate Pair

Recall that the primary user reserves the right not to cooperate with the secondary user unless cooperation yields a higher secrecy rate than the bottom line C_P given in (6.4). Therefore, the overall achievable rate pair is

$$(\overline{Q_P}, \overline{R_S}) = \begin{cases} (Q_P^\star, R_S^\star), & \text{if } Q_P^\star > C_P; \\ (C_P, 0), & \text{otherwise,} \end{cases} \tag{6.19}$$

which is always bounded below by C_P. We could relax the definition of Q_P without affecting rates $(\overline{Q_P}, \overline{R_S})$, e.g., by removing the non-negative constraint. Slightly abusing the notations, we keep using the same notations after relaxation.

Proposition 16 *Relaxing the definition of Q_P in (6.15) to $Q_P(R_S) \triangleq f_C(R_S) -$*

$\overline{f_M}(R_S)$ will not affect $(\overline{Q_P}, \overline{R_S})$, where $\overline{f_M}(R_S)$ inherits from $f_M(R_S)$ except extending the line segment $\gamma_M - R_S$ to the entire range $[0, \gamma(g_{SM}p_S)]$. Then, the optimal rate pair $(Q_P^\star, R_S^\star)$ defined in (6.13) and (6.14) is given by $Q_P^\star = Q_P(R_S^\star) = Q_P(R_S^\dagger)$ and $R_S^\star = \max\{R|Q_P(R) = Q_P^\star\}$, where the auxiliary variable $R_S^\dagger$ is,

$$R_S^\dagger = \begin{cases} \gamma(g_S p_S/(1+g_{PS}p_P)), & (C1); \\ \min(\gamma(g_S p_S), \gamma(g_{SM}p_S)) & \textit{otherwise;} \end{cases}$$

with condition $(C1)$ being that $f_C(R_S)$ is discontinuous at $\gamma(g_S p_S/(1+g_{PS}p_P))$ and $g_S/(1+g_{PS}p_P) \le g_{SM}$. Furthermore, $R_S^\star$ differs from $R_S^\dagger$ only when $R_S^\dagger = \gamma(g_{SM}p_S)$ and $f_C'(\gamma(g_{SM}p_S)) = 0$.

We omit the proof of Proposition 16, which can be found in [22]. $(Q_P^\star, R_S^\star)$ is first calculated from Proposition 16. If $Q_P^\star \le C_P$, the primary user does not bother to cooperate, receiving a bottom line secrecy rate C_P; otherwise, the primary user has the incentive to cooperate, stochastically encoding using the scheme in Proposition 15 with $R_P = f_C(R_S^\star), R_{PM} = f_M(R_S^\star)$, and allowing the secondary user to transmit with the rate $R_S^\star$. In the following, we will present a more specific expression of $(Q_P^\star, R_S^\star)$ depending on numerous subcases and branches, because different subcases may correspond to different shapes of the frontier $f_C(R_S)$ even for the same case. For convenience, some commonly used terms are listed in Table 6.2.

$\diamondsuit$ **Case A**. $g_P \le g_{PS}, g_S \le g_{SP}$

Subcase A1. When $p_P \le (g_{SP}/g_S - 1)/g_P$ and $p_S \le (g_{PS}/g_P - 1)/g_S$.

If $g_{SM} \ge g_S$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q5}, \gamma_{R2}). \tag{6.20}$$

Table 6.2: A list of some commonly used expression for the achievable rate.

$$
\begin{aligned}
&\gamma_{Q1} = \gamma(g_P p_P) - \gamma\left(g_{PM} p_P/(1 + g_{SM} p_S)\right),\\
&\gamma_{Q2} = \gamma(g_P p_P + g_{SP} p_S) - \gamma(g_{PM} p_P + g_{SM} p_S),\\
&\gamma_{Q3} = \gamma(g_{PS} p_P + g_S p_S) - \gamma(g_{PM} p_P + g_{SM} p_S),\\
&\gamma_{Q4} = \gamma(g_P p_P/(1 + g_{SP} p_S)) - \gamma(g_{PM} p_P/(1 + g_{SM} p_S)),\\
&\gamma_{Q5} = \gamma(g_P p_P) + \gamma(g_S p_S) - \gamma_M,\\
&\gamma_{Q6} = \gamma(g_P p_P) + \gamma(g_S p_S/(1 + g_{PS} p_P)) - \gamma_M,\\
&\gamma_{Q7} = \gamma(g_S p_S) + \gamma(g_P p_P/(1 + g_{SP} p_S)) - \gamma_M,\\
&\gamma_{Q8} = \gamma(g_P p_P/(1 + g_{SP} p_S)) + \gamma(g_S p_S/(1 + g_{PS} p_P)) - \gamma_M;\\
&\gamma_{R1} = \gamma(g_{SM} p_S),\\
&\gamma_{R2} = \gamma(g_S p_S),\\
&\gamma_{R3} = \gamma(g_{SP} p_S/(1 + g_P p_P)),\\
&\gamma_{R4} = \gamma(g_S p_S/(1 + g_{PS} p_P)),\\
&\gamma_{R5} = \gamma_S - \gamma(g_P p_P/(1 + g_{SP} p_S)),\\
&\gamma_{R6} = \gamma_S - \gamma(g_P p_P).
\end{aligned}
$$

If $g_{SM} < g_S$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q1}, \gamma_{R2}). \tag{6.21}$$

Subcase A2. When $p_P > (g_{SP}/g_S - 1)/g_P$ and $(g_{PS} - g_P)p_P \geq (g_{SP} - g_S)p_S$.

If $p_P \leq (g_{SP}/g_{SM} - 1)/g_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q1}, \gamma_{R3}). \tag{6.22}$$

If $p_P > (g_{SP}/g_{SM} - 1)/g_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q2}, \min\{\gamma_{R1}, \gamma_{R2}\}). \tag{6.23}$$

Subcase A3. When $p_S > (g_{PS}/g_P - 1)/g_S$ and $(g_{SP} - g_S)p_S > (g_{PS} - g_P)p_P$.

If $g_{SM} p_S + g_P p_P + g_{SM} p_S g_P p_P \leq g_S p_S + g_{PS} p_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q1}, \gamma_{R6}). \tag{6.24}$$

If $g_{SM} p_S + g_P p_P + g_{SM} p_S g_P p_P > g_S p_S + g_{PS} p_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q3}, \min\{\gamma_{R1}, \gamma_{R2}\}). \tag{6.25}$$

$\diamondsuit$ **Case B**. $g_P > g_{PS}, g_S \leq g_{SP}$

Subcase B1. When $g_S + g_P g_S p_P \leq g_{SP} + g_{SP} g_{PS} p_P$.

If $p_P \leq (g_S/g_{SM} - 1)/g_{PS}$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q1}, \gamma_{R4}). \tag{6.26}$$

If $p_P > (g_S/g_{SM} - 1)/g_{PS}$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q6}, \gamma_{R4}). \tag{6.27}$$

Subcase B2. When $g_S + g_P g_S p_P > g_{SP} + g_{SP} g_{PS} p_P$.

If $p_P \leq (g_{SP}/g_{SM} - 1)/g_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q1}, \gamma_{R3}). \tag{6.28}$$

If $p_P > (g_{SP}/g_{SM} - 1)/g_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q2}, \min\{\gamma_{R1}, \gamma_{R4}\}). \tag{6.29}$$

$\diamondsuit$ **Case C**. $g_P \leq g_{PS}, g_S > g_{SP}$

Subcase C1. When $g_P + g_P g_S p_S \leq g_{PS} + g_{SP} g_{PS} p_S$.

If $g_{SM} < g_{SP}$ and $p_P \leq (g_{SP}/g_{SM} - 1)/g_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q1}, \gamma_{R3}). \tag{6.30}$$

If $g_{SM} < g_{SP}$ and $p_P > (g_{SP}/g_{SM} - 1)/g_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q2}, \gamma_{R1}). \tag{6.31}$$

If $g_{SP} \leq g_{SM} \leq g_S$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q4}, \gamma_{R2}). \tag{6.32}$$

If $g_{SM} > g_S$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q7}, \gamma_{R2}). \tag{6.33}$$

Subcase C2. When $g_P + g_P g_S p_S > g_{PS} + g_{SP} g_{PS} p_S$.

If $g_{SM} < g_{SP}$ and $p_P \leq (g_{SP}/g_{SM} - 1)/g_P$, the same as (6.30).

If $g_{SM} < g_{SP}$ and $p_P > (g_{SP}/g_{SM} - 1)/g_P$, the same as (6.31).

If $g_{SM} \geq g_{SP}$ and $(1 + g_{SP} p_S)(g_{PS} p_P + g_S p_S - g_{SM} p_S) \geq (1 + g_{SM} p_S) g_P p_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q4}, \gamma_{R5}). \tag{6.34}$$

If $g_{SM} \geq g_{SP}$ and $(1 + g_{SP} p_S)(g_{PS} p_P + g_S p_S - g_{SM} p_S) < (1 + g_{SM} p_S) g_P p_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q3}, \min\{\gamma_{R1}, \gamma_{R2}\}). \tag{6.35}$$

$\diamondsuit$ **Case D**. $g_P > g_{PS}, g_S > g_{SP}$

Subcase D1. When $p_P < (g_S/g_{SP} - 1)/g_{PS}$ and $p_S < (g_P/g_{PS} - 1)/g_{SP}$.

If $g_{SM} < g_{SP}$ and $p_P \leq (g_{SP}/g_{SM} - 1)/g_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q1}, \gamma_{R3}). \tag{6.36}$$

If $g_{SM} < g_{SP}$ and $p_P > (g_{SP}/g_{SM} - 1)/g_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q2}, \gamma_{R1}). \tag{6.37}$$

If $g_{SM} \geq g_{SP}$ and $p_P \leq (g_S/g_{SM} - 1)/g_{PS}$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q4}, \gamma_{R4}). \tag{6.38}$$

If $g_{SM} \geq g_{SP}$ and $p_P > (g_S/g_{SM} - 1)/g_{PS}$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q8}, \gamma_{R4}). \tag{6.39}$$

Subcase D2. When $p_P \geq (g_S/g_{SP} - 1)/g_{PS}$ and $(g_P - g_{PS})p_P > (g_S - g_{SP})p_S$

If $p_P \leq (g_{SP}/g_{SM} - 1)/g_P$, the same as (6.36).

If $(g_{SP}/g_{SM} - 1)/g_P < p_P \leq (g_S/g_{SM} - 1)/g_{PS}$, the same as (6.37).

If $p_P > (g_S/g_{SM} - 1)/g_{PS}$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q2}, \gamma_{R4}). \tag{6.40}$$

Subcase D3. When $p_S \geq (g_P/g_{PS} - 1)/g_{SP}$ and $(g_S - g_{SP})p_S \geq (g_P - g_{PS})p_P$.

If $g_{SM} < g_{SP}$ and $p_P \leq (g_{SP}/g_{SM} - 1)/g_P$, the same as (6.36).

If $g_{SM} < g_{SP}$ and $p_P > (g_{SP}/g_{SM} - 1)/g_P$, the same as (6.37).

If $g_{SM} \geq g_{SP}$ and $(1 + g_{SP}p_S)(g_S p_S + g_{PS}p_P - g_{SM}p_S) \geq (1 + g_{SM}p_S)g_P p_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q4}, \gamma_{R5}). \tag{6.41}$$

If $g_{SM} \geq g_{SP}$ and $(1 + g_{SP}p_S)(g_S p_S + g_{PS}p_P - g_{SM}p_S) < (1 + g_{SM}p_S)g_P p_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q3}, \min\{\gamma_{R1}, \gamma_{R2}\}). \tag{6.42}$$

To sum up, $R_S^\star$ takes one of the six candidate forms $\{\gamma_{Rk}, k = 1, 2, \ldots, 6\}$ depending on the cases and subcases. Let us take a closer look at these candidate forms. $\gamma_{R1} = \gamma(g_{SM}p_S)$ is the critical rate that the malicious user could decode the secondary user's message in the ideal case; in general, transmitting a higher rate than γ_{R1} does not bring further difficulty to the eavesdropper's decoding, but instead affects the primary user's achievable rate. $\gamma_{R2} = \gamma(g_S p_S)$ is the highest possible rate for the secondary user, beyond which no message would be decodable even with perfect interference cancellation. γ_{R4} corresponds to condition (C1) in Proposition 16. The rest forms correspond to the situation where there are multiple R_S's that attains $Q_P^\star$, and thus the maximum R_S is selected as $R_S^\star$ according to (6.14), although the specific form varies case by case. $Q_P^\star$ is the difference of decodable rates of the primary user and the eavesdropper, i.e., $f_C(R_S^\star) - \overline{f_M}(R_S^\star)$ according to Proposition 16. Therefore, it takes the form of rate differences, i.e., one of the possible forms $\{\gamma_{Qk}, k = 1, 2, \ldots, 8\}$ depending on the specific condition.

6.3 Information Secrecy Game

We have derived achievable $(\overline{Q_P}, \overline{R_S})$ in the previous section given fixed power levels p_P and p_S. However, both users have the freedom to select their power under the power constraint $p_P \in [0, p_P^M]$ and $p_S \in [0, p_S^M]$, and they have the incentive to manipulate power levels for a higher rate. We write down the achievable rates as functions of power levels, e.g., $\overline{Q_P}(p_P, p_S)$ and $\overline{R_S}(p_P, p_S)$, to emphasize the dependence.

In this section, we first demonstrate how rate pairs depend on power levels through a 2-D plane representation. Then, we model the cooperation between the primary user and the secondary user as a Stackelberg game, and discuss the game equilibrium in light of the 2-D representation. Finally, we extend the game to the multi-user case.

6.3.1 2-D Representation

The payoff $(\overline{Q_P}(p_P, p_S), \overline{R_S}(p_P, p_S))$ is closely related to $(Q_P^\star(p_P, p_S), R_S^\star(p_P, p_S))$ whose expressions seem rather involved because of numerous cases, subcases, and additional branches. Although varying power levels will not change which case it belongs to (cases are divided purely by the CSI), different power combinations may activate different subcases and/or branches. To circumvent the difficulty, we "translate" the conditions of subcases and branches into the regions on a p_P–p_S plane, and visually show how $(Q_P^\star(p_P, p_S), R_S^\star(p_P, p_S))$ depends on power levels. Discussing the equilibrium on this 2-D plane is much easier.

For Case A, the p_P–p_S plane is divided into regions of different rate expressions, as shown in Fig. 6.3, where the left one corresponds to the the scenario $g_{SM} \geq g_S$, and the right one is for $g_{SM} < g_S$. The equations of rate pair associated with each region are: ① $\sim$ (6.20); ② $\sim$ (6.21); ③ $\sim$ (6.22); ④ $\sim$ (6.23); ⑤ $\sim$ (6.24); ⑥ $\sim$ (6.25). We use circled numbers to denote the regions. The boundaries in the left figure are $p_P = (g_{SP}/g_S - 1)/g_P$ (between ① and ④), $p_S = (g_{PS}/g_P - 1)/g_S$ (between ① and ⑥), and $(g_{PS} - g_P)p_P = (g_{SP} - g_S)p_S$ (between ④ and ⑥). Two additional boundaries can be found in the right figure, $p_P = (g_{SP}/g_{SM} - 1)/g_P$ (between ③ and ④) and $g_{SM}p_S + g_P p_P + g_{SM} p_S g_P p_P = g_S p_S + g_{PS} p_P$ (between ⑤ and ⑥).

Fig. 6.4 shows the regions for Case B. The left figure holds when $g_{SM} > (g_P g_S - g_{SP} g_{PS})/(g_P - g_{PS})$, and the right one holds otherwise. The corresponding equations for each region are: ① $\sim$ (6.26); ② $\sim$ (6.27); ③ $\sim$ (6.28); ④ $\sim$ (6.29). The boundaries are $p_P = (g_{SP} - g_S)/(g_P g_S - g_{SP} g_{PS})$ (between ② and ④, or between ① and ③), $p_P = (g_S/g_{SM} - 1)/g_{PS}$ (between ① and ②), and $p_P = (g_{SP}/g_{SM} - 1)/g_P$ (between ③ and ④). Note that under certain conditions some regions may not exist and the corresponding boundaries are invalid (e.g., negative or infinity), and

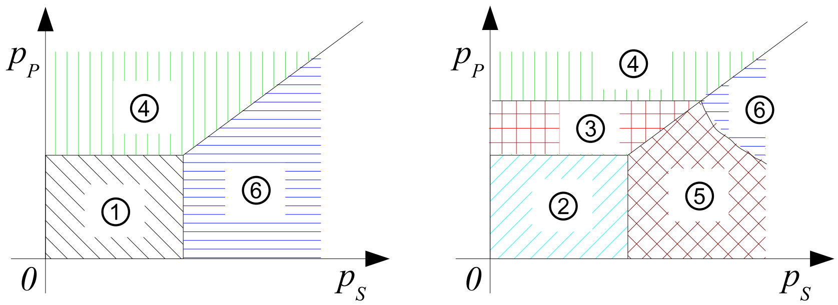


Figure 6.3: Illustration of rate-pair regions on the p_P–p_S plane for Case A.

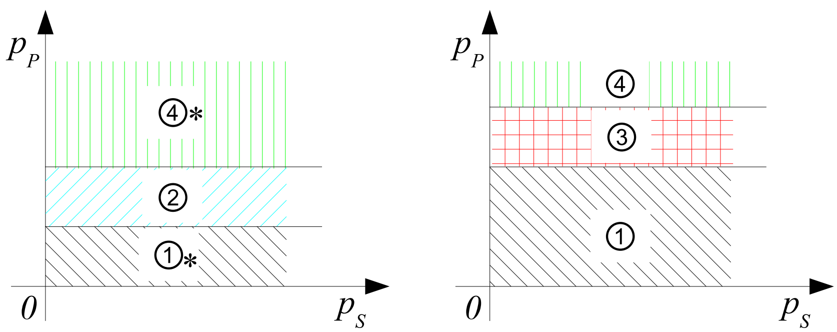


Figure 6.4: Illustration of rate-pair regions on the p_P–p_S plane for Case B.

we mark such regions with a "*" in the figure.

Case C is illustrated in Fig. 6.5, where the mappings are ① $\sim$ (6.30); ② $\sim$ (6.31); ③ $\sim$ (6.32) when $g_{SP} \leq g_{SM} \leq g_S$ or (6.33) when $g_{SM} > g_S$; ④ $\sim$ (6.34); ⑤ $\sim$ (6.35). When $g_{SM} < g_{SP}$, the left figure applies, with the boundary $p_P = (g_{SP}/g_{SM} - 1)/g_P$. Otherwise, the right figure applies, with the boundary $p_S = (g_{PS} - g_P)/(g_P g_S - g_{SP} g_{PS})$, but when $g_P g_S \leq g_{SP} g_{PS}$, the boundary is invalid and the entire plane is a single region. The boundary between ④ and ⑤, when existing, is $(1 + g_{SP} p_S)(g_{PS} p_P + g_S p_S - g_{SM} p_S) = (1 + g_{SM} p_S) g_P p_P$.

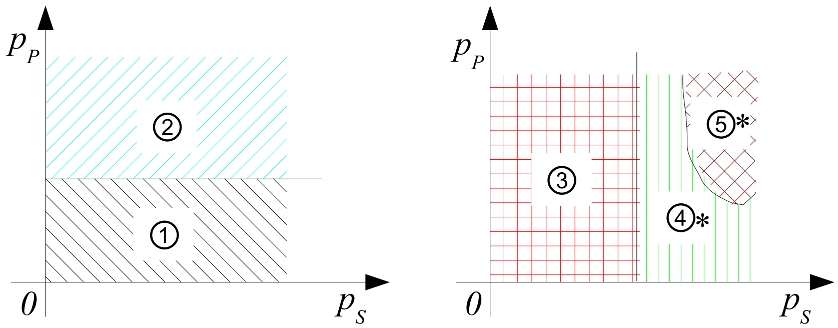


Figure 6.5: Illustration of rate-pair regions on the p_P–p_S plane for Case C.

Finally, the regions for Case D are presented in Fig. 6.6 with corresponding equations: ① $\sim$ (6.36); ② $\sim$ (6.37); ③ $\sim$ (6.38); ④ $\sim$ (6.39); ⑤ $\sim$ (6.40); ⑥ $\sim$ (6.41); ⑦ $\sim$ (6.42). The left figure corresponds to $g_{SM} < g_{SP}$ whereas the right one corresponds to $g_{SM} \geq g_{SP}$. The boundaries are: $p_P = (g_{SP}/g_{SM} - 1)/g_P$ (between ① and ②), $(g_P - g_{PS})p_P = (g_S - g_{SP})p_S$ and $p_P = (g_S/g_{SM} - 1)/g_{PS}$ (between ② and ⑤), $p_P = (g_S/g_{SM} - 1)/g_{PS}$ (between ③ and ④), $(1 + g_{SP}p_S)(g_{PS}p_P + g_S p_S - g_{SM}p_S) = (1 + g_{SM}p_S)g_P p_P$ (between ⑥ and ⑦), $p_P = (g_S/g_{SP} - 1)/g_{PS}$ (between ④ and ⑤), $(g_P - g_{PS})p_P = (g_S - g_{SP})p_S$ (between ⑤ and ⑦), $p_S = (g_P/g_{PS} - 1)/g_{SP}$ (between ③④ and ⑥⑦).

6.3.2 Stackelberg Game

The cooperation procedure can be modeled as a *Stackelberg game* with two *players*: the primary user is the *leader*, while the secondary user is the *follower*. Their *payoffs* are the secrecy rate $\overline{Q_P}(p_P, p_S)$ and the information rate $\overline{R_S}(p_P, p_S)$, respectively, which depend on their *actions* p_P and p_S. We discuss the *Nash equi-*

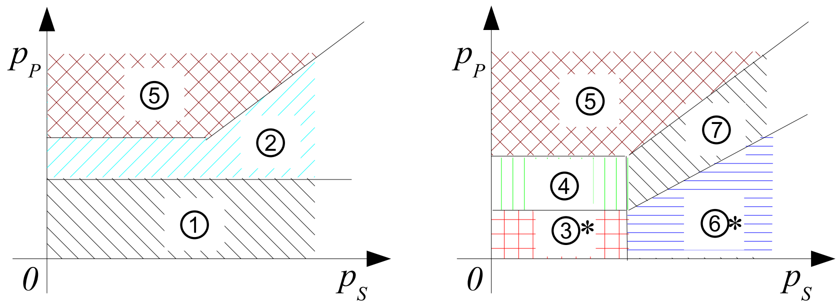


Figure 6.6: Illustration of rate-pair regions on the p_P–p_S plane for Case D.

librium of this information secrecy game based on the 2-D representation.

For a given p_P, a horizonal line segment can be drawn on the p_P–p_S plane with $p_S \in [0, p_S^M]$, which may remain in a single region or cross several regions. Depending on which regions have been passed through, $R_S^\star(p_P, p_S)$ and $Q_P^\star(p_P, p_S)$ may be piece-wise defined functions. The optimal power level $p_S^\star$ is a function of p_P,

$$p_S^\star(p_P) = \underset{p_S \in [0, p_S^M]}{\operatorname{argmax}}\, R_S^\star(p_P, p_S), \\ \text{s.t. } Q_P^\star(p_P, p_S) > C_P. \tag{6.43}$$

The constraint comes from that $\overline{R_S}(p_P, p_S) = R_S^\star(p_P, p_S)$ only when the primary user is willing to cooperate. Thanks to the monotonicity stated in Proposition 17, (6.43) can be further reduced to,

$$p_S^\star(p_P) = \max\{p_S \in [0, p_S^M] \big| Q_P^\star(p_P, p_S) > C_P\}. \tag{6.44}$$

Searching for the maximum can be done piece by piece, and signs of the first-order derivatives are given in Proposition 18, with $a \overset{s}{\sim} b$ denoting that a and b have the same sign. Detailed proofs can be found in [22].

Proposition 17 *With p_P fixed, $R_S^\star(p_P, p_S)$ is a strictly increasing function with regard to p_S.*

Proposition 18 *With p_P fixed, the signs of first-order partial derivatives are as follows: $\partial\gamma_{Q1}/\partial p_S > 0$, and*

$$\partial\gamma_{Q2}/\partial p_S \overset{s}{\sim} g_{SP}(1 + g_{PM}p_P) - g_{SM}(1 + g_P p_P),$$

$$\partial\gamma_{Q3}/\partial p_S \overset{s}{\sim} \partial\gamma_{Q6}/\partial p_S \overset{s}{\sim} g_S(1+g_{PM}p_P)-g_{SM}(1+g_{PS}p_P),$$

$$\partial\gamma_{Q5}/\partial p_S \overset{s}{\sim} g_S(1 + g_{PM}p_P) - g_{SM}.$$

All the above functions are monotonic when p_P is given. The rest functions share the same quadratic form, for $j = 4, 7, 8$,

$$\frac{\partial\gamma_{Qj}}{\partial p_S} \overset{s}{\sim} Fp_S^2 + 2(AC - BD)p_S + (AC - BD)(B + D) - BDF,$$

where $F = B+D-A-C$, $A = (g_P p_P+1)/g_{SP}$, $B = (g_{PM}p_P+1)/g_{SM}$, $D = 1/g_{SP}$, and the parameter C is as follows: $C = 1/g_{SM}$ for γ_{Q4}, $C = 1/g_S$ for γ_{Q7}, and $C = (1 + g_{PS}p_P)/g_S$ for γ_{Q8}.

Predicting that the secondary user will choose the optimal power $p_S^\star(p_P)$ for an announced power level p_P, the primary user is able to maximize the payoff by announce the power level $p_P^\star$ such that

$$p_P^\star = \underset{p_P \in [0, p_P^M]}{\operatorname{argmax}} Q_P^\star(p_P, p_S^\star(p_P)). \tag{6.45}$$

Finally, $(p_P^\star, p_S^\star(p_P^\star))$ is the Nash equilibrium of the game.

In a cognitive radio network, usually there are more than one secondary users. Intuitively, when there are more secondary users in the network, it is more likely that the primary user could find a secondary user in a good location to cooperate with, and hence the secrecy rate may increase. In this case, the primary user plays separate information secrecy games with each individual secondary user who needs to transmit information at the moment, and chooses to cooperate with the "best" secondary user who brings the highest secrecy rate. As expected, the achieved secrecy rate will improve with increasing numbers of secondary users participating in the game. We will show the performance through simulation results later.

6.4 Simulation Studies

In this section, some simulation results are presented. We first fix a channel realization to get some insight of the proposed cooperative transmission scheme, and then we show the average performance by generating thousands of independent channel realizations.

For illustrative purposes, we fix the channel as one realization of Case A: $g_P = g_S = 1$, $g_{PS} = 1.5$, $g_{SP} = 1.3$, $g_{SM} = 0.3$, and $g_{PM} = 1.2$. Note that under this setting $g_P < g_{PM}$, the primary user cannot transmit in secrecy at all without the secondary user's help, because $C_P = 0$ according to (6.4). In Fig. 6.7, we plot the achievable secrecy rate $Q_P^\star(p_P, p_S)$ when the transmit power levels take different values from $[0, 20] \times [0, 20]$. Some rates in the figure are negative, because $Q_P^\star(p_P, p_S)$ is the relaxed rate without considering the non-negative constraint (the overall rate $\overline{Q_P}(p_P, p_S)$, however, is guaranteed to be non-negative). As shown by the figure, the primary user does benefit from simultaneous transmissions of the secondary user.

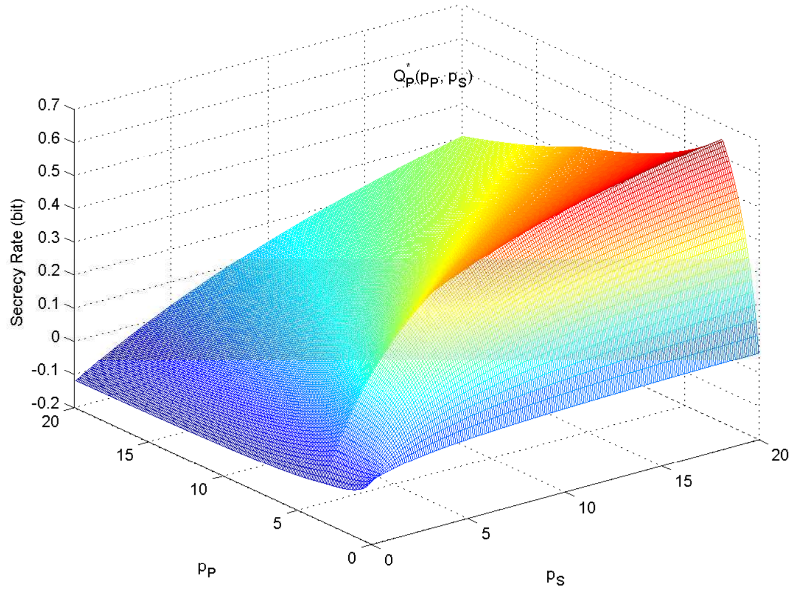


Figure 6.7: Achievable secrecy rate $Q_P^{\star}(p_P, p_S)$ with varying power levels p_P and p_S.

For example, within the power constraint, the primary user is able to reach a secrecy rate of 0.64 bit when $p_P = 2.5$ and $p_S = 20.0$. Moreover, as shown in the figure, it is not always beneficial to use full power; for example, when fixing $p_S = 20.0$, increasing p_P beyond 2.5 will reduce the secrecy rate. The reason is that the secrecy rate depends on the difference of the decoding capability of the primary receiver and the eavesdropper. It is possible that the decodable rate to the primary receiver grows with higher power but the eavesdropper may gain even more, which reduces the secrecy rate.

Next, we vary g_{PM} from 0.2 to 2, with all the other channel coefficients fixed as above. In Fig. 6.8, we compare the bottom line secrecy rate without cooperation and the optimal achievable secrecy rate at the Nash equilibrium of the proposed

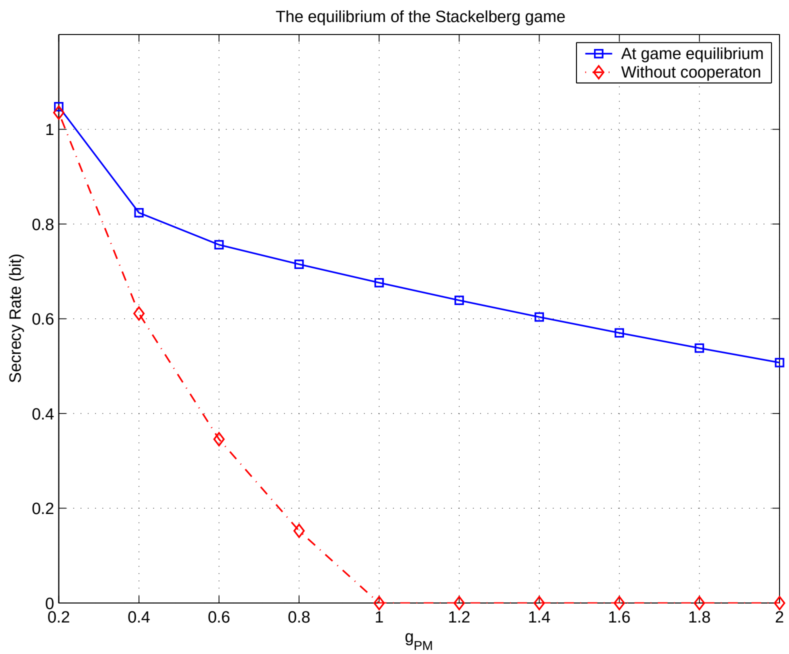


Figure 6.8: The optimal achievable secrecy rate at the game equilibrium and the secrecy rate without the secondary user's cooperation.

Stackelberg game, i.e., when users choose the optimal power levels according to (6.45). As expected, as the channel between the primary transmitter and the eavesdropper becomes better, the eavesdropper is more capable of decoding the primary user's message, and hence the secrecy rate without cooperation becomes lower, and further drops to zero when $g_{PM} > g_P$. When the primary user and the secondary user cooperate with each other, however, the primary user may significantly enhance the secrecy of confidential messages, as shown in the figure. When g_{PM} is small, the eavesdropper receives very weak signals from the primary user, and the gain from a helper becomes limited.

In order to show the average performance of the proposed algorithm, we consider a scenario where all the users lie in a circular area with a radius 1000 meters. The primary transmitter locates at the center of the circle, while the primary user's receiver, the eavesdropper, and the secondary transmitters/receivers are uniformly distributed in this circular area. We assume the channel gain merely depends on the distance from a transmitter to a receiver d, i.e., $g = g_0 d^{-\alpha}$, where the path loss exponent α is set to be 2 in the simulation, and g_0 is the channel gain at a reference point one meter away. We choose p_P^M, p_S^M, and g_0 in such a way that the signal-to-noise ratio (SNR) without considering interference is 15dB when the distance is 300 meters and the transmitter uses the maximum power. In the simulation, we generate 5000 independent channel realizations. For each realization, we uniformly generate the location of users, calculate channel gains based on the distance, and find the equilibrium for this particular game. The results from all independent realizations are plotted in the form of empirical cumulative distribution functions.

In Fig. 6.9, we compare the proposed scheme with the benchmark situation where there is no secondary user assisting the secrecy transmission, referred to as "no cooperation". Moreover, the scheme in [95] is also simulated, in which the helping interferer unconditionally cooperates and does not transmit his/her own useful information at all. Hence, we refer to this scheme as "altruistic helper". From the figure, it can be seen that the proposed game improves the information secrecy rate of the primary user while enabling the simultaneous transmission of a secondary user. The gap between our proposed game and the "altruistic helper" scheme is somewhat like the so-called "price of anarchy" in noncooperative games. Because in our scheme, the secondary user has his/her own interest and transmits meaningful data to his/her own receiver, the game equilibrium takes both users' benefit into consideration. Therefore, from the primary user's point of view, the performance is suboptimal to the unconditional cooperation situation, and the cost is due to competition and compromise between two players in the game.

We have expected that the secrecy rate will improve when there are more secondary users in the network, because the primary user could pick up the best secondary user to cooperate with after playing a game with each individual secondary user separately. We verify this by simulation. In Fig. 6.10, the mean and median values of secrecy rates are plotted versus different numbers of secondary users, and when the number of secondary users equals zero, it actually reduces to the "no cooperation" case. As illustrated by the two figures, secrecy rates are significantly improved by the proposed cooperation scheme, and higher rates are expected when there are more secondary users in the network.

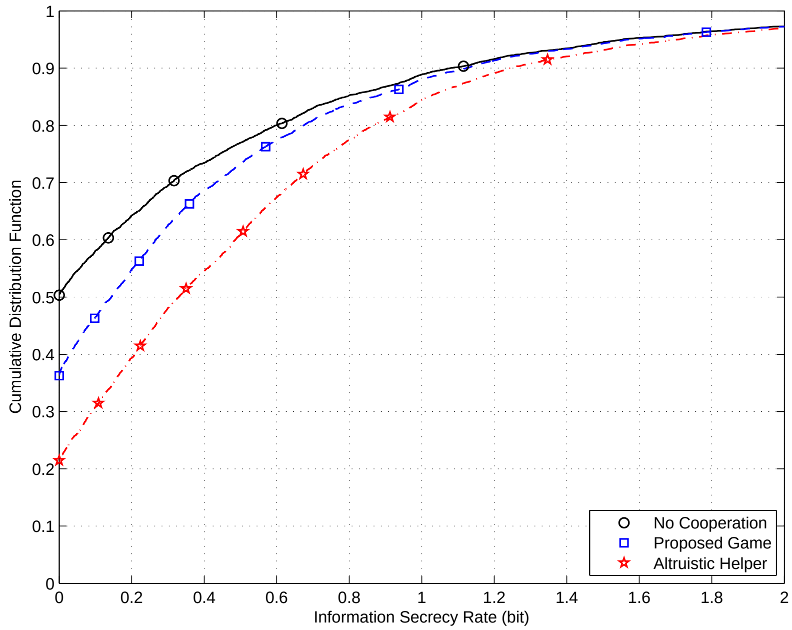


Figure 6.9: Cumulative distribution functions of secrecy rates in scenarios with different levels of cooperation.

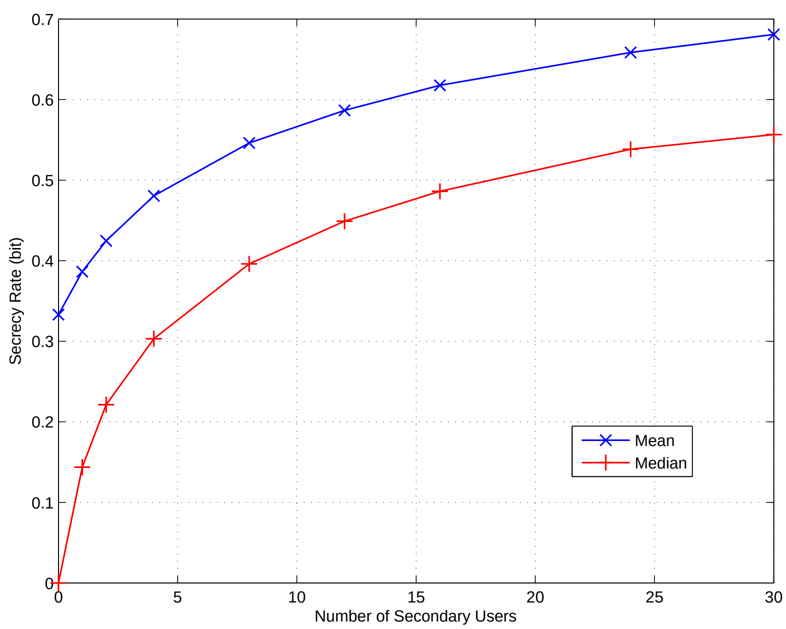


Figure 6.10: The mean and median of secrecy rates with different numbers of secondary users in the network.

Chapter 7

Conclusions and Future Work

7.1 Conclusions

In this dissertation, we have developed and analyzed game-theoretic frameworks to suppress selfish and malicious behaviors in cognitive radio networks, in order to improve the efficiency of spectrum utilization, boost cooperation in spectrum sharing, and protect cognitive radio users from adversaries. After an overview of game theory and its application in cognitive radio networks in Chapter 2 as a background for this dissertation, we have addressed the following problems.

In Chapter 3, we proposed a novel spectrum sharing scheme with cheat-proof strategies to improve the efficiency of open spectrum sharing. The spectrum sharing problem was modeled as a repeated game where any deviation from cooperation would trigger the punishment. We proposed two cooperation rules with efficiency and fairness considered, and optimized the detection time to alleviate the impact due to imperfect detection of the selfish behavior. Moreover, two cheat-proof strategies based on mechanism design and properties of channel statistics were proposed to enforce that selfish users reported their true channel information. Simulation results showed that the proposed scheme efficiently improved the spectrum usage by alleviating the mutual interference.

In Chapter 4, we presented a novel multi-winner auction game for the spectrum auction scenario in a cognitive radio network, in which secondary users could lease some temporarily unused bands from primary users. As this kind of auction had not existed in the literature where commodities were usually quantity-limited, suitable auction mechanisms were developed to guarantee full efficiency of the spectrum utilization, yield higher revenue to primary users, and help eliminate user collusion. To make the proposed scheme scalable, the SDP relaxation was applied to get a near-optimal solution in polynomial time. Moreover, we extended the one-band auction mechanism to the multi-band case. Simulation results were presented to demonstrate performance and complexity of proposed auction mechanisms.

In Chapter 5, we investigated the anti-jamming defense in a cognitive radio network with multiple available channels, by modeling the interaction between a secondary user and attackers as anti-jamming games and studying the optimal strategy and the equilibrium of the games. In the scenario where both the secondary user and attackers were equipped with a single radio and accessed only one channel at any time, the secondary user hopped proactively between channels as the defense strategy. The optimal defense strategy could be solved by finding the optimal policy in a Markov decision process, and learning schemes were proposed based on the maximum likelihood estimation and Q-learning. Extending the anti-jamming problem to the scenario where the multi-radio secondary user could access multiple channels simultaneously, we redefined the game with randomized power allocation as the defense strategy. The defense strategy obtained from the Nash equilibrium was optimal in the sense that it minimized the worst-case damage caused by attackers.

In Chapter 6, we modeled the cooperative transmission in a cognitive radio network as a Stackelberg game, where a secondary user helped a primary user to enhance secrecy against an intelligent and passive eavesdropper. Both the primary user and the secondary user wanted to maximize rates of data transmission, but the primary user had additional secrecy concerns. In order to learn the fundamental limit for this system, we applied information theoretic approaches to derive the secrecy rate for the primary user and the information rate for the secondary user. In order to understand the incentive behind cooperation and predict the equilibrium behavior, we applied game-theoretic approaches to characterize the Nash equilibrium in terms of how much power should be used in cooperative transmissions. Simulation results were presented to verify the performance.

7.2 Future Work

Since cognitive radio is an emerging communication paradigm that will have great impacts on wireless devices and applications in the near future, there are numerous interesting problems that would lead to fruitful research in the area.

In the dissertation, game-theoretic frameworks have been developed to combat two specific security attacks, i.e., the jamming attack and eavesdropping attack, and have been shown to effectively protect secondary users and primary users from those malicious users. However, enabled by the technology evolution and depending on application scenarios, a malicious user may launch a lot of different forms of attacks, such as the denial-of-service attack, primary emulation attack, reputation/trust attack, Byzantine attack, and so on. These security issues are of critical importance and must be taken care of before the successful deployment of cognitive radio networks. Although varying in forms, these attacks can be modeled and mitigated after we capture their characteristics using game-theoretic modeling and carefully define their payoff functions. Therefore, I will extend my dissertation work to model and analyze various kinds of potential attacks and develop effective countermeasures. In addition to game theory, other techniques such as coding, forensics, and dynamic programming, can also be combined to further enhance robustness and efficiency of the defense mechanism.

Furthermore, the concept of cognitive radio does not limit itself to a narrow area in the communications; instead, the "cognitive network" can have a much broader sense, referring to any network consisting of "cognitive" entities, or entities with the capability of learning, reasoning, and adapting. Such candidates may include a peer-to-peer network, an ad hoc network, a multimedia network, an array of devices, a group of vehicles, and so on. Although they may have different concerns and focuses, the existence of selfish users and malicious uses is quite general because of the "cognitive" feature. Therefore, game theory can also be applied to suppress selfish and malicious behaviors in these networks to greatly enhance system performance. This emerging area will be of critical interest to conduct research on.

Bibliography

[1] Federal Communications Commission, "Spectrum policy task force report," *FCC Document ET Docket No. 02-135*, Nov. 2002.

[2] J. Mitola III, "Cognitive radio: an integrated agent architecture for software defined radio," Ph.D. Thesis, KTH Royal Institute of Technology, Stockholm, Sweden, 2000.

[3] W. Lehr, and J. Crowcroft, "Managing shared access to a spectrum commons," in *Proc. IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, Baltimore, Nov. 2005.

[4] R. Etkin, A. Parekh, and D. Tse, "Spectrum sharing for unlicensed bands," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 3, pp. 517–528, Apr. 2007.

[5] S. T. Chung, S. J. Kim, J. Lee, and J. M. Cioffi, "A game-theoretic approach to power allocation in frequency-selective Gaussian interference channels," in *Proc. of IEEE International Symposium on Information Theory (ISIT)*, Pacifico Yokohama, June 2003.

[6] J. Huang, R. Berry and M. Honig, "Distributed interference compensation for wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 5, pp. 1074–1084, May 2006.

[7] D. Cabric, S. M. Mishra, and R. W. Brodersen, " Implementation issues in spectrum sensing for cognitive radios," in *Proc. Asilomar Conference on Signals, Systems and Computers*, pp. 772–776, Asilomar Grounds, Nov. 2004.

[8] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio networks," in *Proc. IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pp. 137–143, Bartimore, Nov. 2005.

[9] B. Wang, Z. Ji, K. J. R. Liu, and C. Clancy, "Primary-prioritized Markov approach for efficient and fair dynamic spectrum allocation," *IEEE Trans. on Wireless Communications*, vol. 8, no. 4, pp. 1854–1865, Apr. 2009.

[10] S. Gandhi, C. Buragohain, L. Cao, H. Zheng, and S. Suri, "A general framework for wireless spectrum auctions," in *Proc. IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pp. 22–33, Dublin, Apr. 2007.

[11] Y. Chen, Y. Wu, B. Wang, and K. J. R. Liu, "Spectrum auction games for multimedia streaming over cognitive radio networks," *IEEE Transactions on Communications*, vol. 58, no. 8, pp. 2381–2390, Aug. 2010.

[12] Z. Ji and K. J. R. Liu, "Multi-stage pricing game for collusion-resistant dynamic spectrum allocation," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 182–191, Jan. 2008.

[13] M. Osborne and A. Rubinstein, *A Course in Game Theory*, MIT press, 1999.

[14] B. Wang, Y. Wu, and K. J. R. Liu, "Game theory for cognitive radio networks: An overview," *Computer Networks*, vol. 54, no. 14, pp.2537–2561, Oct. 2010.

[15] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25–37, Jan. 2008.

[16] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: threats and mitigation," in *Proc. International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, pp. 1–8, Singapore, May 2008.

[17] T. X. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: A multi-dimensional analysis and assessment," *Mobile Networks and Applications*, vol. 13, no. 5, pp. 516–532, Oct. 2008.

[18] W. Wang, H. Li, Y. Sun, and Z. Han, "CatchIt: Detect malicious nodes in collaborative spectrum sensing," in *Proc. IEEE Global Communications Conference (Globecom)*, Hawaii, Dec. 2009.

[19] Y. Wu, B. Wang, K. J. R. Liu, and T. C. Clancy, "Repeated open spectrum sharing game with cheat-proof strategies," *IEEE Transactions on Wireless Communications*, vol. 8, no. 4, pp. 1922–1933, Apr. 2009.

[20] Y. Wu, B. Wang, K. J. R. Liu, and T. C. Clancy, "A scalable collusion-resistant multi-winner cognitive spectrum auction game," *IEEE Transactions on Communications*, vol. 57, no. 12, pp. 3805–3816, Dec. 2009.

[21] Y. Wu, B. Wang, K. J. R. Liu, and T. C. Clancy, "Anti-jamming games in multi-channel cognitive radio networks," *IEEE Transactions on Communications*, submitted.

[22] Y. Wu and K. J. R. Liu, "An information secrecy game in cognitive radio networks," *IEEE Transactions on Information Forensics and Security*, submitted.

[23] D. Monderer and L. Shapley, "Potential games," *Games and Economic Behavior*, vol. 14, no. 1, pp. 124–143, 1996.

[24] R. Yates, "A framework for uplink power control in cellular radio systems," *IEEE Journal on Selected Areas in Communications*, vol. 13, no. 7, pp. 1341–1348, Sept. 1995.

[25] J. Neel, R. Buehrer, J. Reed, and R. Gilles, "Game theoretic analysis of a network of cognitive radios," in *Proc. IEEE Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 409–412, Tulsa, Aug. 2002.

[26] J. Neel, J. Reed, and R. Gilles, "The role of game theory in the analysis of software radio networks," in *SDR Forum Technical Conference*, San Diego, Nov. 2002.

[27] N. Nie and C. Comaniciu, "Adaptive channel allocation spectrum etiquette for cognitive radio networks," *Mobile Networks and Applications*, vol. 11, no. 6, pp. 779–797, Dec. 2006.

[28] C. U. Saraydar, N. B. Mandayam, and D. J. Goodman, "Efficient power control via pricing in wireless data networks," *IEEE Transactions on Communications*, vol. 50, no. 2, pp. 291–303, Feb. 2002.

[29] J. Zhang and Q. Zhang, "Stackelberg game for utility-based cooperative cognitive radio networks," in *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pp. 23–32, New Orleans, May 2009.

[30] K. W. Shum, K.-K. Leung, and C. W. Sung, "Convergence of iterative waterfilling algorithm for gaussian interference channels," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 6, pp. 1091–1100, Aug. 2007.

[31] Y. Su and M. van der Schaar, "A new perspective on multi-user power control games in interference channels," *IEEE Transactions on Wireless Communications*, vol. 8, no. 6, pp. 2910–2919, June 2009.

[32] A. Al Daoud, T. Alpcan, S. Agarwal, and M. Alanyali, "A Stackelberg game for pricing uplink power in wide-band cognitive radio networks," in *Proc. IEEE Conference on Decision and Control (CDC)*, pp. 1422–1427, Cancun, Mexico, Dec. 2008.

[33] F. Wang, M. Krunz, and S. Cui, "Price-based spectrum management in cognitive radio networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, no. 1, pp. 74–87, Feb. 2008.

[34] W. Wang, Y. Cui, T. Peng, and W. Wang, "Noncooperative power control game with exponential pricing for cognitive radio network," in *Proc. IEEE Vehicular Technology Conference (VTC)*, pp. 3125–3129, Dublin, Apr. 2007.

[35] J. Huang, R. Berry, and M. Honig, "Spectrum sharing with distributed interference compensation," in *Proc. IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pp. 88–93, Baltimore, Nov. 2005.

[36] S. Hart and A. Mas-Colell, "A simple adaptive procedure leading to correlated equilibrium," *Econometrica*, vol. 68, no. 5, pp. 1127–1150, Sept. 2000.

[37] M. Maskery, V. Krishnamurthy, and Q. Zhao, "Decentralized dynamic spectrum access for cognitive radios: Cooperative design of a non-cooperative game," *IEEE Transactions on Communications*, vol. 57, no. 2, pp. 459–469, Feb. 2009.

[38] D. Niyato and E. Hossain, "Competitive spectrum sharing in cognitive radio networks: A dynamic game approach," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2651–2660, July 2008.

[39] D. Niyato and E. Hossain, "Competitive pricing for spectrum sharing in cognitive radio networks: Dynamic game, inefficiency of Nash equilibrium, and collusion," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 192–202, Jan. 2008.

[40] J. Jia and Q. Zhang, "Competitions and dynamics of duopoly wireless service providers in dynamic spectrum market," in *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pp. 313–322, Hong Kong, May 2008.

[41] J. Mwangoka, K. Letaief, and Z. Cao, "Joint power control and spectrum allocation for cognitive radio networks via pricing," *Physical Communication*, vol. 2, no. 1-2, pp. 103–115, Mar. 2009.

[42] Z. Han, Z. Ji, and K. J. R. Liu, "A Cartel maintenance framework to enforce cooperation in wireless networks with selfish users," *IEEE Transactions on Wireless Communications*, vol. 7, no. 5, pp. 1889–1899, May 2008.

[43] O. Simeone, I. Stanojev, S. Savazzi, Y. Bar-Ness, U. Spagnolini, and R. Pickholtz, "Spectrum leasing to cooperating secondary ad hoc networks," *IEEE*

Journal on Selected Areas in Communications, vol. 26, no. 1, pp. 203–213, Jan. 2008.

[44] V. Krishna, *Auction Theory*, Academic Press, 2002.

[45] P. Bajari and J. Yeo, “Auction design and tacit collusion in FCC spectrum auctions,” *Information Economics and Policy*, vol. 21, no. 2, pp. 90–100, June 2009.

[46] W. Vickrey, “Counterspeculation, auctions, and competitive sealed tenders,” *The Journal of Finance*, vol. 16, no. 1, pp. 8–37, 1961.

[47] R. Myerson, “Optimal auction design,” *Mathematics of Operations Research*, vol. 6, no. 1, pp. 58–73, Feb. 1981.

[48] P. Cramton, Y. Shoham, and R. Steinberg, *Combinatorial Auctions*, MIT Press, 2006.

[49] J. Huang, R. A. Berry, and M. L. Honig, “Auction-based spectrum sharing,” *Mobile Networks and Applications*, vol. 11, no. 3, pp. 405–418, June 2006.

[50] Y. Chen, G. Yu, Z. Zhang, H. Chen, and P. Qiu, “On cognitive radio networks with opportunistic power control strategies in fading channels,” *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2752–2761, July 2008.

[51] X. Zhou, S. Gandhi, S. Suri, and H. Zheng, “eBay in the sky: Strategy-proof wireless spectrum auctions,” in *Proc. ACM International Conference on Mobile Computing and Networking (MobiCom)*, pp. 2–13, San Francisco, Sept. 2008.

[52] J. Jia, Q. Zhang, Q. Zhang, and M. Liu, “Revenue generation for truthful spectrum auction in dynamic spectrum access,” in *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pp. 3–12, New Orleans, May 2009.

[53] X. Zhou and H. Zheng, “TRUST: A general framework for truthful double spectrum auctions,” in *Proc. IEEE International Conference on Computer Communications (Infocom)*, Rio de Janeiro, Apr. 2009.

[54] R. B. Myerson, “Mechanism design,” in *The New Palgrave Dictionary of Economics*, Palgrave Macmillan, 2008.

[55] D. Fudenberg and J. Tirole, *Game Theory*, MIT Press, 1991.

[56] A. Fattahi, F. Fu, M. van der Schaar, and F. Paganini, “Mechanism-based resource allocation for multimedia transmission over spectrum agile wireless networks,” *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 3, pp. 601–612, Apr. 2007.

[57] B. Wang, Y. Wu, Z. Ji, K. J. R. Liu, and T. C. Clancy, “Game theoretical mechanism design methods: Suppressing cheating in cognitive radio networks,” *IEEE Signal Processing Magazine*, vol. 25, no. 6, pp. 74–84, Nov. 2008.

[58] J. F. Nash Jr, “The bargaining problem,” *Econometrica*, vol. 18, no. 2, pp. 155–162, Apr. 1950.

[59] G. Owen, *Game Theory*, 3rd ed., Academic Press, 1995.

[60] K. Han, J. Li, P. Zhu, and X. Wang, “The frequency-time pre-allocation in unlicensed spectrum based on the games learning,” in *Proc. International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, pp. 79–84, Orlando, Aug. 2007.

[61] A. Attar, M. Nakhai, and A. Aghvami, “Cognitive radio game for secondary spectrum access problem,” *IEEE Transactions on Wireless Communications*, vol. 8, no. 4, pp. 2121–2131, Apr. 2009.

[62] H. Pham, J. Xiang, Y. Zhang, and T. Skeie, “QoS-aware channel selection in cognitive radio networks: A game-theoretic approach,” in *IEEE Global Communications Conference (Globecom)*, New Orleans, Dec. 2008.

[63] L. Cao and H. Zheng, “Distributed spectrum allocation via local bargaining,” in *Proc. IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, pp. 475–486, Santa Clara, Sep. 2005.

[64] J. Suris, L. DaSilva, Z. Han, and A. MacKenzie, “Cooperative game theory for distributed spectrum sharing,” in *IEEE International Conference on Communications (ICC)*, pp. 5282–5287, Glasgow, June 2007.

[65] R. Thrall and W. Lucas, “N-person games in partition function form,” *Naval Research Logistics Quarterly*, vol. 10, no. 1, pp. 281–298, Mar. 1963.

[66] S. Mathur, L. Sankaranarayanan, and N. Mandayam, “Coalitional games in Gaussian interference channels,” in *Proc. IEEE IEEE International Symposiumon Information Theory (ISIT)*, pp. 2210–2214, Seattle, July 2006.

[67] W. Saad, Z. Han, M. Debbah, A. Hjørungnes, and T. Basar, “Coalitional games for distributed collaborative spectrum sensing in cognitive radio networks,” in

Proc. IEEE International Conference on Computer Communications (Infocom), Rio de Janeiro, Apr. 2009.

[68] L. Shapley, "Stochastic games," in *Proceedings of the National Academy of Sciences of USA*, vol. 39, no. 10, pp. 1095–1100, Oct. 1953.

[69] M. L. Puterman, *Markov Decision Processes: Discrete Stochastic Dynamic Programming*, John Wiley & Sons, 1994.

[70] M. Littman, "Markov games as a framework for multi-agent reinforcement learning," in *Proc. International Conference on Machine Learning*, New Brunswick, July 1994.

[71] B. Wang, Y. Wu, and K. J. R. Liu, "An anti-jamming stochastic game for cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, to appear.

[72] F. Fu and M. van der Schaar, "Learning to compete for resources in wireless stochastic games," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 4, pp. 1904–1919, May 2009.

[73] G. Hardin, "The tragedy of the commons," *Science*, vol. 162, pp. 1243–1248, Dec. 1968.

[74] G. Grimmett and D. Stirzaker, *Probability and Random Processes*, Oxford University Press, 2001.

[75] Z. Han and K. J. R. Liu, *Resource Allocation for Wireless Networks: Basics, Techniques, and Applications*, Cambridge University Press, 2008.

[76] F. P. Kelly, A. K. Maulloo, and D. K. H. Tan, "Rate control in communication networks: Shadow prices, proportional fairness and stability," *Journal of the Operational Research Society*, vol. 49, no. 3, pp. 237–252, Mar. 1998.

[77] H. A. David, *Order Statistics*, Wiley, 1970.

[78] F. F. Digham, M.-S. Alouini, and M. K. Simon, "On the energy detection of unknown signals over fading channels," in *Proc. of IEEE International Conference on Communications (ICC)*, Anchorage, May 2003.

[79] F. Kelly, "Charging and rate control for elastic traffic," *European Transactions on Telecommunications*, vol. 8, no. 1, pp. 33–37, Jan. 1997.

[80] L. M. Lawrence and P. R. Milgrom, "Ascending auctions with package bidding," *Frontiers of Theoretical Economics*, vol. 1, no. 1, pp. 1–43, 2002.

[81] R. Day and P. R. Milgrom, "Core-selecting package auctions," *International Journal of Game Theory*, vol. 36, no. 3, pp. 393–407, Mar. 2008.

[82] R.M. Karp, "Reducibility among combinatorial problems," in *Complexity of Computer Computations*, R.E. Miller and J.W. Thatcher (eds.), Plenum Press, pp. 85–103, 1972.

[83] M. Laurent and F. Rendl, *Semidefinite Programming and Integer Programming*, Centrum voor Wiskunde en Informatica, 2002.

[84] P. Gupta and P.R. Kumar, "The capacity of wireless networks," *IEEE Trans. on Information Theory*, vol. 46, no. 2, pp. 388–404, March 2000.

[85] L. Badia, E. Alessandro, L. Lenzini, and M. Zorzi, "A general interference-aware framework for joint routing and link scheduling in wireless mesh networks," *IEEE Network*, vol. 22, no. 1, pp. 32–38, Jan. 2008.

[86] S. P. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.

[87] C. Godsil and G. Royle, *Algebraic Graph Theory*, New York: Springer, 2004.

[88] M. Grötschel, L. Lovász, and A. Schrijver, *Geometric Algorithms and Combinatorial Optimization*, Springer-Verlag, 1993.

[89] E. Altman, K. Avrachenkov, and A. Garnaev, "A jamming game in wireless networks with transmission cost," in *Proc. of NET-COOP 2007. Lecture Notes in Computer Science*, vol. 4465, pp. 1–12, 2007.

[90] S. Khattab, D. Mosse, and R. Melhem, "Jamming mitigation in multi-radio wireless networks: reactive or proactive?," in *Proc. of International Conference on Security and Privacy in Communication Netowrks (SecureComm)*, Istanbul, Turkey, Sept. 2008.

[91] H. Li and Z. Han, "Dogfight in spectrum: Jamming and anti-jamming in multi-channel cognitive radio systems," in *Proc. IEEE Global Communications Conference (Globecom)*, Hawaii, Dec. 2009.

[92] H. Su and X. Zhang, "Cross-layer based opportunistic MAC protocols for QoS provisionings over cognitive radio wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 118–129, Jan. 2008.

[93] Y. Shoham and K. Leyton-Brown, *Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations*, Cambridge University Press, 2008.

[94] B. Roberson, "The Colonel Blotto game," *Economic Theory*, vol. 29, no. 1, pp. 1–24, Sept. 2006.

[95] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *IEEE Transactions on Information Theory*, submitted.

[96] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[97] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[98] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[99] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proceedings of the IEEE*, vol. 97, no. 5, pp. 894–914, May 2009.

[100] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed., John Wiley and sons, 2006.