Security-aware Cooperation in Dynamic Spectrum Access

by

Ning Zhang

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2015

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

We have witnessed a massive growth in wireless data, which almost doubles every year. The wireless data is expected to skyrocket further in the future due to the proliferation of devices and the emerging data-hungry applications. To accommodate the explosive growth in mobile traffic, a large amount of wireless spectrum is needed. With the limited spectrum resource, the current static spectrum allocation policy cannot serve well for future wireless systems. Moreover, it exacerbates the spectrum scarcity by resulting in severe spectrum underutilization. As a promising solution, dynamic spectrum access (DSA) is envisaged to increase spectrum efficiency by dynamic sharing all the spectrum. DSA can be enabled by cognitive radio technologies, which allow the unlicensed users (the secondary users, i.e., SUs) to dynamically access the unused spectrum (i.e., spectrum holes) owned by the licensed users (the primary users i.e., PUs). In order to identify the unused spectrum (spectrum holes), unlicensed users need to conduct spectrum sensing. While spectrum sensing might be inaccurate due to multipath fading and shadowing. To address this problem, user cooperation can be leveraged, with two main forms: cooperative spectrum sensing and cooperative cognitive radio networking (CCRN). For the former, SUs cooperate with each other in spectrum sensing to better detect the spectrum holes. For the latter, SUs cooperate with the PUs to gain access opportunities from the PUs by improving the transmission performance of the PUs.

Whereas cooperation can also incur security issues, e.g., malicious users might participate into cooperation, corrupting or disrupting the communication of legitimate users, selfish users might refuse to contribute to cooperation for self-interests, etc. Those security issues are of great importance and need to be considered for cooperation in DSA. In this thesis, we study security-aware cooperation in DSA. First, we investigate cooperative spectrum sensing in multi-channel scenario such that a user can be scheduled for spectrum sensing and spectrum sharing. The cooperative framework can achieve a higher average throughput per user, which provides the incentive for selfish users to participate in cooperative spectrum sensing. Second, secure communication in CCRN is studied, where the SUs cooperate with the PU to enhance the latter's communication security and then gain transmission opportunities. Partner selection, spectrum access time allocation, and power allocation are investigated. Third, we study risk-aware cooperation based DSA for the multiple channel scenario, where multiple SUs cooperate with multiple PUs for spectrum access opportunities, considering the trustworthiness of SUs. Lastly, we propose an incentive mechanism to stimulate SUs to cooperate with PUs when they have no traffic. The cooperating SUs are motivated to cooperate with PUs to enhance the security of the PUs by accumulating credits and then consume the earned credits for spectrum trading when they have traffic in the future.

Acknowledgements

I would like to express my deepest and sincerest gratitude to my supervisor, Professor Jon W. Mark. It was Professor Mark's invaluable guidance and continuous encouragement that brought me from a graduate student with basic knowledge to a researcher who can tackle the real and challenging problems. Professor Mark has a very high standard on research quality. My weekly meetings with him are always enlightening and rewarding. The strictness, carefulness, and strong commitment that Professor Mark conveyed to me are exactly the essential qualities of an excellent researcher. Professor Mark is and will always be my role model.

I would like to thank Professor Xuemin Shen. His valuable suggestions had significantly improved the quality of my collaborative research with his students and visiting scholars. The weekly group meetings coordinated by Professor Shen provided me an excellent opportunity to broaden my knowledge and improve my presentation skills.

Finally, I would like to thank my parents and my wife for their love, endless support, and encouragement throughout my life

To my dear parents, my son and my wife

Contents

List of Figures

List of Tables

List of Abbreviations

AF	Amplify-and-Forward
BPSK	Binary Phase Shift Keying
BS	Base Station
CCRN	Cooperative Cognitive Radio Network
CR	Cognitive Radio
CRC	Cyclic redundancy check
CRNs	Cognitive Radio Networks
CSI	Channel State Information
DF	Decode and forward
DSA	Dynamic Spectrum Access
DSTC	Distributed Space-Time Coding
NE	Nash Equilibrium
PDF	Probability density function
PHY	Physical layer
PU	Primary User
QPSK	Quadrature Phase Shift Keying
QoS	Quality of service

SU	Secondary User
WRAN	CR-based Wireless Regional Area Network
D	Primary destination
E	Eavesdropper
S	Primary source
R	Relay SU
J	Jammer SU
E	Eavesdropper
D-CSI	The channel state information (CSI) regarding D
E-CSI	The channel state information (CSI) regarding E

List of Mathematical Symbols

α	Time allocation coefficient or bandwidth allocation coefficient
$\bar{R}_{SEC}$	Overall secrecy rate of the PU
h_{ps}^{i}	Channel gain between the PU and SU_i
h_{sb}^{i}	Channel gain between SU_i and the BS
h_{s}^{i}	Channel gain between SU_i and its corresponding receiver
h_{pb}	Channel gain between the PU and the BS
h_{PR}	Channel gain between S and R
h_{RP}	Channel gain between R and D
h_{JP}	Channel gain between J and D
h_{JE}	Channel gain between J and E
h_{RE}	Channel gain between R and E
h_{RR}	Channel gain between R and its corresponding receiver
h_{JJ}	Channel gain between J and its corresponding receiver
N_0	One-sided power spectral density of the additive white Gaussian noise
p	Probability that certain entity behaves well
P_c	Transmission power of PU for cooperation
P_d	Transmission power of PU for the direct transmission

P_s^i	Transmission power of SU_i for both cooperative and secondary transmission
P_{RC}	Transmission power of R for cooperation
P_{JC}	Transmission power of J for cooperation
P_{RS}	Transmission power of R for its own communication
P_{JS}	Transmission power of J for its own communication
P_{max}	Power constraint
R_D	Achievable transmission rate at primary destination D
R_E	Achievable transmission rate at the eavesdropper E
R_{SEC}	Secrecy rate for the primary link
R_{RS}	Achievable rate of R for its own communication
R_{JS}	Achievable rate of J for its own communication
R_{SEC}	Secrecy rate for the primary link
R_c^i	Achievable cooperative rate of the PU when cooperates with SU_i
R_r	Traffic requirement of the PU
R_s^i	Achievable rate of SU_i for the secondary transmission
P'_{max}	Maximum power for cooperation
R_{min}	Minimum required transmission rate of SUs
R_{RC}	Achievable rate at R
$\mathcal{S}$	Primary source
SU_i	The i-th SU
T	Time slot duration
Tr_i	Trust value of SU_i
W	Bandwidth owned by primary users
α_j	Transition rate from state ON to OFF for channel j
β_j	Transition rate from state OFF to ON for channel j

T_{ON}^{j}	Sojourn time for channel j being in ON state
T_{OFF}^{j}	Sojourn time for channel j being in OFF state
δ	Bandwidth owned by primary users
$\boldsymbol{Q}$	Q function
$p_d(i,j)$	Detection probability of SU_i on channel j
$p_f(i,j)$	False alarm probability of SU_i on channel j
$\mathbf{S}_j$	Set of SUs selecting channel j
$F_d(j)$	Cooperative detection probability for channel j
$F_f(j)$	Cooperative false alarm probability for channel j
$F_m(j)$	Cooperative misdetection probability for channel j
$\bar{R}_Q$	Predefined required transmission rate of the PU for the scenario without E-CSI
$\bar{R}_{EX}$	Expected overall transmission rate of SUs
$\bar{R}_{S,i}$	Overall transmission rate of SU_i
$\mathcal{N}$	Set of SUs in the cluster, $\lvert\mathcal{N}\rvert = N$
$\mathcal{M}$	Set of inactive SUs in the cluster, $\lvert\mathcal{M}\rvert = M$
$\mathcal{K}$	Set of channels in the network, $\lvert\mathcal{K}\rvert = K$
$\alpha_i(j)$	Time allocation coefficient when the PU on channel j cooperates with SU_i
$U_p^i(j)$	Utility function of the PU on channel j when cooperating with SU_i
$U_s^i(j)$	Utility function of SU_i when cooperating with the PU on channel j
$P_c^i(j)$	Transmission power of the PU on channel j when cooperating with SU_i
$h_{ps}^i(j)$	Channel gain from PU_j to SU_i
$h_{pb}(j)$	Channel gain from PU_j to the base station
h_{sb}^i	Channel gain from SU_i to the base station
h_s^i	Channel gain from SU_i to the corresponding secondary receiver
Ψ_i	Duration of the rewarding access time of channel i

U_i^j	Utility of SU_i in the congestion game
n_i	Total number of inactive SUs choosing channel i in congestion game
$\zeta(n_i)$	Share of channel i which each SU selecting that channel can obtain
$n(S)$	Congestion vector corresponding to strategy profile S
γ_{sd}	SNR from the direct link (S to D)
γ_d^i	SNR from relay i using Amplify-and-Forward (AF) cooperative protocol
γ_d^j	Interference at D caused by jammer j
γ_e^j	Interference at E caused by jammer j
γ_{se}	SNR at E from the source
γ_e^i	SNR at E from relay i

Chapter 1

Introduction

In recent decades, a massive growth in mobile data has been witnessed, which almost doubles every year. According to Cisco Visual Networking Index (VNI) [2], the mobile data traffic is expected to grow at a Compound Annual Growth Rate (CAGR) of 61 percent from 2013 to 2018. It is predicted that mobile data will continuously grow up to 1000 times by 2020, compared with the volume in the year of 2010 [3]. Therefore, wireless networks are facing the challenges to accommodate such a large volume of data, which is referred to as the 1000x data challenge.

The main factors accounting for the significant growth in mobile data are two-fold: the proliferation of devices and the emerging data-hungry applications [4]. On one hand, with the development of mobile networks, the number of devices also increases exponentially, such as smart phones, tablets, and so forth. The promising machine-to-machine (M2M) application, Internet of things (IoT), Internet of Vehicles (IoV) [5] also lead to more and more connected devices. It is predicted by Qualcomm that 25 billion devices will be connected in 2020 [6]. On the other hand, the data-hungry applications bloom the data traffic, such as image transfer, video streaming, and online gaming. A standard definition movie has 2.49 GB, while a high definition movie has 5.93 GB. It is expected that more and more multimedia-rich applications will emerge and create a tremendous increase in mobile data, which poses an ever-increasing pressure on the network operator to meet the requirements.

Such an exponential growth in mobile traffic and devices imposes huge demands on radio spectrum. While, as a natural resource, radio spectrum is scarce and limited. Nowadays, the spectrum is managed by government agencies (e.g., Federal Communications Commission or FCC) and assigned to licensed users for exclusive use on a long term basis to avoid interference among wireless systems of a large variety. It is recognized that this licensing policy has created a severe shortage of spectrum for unlicensed users. Furthermore, spectrum underutilization by licensed users exacerbates spectrum scarcity. The main reason of spectrum underutilization is that licensed users typically do not fully utilize their allocated bandwidths for most of the time, while unlicensed users are being starved for spectrum availability. Dynamic spectrum access (DSA) is a paradigm created in an attempt to provide high bandwidth to the users and improve spectrum utilization [1] [7] [8]. It can be enabled by cognitive radio (CR), which allows unlicensed users to coexist with licensed users and make use of the underutilized spectrum opportunistically [9] [10].

In dynamic spectrum access or cognitive radio network (CRN)[1], licensed users and unlicensed users are referred to as primary users (PUs) and secondary users (SUs), respectively. With cognitive radio technology, SUs are aware of the radio environment and can select the communication parameters, e.g., carrier frequency, bandwidth and transmit power, to optimize the performance of communications accordingly. Traditionally, SUs perform spectrum sensing before transmission, through which the SUs can identify and exploit the spectrum hole[2] as well as avoid the harmful interference to the PUs. Particularly, the SU scans a certain spectrum range and detects whether the PU is active or not, then selects the available spectrum band for

[1] The term dynamic spectrum access and cognitive radio network is used interchangeably.

[2] That is a band of frequencies assigned to a primary user, which is not being utilized by that user at a specific time and geographic location.

access. During transmission, the SU has to carry out spectrum sensing continuously. When the PU reclaims the frequency band, the SU must refrain from transmitting in the current band and searches for a new band. Thus, spectrum sensing is so critical to both of the primary and the secondary systems, which requires a high detection probability and a low false-alarm probability. However, the outcome of spectrum sensing may be inaccurate due to multipath fading and shadowing , e.g., when the SU is in severe fading or shadowed by buildings while a PU is active in the vicinity. Thus, it fails to detect the PU and then accesses the licensed channel, causing interference to the PU. To deal with these problems, cooperation has been introduced in the CRN. Pertaining to the participation of the PUs, there are mainly two forms of cooperation, i.e., cooperation among unlicensed users and cooperation between SUs and PUs. In the literature, the former is referred to as cooperative spectrum sensing, while the latter is coined as the cooperative cognitive radio networking (CCRN).

1.1 Basics of Cognitive Radio

Cognitive radio (CR) is defined as a radio that can sense the surrounding wireless environments where it operates and adjust the transmission parameters accordingly. To be more precise, FCC gives the definition as follows: *"Cognitive radio: A radio or system that senses its operational electromagnetic environment and can dynamically and autonomously adjust its radio operating parameters to modify system operation, such as maximize throughput, mitigate interference, facilitate interoperability, access secondary markets*." [11].

Two main characteristics that distinguish CR from the traditional wireless radio are cognitive capability and reconfigurability. The former represents the awareness of CR with respect to the transmitted waveform, RF spectrum, communication network, geography, locally available services, user need, security policy and so on, while the latter corresponds to capability of adaption to the obtained information about the wireless environments [10].

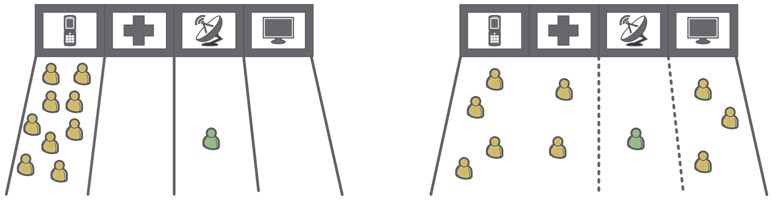
1.1.1 Functions

The main functions of CR include spectrum sensing, spectrum decision, spectrum sharing, and spectrum mobility [1]. Spectrum sensing is a very important function, which should be performed to acquire information from the surrounding environment, such as presence of the PUs and channel availabilities, before transmission [12] [13]. It is necessary for CR to adapt its operational parameters according to the status of the environment. The objectives of spectrum sensing can be classified as follows: i) the operation of unlicensed users must avoid harmful interference to licensed users by either switching to an available band or limiting its interference to licensed users at an acceptable level, and ii) unlicensed users should efficiently and reliably identify the spectrum holes to meet their quality of service (QoS) requirements. Therefore, spectrum sensing is crucial for both the PUs and SUs.

After available channels are detected, spectrum decision is performed to select suitable channels according to the QoS requirement of SUs. The decision is made based on the results of spectrum sensing and the internal policy of the users (e.g., to maximize throughput, reliability, or have the longest transmission time, and so on). Subsequently, the best channel to access is selected among available channels.

When multiple SUs exist, spectrum sharing is necessary, especially for distributed CRN-s. Spectrum sharing refers to the process of sharing the common available channels among multiple SUs. The objective is to utilize the available channels in an efficient and fair way by coordinating the users [14–16].

Since SUs have to vacate the current channel once the presence of PUs is detected, the SUs have to find other available channels to access in order to maintain the ongoing transmissions. This process is referred to as spectrum mobility. The goal is to meet the QoS requirement of SUs by means of choosing the channel to move or sense.



(a) Wireless systems without CR.

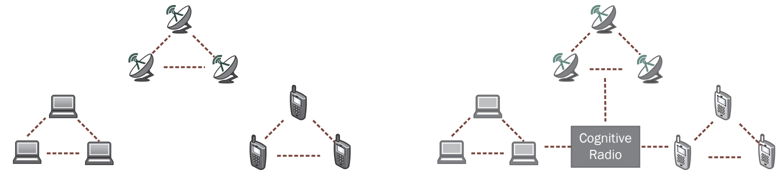
(b) Wireless systems with CR.

Figure 1.1: Dynamic spectrum access.

1.1.2 Applications

Since CR is capable of autonomously adapting its operational parameters (e.g., transceiver parameters) to work in a more efficient way, based on the information acquired from the environment by active monitoring, a large number of promising applications can be facilitated, among which two key applications are identifies: dynamic spectrum access [7, 17–20] and interoperability [21, 22]. Dynamic spectrum access (DSA) refers to the scenario where SUs sense the available channels which are not occupied by PUs, and then access those channels for transmission. Interoperability means that radios can connect different systems operating on different protocols or standards so that they can communicate with each other.

As shown in Fig. 1.1, DSA is the main application, which has received great attention from both academia and industry. The objective of DSA is to efficiently utilize the spectrum to solve the problem of spectrum secrecy, which is the result of the ever increasing mobile devices and the current static spectrum allocation policy. DSA allows SUs to opportunistically utilize the licensed spectrum bands when they are unoccupied. In order to avoid harmful interference to the legacy system, SUs have to carry out spectrum sensing to detect the spectrum holes. Once the available channels are detected, SUs can access for their transmissions. During transmission, spectrum sensing has to be continuously performed to sense the activities of licensed users. When the presence of a PU is detected, the SU vacates the current channel and chooses other channels to sense for transmission opportunities.



(a) Wireless systems without CR.

(b) Wireless systems with CR.

Figure 1.2: Interoperability enabled by cognitive radio.

As the second important application, interoperability has a huge potential impact on the current communication architecture, as shown in Fig. 1.2. It is expected to further affect the personal life of human. Nowadays, we are surrounded by different types of communication systems, e.g., mobile networks, sensor networks, wireless local area network, TV broadcast network, and so on. Those systems are independent and autonomous systems, with different standards, spectrum bands, services, etc. With the technology of cognitive radio, the device can reconfigure itself to communicate with incompatible radios. Specifically, CR first scans the surrounding environment to detect what waveforms or networks are present. Then, it can either reconfigure itself to communicate with the selected network, or it can act as a gateway to connect different systems for communications. By doing so, diverse wireless systems can be connected and communicate with each other.

1.1.3 Network Architecture

With the assistance of CR technology, SUs can coexist with PUs and utilize the temporarily unused spectrum bands owned by PUs. Therefore, the CRN is comprised of two components: the primary network and the secondary network, as shown in Fig. 1.3. Both networks can be deployed in either a centralized or ad hoc mode, where communications are coordinated by central nodes such as base stations or communications are carried out in a peer-to-peer fashion, respectively.

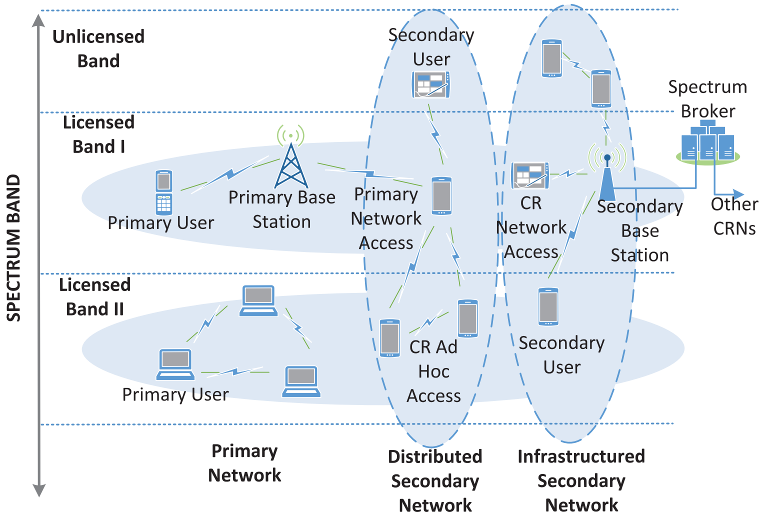


Figure 1.3: Cognitive radio network architecture [1].

The primary network corresponds to an existing network which holds a license for operation in certain spectrum bands. This network has the exclusive privilege to access the assigned spectrum bands. If the primary network has an infrastructure, PUs can be coordinated to access the network through the primary base station. In addition, the primary network might be deployed in ad hoc mode, where PUs communicate with each other without any infrastructure. The PUs' transmissions occurring in the primary network should be protected from being interfered by secondary networks. Generally speaking, PUs and primary base stations are typically not equipped with CR functions. Therefore, it is the responsibility of SUs to sense the channel before transmission and vacate the occupied channel when PUs re-appear.

The secondary network, composed of a set of SUs, does not have the license to operate in any licensed spectrum bands. The secondary network can also be classified into two types: infrastructure-based and ad hoc [23]. An infrastructure-based secondary network has a central controller, e.g., a secondary base station or an access point. Opportunistic spectrum access by SUs is usually coordinated by the central controller. Whereas in an ad hoc secondary network, SUs can communicate with each other via multi-hop wireless links on either the licensed or the unlicensed spectrum bands. Both SUs and secondary base stations are equipped with CR technology.

When some primary systems are willing to lease the spectrum for monetary rewards. The secondary network can also pay a certain amount of money to gain the temporary exclusive rights to use the spectrum. To this end, a spectrum broker is needed to facilitate the spectrum trading.

1.2 Spectrum Sensing

The objective of spectrum sensing is to check the channel availability in order not to adversely affect the performance of PUs [24] [25]. Since spectrum holes can be in specific time, or a frequency band, or at a spatial location, spectrum sensing can be performed in the time, frequency, and space domains. Although the main job of spectrum sensing is to obtain channel availability information, it can also be used to determine the types of signals occupying the spectrum, which may include modulation, carrier frequency, waveform, bandwidth, etc.

1.2.1 Sensing Approaches

Energy Detection

Energy detection is based on the fact that the energy of the signal is usually larger than that of noise. To determine the existence of PUs, the energy detector compares its output (e.g, the average or the total energy of the observed samples) with a predefined threshold, which is derived based on the statistics of noise. If the output is above the threshold, then the energy detector makes the decision that the PU is present; otherwise, it makes the decision that the PU is absent. Energy detection is the most common type of spectrum sensing technology because of the following reasons: i) it is simple to implement; ii) it does not require any a priori information regarding the PUs' signal; iii) the detection time is relatively short [26–29].

Cyclostationarity Feature Detection

Typically, there are certain inherent features associated with the signal transmitted by PUs, which can be exploited to detect the presence of PUs. Considering that for most communication systems the signals are cyclostationary due to the periodicity in the signals or the statistics, while the noise is usually assumed as a wide-sense stationary process without correlation; the cyclostationary features can be leveraged to distinguish the PUs' signal and noise [30, 31]. Through the cyclostationary feature detection, features of PUs' signal can be extracted to determine the existence of PUs. Compared with energy detection, cyclostationary feature detection can provide better performance for the scenario of low SNR, with the price of high complexity. Moreover, a priori knowledge regarding the characteristics of PUs' signal is needed.

Matched Filter Detection

In most wireless systems, pilot bits are periodically transmitted for channel estimation, synchronization, and so on. The pilot bits are public information, which can be used to detect the presence of PUs. When the knowledge about the transmitted signal is available in the first place, matched filter detection will be the optimal detection approach, because it can correlate the received signal with the known primary signal for the detection. Match filter has the advantage of short detection time and it works well in the low SNR regime; but it requires perfect knowledge of the characteristics of PUs' signals, e.g., modulation type, bandwidth, center frequency, etc. Any imperfection about the PU's signal will lead to severe degradation in the detection performance.

1.2.2 Limitations

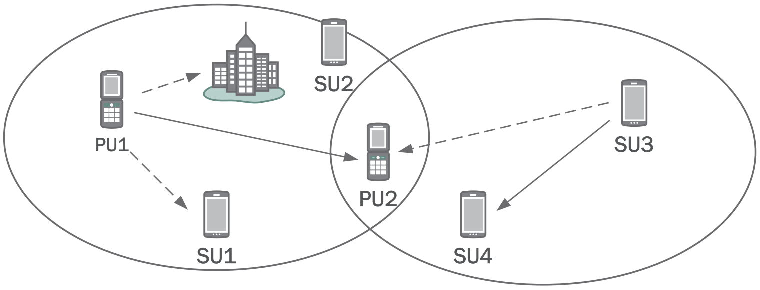


Figure 1.4: Limitations of spectrum sensing.

Spectrum sensing is critical for DSA. However, the performance of sensing is limited by several factors, including multipath fading, shadowing, primary receiver uncertainty problem [32]. When the SU is experiencing multipath fading or shadowing, the reception of PU's signal will be significantly degraded, which adversely affects the detection accuracy. In addition, for SUs which are out of the transmission range of the primary transmitter, they cannot detect the PU's transmission. Therefore, when those SUs start to transmit, harmful interference will be created at the primary receiver, if the primary receiver is unfortunately located within the transmission range of the SUs, which gives rise to primary receiver uncertainty problem. As illustrated in Fig. 1.4, when PU_1 is transmitting data to PU_2, SU_1 can receive signal of PU_1 and know the presence of PUs. However, SU_2 cannot detect PU_1 because the building blocks the signal from PU_1. For SU_3, since it is outside of the transmission range of PU_1, it cannot detect the PU's transmission and therefore it starts its own transmission, which will cause interference to the primary receiver, i.e., PU_2. Moreover, spectrum sensing consumes energy to detect the spectrum holes and has to be continuously carried out during the transmission to detect PUs's activities.

1.2.3 Cooperation in DSA

To overcome the aforementioned issues, user cooperation can be leveraged, mainly in two forms: cooperative spectrum sensing and cooperative cognitive radio networking (CCRN) [33]. For the former, the cooperation is carried out among SUs, where multiple SUs cooperate with each other to enhance the detection performance. For the latter, the cooperation is carried out between SUs and PUs, where SUs cooperate with PUs to improve the transmission performance of the latter and then gain spectrum access opportunities as a reward.

Cooperative Spectrum Sensing

Cooperative spectrum sensing that relies on spatial diversity and multiuser diversity can improve the detection performance in terms of increasing the detection probability and reducing the false-alarm probability [34] [35], as shown in Fig. 1.5. Instead of using individual decision, multiple SUs share the sensing results to make a combined decision through cooperation. Particularly, each SU performs local sensing and reports the detection results to a fusion center to make a final decision in a centralized fashion, or exchange the local detection results among themselves in a distributed fashion. Through cooperation, SUs share their sensing results and make a combined cooperative decision derived from the spatially collected observations, which can overcome the deficiency of individual observations at each SU. It has been shown that cooperative spectrum sensing can effectively combat multipath fading and shadowing, mitigate the receiver uncertainty problem, and hence significantly improve the detection performance [36–39].

Typically, for centralized cooperative spectrum sensing, it is carried out following a three-step process. First, individual SUs perform local sensing separately. Then, all the cooperating SUs forward the sensing results to the fusion center, which might be the base station, a common receiver and so on. Last, the fusion center combines all the received sensing results and makes a

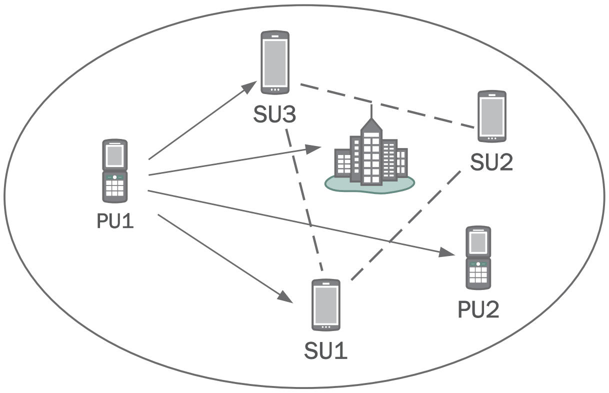


Figure 1.5: Cooperative sensing.

final decision on whether the PU is present or absent on the observed band. For the distributed cooperative spectrum sensing, where there is no fusion center, SUs exchange the detection results among themselves and then converge to a final decision after several iterations.

Cooperative Cognitive Radio Networking

Cooperative communications have been extensively studied in the literature. The basic idea behind cooperative communication is as follows: when the source transmits message to the destination, the nodes in between can also receive it due to the broadcast nature of the wireless media. Those nodes can process the received signal and retransmit to the destination. Therefore, the destination can make use of the multiple copies of the message to create spatial diversity to improve the reception performance. It is recognized that cooperative communications can improve the transmission rate, save energy, enhance the reliability and so on.

Because of the benefits of cooperative networking, there is a strong interest to introduce cooperative networking to the CRN to deal with challenges of spectrum sensing and better explore transmission opportunities. In cooperative cognitive radio networking (CCRN), SUs cooperate with PUs to improve the latter's performance in terms of transmission rate, reliability, energy efficiency and so on, and in return gain transmission opportunities [40–50]. Specifically,

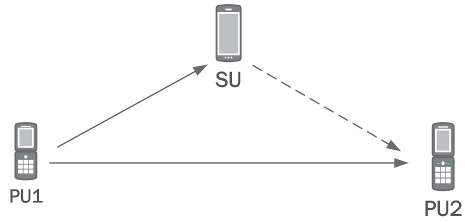


Figure 1.6: Cooperative cognitive radio networking.

an SU acts as a relay to improve a PU's transmission performance. Then, the PU grants a period of time to the SU as a reward, in which the SU can access the spectrum bands for transmissions. By leveraging cooperation between PUs and SUs, a ”win-win” situation is created, where the PU's performance is enhanced and SUs can access the channel in the rewarding time. By this emerging cooperative networking, SUs can be relieved from the burden of spectrum sensing.

1.3 Motivation and Research Contributions

1.3.1 Motivations

If all the SUs are well-behaved, cooperation can bring various benefits, e.g., cooperation in spectrum sensing can increase the detection probability and reduce the false alarm probability, while CCRN can create more transmission opportunities and relieve SUs from the burden of spectrum sensing, which is energy consuming and sometimes inaccurate, etc. However, it might not be always true that all the users are well-behaved in reality. Especially in an untrusted environment, there may exist some dishonest users, even malicious ones. In such a scenario, cooperation could incur critical security issues, e.g., the malicious or compromised users might participate in cooperation, corrupting or disrupting the normal operation of DSA.

For cooperative spectrum sensing, most previous works have focused on the cooperation scheme design to achieve accurate sensing results [37] [51] [39] [52] [53]. However, in an untrusted, even hostile environment, malicious users might launch different attacks to disturb the detection, then jeopardize the operations in DSA. For instance, malicious users might transmit signals presenting similar characteristics to those of PUs or just send jamming signals to the target channel to interfere with the sensing process and significantly reduce the throughput of legitimate SUs. The former is usually referred to as primary user emulation (PUE) attack, while the latter is called jamming attack. Moreover, the malicious user might send false sensing report to the fusion center, so as to mislead the spectrum sensing results and severely degrade the performance of cooperative sensing [38], which is called false sensing report attack. The countermeasures for those two attacks can be found in [54] [55]. In addition, one fundamental security issue, i.e., the selfishness need to be considered as well. For instance, in cooperative sensing, all the SUs are assumed to be cooperative, which might not be true in reality. Since the user consumes energy to participate into cooperation and it may not have data to transmit or not be the beneficial owner who accesses the channel later. The issue of how to stimulate cooperation in spectrum sensing needs to be studied.

For the works in CCRN, all the cooperative frameworks only consider a friendly environment, where users are assumed trustworthy and well-behaved [40, 41, 44, 46, 56–58]. However, in such an untrusted environment, dishonest users, even malicious ones, might be selected for cooperation. Consequently, the performance can be compromised. For instance, a malicious SU might be selected for cooperation, then it can alter the packets from the PU or fabricate packets and then forward them to the destination. A dishonest SU may not obey the cooperation rule during the cooperative transmission to pursue more self-benefits, e.g., it may transmit its own packets instead of relaying the packets from the PU. Without considering these security threats, the PU may choose an untrustworthy SU for cooperation, which may cause failure in the cooperation and degrade its QoS. Thus, security needs to be considered for this emerging cooperative networking.

As the explanation above, cooperation can encounter various security issues, which should be taken into consideration. At the same time, security also brings opportunities for cooperation, which can be explored to implement an alternative cooperative framework. Considering that when the primary sender transmits information to its receiver, there may exist some eavesdroppers. Due to the broadcast nature of wireless communication, these eavesdroppers can easily overhear the ongoing transmission. This not only hurts the confidentiality of communications, but also exposes the risks and vulnerabilities that a malicious user can exploit to launch attacks. To secure the communication effectively, there is a novel approach at the physical (PHY) layer, which exploits the characteristics of the wireless channel to secure the transmission. For the CRN, the PUs can choose friendly SUs for cooperation to enhance the security of the primary link. In return, the cooperating SUs can access the channel as a reward for their own transmission. For such a cooperation scheme, the issues related to the relay selection and resource allocation need to be investigated.

Lastly, all the literature works in CCRN study the cooperation when the SUs have traffic to send. To transmit their traffic, SUs help PUs to improve the latter's transmission performance, and in return access the channel during the rewarding time slots. However, when SUs have no traffic at that time, they might not be interested to cooperate with PUs. How to simulate cooperation in such a scenario needs to be studied.

In a nutshell, security is indispensable to be taken into consideration, when cooperation is performed in DSA. Therefore, the security aspects of cooperation in DSA need to be extensively investigated.

1.3.2 Contributions

The research objective is to develop cooperation schemes in DSA to improve the spectrum efficiency and the accuracy of sensing, taking into consideration the security issues. Firstly, cooperative spectrum sensing in a multi-channel CRN is studied, where multiple SUs cooperate with each other to detect unused channels and then share them. Specifically, for spectrum sensing, the objective of the CRN is to maximize the expected available time while keeping the interference to PUs under a predefined level. With the dynamics in the channel usage characteristics and the detection capacities, the coordination problem is formulated as a nonlinear integer programming problem. To find the solution efficiently, the deterministic optimization problem is first transformed to an associated stochastic optimization problem, which is then solved by cross-entropy (CE) method of stochastic optimization. Then, the sharing of the available channels by SUs after sensing is modeled by a channel access game, based on the framework of weighted congestion game. An algorithm for SUs to select access channels to achieve Nash equilibrium (NE) is proposed. The proposed cooperative framework can achieve a higher throughput per user, which provides the incentive for SUs to participate into cooperation.

Secondly, cooperative cognitive radio networking is studied, which aims to enhance the security of PUs and provide transmission opportunities to SUs. Two types of cooperation schemes are proposed, whereby the PU either cooperates with two individual SUs or a cluster of SUs, which are referred to as relay-jammer (R-J) scheme and cluster-beamforming (C-B) scheme, respectively. In R-J scheme, two individual SUs act as a relay and a friendly jammer to improve the PU's secrecy; In return, the PU allocates a fraction of access time for SUs' transmission. To achieve the maximum secrecy rate, joint time and power allocation is considered. Particularly, the cooperating relay and jammer determine the optimal transmission power, while the PU decides the optimal time allocation strategy. In C-B scheme, the PU cooperates with a cluster of SUs to enhance the secrecy of the primary link via collaborative beamforming, where three different approaches are proposed for the scenarios with one eavesdropper, with multiple eavesdroppers, and without eavesdroppers' information, respectively. To maximize the secrecy rate, weight selection and time allocation are also studied.

Thirdly, we study risk-aware cooperation in a multi-channel CRN, whereby multiple PUs operating over different channels choose trustworthy SUs as relays to improve throughput, and in return SUs gain transmission opportunities. To study the multi-channel cooperative spectrum access, cooperation over a single channel is investigated first, which involves a PU selecting a suitable SU and granting a period of access time to the selected SU as a reward, considering trustworthiness of SUs. The above procedure is modeled as a Stackelberg game, through which access time allocation and power allocation are obtained. Based on the above results, cooperation over multiple channels is studied from the perspective of the secondary network and a secondary network-centric cluster-based (SCC) scheme is proposed. In SCC scheme, SUs first form a cluster to share the channel state information (CSI), and the best SUs are selected for cooperation with PUs over different channels to obtain the maximum aggregate access time for the secondary network. Then, SUs share the obtained resource using congestion game and quadrature signalling.

Lastly, we study the user cooperation when SUs have no traffic. We propose a cooperative framework, whereby the PU selects multiple SUs and stimulates them by granting an amount of reward to transmit message securely in the presence of multiple eavesdroppers. The earned credits can be utilized by SUs for spectrum leasing in the future when they have traffic. In other words, the SUs can earn credits through cooperation with PUs and consume credits in spectrum trading market when needed. In the cooperative framework, multiple cooperative SUs, acting as relays and jammers, are selected by the PU using greedy or cross-entropy based approaches. Then, the PU and the partners negotiate for the payment and transmission power, which is modeled as a two-layer game. At the top layer, a buyer-seller game is utilized, where the PU buys the service provided by the partners. At the bottom layer, all the partners share the reward by determining their transmission powers in a distributed way, which is formulated as a non-cooperative power selection game. By analyzing the game, the partners can determine the transmission powers for cooperation, while the PU can select the best payment.

1.4 Outline of the Thesis

This thesis is organized as follows: Chapter 2 studies cooperative spectrum sensing for a multi-channel CRN. The user scheduling and spectrum sharing are devised. Chapter 3 and Chapter 4 focus on cooperation between SUs and PUs for access. In Chapter 3, the SUs cooperate with the PUs to enhance the security of the PUs and gain spectrum access opportunities. Chapter 4 studies risk-aware cooperation in a multi-channel CRN for access, taking into consideration the trustiness of SUs. Chapter 5 investigates cooperation with PUs for credits. The partner selection and payment determination are studied. Finally, Chapter 6 concludes this research and outlines some further research topics.

Chapter 2

Cooperative Spectrum Sensing in Multi-Channel CRNs

In this chapter, we study dynamic spectrum sensing in a multi-channel environment, which integrates cooperative spectrum sensing and spectrum sharing [59]. Due to hardware limitation, each SU can only choose one channel in spectrum sensing and access one channel at a time for spectrum sharing. The objective of the CRN is to maximize the expected available time of all the channels, under the constraint that the PUs are sufficiently protected. To this end, SUs decide which channels to be sensed. Different from the existing works, a more general scenario is considered in this chapter, where the main differences are: i) the detection performance of individual SU depends on the channel condition, which may differ from user to user; and ii) the channels are considered to present different usage characteristics, such as average sojourn idle time and the probability of being idle. Due to those factors, the channel selection problem becomes more challenging. We formulate the channel selection problem as a nonlinear integer programming problem. Depending on the problem formulation, we first define an associated stochastic optimization problem of the original deterministic optimization problem. Then, we apply the cross-entropy (CE) method of stochastic optimization to find the channel selection solution efficiently. After spectrum sensing, we study spectrum sharing, which is modeled using a more general game based on the framework of weighted congestion game. SUs with different channel conditions are assigned different weights, with the purpose of favoring SUs with better channel conditions. In the proposed game, each SU chooses a channel from the available channel set to maximize their own interests. An algorithm that can help SUs to achieve Nash Equilibrium (NE) is proposed. It is proved that the algorithm can achieve NE. Simulation results are provided to show the performance of the proposed algorithms.

2.1 Literature Review

In the literature, many works on cooperative spectrum sensing for the single channel case have been reported [37, 39, 51, 52, 60]. The authors in [37] propose a cooperative spectrum sensing scheme to improve the spectrum sensing in the presence of shadowing or fading effects. In [52], the authors propose a relay-based cooperation mechanism, which is a two-user cooperative spectrum sensing scheme. This cooperation scheme shows that the detection time can be reduced. The authors in [51] propose a selective-relay based cooperative sensing scheme with no dedicated reporting channel. In [60], they also study the sensing and transmission trade-off and show that the performance in terms of the spectrum hole utilization can be significantly improved using cooperative relaying. An optimal sensing scheme for the multiuser cooperation is proposed in [39]. Since there usually exist multiple channels in the system, DSA in multi-channel CRNs has drawn increasing attentions recently.

For *spectrum sensing* in multi-channel scenarios, from the single user's perspective, the quickest detection is studied with the objective of finding an idle period from multiple channels as fast as possible using the theory of partially observable Markov decision process (POMDP) in [61] and dynamic programming in [62], respectively. Besides that, from the system's perspective, the issue regarding how to assign SUs to different channels for maximizing the system performance are studied in [63–67]. In [63], heuristic channel selection algorithms are designed for cooperative spectrum sensing to maximize the number of available channels. In [65], the authors study this issue to maximize the throughput of SUs. However, a common assumption is made that all the SUs have the same sensing performance for all channels. In practice, the sensing performance of SUs depends on the channel conditions from the PUs to the SUs, which usually differs from user to user. Moreover, the channel usage characteristics of PUs are not taken into consideration in the existing literature.

For *spectrum sharing*, diverse approaches have been proposed in the literature. In [68], the auction game is utilized, where SUs, PUs, and spectrum bands, are modeled as auctioneers, bidders and bidding articles, respectively. In [69], SUs share the available channels by accessing the channel with equal probability. In [70], the spectrum access based on multi-channel ALOHA protocol is studied using the theory of potential games, without considering available duration of channels. In [71], channel allocation is studied using a stable marriage game, which aims to find the most stable pairings between the users and channels. Recently, congestion game has gained much attentions, which is a prominent approach to model the scenario where multiple rational users share a set of common resource. It has been utilized to solve the issue of spectrum sharing in [19,72,73], where congestion game is utilized for SUs to share the channels and each SU chooses one channel for accessing to maximize its own utility. However, all SUs are treated equally, ignoring their channel conditions.

To simulate cooperative spectrum sensing in multi-channel CRNs, spectrum sensing and spectrum sharing needs to be considered jointly. By carefully designing spectrum sensing and sharing strategies, individual SU can be motivated to participate into cooperative spectrum sensing. In this chapter, we propose a cooperative framework to improve the performance of each individual SU so that selfish SUs are interested in the cooperation, which integrates user scheduling for spectrum sensing and spectrum sharing, considering i) various detection capabilities of individual SUs due to different the channel conditions and ii) dynamic of channel

Table 2.1: Summary of important symbols.

Symbol	Definition
N	The number of SUs
K	The number of channels
α_j	Transition rate from state ON to OFF for channel j
β_j	Transition rate from state OFF to ON for channel j
T_{ON}^{j}	Sojourn time for channel j being in ON state
T_{OFF}^{j}	Sojourn time for channel j being in OFF state
P_{PU}	The transmission power of the PU
M	The number of samples in observation period
δ	The detection threshold
Q	Q function
$h_{i,j}$	Average channel gain from the PU_j to SU_i
σ^2	Variance of the Gaussian noise
$p_d(i,j)$	Detection probability of SU_i on channel j
$p_f(i,j)$	False alarm probability of SU_i on channel j
$\overline{\gamma}_{i,j}$	Average received SNR at SU_i from PU_j
$\mathbf{S}_j$	Set of SUs selecting channel j
$F_d(j)$	Cooperative detection probability for channel j
$F_f(j)$	Cooperative false alarm probability for channel j
$F_m(j)$	Cooperative misdetection probability for channel j

usage characteristics in terms of average sojourn idle time and the probability of being occupied.

2.2 System Model

2.2.1 Network Architecture

We consider a cognitive radio network, where the SUs do not own any spectrum and can only opportunistically access the unused spectrum of the PUs for transmission. The amount of spectrum accessible to the SUs is further divided into a set of channels, each of which has a fixed amount of frequency bandwidth.

In the network, there exist K licensed bands (channels) which allow PUs to transmit simul-

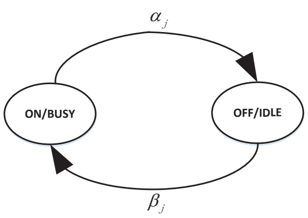


Figure 2.1: ON-OFF model for a given channel.

taneously. Suppose that a PU operates in a channel, which can be either active or inactive. In the same area, N SUs ($N \geq K$) seek for transmission opportunities. In order to avoid interference to the PUs, the SUs perform spectrum sensing before transmission to detect the unused channels.

2.2.2 Channel Usage Characteristics

Similar to [74], an ON-OFF channel usage model is applied to model the status of each channel. The status of the channel alternates between ON (busy) and OFF (idle). The SU can access the channel only when it is in the state OFF. Suppose that PU_j operates over channel j and the state of each channel changes independently. Denote by α_j the transition rate for channel j ($1 \leq j \leq K$) from state ON to state OFF and β_j vice versa. Then, the two-state Markov chain in Fig. 2.1 can describe the status of a given channel. Note that the channel usage characteristics may not be the same for all the channels. In other words, α_i and β_i for channel i are not necessarily the same as α_j and β_j for channel j.

2.2.3 Individual Spectrum Sensing

Spectrum sensing is carried out to detect the status of the channels. Let H_1 denote the state that the PU is present in the channel of interest and H_0 denote the state that the PU is absent. In the literature, popular detection techniques include energy detection, cyclostationary detection, and matched filtering. In this work, we adopt energy detection due to its simplicity and minimal time overhead (typically less than 1 ms). When energy detector is adopted in spectrum sensing, the detection probability p_d and the false alarm probability p_f are defined as

$$p_d = Pr(D > \delta | H_1),\ p_f \ \ = Pr(D > \delta | H_0) \tag{2.1}$$

where δ is the detection threshold and D is the test statistic. In particular, $D = \frac{1}{M}\sum_{n=1}^{M}|y(n)|^2$, where M is the number of samples in an observation period and $y(n)$ is the n-th sample of the received signal.

Without loss of generality, similar to [12], we focus on the case of the complex-valued PSK signal and Circular Symmetric Complex Gaussian (CSCG) noise. According to [12], the false alarm probability of SU_i for channel j can be given by

$$p_f(i,j) = \mathcal{Q}((\frac{\delta}{\sigma^2} - 1)\sqrt{M}) \tag{2.2}$$

where $\mathcal{Q}(\cdot)$ is the complementary distribution function of the standard Gaussian. We consider the Neyman-Pearson criterion [75], where the false alarm probability is fixed. In other words, the false alarm probabilities for all SUs are the same and denoted by p_f for simplicity. Therefore, all SUs have the same value of δ.

The detection probability of SU_i for channel j is calculated as follows:

$$p_d(i,j) = \mathcal{Q}((\frac{\delta}{\sigma^2} - \overline{\gamma}_{i,j} - 1)\sqrt{\frac{M}{2\overline{\gamma}_{i,j}+1}}) \tag{2.3}$$

where $\overline{\gamma}_{i,j}$ is the average received signal-to-noise ratio (SNR) from PU_j at SU_i. In particular, $\overline{\gamma}_{i,j} = \frac{P_{PU}h_{i,j}}{\sigma^2}$, where P_{PU} is the transmission power of the PU, $h_{i,j}$ is the average channel gain from PU_j to SU_i, and σ^2 is the variance of the Gaussian noise.

Given $p_f(i,j)$, based on (2.2) and (2.3), the detection probability $p_d(i,j)$ can be calculated as follows:

$$p_d(i,j) = Q(\frac{1}{\sqrt{2\overline{\gamma}_{i,j}+1}}(Q^{-1}(p_f(i,j)) - \sqrt{M}\gamma_{i,j})). \tag{2.4}$$

2.2.4 Cooperative Spectrum Sensing

In cooperative spectrum sensing, SUs cooperate with each other to improve the sensing performance. Specifically, SUs share the sensing results to output a combined decision on whether the PU is present or absent using a decision fusion rule. The decision rules include AND rule, OR rule, the soft combination rule, or the majority rule. In order to minimize the communication overhead and transmission delay, SUs only share their final 1-bit decisions (e.g., bit 0 and 1 represent the idle and busy states, respectively) rather than their decision statistics. When OR rule is adopted, PUs are considered to be present if at least one SU claims the presence of PUs. Suppose that each SU selects a channel for sensing at one time and let $\mathbf{S}_j$ be the set of SUs selecting channel j. Then, the cooperative detection probability and the cooperative false alarm probability can be given as follows:

$$F_d(j) = 1 - \prod_{i \in \mathbf{S}_j}(1 - p_d(i,j)) = 1 - \prod_{i \in \mathbf{S}_j} p_m(i,j) \tag{2.5}$$

$$F_f(j) = 1 - \prod_{i \in \mathbf{S}_j}(1 - p_f(i,j)) = 1 - \prod_{i \in \mathbf{S}_j} p_s(i,j) \tag{2.6}$$

where $p_m(i,j) = Pr(D < \delta|H_1) = 1 - p_d(i,j)$ and $p_s(i,j) = Pr(D < \delta|H_0) = 1 - p_f(i,j)$. The cooperative misdetection probability F_m^j is defined as the probability that the presence of PU is not detected, i.e., $F_m^j = 1 - F_d^j$.

If AND rule is adopted, PUs are considered to be present if all the SUs report the result of presence. The cooperative detection probability and the cooperative false alarm probability are respectively given by

$$F_d(j) = \prod_{i \in \mathbf{S}_j} p_d(i,j),\ F_f(j) = \prod_{i \in \mathbf{S}_j} p_f(i,j). \tag{2.7}$$

Note that in spectrum sensing, adopting the AND rule is more aggressive for SUs, while adopting the OR rule is more conservative. Adopting AND rule leads to a smaller false alarm probability, which means SUs are more aggressive to explore the spectrum access opportunities, while adopting OR rule results in a greater detection probability, which means SUs are more conservative to explore the spectrum access opportunities [76].

2.3 Spectrum Sensing in Multi-Channel CRNs

From the point of view of the SUs' interests, SUs act more aggressively in spectrum sensing and hence AND rule is adopted. The objective is to maximize the expected available time of all the channels, under the constraint that the PUs are sufficiently protected. In the following, the channel selection problem is formulated first. Then, the problem is solved based on a cross-entropy (CE) approach.

2.3.1 Problem Formulation

Denote the sojourn times of ON state and OFF state for channel j by T_{ON}^j and T_{OFF}^j, respectively, which are assumed to follow exponential distributions with means given by

$$\overline{T}_{ON}^j = \frac{1}{\alpha_j},\ \overline{T}_{OFF}^j \ = \frac{1}{\beta_j}. \tag{2.8}$$

The probabilities that channel j is in ON state and OFF state are denoted by P_{ON}^{j} and P_{OFF}^{j}, respectively. P_{ON}^{j} and P_{OFF}^{j} can be calculated as

$$P_{ON}^{j} = \frac{\beta_j}{\alpha_j + \beta_j},\ P_{OFF}^{j} \ \ = \frac{\alpha_j}{\alpha_j + \beta_j}. \tag{2.9}$$

If channel j is sensed to be in the OFF state when it is actually idle, the SUs have an average period of $\overline{T}_{OFF}^{j}$ to access. If channel j is sensed to be in the OFF state when it is busy in fact, the SUs will access the channel, interfering with the PUs.

When channel j is detected to be in OFF state and it is actually idle, on average, the SUs have $\overline{T}_{OFF}^{j}$ for access. Further, we define a channel selection matrix $\mathbf{I} = (I_{i,j})_{N\times K}$, where $I_{i,j} = \{0, 1\}$ indicates whether or not SU_i selects channel j for sensing. When $I_{i,j} = 1$, SU_i selects channel j for sensing, and vice versa. Based on $\mathbf{I}$, the set of SUs choosing channel j can be determined by $\mathbf{S}_j = \{SU_i, I_{i,j} = 1\}$. The objective for SUs is to maximize the total average available time, which can be formulated as follows:

$$\begin{aligned}
\max_{\mathbf{I}} \sum_{j=1}^{j=K} & \overline{T}_{OFF}^{j} P_{OFF}^{j} (1 - F_f(j)) \\
s.t. \sum_{j=1}^{j=K} & I_{i,j} \leq 1, i \in \{1, 2, ..., N\} \\
& (1 - F_d(j)) P_{ON}^{j} \leq P_i \\
& I_{i,j} = \{0, 1\}
\end{aligned} \tag{2.10}$$

where P_i is the probability of inference to the PU over channel i.

By using exterior point method which permits the variables to violate the inequality constraint during the iterations, the constraint that $(1 - F_d(j))P_{ON}^{j} \leq P_i$ can be removed. Then, the above problem can be transformed into the following format:

$$\begin{aligned} &\max_{\mathbf{I}} \sum_{j=1}^{j=K} [\overline{T}^{j}_{OFF} P^{j}_{OFF}(1 - F_f(j)) - A(F_d(j))U_0(1 - F_d(j))P^{j}_{ON}] \\ &\quad s.t. \sum_{j=1}^{j=K} I_{i,j} \leq 1, i \in \{1, 2, ..., N\} \\ &\quad I_{i,j} = \{0, 1\} \end{aligned} \tag{2.11}$$

where $U_0 > 0$ is a linear penalty factor when the constraint $(1 - F_d(j))P^j_{ON} \leq P_i$ is violated. $A(F_d(j))$ is the indicator function, where $A(F_d(j)) = 1$ when $(1 - F_d(j))P^j_{ON} \geq P_i$, and $A(F_d(j)) = 0$, otherwise.

In what follows, we apply the C-E method of stochastic optimization to solve the above problem.

2.3.2 Cross-Entropy Based Approach

Cross-Entropy

The Cross-Entropy (C-E) method was first introduced to estimate the probabilities of rare events in complex stochastic networks [77]. It was realized that a simple cross-entropy modification of C-E method could also be used to solve difficult combinational optimization problems. In C-E method, the deterministic optimization problem should be translated into a related stochastic optimization problem, where the rare event simulation techniques similar to [77] can be utilized. In other words, the main idea behind the C-E method is to define for the original optimization problem an associated stochastic problem (ASP) and then efficiently solve the ASP based on an adaptive scheme. It sequentially generates random solutions which converge stochastically to the optimal or near-optimal one.

C-E algorithm:

The basic idea of C-E algorithm is to generate a random data sample according to a specified stochastic policy, and update the stochastic policy based on the outcome of the sample to produce a ”better” sample in the next iteration. Algorithm 1 presents the detailed procedure of channel selection, which consists of five main steps as follows.

Define the strategy space $\mathbb{S}$ for SUs as follows:

$$\mathbb{S} := \{ch_1, ch_2, ..., ch_K\}, \tag{2.12}$$

where each SU can only choose one channel from $\mathbb{S}$. Define the probability vector associated with the strategy space as follows:

$$\mathbb{P}_t^i := \{p_{1,t}^i, p_{2,t}^i, ..., p_{K,t}^i\}, \sum_{j=1}^{K} p_{j,t}^i = 1, \tag{2.13}$$

where $\mathbb{P}_t^i$ denotes the stochastic policy of SU_i on the strategy space $\mathbb{S}$ at t-th iteration, and $p_{j,t}^i$ denotes the probability that SU_i chooses channel j at t-th iteration.

1. (Initialization). Set the iteration counter $t := 1$. Set the initial stochastic policy $\mathbb{P}_0^i$ of all SUs to be a uniform distribution on the strategy space $\mathbb{S}$. In other words, for each SU, it picks the strategy from the strategy space uniformly, with equal probability $1/K$.

2. (Generation samples). Based on the stochastic policy of all SUs, Z samples of the strategy vector are generated, which can be given as follows:

$$\mathbb{S}^i(z) := \{I_{i,1}(z), I_{i,2}(z), ..., I_{i,K}(z)\}, \tag{2.14}$$

where $\mathbb{S}^i(z)$ is the z-th strategy vector of SU_i with only one element to be ”1” and the rest are "0". The probability for the $I_{i,j}$ to be "1" is $p^i_{j,t}$.

3. (Performance evaluation). Substitute the samples into (2.11) to calculate the utilities $U(z)$. Arrange the $U(z)$ in a nonincreasing order according to the values, i.e., $U^1 \geq U^2 \geq ... \geq U^Z$. Let υ be the $(1-\rho)$-th sample, i.e., $\upsilon = U_{\lceil(1-\rho)Z\rceil}$, where ρ is the percentage of samples obsolete at each iteration and $\lceil\cdot\rceil$ is the ceiling function.

4. (Stochastic policy update). Based on the same sample, calculate $\mathbb{P}^i_t := \{p^i_{1,t}, p^i_{2,t}, ..., p^i_{K,t}\}$ using the following equation:

$$p^i_{j,t} = \frac{\sum_{z=1}^{N} X_{U^z \geq \upsilon} I_{i,j}(z) = 1}{\sum_{z=1}^{N} X_{U^z \geq \upsilon}}, \tag{2.15}$$

   where $X_{U^z \geq \upsilon}$ is defined as follows:

$$X_{U^z \geq \upsilon} = \begin{cases} 1 & U^z \geq \upsilon \\ 0 & \text{otherwise} \end{cases} \tag{2.16}$$

5. If the stopping criterion is met, which is the maximum number of iterations (i.e., T), then stop; otherwise increase the iteration counter t by 1, and reiterate from step 2.

2.4 Spectrum Sharing in Multi-Channel CRN

After spectrum sensing, available channels can be detected. Subsequently, SUs start the process of spectrum sharing. In this section, based on weighted congestion game, a channel access game is utilized to model the behavior of SUs during spectrum sharing. A brief review of congestion game is given first, followed by the proposed channel access game. Finally, a channel access algorithm is proposed for SUs to achieve NE in spectrum sharing.

Algorithm 1 Channel Selection Algorithm

```
// **Initialization**
$p^i_{j,t} = 1/K$.
for $t = 1 : T$ do
    for $z = 1 : Z$ do
        for $n = 1 : N$ do
            Generate samples of the strategy vector.
        end for
    end for
    for $z = 1 : Z$ do
        Calculate the utilities $U(z)$ according to (2.11).
    end for
    Order the utilities $U(z)$ in a nonincreasing manner.
    for $j = 1 : N$ do
        for $k = 1 : K$ do
            Update $\mathbb{P}^i_t$ using (5.15)
        end for
    end for
end for
return
```

2.4.1 Channel Access Game

Congestion game is a prominent approach to model the scenario where multiple rational users share a set of common resource. In congestion game, each individual player strives to maximize its own utility by selecting a set of resources. The share of each resource is a non-increasing function with respect to the number of players choosing it. The formal definition of congestion game is given as follows.

The standard congestion game is defined by the tuple $\{\mathcal{N}, \mathcal{R}, (\sum i)_{i\in\mathcal{N}}, (U^r_j)_{j\in\mathcal{R}}\}$, where $\mathcal{N} = \{1, 2, ..., N\}$ denotes the set of players, $\mathcal{R} = \{1, 2, ..., R\}$ denotes the set of resources, $(\sum i)$ represents the strategy space of player i, and U^r_j is the payoff associated with resource j, which is a function of the total number of players sharing it. U^r_j is a decreasing function due to competition or congestion, e.g., $U^r_j = 1/n_j$, where n_j is the total number of players choosing resource i. Denote by $S = (s_1, s_2, \ldots, s_N)$ the strategy profile of the game, where $s_i \in \sum i_{i\in\mathcal{R}}$ and s_i corresponds to the strategy of player i. Denote by $n = \{n_1, n_2, \ldots, n_R\}$ the congestion vector, where n_j represents the total number of players sharing resource j. The utility of player i is given as follows:

$$U_i = \sum_{j\in s_i} U_j^r(n_j(S)). \tag{2.17}$$

A more general version of congestion game is the weighted congestion game, where each player is assigned a weight. Denote by $w = (w_1, w_2, \ldots, w_N)$ the weight vector of the players, where w_i is the weight of player i. Different from the standard congestion game, the payoff associated with resource j is a function of the total weights of players sharing resource i. It has been proved in [78] that every standard congestion game admits an NE. However, the weighted congestion games do not necessarily possess an NE.

We model the channel access procedure of SUs based on weighted congestion game, where SUs with good channel conditions are favored by being assigned a higher weight. The channel access game Γ is defined by $\{\mathcal{N}, \mathcal{K}, (w_i)_{i\in\mathcal{N}}, (\sum i)_{i\in\mathcal{N}}, (U_j^i)_{i\in\mathcal{N}, j\in\mathcal{K}}\}$, where $\mathcal{N} = \{1, 2, ..., N\}$ denotes the set of SUs, $\mathcal{K} = \{1, 2, ..., K\}$ denotes the set of channels, w_i denotes the weight associated with SU_i, $\sum i$ represents the strategy space of SU_i, and U_i^j is the utility function of SU_i for selecting channel j. U_i^j is a function of the sum of weights of SUs choosing the same channel, which is a decreasing function. Each SU aims to maximize its utility by deciding which channel to be accessed and the utility function of SU_i can be given by

$$U_i^j = \frac{w_i \Psi_j}{\sum_{j\in s_i} w_i} = w_i \zeta_j(W_j) \tag{2.18}$$

where Ψ_j is the average sojourn time of state OFF of channel j, W_j is the sum of weights of SUs choosing channel j, and $\zeta_j(W_j) = \frac{\Psi_j}{\sum_{j\in s_i} w_i}$ is the payoff function of resource j, which depends on the sum of weights of channel j. Therefore, U_j^i represents the access time that SU_i

can obtain. Note that when $w_i = 1$ for all SUs, the channel access game Γ becomes a standard congestion game, i.e., all the SUs are equally treated to share the common resource and select the access channel to maximize their own interests. Thus, a higher fairness can be achieved. On the other hand, the overall throughput of the secondary network needs to be considered when sharing the available channels. In order to favor the users with good channel conditions, greater weights can be assigned to them such that they have higher priority in the resource sharing procedure. In other words, the SUs with greater weights can have longer average time for transmissions, which consequently increases the overall throughput of the secondary network. To this end, the channel is considered to be in a good or bad state, when compared with a predefined threshold. The weights w' and w ($w' > w$) are assigned to the SUs with good channel and bad channel conditions, respectively.

2.4.2 Game Analysis

In this game, each SU chooses a single channel to access for maximizing its utility. The solution of this game is Nash Equilibrium (NE). If each one has chosen a strategy and no SU can increase its utility by changing strategy while the strategies of others keep unchanged, then the current set of strategies constitutes an NE.

Definition 3: A strategy profile $S^* = (s_1^*, s_2^*, \ldots, s_M^*)$ is an NE if and only if

$$U_j(s_i^*, s_{-i}^*) \geq U_j(s_i', s_{-i}^*), \forall i \in \mathcal{N}, s_i' \in S_i, \tag{2.19}$$

where s_i and s_{-i} are the strategies selected by SU_i and all of its opponents, respectively. NE means no one can increase its utility unilaterally.

The potential function approach is a well-known method to prove the existence of NE in the congestion games. We can define a potential function with respect to the strategies of players, in which every strictly improving move by a player will improve the value of this function. If there exists a potential function for a game, then it is guaranteed that the game exists an NE. In the following, we will prove that the channel access game Γ is a weighted potential game, and there exists an NE.

Definition 1: A game Υ is an ordinal potential game if there exists an ordinal potential function P which satisfies the following condition:

$$U^i(s_{-i}, s_i') - U^i(s_{-i}, s_i) > 0 \text{ iff } P(s_{-i}, s_i') - P(s_{-i}, s_i) > 0.$$

Definition 2: A game Υ associated with a weight vector $w = (w_1, w_2, \ldots, w_N)$ is a weighted potential game if there exists a weighted potential function P satisfying the following condition:

$$U^i(s_{-i}, s_i') - U^i(s_{-i}, s_i) = w_i[P(s_{-i}, s_i') - P(s_{-i}, s_i)]. \tag{2.20}$$

To prove the existence of NE in the channel access game Γ, we use Rosenthal's potential function $\Re(S)$ [72], which is defined as follows:

$$\begin{aligned}\Re(S) &= \sum_{j\in\mathcal{K}} \sum_{i=w}^{W_j} \zeta_j(i)\\ &= \sum_{i=1}^{N} \sum_{j\in s_i} \zeta_j(W_j^i),\end{aligned} \tag{2.21}$$

where W_j^i is the sum of weights of SUs selecting channel j whose indices do not exceed i.

Suppose SU_i unilaterally deviates from strategy s_i to s_i'. The change in the potential $\Re(S)$

can be obtained as follows:

$$\begin{aligned}\triangle\ \Re(s_i \rightarrow s_i') &= \zeta_{j\in s_i'}(W_j + w_i) - \zeta_{k\in s_i}(W_k)\\ &= \zeta_{j\in s_i'}(W_j(s_{-i}, s_i') - \zeta_{k\in s_i}(W_k(s_{-i}, s_i))\\ &= \frac{1}{w_i}[U^i(s_{-i}, s_i') - U^i(s_{-i}, s_i)],\end{aligned} \tag{2.22}$$

where U^i is the utility function of SU_i. Therefore, the channel access game Γ is a weighted potential game.

In [79], for every finite ordinal potential game, there exists an NE. Since weighted potential game is a subset of ordinal potential games, there exists an NE in the weighted potential game. Therefore, an NE exists in the channel access game Γ. It is well known that an NE can be achieved when each SU strives to optimize their own utilities after a finite number of steps [72]. Therefore, we propose a channel access algorithm, Algorithm 2. The main idea of the proposed algorithm is that each SU aims at improving its own utility and then they end up optimizing the global objective, i.e., the potential function. By doing so, the NE can be obtained. The proof that the algorithm can achieve NE is given in Appendix A.

2.5 Simulation Results

In this section, simulation results are provided to validate the performance of the proposed algorithms. The simulation is set up as follows. In a 2 km×2 km area, there is a set of PUs located inside the circle with 1 km radius, while a group of SUs seeking for transmission opportunities is randomly distributed outside the circle. The transmission power of PUs is set to 10 mw, while the variance of noise is set to -80 dB. The channel gain between a given SU and a PU is calculated by $h = \frac{k}{d^\mu}$, where $k = 1$ and $\mu = 3.5$. The value of p_f is set to 0.1 for all SUs. For simplicity, let $w' = 2w$ and $w = 1$. The detailed simulation parameters are shown

Algorithm 2

```
// **Channel Access Algorithm**
Set congestion vector $W(S) = (W_1, ..., W_K) = (0, 0, ..., 0)$.
**for** each $SU_i \subseteq \mathcal{N}$ **do**
    **if** Channel $i$ for $SU_i$ pair is in good state **then**
        $w_i \Leftarrow w'$ and put $SU_i$ into the set $U_{G1}$
    **else**
        $w_i \Leftarrow w$ and put $SU_i$ into the set $U_{G2}$
    **end if**
**end for**
Order the rewarding periods on each channel $[\Psi_1, \Psi_2, \ldots, \Psi_K]$ decreasingly according to
    the length.
Order the SUs in the user set $U_{G1}$ and $U_{G2}$ decreasingly according to the channel gain
**for** each $SU_i \subseteq U_{G1}$ **do**
    $SU_i$ calculates $w_i\zeta_j(W_j + w')$
    $SU_i$ selects the channel with maximum $w_i\zeta_j(W_j + w')$
    $W_j \Leftarrow W_j + w'$
**end for**
**for** each $\Psi_j$, where $j \subseteq U_{G2}$ **do**
    $SU_i$ calculates $w_i\zeta_j(W_j + w)$
    $SU_i$ selects the channel with maximum $w_i\zeta_j(W_j + w)$
    $W_j \Leftarrow W_j + w$
**end for**
**return**
```

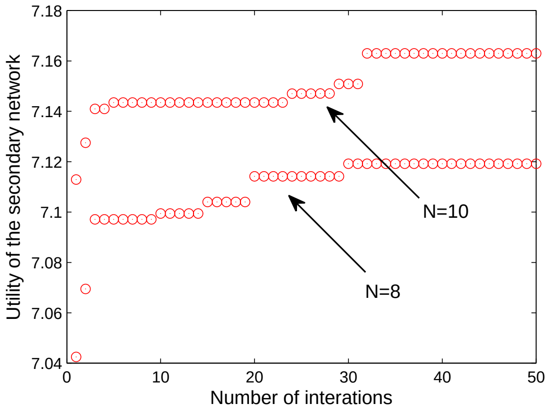


Figure 2.2: Convergence of C-E algorithm.

in Table II. We obtain the average results using Monte Carlo simulation.

Table 2.2: Parameters used in the simulations

Parameters	Value
Number of channels	[3, 4, 5, 6, 7]
Number of samples	6000
Transmission power of PUs	10mw
Variance of noise	-80dB
Path loss exponent μ	3.5
$\overline{P}_{rm}$	0.1
p_f	0.1
T_{OFF}	[4, 4, 5, 5]
α	[0.6, 0.8, 1, 1.2]
U_0	2
Simulation times	200

Fig. 2.2 shows the convergence speed of the proposed C-E algorithm for the case when the number of channel is set to 5. It can be seen that after a few iterations the C-E algorithm converges, which means all SUs select a channel for sensing with probability 1. It can also be seen that a larger number of SUs results in a larger utility.

Fig. 2.3 shows the utility of the secondary network with respect to the number of SUs for different approaches when the number of channels is 4. We compare the proposed C-E algorithm with the greedy algorithm in [65]. Greedy 1 algorithm does not consider the dynamics of channels and detection probabilities of SUs, while Greedy 2 algorithm does. It can be seen that Greedy 2 algorithm can achieve higher utility than Greedy 1 algorithm. In C-E algorithm, ρ and Z are set to 0.2 and 100, respectively. It can also be seen that the C-E algorithm can achieve higher utility than the Greedy algorithms.

Fig. 2.4 shows the utility of the secondary network with respect to the number of channels for different approaches when the number of SUs is 10. It can be seen that as the number of channels increases, the utility of the secondary network increases. It can also be seen that Greedy 2 algorithm performs slightly better than Greedy 1 algorithm, while the proposed C-E algorithm can achieve the highest utility among these algorithms.

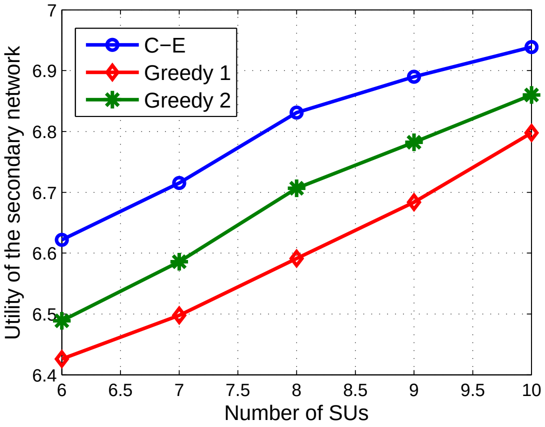


Figure 2.3: Utility of SUs versus the number of SUs.

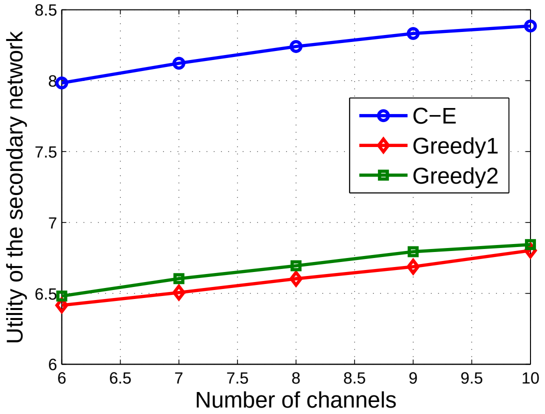


Figure 2.4: Utility of SUs versus the number of channels.

Fig. 2.5 shows the throughput of the secondary network with respect to the number of SUs by using the weighted congestion game and standard congestion game when the number of channels is set to 5. The throughput is calculated using the Shannon capacity formula. For each SU, the channel condition is randomly generated, which takes value from [15dB, 35dB] using a uniform distribution. The threshold is set to 25dB. If the channel gain is greater than the threshold, it is treated as good channel and the SU will be assigned a larger weight in weighted congestion game. From the figure, it can be seen that the weighted congestion game can achieve higher throughput compared with the standard congestion game. This is because

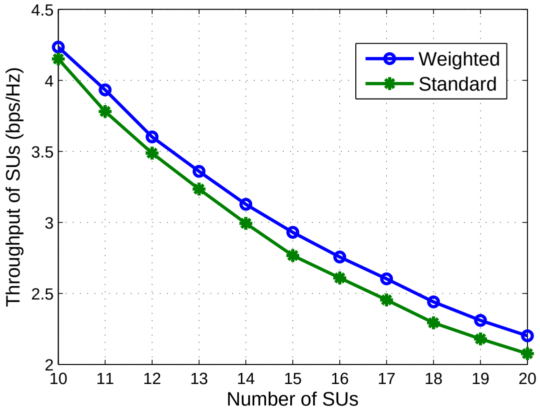


Figure 2.5: Throughput of SUs versus the number of SUs.

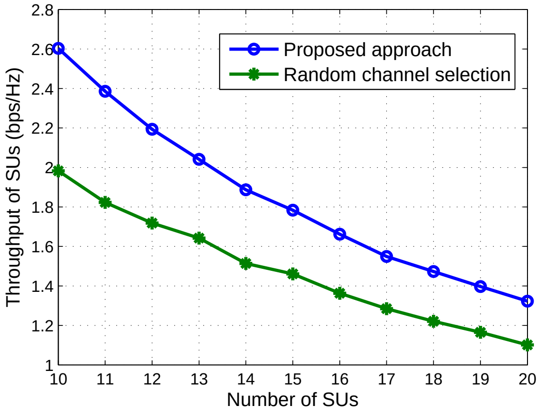


Figure 2.6: The proposed framework versus random channel access.

the SUs with good channel conditions are favored, which can obtain a relatively larger share of the available channel.

Fig. 2.6 shows the average throughput per user for the proposed sensing and access strategy and random channel access strategy, respectively, when the number of channels is set to 5. With the random channel access strategy, SUs randomly choose a channel for sensing and access the channel when it is detected idle. From the figure, it can be seen that the proposed sensing and access strategy can achieve higher throughput per user. It implies that SUs have the incentive to participate in the proposed sensing and access strategy since they can achieve higher utility.

2.6 Summary

In this chapter, we have proposed a cooperative framework for a multi-channel CRN, which integrates cooperative spectrum sensing and spectrum sharing, considering both the diverse channel usage characteristics and the diverse sensing performance of individual SUs. To maximize the expected available time of all the channels, a cross-entropy based approach is proposed. For spectrum sharing, a channel access game is formulated based on weighted congestion game. An channel access algorithm is proposed to achieve NE. Simulation results have demonstrated that, with the proposed cooperative framework, a higher throughput per user can be achieved.

Chapter 3

Secure Communications in CCRN

In this chapter, we investigate the cooperative framework which targets for improving the secure transmission of PUs via cooperation with SUs that have incentive to gain certain transmission opportunities. Two types of cooperation schemes are proposed, whereby the PU either cooperates with two individual SUs or a cluster of SUs, which are referred to as relay-jammer (R-J) scheme and cluster-beamforming (C-B) scheme, respectively. In R-J scheme, two individual SUs act as a relay and a friendly jammer to improve the PU's secrecy; in return, the PU allocates a fraction of access time for SUs' transmission. To achieve the maximum secrecy rate, joint time and power allocation is considered. Particularly, the cooperating relay and jammer determine the optimal transmission power, while the PU decides the optimal time allocation strategy. In C-B scheme, the PU cooperates with a cluster of SUs to enhance the secrecy of the primary link via collaborative beamforming, where three different approaches are proposed for the scenarios with one eavesdropper, with multiple eavesdroppers, and without eavesdroppers' information, respectively. To maximize the secrecy rate, the weight selection and time allocation are also studied.

3.1 Literature Review

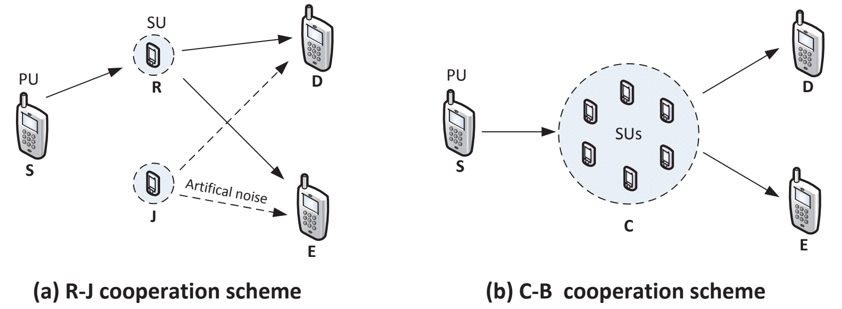
Since security is a critical issue in wireless environments due to the broadcast nature of wireless communications [80], PUs also have the need for secure communications. Traditionally, the security is dealt with by encryption at upper layers; yet, it becomes very challenging for a network without infrastructure [81]. Moreover, the encryption algorithms could be compromised and an alternative way for enhancing the security is to protect the transmitted signal from being received or decoded by the eavesdroppers [82]. Recently, physical (PHY) layer security, or information-theoretic security, has attracted a lot of attentions in the research community [83–85], which exploits the properties of the wireless channel to secure communications. In [83], it is shown that the perfectly secure information can be transmitted at a nonzero rate from the source to the destination, while the eavesdropper cannot learn anything regarding it. This rate is referred to the *secrecy rate*, which is defined as the difference between the transmission rate of the source-destination link and that of the source-eavesdropper link. However, the secrecy rate would be equal to zero when the source-destination channel is worse than that of the source-eavesdropper channel.

To address the above issue, user cooperation has been introduced to enhance the secrecy of communications [86–90]. In [86], three types of schemes using decode-and-forward (DF), amplify-and-forward (AF), and cooperative jamming, are proposed to improve the secrecy via cooperation. In [87], distributed beamforming is leveraged at relays to enhance the source's secrecy. Nevertheless, these schemes cannot be applied directly to CRNs because the special features of CRNs have not been taken into consideration: i) PUs have higher priorities for spectrum usage in CRNs; ii) it might not be reasonable to assume that PUs and SUs cooperate unconditionally with each other, since they have their own interests. Considering the features of CRNs, a cooperation based spectrum access is studied in [91], which improves the security of the primary link and provides transmission opportunities to SUs. However, the cooperation

Table 3.1: The key notations.

Symbol	Definition
N	The number of SUs
S	The primary source
D	The primary destination
R	The relay SU
J	The jammer SU
E	Eavesdropper
C	The cluster of SUs
E-CSI	The channel state information (CSI) regarding E
$\bar{R}_{EX}$	The expected overall transmission rate of SUs
P_{max}^{C}	The maximum power of SU(s) for cooperation
P_{max}	The power budget of individual user or the cluster
$R_{S,i}$	The overall transmission rate of SU_i
$U_{S,i}$	The satisfaction of SU_i for the transmission rate via cooperation
h_{SD}	The channel gain from S to D
h_{SE}	The channel gain from S to E
h_{SR}	The channel gain from S to R
h_{RD}	The channel gain from R to D
h_{RE}	The channel gain from R to E
h_{JD}	The channel gain from J to D
h_{JE}	The channel gain from J to E
α, β	The access time allocation coefficient
$\bar{R}_Q$	The predefined required transmission rate of the PU for the scenario without E-CSI
P_R	The transmission power of R during cooperation
P_J	The transmission power of J during cooperation
$\bar{R}_{SEC}$	The overall secrecy rate of the PU

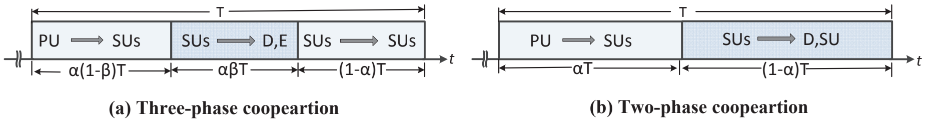
objective is achieved at the expense of employing multiple antennas and only the scenario with a single eavesdropper is considered. In reality, the assumption of multiple antennas might not be feasible. Moreover, more practical scenarios, where there exist multiple eavesdroppers or the information regarding eavesdropper(s) is not available, need to be investigated.



(a) R-J cooperation scheme

(b) C-B cooperation scheme

Figure 3.1: System model for secure communication in CCRN.



(a) Three-phase coopeartion

(b) Two-phase coopeartion

Figure 3.2: Time frame structure for cooperation

3.2 System Model

We present the system model in this section. As depicted in Fig. 3.1, the system consists of a primary source (S), a primary destination (D), multiple SUs, and an eavesdropper (E) or multiple eavesdroppers who aim to decode the PU's information [92]. In the primary network, S holds a time slot of duration T to communicate with D over a bandwidth of W Hz. Different from [92] [93], which assume that there is no direct link between S and either D or E, and only focus on the secure information transfer from the relays to D, we consider a more general case where there exist direct links. It is known that when the channel between S and D is worse than that between S and E, the secrecy rate is zero. To transfer information securely, S either chooses two cooperating SUs, i.e., a relay SU (R) and a jammer SU (J), or a cluster (C) of SUs for cooperation, which are all considered friendly[1]. This common assumption can be found in [87–94]. The cooperation between the PU and untrusted SUs has been studied in one of our

[1] For SUs, the first and foremost need is to acquire access opportunities for transmissions. In this regard, SUs don't have much motivation to compromise PUs' secrecy. Otherwise, PUs may not be interested in cooperation with SUs. As a consequence, SUs will lose transmission opportunities.

previous work [95], where trust values of SUs are taken into consideration.

Cooperation can be performed in a three-phase fashion or a two-phase fashion. The time structure for the three-phase cooperation is shown in Fig. 1(a). A fraction α of the duration T is used for the transmission from S to D, which is further divided into two parts according to β, where $0 < \alpha, \beta < 1$. Particularly, in the first phase of $\alpha(1-\beta)T$, S transmits data to cooperating SUs, which is also overheard by D and E. In the second phase, a subsequent duration of $\alpha\beta T$ is leveraged for the transmission from cooperating SUs to D. For R-J scheme, shown in Fig. 1(a), R employs DF protocol to relay the PU's message to D, and simultaneously J transmits an artificial jamming signal to confound E. For C-B scheme, shown in Fig. 1(b), the SUs in C first decode the PU's message and then each of them forwards a weighted version of that message to D via collaborative beamforming. In the last phase, the remaining $(1-\alpha)T$ is granted to cooperating SUs for transmitting their own data as a reward, in which the relay SU and jammer SU access the channel in a TDMA fashion, while the SUs in C transmit the data to a common secondary receiver via collaborative beamforming [96]. To ease presentation, the period for the first two phases, i.e., (αT), is termed as cooperation period, while the last phase of $(1-\alpha)T$ is termed as rewarding period. When there exist multiple eavesdroppers, C-B scheme is carried out in a two-phase fashion, as shown in Fig. 1(b). The operation in the first phase is the same as that of the previous cases. In the second phase, the cluster simultaneously transmits the PU's message and its own data.

Since SUs will not cooperate with the PU unconditionally, SUs have a requirement on the *expected* overall transmission rate $\bar{R}_{EX}$, which SUs desire through cooperation. However, for the three-phase cooperation, the *actual* average transmission rate of SUs depends on the time period granted by the PU. From the PU's perspective, it tends to grant less time to SUs, and hence transmission rate of SUs obtained via cooperation will be much less than $\bar{R}_{EX}$. In order to enforce the PU to grant an acceptable rewarding time, SUs' strategy is to determine the effort that they are willing to make during cooperation, i.e., the maximum power P_{max}^{C} for cooperation, according to the transmission rate obtained. As a result of the SUs' strategy[2], if the PU chooses a lager α, although the cooperation period is prolonged, the cooperating SUs will choose a lower transmission power, which will lead to a decrease in the performance during the cooperation period. Then, the overall secrecy rate may be reduced. If the PU chooses a smaller α to acquire more effort from SUs during the cooperation period, although the performance in the cooperation period is increased, the time for that period is reduced, which may cause a drop in the overall secrecy rate.

A slow, flat, block Rayleigh fading environment is considered, where the channel remains static in one time slot and changes independently over different time slots. The channel coefficient from S to D is denoted by h_{SD}. Similarly, we have h_{SR}, h_{SE}, h_{RD}, h_{RE}, h_{JD}, and h_{JE}. The global CSI is available for the system, including D-related CSI (D-CSI) and E-related CSI (E-CSI), which is a common assumption in PHY layer security literature. The cooperation when E-CSI is unavailable will be discussed in Section V. In addition, additive white Gaussian noise is assumed with zero mean and the one-side power spread density is N_0. Moreover, each node is equipped with a single antenna and communicates with each other in a half-duplex mode.

In the following, matrices and vectors are denoted by bold uppercase letters and bold lowercase letters, respectively. $(\cdot)^*$, $(\cdot)^T$, and $(\cdot)^\dagger$ denote the conjugate, transpose, and conjugate transpose, respectively. $\mathbf{I}$ denotes the identity matrix. $[x]^+$ denotes the maximum value between x and 0, while $x^\star$ denotes the optimal value of x. $|\cdot|$ denotes the magnitude of a channel or the absolute value of a complex number, while $\|\cdot\|$ is the Euclidean norm of a vector or a matrix.

[2] The strategy of SUs for the two-phase cooperation is explicitly explained in Section 3.4.2 and Section 3.5, respectively.

3.3 R-J Cooperation Scheme

3.3.1 Problem Formulation

Secrecy Rate of PU

We use secrecy rate as a measure for the secure communication. To obtain the secrecy rate, the transmission rates at different nodes are calculated as follows.

In the first phase, S transmits data to R and the transmission rate at R is given by

$$R_R = W \log_2(1+\gamma), \tag{3.1}$$

where $\gamma = \frac{P|h_{SR}|^2}{WN_0}$ and P is the transmission power of the PU.

In the second phase, R relays the PU's message to D using DF protocol, and simultaneously J broadcasts an artificial jamming signal. Since D receives signals in both the first and second phases, the transmission rate R_D at D using maximal ratio combining (MRC) is given by

$$R_D = W \log_2(1+\xi+\frac{P_R|h_{RD}|^2}{WN_0+P_J|h_{JD}|^2}), \tag{3.2}$$

where $\xi = P|h_{SD}|^2/(WN_0)$ is the SNR from the first phase, and P_R and P_J are the transmission power of R and J during cooperation, respectively.

Likewise, E also receives signals during the first two phases. Therefore, the transmission rate at E can be expressed as follows:

$$R_E = W \log_2(1+\delta+\frac{P_R|h_{RE}|^2}{WN_0+P_J|h_{JE}|^2}), \tag{3.3}$$

where $\delta = P|h_{SE}|^2/(WN_0)$ is the SNR from the first phase.

When the DF cooperative communication is applied, the overall transmission rate of D and E equal to the minimum rate of the first two phases, respectively [97], i.e.,

$$\begin{aligned}\bar{R}_D &= \min\{\alpha(1-\beta)R_R, \alpha\beta R_D\}\\ \bar{R}_E &= \min\{\alpha(1-\beta)R_R, \alpha\beta R_E\}\end{aligned} \tag{3.4}$$

By definition, the *secrecy rate* R_{SEC} is given by:

$$R_{SEC} = [R_D - R_E]^+, \tag{3.5}$$

Substituting (3.4) into (3.5), the overall secrecy rate is then given by

$$\bar{R}_{SEC} = [\min\{\alpha(1-\beta)R_R, \alpha\beta R_D\} - \alpha\beta R_E]^+ \tag{3.6}$$

Overall Transmission Rate of SUs

Let $P_{S,i}$ be the transmission power of SU_i for its own communication, where $i = \mathsf{R}$ or J. SUs are considered to have the same power constraint P_{max}. R and J transmit in a TDMA mode and the overall transmission rate of SU_i is given by

$$\bar{R}_{S,i} = \frac{1-\alpha}{2} W \log_2(1 + \frac{P_{S,i}|h_{S,i}|^2}{WN_0}), \tag{3.7}$$

where $h_{S,i}$ is the channel coefficient from i to its corresponding receiver.

As mentioned in the system model, SUs have a requirement on the *expected* overall transmission rate $\bar{R}_{EX}$ via cooperation. From (3.7), $\bar{R}_{S,i}$ is related to the time period granted by the PU. To measure SUs' degree of satisfaction on $\bar{R}_{S,i}$, $U_{S,i}$ is defined as $U_{S,i} = \min\{\frac{\bar{R}_{S,i}}{\bar{R}_{EX}}, 1\}$, which implies how satisfactory SU_i is with $\bar{R}_{S,i}$. For instance, if $\bar{R}_{S,i} = \bar{R}_{EX}$, $U_{S,i}$ is equal to 1. In order to enforce the PU to grant an acceptable rewarding time, SUs' strategy is to determine the effort that they are willing to make during cooperation, i.e., the maximum power P^C_{max} for cooperation, according to the degree of satisfaction. For simplicity, $P^C_{max} = U_{S,i} \cdot P_{max}$. In other words, the degree of effort that the SU is willing to make depends on the degree of the satisfaction obtained. For example, if $U_{S,i} = 1$, the SU is willing to devote full power P_{max} for cooperation, i.e., $P^C_{max} = P_{max}$.

Secrecy Rate Maximization

Since the SU typically does not have much transmission opportunities, it aims at maximizing the throughput by adopting P_{max} for its own transmission. Thus, given a certain α, $\bar{R}_{S,i} = \frac{1-\alpha}{2} W \log_2(1 + \frac{P_{max}|h_{S,i}|^2}{WN_0})$. Based on the degree of the satisfaction, P^C_{max} can be determined, which is a function of α. As shown in (3.6), $\bar{R}_{SEC}$ is related to α, β, and the transmission power P_R and P_J, which are constrained by P^C_{max}. From PU's perspective, the objective of cooperation is to maximize the overall secrecy rate $\bar{R}_{SEC}$. Therefore, the PU chooses the time allocation coefficients α and β, while the SUs determine the optimal transmission power for cooperation, which can be formulated as the following optimization problem:

$$\begin{aligned} &\max_{\alpha,\beta,P_R,P_J} \bar{R}_{SEC} \\ \text{s.t. } 0 < \alpha,\ \beta < 1,\ 0 \leq P_R \leq &P^C_{max},\ 0 \leq P_J \leq P^C_{max}. \end{aligned} \tag{3.8}$$

3.3.2 Cooperation Parameters Determination

The time allocation coefficients and transmission power can be optimized by solving the above optimization problem. To do this, the procedure can be divided into two steps: i) given α, R and J select the optimal transmission power; and ii) S selects the optimal $\alpha^\star$, $\beta^\star$ to maximize the secrecy rate, aware of the results of the first step.

From (3.6), for a given α, the overall secrecy rate $\bar{R}_{SEC}$ not only depends on $R_D - R_E$, but also on β. In fact, $\bar{R}_{SEC}$ can be further expressed as follows:

$$\begin{aligned}\bar{R}_{SEC} &= [\alpha\beta(R_D - R_E)]^+ = \alpha[\frac{R_R(R_D - R_E)}{R_R + R_D}]^+ \\ &= \alpha[R_R - \frac{R_R(R_R + R_E)}{R_R + R_D}]^+,\end{aligned} \tag{3.9}$$

where R_R, R_D and R_E are given by (3.1), (3.2), and (3.3), respectively. The derivation is given in the Appendix B. Note that given α, the optimal $\beta^\star = \frac{R_R}{R_R + R_D}$.

In the literature, most of the existing works assume the time duration for the transmission from S to R and from R to D are equal, and try to maximize $R_D - R_E$ based on this assumption. However, R_R and R_D are typically not the same. Furthermore, the overall transmission rate is the minimum one between $\bar{R}_R$ and $\bar{R}_D$ for DF strategy. Thus, it is not optimal to assign equal duration for these two phases. From (3.9), it can be seen that the secrecy rate cannot achieve the optimum value by only maximizing $R_D - R_E$. This is because when R_D increases, $R_D - R_E$ increases, but β decreases. Note that the objective function in (3.9) has encapsulated the above factors and in this chapter we study the nontrivial case where the secrecy rate is positive.

Power Allocation

Since the relay is leveraged to increase the transmission rate at destination compared with that at the eavesdropper, it requires that $|h_{RD}| > |h_{RE}|$. The job of the jammer is to create more interference at the eavesdropper than at the destination and it is necessary that $|h_{JE}| > |h_{JD}|$. In what follows, to achieve the maximum secrecy rate, the optimal transmission power of relay SU and jammer SU are analyzed, respectively, when α is given.

Relay SU: Since R_R is fixed, maximizing $\bar{R}_{SEC} = R_R - R_R(R_R + R_E))/(R_R + R_D)$ is equivalent to minimizing $f(P_R, P_J) \triangleq (R_R + R_E)/(R_R + R_D)$. Similar to [98], we study the case in the low SNR regime, which corresponds to the cases of long-distance transmissions or energy-limited scenarios. We approximate $\log_2(1 + snr) \approx snr$ [99]. Based on (3.1), (3.2), (3.3), and the approximation, we have

$$f(P_R, P_J) = \frac{\Psi_E + P_R|h_{RE}|^2/(WN_0 + P_J|h_{JE}|^2)}{\Psi_D + P_R|h_{RD}|^2/(WN_0 + P_J|h_{JD}|^2)}, \tag{3.10}$$

where $\Psi_D = \gamma + \xi$ and $\Psi_E = \gamma + \delta$. Take the first order derivative of f with respect to P_R and it is always negative because $|h_{RD}| > |h_{RE}|$. Therefore, $f(P_R, P_J)$ is a monotonically decreasing function of P_R and the optimal transmission power $P_R^\star$ is P_{max}^C for maximizing the secrecy rate. Note that P_{max}^C is a function of α.

Jammer SU: The optimal transmission power $P_J^\star$ is selected such that the objective function in (3.10) can be maximized. The derivative of (3.10) with respect to P_J is proportional to a quadratic function in the following form:

$$\frac{\partial f}{\partial P_J} \propto \psi_1 \cdot P_J^2 + \psi_2 \cdot P_J + \psi_3, \tag{3.11}$$

where

$$\begin{aligned}
\psi_1 =& |h_{JD}||h_{JE}|P_R(|h_{RD}|\Psi_E|h_{JE}| - |h_{RE}|\Psi_D|h_{JD}|) \\
\psi_2 =& 2|h_{JD}||h_{JE}|N_0P_R(|h_{RD}|\Psi_E - |h_{RE}|\Psi_D) \\
\psi_3 =& |h_{RD}||h_{RE}|P_R^2N_0(|h_{JD}| - |h_{JE}|) + \\
& N_0^2(|h_{RD}|\Psi_E|h_{JE}| - |h_{RE}|\Psi_D|h_{JE}|).
\end{aligned}$$

Since $|h_{RD}| > |h_{RE}|$ and $|h_{JE}| > |h_{JD}|$, we have $\psi_1 > 0$, $\psi_2 > 0$, and $P_R = P_{max}^C$. If $\psi_3 > 0$, there is no positive root for the quadratic function in (3.11) and $\frac{\partial f}{\partial P_J} > 0$ for the range from 0 to P_{max}^C. Thus, $P_J^\star$ equals to 0 to maximize the secrecy rate, indicating a non-jamming scenario. If $\psi_3 < 0$, there is one positive root $\frac{-\psi_2+\sqrt{\psi_2^2-4\psi_1\psi_3}}{2\psi_1}$. When $\frac{-\psi_2+\sqrt{\psi_2^2-4\psi_1\psi_3}}{2\psi_1} > P_{max}^C$, $\frac{\partial f}{\partial P_J} < 0$ for the range from 0 to P_{max}^C and hence $P_J^\star$ should be selected as P_{max}^C. Otherwise, $P_J^\star$ should be equal to $\frac{-\psi_2+\sqrt{\psi_2^2-4\psi_1\psi_3}}{2\psi_1}$.

Time Allocation

From (3.9), the objective function has taken the factor of β into consideration. Given α, the optimal transmission power of SUs has been obtained in the previous section. Therefore, the optimal $\beta^\star$ can be easily determined by

$$\beta^\star = \frac{R_R}{R_R + R_D}, \tag{3.12}$$

where R_D is the transmission rate at D when R and J choose the optimal transmission power.

The optimal $\alpha^\star$ can be determined by solving the following equation:

$$\alpha^\star = \arg\max \alpha\beta(R_D - R_E) \tag{3.13}$$

Note that β, R_D, and R_E are all functions of α ($0 < \alpha < 1$).

3.4 C-B Cooperation Scheme with E-CSI

In this section, we discuss the cooperation between the PU and a cluster of SUs when E-CSI is available. We propose a three-phase cooperation scheme and a two-phase cooperation scheme for the scenarios in the presence of an eavesdropper and multiple eavesdroppers, respectively. To maximize the secrecy rate, time allocation and weights selection are jointly considered.

3.4.1 C-B Scheme for Single Eavesdropper (CBSE)

Problem Formulation

Secrecy Rate of PU: In the presence of one eavesdropper, the cooperation is performed in a three-phase fashion, as shown in Fig. 2(a). In the first phase, the PU broadcasts to the cluster the signal $\sqrt{P}s$, where s is the information symbol with $E\{|s|^2\} = 1$, which is overheard by D and E. In order for all the cluster members to successfully decode the signal, the transmission rate R_R from S to C is determined by the worst channel between S and the cluster members.

$$R_R = W \log_2(1 + \min_i \frac{P|h_{SR,i}|^2}{N_0 W}), \tag{3.14}$$

where $h_{SR,i}$ is the channel from S to ith SU in the cluster. Denote by $y_{D,1}$ and $y_{E,1}$ the signal received at D and E in the first phase, respectively, which can be given by

$$\begin{aligned} y_{D,1} &= \sqrt{P} h_{SD} s + n_{SD} \\ y_{E,1} &= \sqrt{P} h_{SE} s + n_{SE} \end{aligned} \tag{3.15}$$

where n_{SD} and n_{SE} are the noise at D and E, respectively.

In the second phase, each SU in the cluster decodes the received symbol and forwards a weighted version of the re-encoded symbol $\tilde{s}$ to D. Let $\mathbf{w}$ be the column vector of the weights of all SUs in the cluster and N be the number of SUs in the cluster. Then, the received signals $y_{D,2}$ and $y_{E,2}$ at D and E in the second phase can be written respectively as:

$$\begin{aligned} y_{D,2} &= \mathbf{h}_{RD}^{\dagger} \mathbf{w} \tilde{s} + n_{RD} \\ y_{E,2} &= \mathbf{h}_{RE}^{\dagger} \mathbf{w} \tilde{s} + n_{RE} \end{aligned} \tag{3.16}$$

where $\mathbf{h}_{RD} = [h_{D,1}^*, h_{D,2}^*, ..., h_{D,N}^*]^T$ and $\mathbf{h}_{RE} = [h_{E,1}^*, h_{E,2}^*, ..., h_{E,N}^*]^T$. Note that $h_{D,i}$ and $h_{E,i}$ are the complex channel coefficients from the ith SU in the cluster to D and E, respectively, where $i \in \{1, 2, ..., N\}$. n_{RD} and n_{RE} are the noise at D and E, respectively.

Assume that the cooperating SUs use the same codewords as S. The transmission rate at D and E are given as follows:

$$\begin{aligned} R_D &= W\log_2(1+\xi+\frac{\mathbf{w}^\dagger\mathbf{h}_{RD}\mathbf{h}_{RD}^\dagger\mathbf{w}}{N_0W}) \\ R_E &= W\log_2(1+\delta+\frac{\mathbf{w}^\dagger\mathbf{h}_{RE}\mathbf{h}_{RE}^\dagger\mathbf{w}}{N_0W}), \end{aligned} \tag{3.17}$$

where ξ and δ are the same as that in (3.2) and (3.3), respectively. Substituting (3.14) and (3.17) into (3.6), we can obtain the overall secrecy rate.

Overall Transmission Rate of SUs: In the third phase, the SUs in the cluster transmit the data to the secondary receiver via collaborative beamforming. The overall rate $\bar{R}_S$ at the secondary receiver can be given by

$$\bar{R}_S = (1-\alpha)W\log_2(1+\frac{\mathbf{v}^\dagger\mathbf{h}_{RS}\mathbf{h}_{RS}^\dagger\mathbf{v}}{N_0W}), \tag{3.18}$$

where **v** is the column vector of the weights of all cooperating SUs for the secondary transmission and $\mathbf{h}_{RS} = [h_{S,1}^*, h_{S,2}^*, ..., h_{S,N}^*]^T$. Note that $h_{S,i}$ is the complex channel coefficient from the ith SU in the cluster to the secondary receiver. To maximize the transmission rate, the SUs select the optimal $\mathbf{v}^\star$, under the total power constraint, which can be formulated as follows:

$$\begin{aligned} &\max_{\mathbf{v}} \ \mathbf{v}^\dagger\mathbf{h}_{RS}\mathbf{h}_{RS}^\dagger\mathbf{v} \\ &\quad s.t. \ \mathbf{v}^\dagger\mathbf{v} \leq P_{max} \end{aligned} \tag{3.19}$$

To achieve the maximum transmission rate, **v** should lie in the space spanned by $\mathbf{h}_{RS}$. Thus, $\mathbf{v}^\star$ can be given by $\mathbf{v}^\star = \sqrt{P_{max}}\frac{\mathbf{h}_{RS}}{\|\mathbf{h}_{RS}\|}$, where $\| \mathbf{h}_{RS} \|$ is the Euclidean norm of $\mathbf{h}_{RS}$. Therefore, given a certain α, the overall transmission rate $\bar{R}_S$ is given by

$$\bar{R}_S = (1-\alpha)W\log_2(1+\frac{P_{max} \parallel \mathbf{h}_{RS} \parallel^2}{N_0 W}). \tag{3.20}$$

Secrecy Rate Maximization: Similar to Section 3.3.1 and 3.3.1, the cluster of SUs, as a whole, determines the maximum power P_{max}^C for cooperation based on the satisfaction obtained. Substituting (3.14) and (3.17) into (3.9), we can obtain $\bar{R}_{SEC}$. To maximize $\bar{R}_{SEC}$, the PU selects the optimal time allocation coefficients and the SUs determine the best beamforming weights under a total power constraint.

Cooperation Parameters Determination

Optimal Weight Selection: The SUs select the optimal weight $\mathbf{w}^\star$ to maximize the secrecy rate $\bar{R}_{SEC}$. From (3.9), given α, maximizing $\bar{R}_{SEC}$ is equivalent to maximizing $(R_R + R_D)/(R_R + R_E)$. Substituting (3.17) into it, the optimal weight can be determined by solving the following problem.

$$\begin{gathered}\max_{\mathbf{w}} \frac{\Psi_D + \mathbf{w}^\dagger \mathbf{h}_{RD}\mathbf{h}_{RD}^\dagger \mathbf{w}}{\Psi_E + \mathbf{w}^\dagger \mathbf{h}_{RE}\mathbf{h}_{RE}^\dagger \mathbf{w}} \\ s.t. \quad \mathbf{w}^\dagger \mathbf{w} \le P_{max}^C\end{gathered}$$

where $\Psi_D = (\gamma + \xi)N_0 W$ and $\Psi_E = (\gamma + \delta)N_0 W$. Let us rewrite $\mathbf{w} = \sqrt{P_{max}^C}\hat{\mathbf{w}}$, where $\hat{\mathbf{w}}^\dagger\hat{\mathbf{w}}$=1. The above problem is then transformed into the following form:

$$\begin{gathered}\max_{\mathbf{w}} \frac{\Psi_D + p\hat{\mathbf{w}}^\dagger \mathbf{h}_{RD}\mathbf{h}_{RD}^\dagger \hat{\mathbf{w}}}{\Psi_E + p\hat{\mathbf{w}}^\dagger \mathbf{h}_{RE}\mathbf{h}_{RE}^\dagger \hat{\mathbf{w}}} \\ s.t. \quad \hat{\mathbf{w}}^\dagger \hat{\mathbf{w}} = 1, p \le P_{max}^C\end{gathered} \tag{3.21}$$

To guarantee $\bar{R}_{SEC}$ to be positive, it is necessary that the numerator should be greater than the denominator. Due to this necessary condition, the derivative of the objective function in (3.21) with respect to p is positive and $\bar{R}_{SEC}$ is maximized when $p = P^C_{max}$. Thus, the above optimization problem can be further rewritten as

$$\begin{aligned} &\max_{\hat{\mathbf{w}}} \frac{\hat{\mathbf{w}}^\dagger \mathbf{Q}_{RD} \hat{\mathbf{w}}}{\hat{\mathbf{w}}^\dagger \mathbf{Q}_{RE} \hat{\mathbf{w}}} \\ &s.t. \quad \hat{\mathbf{w}}^\dagger \hat{\mathbf{w}} = 1 \end{aligned} \tag{3.22}$$

where

$$\mathbf{Q}_{RD} = \frac{\Psi_D}{P^C_{max}} \mathbf{I} + \mathbf{h}_{RD} \mathbf{h}^\dagger_{RD} \text{ and } \mathbf{Q}_{RE} = \frac{\Psi_E}{P^C_{max}} \mathbf{I} + \mathbf{h}_{RE} \mathbf{h}^\dagger_{RE}.$$

The problem in (3.22) is a generalized eigenvector problem and the optimal $\hat{\mathbf{w}}^\star$ is selected as the uniform eigenvector of $\mathbf{Q}_{RD}\mathbf{Q}^{-1}_{RE}$ corresponding to its largest eigenvalue. Therefore, given α, the optimal $\mathbf{w}^\star = \sqrt{P^C_{max}} \hat{\mathbf{w}}^\star$.

Time Allocation: Similar to 3.3.2, $\beta^\star$ can be determined by substituting (3.17) into (3.12), when optimal $\mathbf{w}$ is selected. The optimal $\alpha^\star$ can be determined by solving the following problem, when the optimal weights and β are selected.

$$\alpha^\star = \arg\max \alpha\beta(R_D - R_E) \tag{3.23}$$

Note that β, R_D, and R_E are all functions of α $(0 < \alpha < 1)$.

3.4.2 C-B Scheme for Multiple Eavesdroppers (CBME)

Problem Formulation

For the case of multiple eavesdroppers, the cooperation can be performed in a two-phase way, as shown in Fig. 2(b). The operation in the first phase is the same as that in the previous cases and the transmission rate R_R is given in (3.14).

In the second phase, instead of relaying the PU's data and transmitting its own data in different phases, the cluster transmits **x** which is the sum of the weighted version of the PU's information symbol $\tilde{s}$ and its information symbol z with $E\{|z|^2\} = 1$. Therefore, **x** can be represented by $\mathbf{x} = \mathbf{w}\tilde{s} + \mathbf{v}z$, where **w** and **v** are the column vectors of the weights of all SUs for transmitting the PU's symbol and SUs' symbol, respectively. Then, the received signals $y_{D,2}$ and $\mathbf{y}_{E,2}$ at D and eavesdroppers in the second phase can be written respectively as:

$$\begin{aligned} y_{D,2} &= \mathbf{h}_{RD}^{\dagger}\mathbf{w}\tilde{s} + \mathbf{h}_{RD}^{\dagger}\mathbf{v}z + n_{RD} \\ \mathbf{y}_{E,2} &= \mathbf{H}_{RE}^{\dagger}\mathbf{w}\tilde{s} + \mathbf{H}_{RE}^{\dagger}\mathbf{v}z + \mathbf{n}_{RE} \end{aligned} \tag{3.24}$$

where $\mathbf{H}_{RE}$ is the matrix of channel coefficients between the SUs and eavesdroppers, and $\mathbf{n}_{RE}$ is the noise vector at eavesdroppers. To transmit the PU's data and its own data simultaneously, the cluster utilizes the approach based on zero-forcing beamforming, which is similar to the work in [100]. By doing so, the SUs' transmission will not interfere with the concurrent transmission of the PU, and vice versa. To this end, **v** should be in the null space of $\mathbf{h}_{RD}^{\dagger}$ such that $\mathbf{h}_{RD}^{\dagger}\mathbf{v} = 0$ and **w** should be in the null space of $\mathbf{h}_{RS}^{\dagger}$ such that $\mathbf{h}_{RS}^{\dagger}\mathbf{w} = 0$. Therefore, the overall transmission rate $\bar{R}_S$ at the secondary receiver is

$$\bar{R}_S = (1-\alpha)W\log_2(1 + \frac{|\ \mathbf{h}_{RS}^{\dagger}\mathbf{v}\ |^2}{N_0 W}). \tag{3.25}$$

Different from the pervious case, it is not necessary to enforce the PU to grant a reasonable period of time to SUs due to the following reasons: i) relaying PU's data and transmitting SUs' data occupy the same period, and hence, the PU itself will not just allocate a quite short duration for the second phase, which affects the PU's performance as well; and ii) the cluster can achieve the expected transmission rate $\bar{R}_{EX}$ on its own, i.e., $\bar{R}_S = \bar{R}_{EX}$, by choosing **w** and **v**. Denote by P_1 and P_2 the transmission power for relaying the PU's data $\tilde{s}$ and transmitting its own data z, respectively, where $P_1 = \mathbf{w}^\dagger\mathbf{w}$ and $P_2 = \mathbf{v}^\dagger\mathbf{v}$. Since the cluster has a total power budget P_{max}, it holds that $P_1 + P_2 \leq P_{max}$. To maximize the secrecy rate of the PU and guarantee the expected transmission rate $\bar{R}_{EX}$ of the SUs, the cluster chooses the suitable **w** and **v** under the total power constraint, while the PU determines α.

Cooperation Parameters Determination

For convenience, let $\mathbf{w} = \sqrt{P_1}\hat{\mathbf{w}}$ and $\mathbf{v} = \sqrt{P_2}\hat{\mathbf{v}}$, respectively, where $\hat{\mathbf{w}}^\dagger\hat{\mathbf{w}} = 1$ and $\hat{\mathbf{v}}^\dagger\hat{\mathbf{v}} = 1$. To select the optimal $\mathbf{w}^\star$ and $\mathbf{v}^\star$, we perform the following two steps: i) determine the optimal $\hat{\mathbf{w}}^\star$ and $\hat{\mathbf{v}}^\star$ given P_1 and P_2; and ii) select P_1 and P_2, based on the results of the previous step.

Step 1: We first determine the optimal $\hat{\mathbf{w}}^\star$ and $\hat{\mathbf{v}}^\star$. For $\hat{\mathbf{v}}$, the objective is to maximize the transmission rate at the secondary receiver, under the constraint of no interference at D. Therefore, the optimal $\hat{\mathbf{v}}^\star$ can be determined by solving the following optimization problem.

$$\begin{aligned} &\max_{\hat{\mathbf{v}}} |\ \mathbf{h}_{RS}^\dagger \hat{\mathbf{v}}\ |^2 \\ &s.t.\ \mathbf{h}_{RD}^\dagger \hat{\mathbf{v}} = 0 \text{ and } \hat{\mathbf{v}}^\dagger\hat{\mathbf{v}} = 1 \end{aligned} \tag{3.26}$$

From (3.26), it can be seen that $\hat{\mathbf{v}}$ is orthogonal to $\mathbf{h}_{RD}$, which means $\hat{\mathbf{v}}$ belongs to the subspace of $\mathbf{h}_{RD}^\perp$, i.e., the null space of $\mathbf{h}_{RD}$. To maximize the objective function in (3.26), the optimal $\hat{\mathbf{v}}^\star$ should be selected in the direction of the orthogonal projection of $\mathbf{h}_{RS}$ onto $\mathbf{h}_{RD}^\perp$.

Thus, $\hat{\mathbf{v}}^\star$ can be determined as follows:

$$\hat{\mathbf{v}}^\star = \frac{(\mathbf{I} - \hat{\mathbf{h}}_{RD}\hat{\mathbf{h}}_{RD}^\dagger)\mathbf{h}_{RS}}{\parallel (\mathbf{I} - \hat{\mathbf{h}}_{RD}\hat{\mathbf{h}}_{RD}^\dagger)\mathbf{h}_{RS} \parallel}, \tag{3.27}$$

where $\mathbf{I} - \hat{\mathbf{h}}_{RD}\hat{\mathbf{h}}_{RD}^\dagger$ is the orthogonal projector onto $\mathbf{h}_{RD}^\perp$ and $\hat{\mathbf{h}}_{RD}$ is the normalized vector of $\mathbf{h}_{RD}$.

For $\hat{\mathbf{w}}$, the objective is to maximize the secrecy rate of the PU. Due to the presence of multiple eavesdroppers, it is typically difficult to obtain the optimal $\hat{\mathbf{w}}^\star$. Instead, a suboptimal solution is devised as follows. The cluster selects $\hat{\mathbf{w}}$ to null out the PU's information at all eavesdroppers[3], i.e., $\mathbf{H}_{RE}^\dagger\hat{\mathbf{w}} = 0$. By doing so, the transmission rate at all eavesdroppers are zero. Thus, maximizing the secrecy rate is equivalent to maximizing R_D, which can be given by

$$R_D = W \log_2(1 + \xi + P_2 \frac{\mid \mathbf{h}_{RD}^\dagger\hat{\mathbf{w}} \mid^2}{N_0 W}), \tag{3.28}$$

where ξ is the same as that in (3.2).

As mentioned before, $\mathbf{w}$ should also be in the null space of $\mathbf{h}_{RS}^\dagger$. Thus, the optimal $\hat{\mathbf{w}}^\star$ can be selected such that $\mid \mathbf{h}_{RD}^\dagger\hat{\mathbf{w}} \mid$ is maximized under the constraint that $\mathbf{H}_{RE}^\dagger\hat{\mathbf{w}} = 0$ and $\mathbf{h}_{RS}^\dagger\mathbf{w} = 0$. Define a matrix $\mathbf{H}_R$, which contains $\mathbf{h}_{RS}$ and $\mathbf{H}_{RE}$, i.e., $\mathbf{H}_R = [\mathbf{h}_{RS}\ \mathbf{H}_{RE}]$. Then, the constraint becomes $\mathbf{H}_R^\dagger\mathbf{w} = 0$. To satisfy it, $\hat{\mathbf{w}}$ should belong to the subspace of $\mathbf{H}_R^\perp$, i.e., the null space of $\mathbf{H}_R$. To maximize $\mid \mathbf{h}_{RD}^\dagger\hat{\mathbf{w}} \mid$, the optimal $\hat{\mathbf{w}}^\star$ should be closest to $\mathbf{h}_{RD}^\dagger$ and meanwhile belongs to $\mathbf{H}_R^\perp$. Thus, $\hat{\mathbf{w}}^\star$ should be the orthogonal projection of $\mathbf{h}_{RD}$ onto the subspace $\mathbf{H}_R^\perp$. Then, $\hat{\mathbf{w}}^\star$ can be given by

$$\hat{\mathbf{w}}^\star = \frac{(\mathbf{I} - \mathbf{H}_R(\mathbf{H}_R^\dagger\mathbf{H}_R)^{-1}\mathbf{H}_R^\dagger)\mathbf{h}_{RD}}{\parallel (\mathbf{I} - \mathbf{H}_R(\mathbf{H}_R^\dagger\mathbf{H}_R)^{-1}\mathbf{H}_R^\dagger)\mathbf{h}_{RD} \parallel}, \tag{3.29}$$

[3] Note that the number of SUs needs to be greater than that of eavesdroppers for this purpose.

where $\mathbf{I} - \mathbf{H}_R(\mathbf{H}_R^\dagger \mathbf{H}_R)^{-1}\mathbf{H}_R^\dagger$ is the orthogonal projector on $\mathbf{H}_R^\perp$.

Step 2: Determination of P_1, P_2 and α. Substituting (3.27) and (3.29) into (3.25) and (3.28), respectively, it can be seen that $\bar{R}_S$ is a function of P_1 and α, while R_D is a function of P_2. Given a certain α, the cluster needs to select P_1 to meet the expected transmission rate $\bar{R}_{EX}$ and the rest of power, i.e., P_2, contributes to R_D. Similar to the Appendix, when the secrecy rate is maximized, we have $\alpha = \frac{R_D}{R_R+R_D}$. Therefore, we have the following equations:

$$\begin{aligned}(1-\alpha)W\log_2(1+\frac{P_1 \mid \mathbf{h}_{RS}^\dagger \hat{\mathbf{v}}^\star \mid^2}{N_0 W}) &= \bar{R}_{EX} \\ \alpha = \frac{R_D}{R_R+R_D} \quad & P1+P2 = P_{max}.\end{aligned} \tag{3.30}$$

Solving the above equations, we have

$$\begin{aligned}P_1 &= \frac{(R_R N_0 + W\xi N_0 + \mid \mathbf{h}_{RD}^\dagger \hat{\mathbf{w}}^\star \mid^2)\bar{R}_{EX}}{R_R \mid \mathbf{h}_{RS}^\dagger \hat{\mathbf{v}}^\star \mid^2 + \mid \mathbf{h}_{RD}^\dagger \hat{\mathbf{w}}^\star \mid^2 \bar{R}_{EX}} \\ \alpha &= 1 - \frac{N_0 \bar{R}_{EX}}{P_1 \mid \mathbf{h}_{RS}^\dagger \hat{\mathbf{v}}^\star \mid^2}\end{aligned} \tag{3.31}$$

3.5 C-B Cooperation Scheme without E-CSI (CBNE)

When E-CSI is unknown, it is impossible for the PU to determine the optimal length for the rewarding time, i.e., $(1-\alpha)T$. Therefore, from the perspective of the PU, it desires that the SUs will make their best efforts to help for secure communication. To this end, the PU grants a period time to SUs such that the need of SUs can be met, i.e., $\bar{R}_{EX}$ of the SUs can be obtained. In return, the SUs will make the best efforts to help the PU, i.e., to devote the maximum power P_{max} for cooperation.

3.5.1 Problem Formulation

The cooperation is carried out in a three-phase fashion, as shown in Fig. 2(a). In the first phase, the transmission rate from S to the cluster and D are the same as in Section 3.4.1, which are given by (3.14) and (3.17), respectively.

In the second phase, all the cluster members transmit a combination of a weighted version of the re-encoded symbol $\tilde{s}$ and an artificial noise. Similar to [101], the artificial noise is leveraged to mask the concurrent transmission from S to D. As such, the cluster transmits $\mathbf{x}$, which is given by $\mathbf{x} = \mathbf{w}\tilde{s} + \mathbf{n}_a$, where $\mathbf{w}$ is the column vector of the weights of all SUs in the cluster and $\mathbf{n}_a$ is the artificial noise. Then, the received signals $y_{D,2}$ and $\mathbf{y}_{E,2}$ at D and eavesdroppers in the second phase can be written as:

$$\begin{aligned} y_{D,2} &= \mathbf{h}_{RD}^{\dagger}\mathbf{w}\tilde{s} + \mathbf{h}_{RD}^{\dagger}\mathbf{n}_a + n_{RD} \\ \mathbf{y}_{E,2} &= \mathbf{h}_{RE}^{\dagger}\mathbf{w}\tilde{s} + \mathbf{h}_{RE}^{\dagger}\mathbf{n}_a + \mathbf{n}_{RE} \end{aligned} \tag{3.32}$$

As mentioned before, the total power constraint of the cluster for cooperation is P_{max}. Denote the power spent for transmitting the information symbol $\tilde{s}$ and the artificial noise $\mathbf{n}_a$ by P_I and P_N, respectively. It holds that $P_I + P_N \leq P_{max}$. To enhance the security of the PU, the cluster has to allocate the power properly.

Due to the unknown CSI related to the eavesdroppers, the cluster performs in the following way. In order to avoid interfering with D, the artificial noise should be transmitted in the null space of $\mathbf{h}_{RD}$ such that $\mathbf{h}_{RD}^{\dagger}\mathbf{n}_a = 0$. Moreover, instead of transmitting in certain dimension, the power of artificial noise should be spread uniformly in the dimensions of the null space of $\mathbf{h}_{RD}$ [97]. Since the artificial noise does not interfere with D but the eavesdroppers, more power allocated to the artificial noise is more beneficial to increase the secrecy rate. However, allocating all the power to the artificial noise will cause that the transmission rate at D becomes extremely low, which is not desired. To avoid this, the power allocated to information symbol transmission, i.e., $\mathbf{w}^{\dagger}\mathbf{w}$, should guarantee that the transmission rate at D is above a predefined required transmission rate, which is similar to the work in [87]. Denote this predefined rate by $\bar{R}_Q$ and $\bar{R}_D$ should be greater than $\bar{R}_Q$ in order to meet this requirement. Therefore, the cluster allocates the minimum power for the information symbol transmission to achieve $\bar{R}_Q$ so that more power can be left to be utilized to confound the eavesdroppers.

The last phase is the same as that in Section 3.4.1 and the overall transmission rate $\bar{R}_S$ can be expressed as (3.20), for a given α.

3.5.2 Cooperation Parameters Determination

Optimal Weight Selection

To achieve the above goal, we first determine the minimum power for $\bar{R}_Q$, which can be obtained by solving the following problem:

$$\begin{aligned} &\min_{\mathbf{w}} \ \ \mathbf{w}^{\dagger}\mathbf{w} \\ &s.t. \ \ \alpha W \log_2(1+\xi+\frac{\mathbf{w}^{\dagger}\mathbf{h}_{RD}\mathbf{h}_{RD}^{\dagger}\mathbf{w}}{N_0 W}) \geq \bar{R}_Q, \end{aligned} \tag{3.33}$$

where ξ is the same as in (3.2). The left hand side of the constraint is the overall transmission rate, which equals to α multiplied by R_D in (3.17). The inequality constraint yields the same result as the equality constraint. Thus, for the low SNR regime, the constraint can be further represented by

$$\mathbf{w}^{\dagger}\mathbf{h}_{RD}\mathbf{h}_{RD}^{\dagger}\mathbf{w} = \vartheta, \tag{3.34}$$

where $\vartheta = N_0 W(\frac{R_Q}{\alpha W} - \xi)$. Defining $\widetilde{\mathbf{H}} = \mathbf{h}_{RD}\mathbf{h}_{RD}^{\dagger}$ and applying the method of Lagrange multipliers, the Lagrange multiplier function is given by

$$L(\mathbf{w}, \lambda) = \mathbf{w}^{\dagger}\mathbf{w} - \lambda(\mathbf{w}^{\dagger}\widetilde{\mathbf{H}}\mathbf{w} - \vartheta), \tag{3.35}$$

where λ is the Lagrange multiplier. Take the derivative of $L(\mathbf{w}, \lambda)$ with respect to $\mathbf{w}^{\dagger}$, and let it be equal to zero. Then, we have $\widetilde{\mathbf{H}}\mathbf{w} = \frac{\mathbf{w}}{\lambda}$. It can be seen that $1/\lambda$ is the eigenvalue of $\widetilde{\mathbf{H}}$, while $\mathbf{w}$ is the corresponding eigenvector. Multiplying both sides of this equation by $\mathbf{w}^{\dagger}\lambda$, we can obtain

$$\mathbf{w}^{\dagger}\mathbf{w} = \lambda\mathbf{w}^{\dagger}\widetilde{\mathbf{H}}\mathbf{w} = \lambda\vartheta, \tag{3.36}$$

where the last equality holds due to the constraint in (3.34). It can be seen that minimizing the transmission power, i.e., $\mathbf{w}^{\dagger}\mathbf{w}$, is equivalent to minimizing λ or to maximizing $1/\lambda$, since ϑ is a constant. Therefore, the optimal $\mathbf{w}^{\star}$ should be selected as the eigenvector of $\widetilde{\mathbf{H}}$ corresponding to its largest eigenvalue. In other words, $\mathbf{w}^{\star}$ can be given by $\mathbf{w} = \varsigma\mathbf{n}$, where $\mathbf{n}$ is the normalized principal eigenvector of $\widetilde{\mathbf{H}}$ and the scalar ς is given by $\varsigma = \sqrt{\frac{\vartheta}{\mathbf{n}^{\dagger}\widetilde{\mathbf{H}}\mathbf{n}}}$. With $\mathbf{w}^{\star}$, the cluster spends the minimum power to meet the QoS requirement, and then, more power can be utilized to spread the artificial noise to confound the eavesdroppers.

Time Allocation

$\beta^{\star}$ can be determined by substituting (3.17) into (3.12), when the optimal $\mathbf{w}^{\star}$ is selected. The PU selects α such that the SUs can achieve the expected transmission rate and in return the SUs make their best efforts to help the PU. The overall transmission rate $\bar{R}_S$ at the secondary receiver is given in (3.20). To achieve $\bar{R}_{EX}$, α can be determined as

$$\alpha = 1 - \frac{\bar{R}_{EX}}{P_{max} \parallel \mathbf{h}_{RS} \parallel^2} \tag{3.37}$$

3.6 Simulation results

In this section, we present simulation results to provide insight of the proposed cooperation schemes. In the simulation, the bandwidth W and T are set to be one unit, while P_{max} and noise power are set to 2 mw and 1 mw, respectively. For R-J scheme, Fig. 3.3 shows the trends of the overall secrecy rate $\bar{R}_{SEC}$ of the PU with respect to the time allocation coefficient α, for different channel h_S between the SU and its corresponding receiver. It can be seen that $\bar{R}_{SEC}$ first increases and then decreases with α increasing due to the fact that SUs determine their effort according to the time that the PU grants to them. In addition, the maximum $\bar{R}_{SEC}$ is circled for the three lines and the corresponding optimal $\alpha^{\star}$ is 0.5, 0.55, and 0.6, respectively. Moreover, both $\bar{R}_{SEC}$ and the optimal $\alpha^{\star}$ increase when the channel gain $|h_S|$ increases. This is because a better channel condition between the SU and its corresponding receiver results in a better transmission rate, and hence, the PU can allocate a shorter period of time to SUs to achieve the same level of SUs' effort, or the SUs are willing to devote more transmission power for cooperation when given the same rewarding time.

Fig. 3.4 shows $\bar{R}_{SEC}$ of the PU obtained by using R-J scheme and equal-duration relay jammer (EDRJ) scheme. The only difference between EDRJ scheme and R-J scheme is that the time durations for the first two phases in EDRJ are equal and the secrecy rate is maximized without considering time allocation. It can be seen that R-J scheme outperforms EDRJ because R-J scheme jointly optimizes the time and transmission power to maximize $\bar{R}_{SEC}$. In other words, the scheme without considering time allocation is not optimal, which is consistent with the analysis in Section 3.3.2.

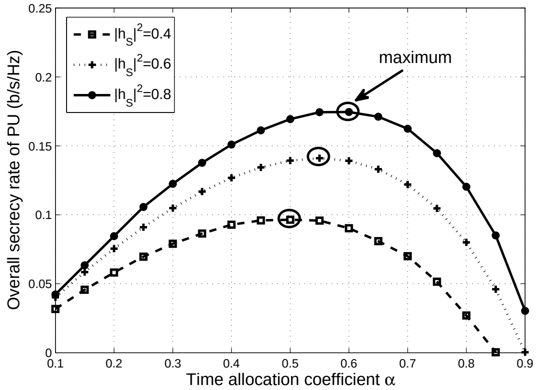


Figure 3.3: Overall secrecy rate of PU versus α for R-J scheme for $|h_S^2|$ =0.4, 0.6, 0.8, respectively ($|h_{RD}|^2 = 0.8$, $|h_{RE}|^2 = 0.5$, $|h_{JD}|^2 = 0.4$, $|h_{JE}|^2 = 0.8$, and R_{EX}=0.4 bit/s/Hz).

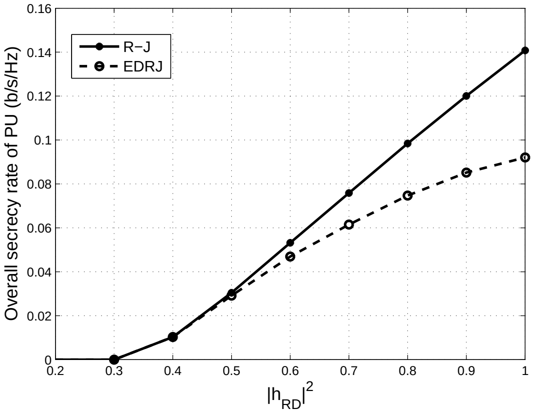


Figure 3.4: Comparison between R-J scheme and EDRJ scheme ($|h_{SD}|^2 = 0.3$, $|h_{SE}|^2 = 0.4$, $|h_{SR}|^2 = 0.6$, $|h_{RE}|^2 = 0.3$, $|h_{JD}|^2 = 0.3$, and $|h_{JE}|^2 = 0.5$)

Fig. 3.5 shows the access time of SUs (i.e., $1-\alpha^*$) when cooperating with the PU using R-J scheme. It can be seen that the access time decreases when the channel gain of h_{RS} increases. This is because with a better channel, the PU can grant a shorter time to SUs to obtain the same level of efforts from SUs to maximize the PU's secrecy rate. It also shows that with a smaller expected transmission rate, the PU can grant a shorter time to SUs to achieve the same level of SUs' effort, or the SUs are willing to devote more transmission power for cooperation when

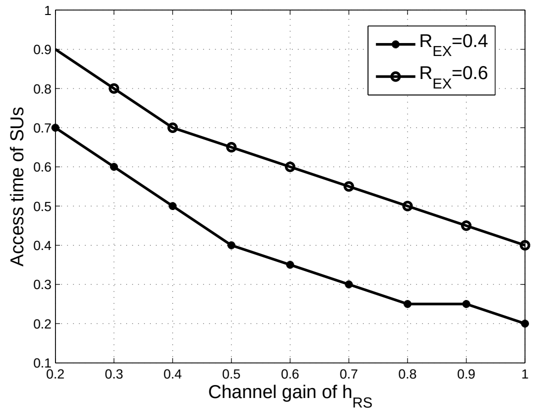


Figure 3.5: Access time of SUs versus channel condition h_{RS} for R-J scheme.

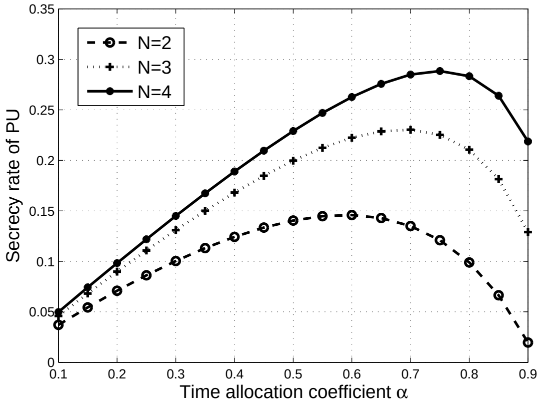


Figure 3.6: Overall secrecy rate of the PU versus α for CBSE scheme ($|h_{SD}|^2 = 0.3$, $|h_{SE}|^2 = 0.4$, the worst channel $|h_{SR,i}|^2$ is set to 0.4).

given the same rewarding time.

Fig. 3.6 shows $\bar{R}_{SEC}$ of the PU when cooperating with a cluster of SUs. For simplicity, the complex channels between all the SUs and D are approximately the same and equal to $e^{j\frac{\pi}{4}}$; similarly the complex channels between SUs and E are set to $0.8e^{j\frac{\pi}{4}}$. It can be seen that there exists an optimal $\alpha^{\star}$ such that $\bar{R}_{SEC}$ can achieve the maximum value. This is because of the result of the strategy of SUs, which is presented in the system model. Moreover, $\bar{R}_{SEC}$ increases when the total number of SUs (N) in the cluster increases. This is because more SUs

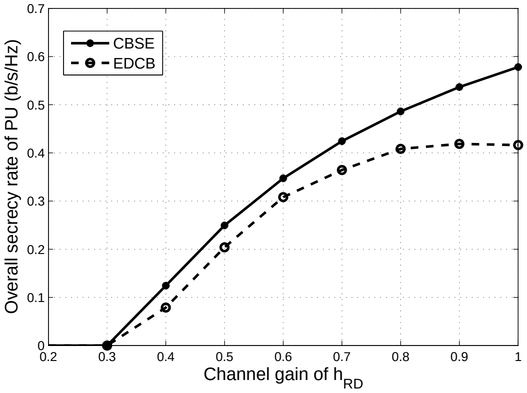


Figure 3.7: Comparison between CBSE scheme and EDCB scheme ($|h_{RE}| = 0.3$, $|h_{SD}| = 0.3$, $|h_{SE}| = 0.4$, $N = 3$, and the worst channel $|h_{SR,i}|^2 = 0.4$).

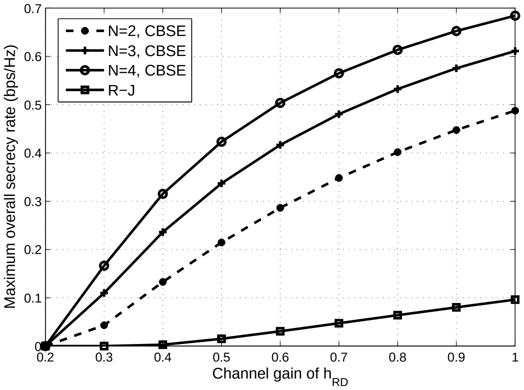


Figure 3.8: Comparison between R-J scheme and CBSE scheme.

can provide larger array gain to increase the secrecy rate.

In the following simulations, the complex channel coefficient h is given by $|h| \cdot e^{j\theta}$, where $|h|$ is the channel gain and θ is uniformly distributed in $[0, 2\pi)$. We obtain the average results using Monte Carlo simulation which consists of 1000 trials. Fig. 3.7 shows $\bar{R}_{SEC}$ of the PU obtained by using CBSE and equal-duration cluster beamforming scheme (EDCB) in the presence of an eavesdropper. The only difference between EDCB and CBSE is that the time durations for the first two phases are equal in EDCB and the secrecy rate is maximized without

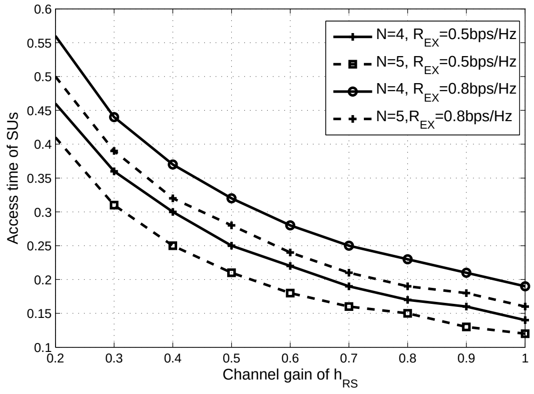


Figure 3.9: Access time versus channel condition h_{RS}.

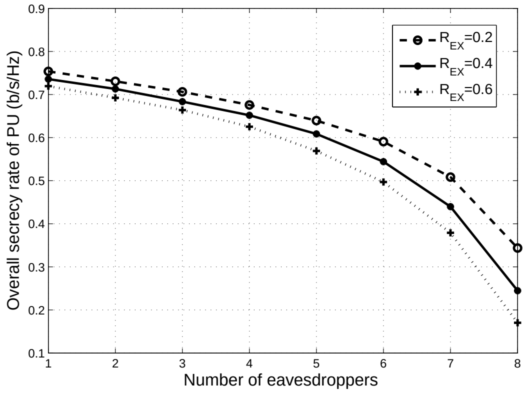


Figure 3.10: $\bar{R}_{SEC}$ of PU versus the number of eavesdroppers for CBME scheme ($|h_{RE}| = 0.4$, $|h_{RD}| = 0.5$, $|h_{RS}| = 0.6$, and $N = 10$).

considering time allocation. It can be seen that CBSE outperforms EDCB. That is because CBSE jointly optimizes the time and beamforming weights to maximize $\bar{R}_{SEC}$.

Fig. 3.8 shows $\bar{R}_{SEC}$ of the PU obtained by using CBSE scheme and R-J scheme. When the size of the cluster is equal to 2, which is the same to the number of SUs in R-J scheme, the secrecy rate obtained using CBSE is higher than that of R-J scheme. Moreover, the secrecy rate increases with the number of SUs in the cluster. This is because more SUs can provide larger array gain to increase the secrecy rate.

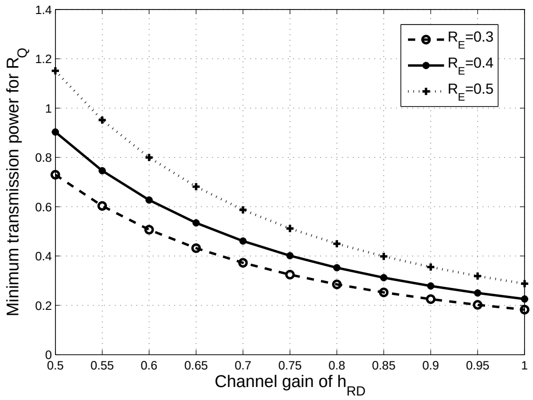


Figure 3.11: Minimum transmission power versus $|h_{RD}|$ for CBNE scheme ($|h_{RE}| = 0.4$, $|h_{RD}| = 0.5, 0.1$, $\bar{R}_Q = 0.5$ b/s/Hz and $N = 3$).

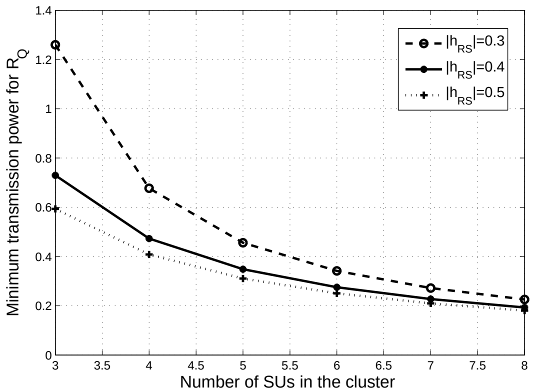


Figure 3.12: Minimum transmission power versus the number of SUs for CBNE scheme ($|h_{RD}| = 0.5$, $\bar{R}_{EX} = 0.3$ b/s/Hz).

Fig. 3.9 shows the access time of SUs using CBSE scheme when cooperating with the PU. It reveals that the access time reduces when the channel gain increases. The reason is that the PU can grant a shorter time to SUs to get the same efforts from SUs. Moreover, a smaller expected rate results in a shorter access time, since SUs needs less time for a smaller expected rate. With more SUs in the cluster, the access time will be reduced because more SUs provide larger array gain to increase the transmission rate.

Fig. 3.10 shows the overall secrecy rate of the PU with respect to the number of eavesdroppers (M) for different expected transmission rate of SUs. It can be seen that $\bar{R}_{SEC}$ drops as M increases. Moreover, it can also be seen that a lower $\bar{R}_{EX}$ results in a larger overall secrecy rate. This is because the SUs can spend less transmission power to achieve a lower $\bar{R}_{EX}$, and hence more power can be used to increase the secrecy rate of the PU.

Fig. 3.11 shows the minimum transmission power of SUs with respect to $|h_{RD}|$ for different expected transmission rate of SUs. It can be seen that the minimum transmission power drops as $|h_{RD}|$ increases. This is because SUs can spend less transmission power to achieve the same QoS requirement, with a better channel condition. It can also be seen that a smaller $\bar{R}_{EX}$ results in a lower transmission power. The reason is that only a shorter time is needed for SUs to achieve a smaller $\bar{R}_{EX}$, which causes a larger α; and then, the SUs can spend less transmission power to achieve the same $\bar{R}_{Q}$.

Fig. 3.12 shows the trends of the minimum transmission power of SUs versus the number of SUs in the cluster. It can be seen that the minimum transmission power drops as the number of SUs increases. Moreover, a smaller $|h_{RS}|$ results in a larger transmission power. This is because a longer duration for rewarding time is needed for SUs to achieve $\bar{R}_{EX}$ when $|h_{RS}|$ is smaller, which causes a smaller α; and hence, the SUs need to spend more transmission power to help the PU to satisfy the QoS requirement.

3.7 Summary

In this chapter, we have proposed two types of cooperative spectrum access to enhance the security of the PU and provide channel access opportunities to SUs. In order to enhance the security, the PU can either cooperate with two individual SUs (R-J scheme) or a cluster of SUs (C-B scheme). For R-J scheme, the two SUs act as one relay and one friendly jammer to increase the secrecy rate of the PU in the presence of one eavesdropper. For C-B scheme, a cluster of SUs enhance the secrecy of the PU's communication via collaborative beamforming.

Especially, for C-B scheme, three cooperation approaches have been proposed for the scenarios with one eavesdropper, with multiple eavesdroppers, and without any information about eavesdroppers. To maximize the secrecy rate, joint time and transmission power allocation is considered in R-J scheme, while time allocation and weight selection are jointly optimized in C-B schemes. We have shown through simulation results that with the proposed schemes, the secrecy of PU's communications can be significantly enhanced and the SUs can acquire certain access time.

Chapter 4

Risk-aware Cooperation for Access in Multi-channel CRNs

In this chapter, risk-aware cooperative spectrum access schemes for the CRN with multiple channels are proposed, whereby multiple PUs operating over different channels choose trustworthy SUs as relays to improve throughput, and in return SUs gain transmission opportunities. Specifically, cooperation over a single channel is studied first, which involves a PU selecting the suitable SU and granting a period of access time to the selected SU as a reward, considering trustworthiness of SUs. The above procedure is modeled as a Stackelberg game, through which access time allocation and power allocation are obtained. Based on the outcomes of the single-channel scenario, cooperation over multiple channels is studied. In order to better exploit spectrum access opportunities, a secondary network-centric cluster-based (SCC) scheme is proposed for the multi-channel scenario, whereby SUs first form a cluster, select the best SUs to obtain the maximum aggregate access time using maximum weight matching, and then share the obtained channels fairly using congestion game and quadrature signalling. The condition for Nash Equilibrium (NE) of the congestion game is provided and an algorithm for the SCC scheme is devised. Numerical results demonstrate that, with the proposed scheme, PUs can achieve higher throughput, while SUs can get more average access time and achieve higher fairness, compared with the random channel access approach.

4.1 Literature Review

Cooperative cognitive radio networking have been proposed to overcome the limitations of the spectrum sensing [40–42,44,46,56], whereby SUs cooperate with PUs to improve latter's transmission performance, and in return gain transmission opportunities. Therefore, both PUs and SUs can benefit from cooperation, which creates a win-win situation. In [41], the PU leases a fraction of access time to SUs in exchange for cooperation to increase the transmission rate, and during the rewarding time the SUs transmit simultaneously by selecting suitable transmission power. In [40], SUs cooperate to improve the PU's transmission rate and share the rewarding resource via a payment mechanism. A two-phase cooperation scheme is proposed in [46], whereby the PU transmits its signal to the SU in the first phase, and then the SU decodes the received signal and superimposes it with its own signal to broadcast in the second phase, using different power levels. In [42], different cooperation schemes are proposed, whereby the PU can cooperate with trustworthy SUs to enhance its security level and SUs can gain transmission opportunities.

However, all the above works only consider cooperation at the transmission link, i.e., one pair of PU and SU(s), which might not be sufficient to exploit the cooperation benefits in the whole network. This is because there exist multiple links in the network, which causes competition among PUs when they choose SUs. In [47], the authors consider multiple PUs performing cooperation with multiple SUs in the network, where the transmission of PUs are divided into different frames and different pairs of PU and SU perform cooperation over different frames. However, it is still limited to a single channel. In practice, a system usually consists of multiple channels, allowing users to communicate simultaneously. Therefore, a more realistic scenario

Table 4.1: The main notations.

Symbol	Definition
$\mathcal{N}$	The set of SUs in the cluster, $\lvert\mathcal{N}\rvert = N$
$\mathcal{M}$	The set of inactive SUs in the cluster, $\lvert\mathcal{M}\rvert = M$
$\mathcal{K}$	The set of channels in the network, $\lvert\mathcal{K}\rvert = K$
$\alpha_i(j)$	The access time allocation coefficient when the PU on channel j cooperates with SU_i
$U_p^i(j)$	The utility function of the PU on channel j when cooperating with SU_i in Stackelberg game
$U_s^i(j)$	The utility function of SU_i when cooperating with the PU on channel j in Stackelberg game
$P_c^i(j)$	The transmission power of the PU on channel j when cooperating with SU_i
$h_{ps}^i(j)$	The channel gain from PU_j to SU_i
$h_{pb}(j)$	The channel gain from PU_j to the base station
h_{sb}^i	The channel gain from SU_i to the base station
h_s^i	The channel gain from SU_i to the corresponding secondary receiver
P_s^i	The transmission power of SU_i
Tr_i	The trust value of SU_i
Ψ_i	The duration of the rewarding access time of channel i
U_i^j	The utility of SU_i in the congestion game
n_i	The total number of inactive SUs choosing channel i in congestion game
$\zeta(n_i)$	The share of channel i which each SU selecting that channel can obtain
$n(S)$	The congestion vector corresponding to strategy profile S

is that cooperation among multiple PUs and multiple SUs could be performed over different channels simultaneously. However, the existing solutions might not be applicable, since they are designed either for one pair of PU and SU or multiple PUs and multiple SUs over one channel. Moreover, it is often assumed that SUs are well-behaved during cooperation. When there exist some dishonest users, or even malicious ones, those SUs can participate in cooperation, and hence cooperation may incur risks

4.2 System Model

This section presents the details of the cooperative cognitive radio networking model under consideration, together with the main system parameters, shown in Table 4.1.

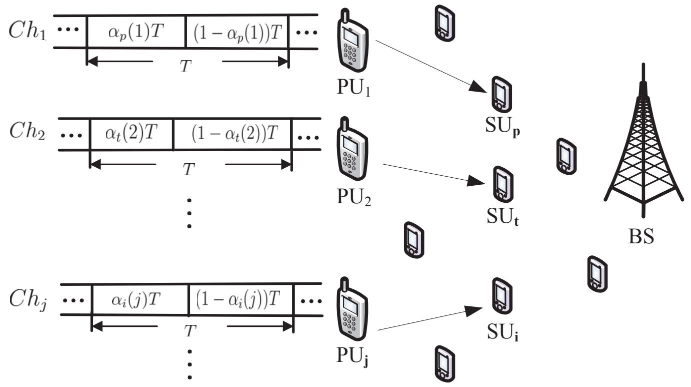


Figure 4.1: Cooperative cognitive radio network with multiple channels

4.2.1 MAC Layer

As shown in Fig. 4.1, the system consists of two components, the infrastructure-based primary network and the ad hoc secondary network. The primary network with multiple channels (K channels) allows K PUs to transmit data simultaneously. Each PU communicates with the base station (BS) over one channel in a time slot with length T, and the PU over a ceratin channel can be indicated by the channel index, e.g., PU_j denotes the PU operating over channel j, where $j \in \{1, 2, ..., K\}$. In the secondary network, SUs transmit data to the corresponding receivers. Motivated by the poor quality of the primary link or large volume of data transmission requirement, PUs may seek for the opportunities to cooperate with SUs to increase the throughput. For cooperation, one PU selects one SU as a relay which adopts the Amplify-and-Forward (AF) mode [102] to forward the PU's message to improve the throughput[1]. In return, the PU grants a period of access time as a reward to the cooperating SU. Specifically, for a given channel, e.g., channel j, the cooperation between PU_j and SU_i is carried out in the following way. A fraction $\alpha_i(j)$ of the time slot duration T ($0 < \alpha_i(j) \leq 1$) is used for cooperative communication. Note that for $\alpha_i(j)$, i corresponds to SU_i and j corresponds to channel j or PU_j. In the first duration

[1] The analysis for Decode-and-Forward (DF) mode is similar to that of AF mode. Hence, we only focus on AF cooperative scheme.

of $\frac{\alpha_i(j)T}{2}$, PU_j transmits data to SU_i, and in the subsequent duration of $\frac{\alpha_i(j)T}{2}$, SU_i relays the received data to BS. In the last period of $(1-\alpha_i(j))T$, which is the rewarding time, the cooperating SU_i transmits its own data to the corresponding secondary receiver. A common control channel is assumed for exchanging information among PUs, SUs, and BS (e.g., CSI), and for delivering the decision of the PUs to the secondary network.

4.2.2 Physical Layer

The channels between nodes are modeled as rayleigh block-fading channels, constant within each slot and varying over different slots. The channel gains from PU_j to BS, from PU_j to SU_i, from SU_i to BS, and from SU_i to its corresponding secondary receiver are denoted by $h_{pb}(j)$, $h_{ps}^i(j)$, h_{sb}^i, and h_s^i, respectively. Similar to [40,41,46,57], the channel state information (CSI) is assumed available in the system, which can be obtained by periodical pilots. The bandwidth for each channel is W. For cooperation, PU_j chooses power $P_c^i(j)$ for the transmission from PU_j to SU_i. SU_i is constrained to spend the same power P_s^i for both the cooperation and its own transmission so as to ensure that SU_i spends at least the same power for cooperation as which it is willing to spend for its own transmission. The one-sided power spectral density of the independent additive white Gaussian noise is N_0.

4.2.3 Security Threats

If all the SUs are well-behaved, both PU and SU can benefit from their cooperation. However, when there exist some dishonest or malicious SUs, the normal operation of CCRN cannot be guaranteed. Specifically, the following security issues arising in CCRN need to be considered.

During cooperation, the malicious SUs can alter the packets from the PU or fabricate packets and then forward them to the destination. A legitimate SU may be compromised and misbehaves when it is selected to cooperate with the PU, e.g., it may launch black or grey hole attack, etc. A dishonest SU may not obey the cooperation rule during cooperation to pursue more self-benefits, e.g., it may transmit its own packets instead of relaying the packets from the PU. Moreover, considering the mobility of SUs, the malicious or dishonest SUs may misbehave at one place and then move to other places. Since there is no record of the past behaviors, these users can have the same opportunity to be selected to cooperate with the PU, and then continue to harm the system. As a summary, we list the potential misbehaviors in CCRN as follows.

1. Selfishness: the cooperating SU may choose a lower transmission power than the expected one during cooperation or it just chooses not to forward the PU's message to save energy.
2. Maliciousness: the malicious SU may delete, modify or replace the bits in the DF mode. In AF mode, it may intentionally add some jamming signals to corrupt the PU's signal.
3. Dishonesty: the dishonest SU may provide fake CSI to gain transmission opportunities.

Without considering these security threats, the PU may choose an untrustworthy SU for cooperation, which may cause the failure of cooperation and degrade the QoS of PUs.

4.3 Cooperation over Single Channel

In this section, we will discuss the cooperation between a PU and an SU over channel j. Since we focus on a single channel, for ease of presentation, the channel indices in related notations are omitted, e.g., $\alpha_i(j)$ becomes α_i, $h_{ps}^i(j)$ becomes h_{ps}^i, and so on. Due to the poor channel condition or the traffic requirement, the PU may desire higher throughput which the direct transmission cannot achieve. In this case, the PU can choose an SU to act as a cooperating relay to increase its throughput, while in return grant a period of access time to the SU. Therefore, the cooperation can be performed on a basis of mutual benefits, where the PU can increase its throughput while the SU can gain transmission opportunities. To evaluate the risks of cooperation, trust value is applied and the above cooperation procedure is modeled using Stackelberg game. In such a game, the utilities of both the PU and the SU are presented and analyzed. By analyzing the game, the close-form solutions for the players' best strategies are derived, which constitute the Stackelberg equilibrium.

4.3.1 Trust Computational Model

In an unfriendly environment, the aforementioned security issues may rise, which cannot be well mitigated by means of cryptographic methodologies [103]. Thus, trust and reputation system is applied to address these issues [104]. Specifically, trust values are assigned to SUs and utilized to evaluate the behaviors of SUs. The primary system maintains a table for recording identities and the corresponding trust values of its one-hop neighboring SUs. In addition, BS keeps the trust values of all SUs in its domain. Each time after cooperation, the behavior of the selected SU will be evaluated and the trust value will be updated accordingly. Then, the trust value will be exchanged periodically between the PUs and the BS.

We use a Bayesian framework [105] [106] to evaluate the trust values: each entity is assumed to behave well with probability p, and misbehave with probability $(1-p)$, i.e., the behavior of the entity follows a Bernoulli distribution. Through a series of observations, a posteriori probability can be derived to estimate the future behaviors of the entity. Posteriori probabilities of binary events can be represented as the beta distribution. An expression of the probability density function (PDF) $f(\hat{p}|\kappa,\iota)$ in terms of the gamma function Γ is given by:

$$f(\hat{p}|\kappa,\iota)=\frac{\Gamma(\kappa+\iota)}{\Gamma(\kappa)\cdot\Gamma(\iota)}\cdot\hat{p}^{(\kappa-1)}\cdot(1-\hat{p})^{(\iota-1)}, \tag{4.1}$$

where $\hat{p}$ is the estimate of p, and κ, ι are the two parameters. The expectation of beta distribution is given by $E(\hat{p}) = \frac{\kappa}{(\kappa+\iota)}$, which can be used to represent the trust value of the relevant entity.

In our system, a malicious or dishonest SU_i behaves well with probability p_i and misbehaves with probability $1 - p_i$. In order to estimate the trustworthiness of SUs, BS needs to observe the ongoing transmission and evaluate the activities of SUs according to the received signals. To determine whether the relaying SU misbehaves or not, one approach is to utilize tracing symbols, which are known at both the source and the destination [107] [108]. Another way is based on the correlation between signals received from the source and the relay [109]. In addition, the misbehavior can also be detected based on the success or failure of transmitted frames via acknowledgment (ACK/NACK) [110]. Based on existing works in the literature, it is assumed that the misbehavior of relaying nodes can be detected. Consider a process with two possible outcomes (misbehavior or well-behavior), and let μ and ν be the observed number of good behaviors and misbehaviors, respectively. Then, the PDF of observing outcomes in the future can be expressed as a function of past observations by setting: $\kappa = \mu + 1$ and $\iota = \nu + 1$. Thus, the expected value of $\hat{p}$ can be determined from observations as follows:

$$E(\hat{p}) = \frac{\mu + 1}{(\mu + \nu + 2)}, \tag{4.2}$$

which is used as the trust value Tr_i of SU_i.

When new observations of a particular SU are made, e.g., δ observed misbehaviors and ξ observed good behaviors, the associated trust value can be updated using (4.2) by setting $\nu := \nu + \delta$ and $\mu := \mu + \xi$.

4.3.2 Stackelberg Game between PU and SU

Since the primary user and secondary user are selfish and rational, they might not have a common objective, i.e., the PU and the SU are interested in maximizing their own utilities. Thus, game theory can be applied to model the interactions between the two users. Moreover, considering different priorities for spectrum usage of PUs and SUs, Stackelberg game is most suitable to model the cooperation procedure. In the Stackelberg game, the PU acts as the leader and the SU acts as the follower. As the leader, the PU can choose the best strategies, aware of the effect of its decision on the strategies of the follower (the SU); while the SU can just choose its own strategies given the selected parameters of the PU. The utility functions for both PU and SU are respectively defined in the following. By analyzing the game, the best cooperating SU and the optimal cooperation parameters can be determined.

Primary User

Given a fixed time duration T, increasing the throughput is equivalent to increasing the average transmission rate. To this end, the PU selects the most suitable SU from the set $\mathbf{S}_p$ of its one-hop neighbors. Suppose that SU_i is chosen for cooperation, the PU decides the slot allocation parameter α_i and its transmission power P_c^i to maximize the potential profit, on the basis of available instantaneous CSI.

Without cooperation, the transmission rate of the direct communication can be given by

$$R_d = W \log_2(1 + \frac{P \left|h_{pb}\right|^2}{N_0}). \tag{4.3}$$

For cooperation, the transmission rate R_c^i through AF cooperative communication between the PU and SU_i is given as follows:

$$R_c^i = \frac{\alpha_i W}{2} \log_2[1 + \frac{P_c^i \left|h_{pb}\right|^2}{N_0} + f(P_c^i \left|h_{ps}^i\right|^2, P_s^i \left|h_{sb}^i\right|^2)], \tag{4.4}$$

where

$$f(P_c^i \left|h_{ps}^i\right|^2, P_s^i \left|h_{sb}^i\right|^2) = \frac{1}{N_0} \frac{P_c^i \left|h_{ps}^i\right|^2 P_s^i \left|h_{sb}^i\right|^2}{P_c^i \left|h_{ps}^i\right|^2 + P_s^i \left|h_{sb}^i\right|^2 + N_0}.$$

The factor $\frac{\alpha_i}{2}$ accounts for the fact that $\alpha_i T$ is used for cooperative relaying, which is further split into two phases. The PU chooses cooperation only when the transmission rate via cooperation is greater than that of the direct communication. Considering the trust value Tr_i of each neighboring SU_i, the utility function is given by

$$U_p^i = Tr_i \cdot R_c^i, \tag{4.5}$$

which indicates the expected transmission rate the PU can achieve through cooperation with SU_i. The objective of the PU is to maximize its utility function and the strategy is to choose the most suitable SU from the set of its one-hop neighboring SUs and the cooperation parameters, i.e., the slot allocation parameters α_i and the transmission power P_c^i for cooperation with the selected SU_i.

Secondary User

The SU can gain transmission opportunities through cooperation with the PU. In particular, the SU relays PU's data in the second phase and transmits its own data in the last phase. Assuming cooperation with the PU, the selected SU_i decides its transmission power, pertaining to the given α . The target of the SU is to maximize throughput (equivalent to the transmission rate) without expending too much energy. Following the cooperation agreement, SU_i spends the same power P_s^i for both cooperative and secondary transmissions. In particular, the transmission rate R_s^i for secondary transmission between SU_i and its corresponding receiver is given by

$$R_s^i(\alpha_i) = (1-\alpha_i)W\log_2(1+\frac{P_s^i\left|h_s^i\right|^2}{N_0}). \tag{4.6}$$

With energy consumption $P_s^i(1-\frac{\alpha_i}{2})T$, the utility function of SU_i can be represented by $R_s^i(\alpha_i)T - c\cdot P_s^i(1-\frac{\alpha_i}{2})T$, where c $(0 < c < 1)$ is the weight of energy consumption in the overall utility. With a smaller c, the SU values throughput more than energy consumption, and vice versa. Over the period of T, the utility function of SU_i is given by

$$U_s^i(\alpha_i) = \quad W\log_2(1+\tfrac{P_s^i\left|h_s^i\right|^2}{N_0})(1-\alpha_i) - c(1-\tfrac{\alpha_i}{2})P_s^i. \tag{4.7}$$

The objective of SU_i in the game is to maximize its utility by choosing the optimal transmission power P_s^i.

4.3.3 Game Analysis

As a sequential game, the Stackelberg game can be analyzed by the backward induction method. First, the optimal strategy of the SU (the follower) is analyzed, assuming the strategy of the PU (the leader) is fixed. Second, the PU decides the optimal strategy, aware of the outcomes of the first step. By doing so, the best response functions of both the PU and the SU are derived such that the corresponding utilities can be maximized. Then, the Stackelberg equilibrium of the proposed game can be achieved based on the best response functions.

Best Response Function of the SU

Assuming that the PU uses α_i for cooperation, SU_i selects the optimal transmission power to maximize its utility, which can be formulated as the following optimization problem:

$$\max_{P_s^i} U_s^i(\alpha_i) = (1-\alpha_i)W\log_2(1+\tfrac{P_s^i\left|h_s^i\right|^2}{N_0}) - c(1-\tfrac{\alpha_i}{2})P_s^i$$
$$\text{s.t. } 0 \leq P_s^i \leq P_{max},$$

where P_{max} is the power constraint for SU_i. Solving the above problem, the optimal transmission power can be determined.

Definition 1: Let $P_s^{*i}(\alpha_i)$ be the best response function of the secondary user if the utility of SU_i can achieve the maximum value when $P_s^{*i}(\alpha_i)$ is selected, for any given α_i, i,e., $\forall\ 0 < \alpha_i < 1, U_s^i(P_s^{*i}(\alpha_i), \alpha_i) \geq U_s^i(P_s^i(\alpha_i), \alpha_i)$.

Theorem 1. *The best response function of the secondary user $P_s^{*i}(\alpha_i)$ is given by $P_s^{*i}(\alpha_i) = \min\{\frac{(1-\alpha_i)W}{c(1-\frac{\alpha_i}{2})\ln 2} - \frac{N_0}{|h_s^i|^2}, P_{max}\}$, when the primary user selects a certain α_i for cooperation.*

Proof. Given the time allocation coefficient α_i, the utility function of SU_i is given as follows:

$$U_s^i(\alpha_i) = (1-\alpha_i)W\log_2(1+\frac{P_s^i\left|h_s^i\right|^2}{N_0}) - c(1-\frac{\alpha_i}{2})P_s^i. \tag{4.8}$$

From the above equation, it is easy to prove that the utility function first increases and then decreases with the increase of P_s^i without considering the power constraint. Therefore, there exists an optimal power such that U_s^i can reach the maximum value at that transmission power. Taking the first order partial derivative of the utility function with respect to P_s^i yields

$$\frac{\partial U_s^i}{\partial P_s^i} = \frac{(1-\alpha_i)W\left|h_s^i\right|^2}{(1+\frac{P_s^i h_s^{i2}}{N_0})N_0\ln 2} - c(1-\frac{\alpha_i}{2}). \tag{4.9}$$

Setting $\frac{\partial(U_s^i)}{\partial(P_s^i)} = 0$ yields the optimal transmission power, which is given by

$$\frac{(1-\alpha_i)W}{c(1-\frac{\alpha_i}{2})\ln 2} - \frac{N_0}{\left|h_s^i\right|^2}. \tag{4.10}$$

Taking the power constraint into consideration, the best response function $P_s^{*i}(\alpha_i)$ will be

$$P_s^{*i}(\alpha_i) = \min\{\frac{(1-\alpha_i)W}{c(1-\frac{\alpha_i}{2})\ln 2} - \frac{N_0}{|h_s^i|^2}, P_{max}\}. \tag{4.11}$$

This completes the proof. □

The first order derivative of the best response function with respect to α_i is given by $\frac{-\alpha_i W}{(-2+a)^2 c \ln 2)}$, which is negative. Therefore, the best transmission power of SU_i is a decreasing function of α_i. It is explained by that the SU is willing to spend more transmission power during cooperation if the PU allocates more time for the SU's transmission.

Best Response Function of the PU

Aware of the best response function of the SU, the PU decides its own best strategy for utility maximization. Thus, the best response function can be derived by solving the following optimization problem:

$$\max_{\alpha_i, P_c^i, i} \ \tfrac{\alpha_i W}{2} \log_2[1 + \tfrac{P_c^i |h_{pb}|^2}{N_0} + f(P_c^i \left|h_{ps}^i\right|^2, P_s^i \left|h_{sb}^i\right|^2)]$$
$$\text{s.t. } 0 < P_c^i \leq P_{max}, 0 < \alpha_i \leq 1, SU_i \subseteq \mathbf{S}_p.$$

Definition 2: Let $\alpha^*, P_c^{*i^*}, i^*$ be associated with the best response function of the primary user if the utility of the PU can achieve the maximum value when this strategy is selected.

Theorem 2. *The best response function of the primary user* $\alpha^*, P_c^{*i^*}, i^*$ *can be given by* $(\alpha^*, P_c^{*i^*}, i^*) = \arg\max_{\alpha_i, P_c^i, i} U_p^i$. *In particular,* $i^* = \arg\max U_p^i(P_c^{*i}, \alpha_i^*)$, *where*

$$P_c^{*i} = P_{max}$$

$$\alpha_i^* = \begin{cases} (15),\ \textit{if}\ \frac{W}{c\ln 2} - \frac{N_0}{|h_s^i|^2} < P_{max} \\ \max\{2 + \frac{2}{\frac{c\ln 2}{W}(P_{max} + \frac{N_0}{\left|h_s^i\right|^2}) - 2}, (15)\},\ \textit{otherwise} \end{cases} \tag{4.12}$$

P_c^{*i} and α_i^* are the optimal transmission power and time allocation coefficient respectively, assuming cooperation with SU_i. The optimal $P_c^{*i^*}$ and α_i^* correspond to the selected i^*.

Proof. Since the first order derivative of the utility function with respect to P_c^i is always positive, U_p is a monotonically increasing function as P_c^i increases. Moreover, considering the parameters P_c^i and α_i are independent, P_c^i should be selected as the maximum power so that the utility can reach the maximum value. Therefore, to solve the optimization problem, it is equivalent to optimize the utility function when $P_c^i = P_{max}$ and SU_i selects the best response $P_s^{*i}(\alpha_i)$. Since the first term in (4.11) monotonically decreases with respect to α_i, its maximum value is $\frac{W}{c\ln 2} - \frac{N_0}{|h_s^i|^2}$.

When $\frac{W}{c\ln 2} - \frac{N_0}{|h_s^i|^2} < P_{max}$, $P_s^{*i}(\alpha_i)$ always takes the value of the first term in (4.11). Substituting $P_c^i = P_{max}$ and $P_s^{*i}(\alpha_i) = \frac{(1-\alpha_i)W}{c(1-\frac{\alpha_i}{2})\ln 2} - \frac{N_0}{|h_s^i|^2}$ into the utility function of PU, the utility can be expressed by

$$\begin{aligned} U_p^i = \frac{\alpha_i W}{2}\log_2[1 + \frac{P_{max}\left|h_{pb}\right|^2}{N_0} + \\ f(P_{max}\left|h_{ps}^i\right|^2, P_s^{*i}(\alpha_i)\left|h_{sb}^i\right|^2)], \end{aligned} \tag{4.13}$$

which is a function of α_i. The first order derivative of (4.13) is given by

$$\frac{\partial U_p^i}{\partial \alpha_i} = A \cdot \alpha_i^2 + B \cdot \alpha_i + C, \tag{4.14}$$

where

$$\begin{aligned}
A =&P_{max}\left|h_{ps}^i\right|^2 c+2W\left|h_{sb}^i\right|^2+N_0c\\
B =&-2P_{max}\left|h_{ps}^i\right|^2 c-4W\left|h_{sb}^i\right|^2-2N_0c=-2\cdot A\\
C =&2W\left|h_{sb}^i\right|^2.
\end{aligned}$$

To find the optimal α_i^* such that U_p can be maximized, set first order derivative of (4.13) equal to 0. Since $C < A$, we have $B^2-4AC > 0$. Thus, the above quadratic function has real root(s). Considering the range of α_i ($0 < \alpha_i < 1$), there exists one and only one root α_r. The optimal α_i^* is given by

$$\begin{aligned}
\alpha_i^* &= \alpha_r = 1-\sqrt{1-\frac{C}{A}}\\
&= 1-\sqrt{1-\frac{2W\left|h_{sb}^i\right|^2}{P_{max}\left|h_{ps}^i\right|^2 c+2W\left|h_{sb}^i\right|^2+N_0c}}
\end{aligned} \tag{4.15}$$

When $\frac{W}{c\ln 2}-\frac{N_0}{|h_s^i|^2}\geq P_{max}$, there exists α_0 in the range from 0 to 1, such that $P_s^*(\alpha_0)=P_{max}$. Specifically, $\alpha_0=2+\frac{2}{D-2}$, where $D=\frac{c\ln 2}{W}(P_{max}+\frac{N_0}{|h_s^i|^2})$. The reason is that the range of D is from 0 to 1 due to the assumption that $\frac{W}{c\ln 2}-\frac{N_0}{|h_s^i|^2}\geq P_{max}$. For $\alpha_i \leq\ \alpha_0$, $P_s^{*i}(\alpha_i)$ always takes the value of P_{max}. Hence, U_p^i reaches the maximum value in that range when α_0 is chosen. For $\alpha_0 < \alpha_i \leq 1$, there exists one and only one root α_r for the above quadratic function, which is in the range from 0 to 1. If $\alpha_r < \alpha_0$, then $\frac{\partial U_p}{\partial \alpha_i} < 0$ when $\alpha_0 < \alpha_i \leq 1$. The derivative of U_p with respect to α_i is monotonically decreasing. Thus, the optimal $\alpha_i^*=\alpha_0$. Otherwise, the optimal $\alpha_i^*=\alpha_r$.

Based on the above analysis, the optimal α_i^* can be given as (4.12) in the theorem 2.

This completes the proof. □

4.3.4 Existence of the Stackelberg Equilibrium

In this section, we prove that the solutions P_s^* in (4.11) and α^* in (4.12) are the Stackelberg Equilibrium. For this purpose, we discuss the two cases with/without considering the power constraint of the SU using the following properties. The detailed proof for the properties can be found in Appendix C. Based on the properties, we first prove the existence of Stackelberg Equilibrium when the power constraint is not considered.

Property 1. The utility function U_s of the SU is concave with respect to its own power level P_s when the time allocation coefficient α is fixed.

For both cases, Property 1 always holds, which shows the concavity of the utility function of the SU. Due to Property 1, U_s is concave with respect to P_s. Without considering the power constraint, setting $\frac{\partial(U_s^i)}{\partial(P_s^i)} = 0$ yields the optimal transmission power P_s^*, which is given in (4.10). With P_s^* in (4.10), the SU can maximize its utility U_s.

For the case without considering the power constraint, we also have the following properties.

Property 2. For all SUs, the optimal transmission power P_s^* in (4.10) decreases with the time allocation coefficient α.

Property 3. The utility function of the primary user is concave with respect to the time allocation coefficient α, given that the optimal transmission power P_s^* of the SU in (4.10) is fixed.

Due to Property 2, there is a trade-off for the PU to select the time allocation coefficient α. When the PU allocates less time to the cooperating SU for transmission, the SU will choose a lower transmission power during cooperation, which results in a reduction in the utility of the PU. When the PU allocates more time for the SU, the PU will have less time for its own transmission, which may also lead to a decrease in its utility. In other words, the PU cannot keep increasing its utility by increasing α.

Due to Property 3, the optimal α can be obtained by setting $\frac{\partial U_p}{\partial \alpha} = 0$, since the utility function of the PU is concave with respect to α. Therefore, the PU can always find its optimal time allocation coefficient α^* in (4.15) such that $U_p(\alpha^*) \geq U_p(\alpha)$. Together with Property 1, given the time allocation coefficient α, the SU can always find its optimal transmission power P_s^* in (4.10). Then, P_s^* in (4.10) and α^* in (4.15) are the Stackelberg Equilibrium.

In the following, we will discuss the case with power constraint. Due to Property 2, P_s^* in (4.10) increases as α decreases. For a given value of α, P_s^* may achieve its maximum value P_{max}. Since the scenario before P_s^* approaches P_{max} is the same as the case without power constraint, we only discuss the case when $P_s^* = P_{max}$. When the SU chooses P_{max}, it is optimal for the PU to choose α_0, as in the analysis of α^* in Section 4.3.3. Therefore, we conclude that the solutions P_s^* in (4.11) and α^* in (4.12) are the Stackelberg Equilibrium.

4.3.5 Numerical Results

In this part, we present numerical results so as to provide insight into the proposed cooperative framework. Similar to [41], by normalizing the distance between PU and BS, the SU is approximately placed at the distance $d \in (0, 1)$ from the PU and $1 - d$ from the BS. Considering a path loss model, the average power gains between the PU and SU, and between the SU and BS, are $\left|h_{ps}^i\right|^2 = \frac{1}{d^\zeta}$ and $|h_{sb}^i|^2 = \frac{1}{(1-d)^\zeta}$, respectively, where $\zeta = 3.5$ is the path loss coefficient. Aiming at reducing the system parameters, the maximum secondary transmission power P_{max} is normalized to 1 and we choose $P_{max}/N_0 = 0$ dB.

Fig. 4.2 shows the the PU's throughput on certain channel, averaged over fading, versus the normalized distance d, for c = 0.2 and 0.5. It is seen that there exists a cooperation range in which the PU can cooperate with the SU to achieve a higher throughput than that of direct transmission. Further, a smaller weight c results in a larger cooperation range.

Fig. 4.3 shows the impact of trust values on the SU selection. A number of SU_i (i =

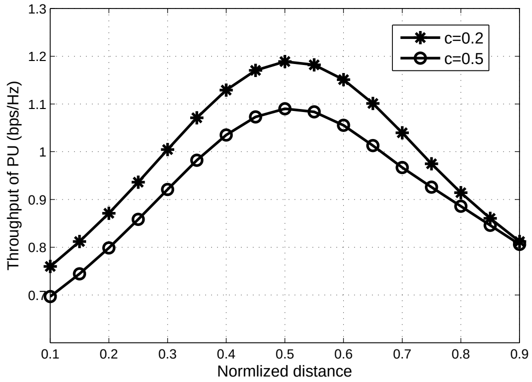


Figure 4.2: Throughput of PU, averaged over fading, versus the normalized distance d.

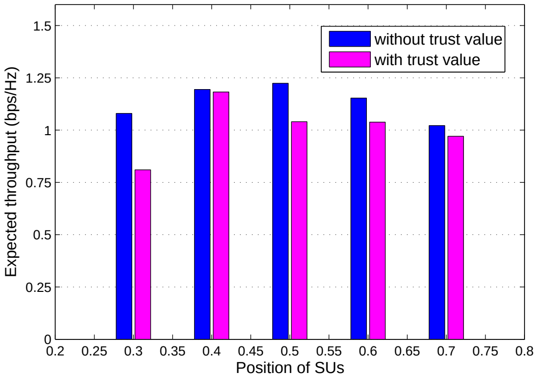


Figure 4.3: The impact of trust value on SU selection.

$1, 2, 3, 4, 5$) with associated trust values 0.75, 0.99, 0.85, 0.9, and 0.95, are located at the normalized distances d = 0.3, 0.4, 0.5, 0.6, and 0.7, respectively. Without considering trust values, the PU should select SU_3 since the PU can achieve the highest throughput via cooperation with SU_3. Considering trust values of SUs, SU_2 is the best choice since the PU can attain highest expected throughput via cooperation with SU_2.

4.4 Cooperation over Multiple Channels

In this section, we extend the cooperation scheme from the single-channel case to the multi-channel case, where each SU can only select one channel each time to perform cooperation over that channel. The approach for the single channel cannot bring the maximum benefit to the whole network because it only focuses on the interest of individual users. It is possible that multiple SUs compete with each other over some channels for transmission opportunities, while no SUs exploit the transmission opportunities over the other channels. Therefore, from the perspective of the whole secondary network, the transmission opportunities are not efficiently utilized; from the perspective of the individual SU, it is not guaranteed that the SU can obtain the chance to access the channel since it also depends on other SUs selecting the same channel. To maximize the total utility of the secondary network, the SCC scheme is proposed for multi-channel CRNs in the section.

4.4.1 SCC Scheme

To exploit the spectrum access opportunities efficiently, the SCC scheme is proposed with the objective of maximizing the total utility of the secondary network, which is defined as the aggregate rewarding access time of all channels. For a given channel, the rewarding access time can be obtained when the SU and the PU use the Stackelberg Equilibrium strategy for cooperation over that channel. Considering the secondary network is formed in ad hoc mode, to maximize the total network utility and the average access time per user, SUs first form a cluster, perform cooperation with PUs to gain transmission opportunities, and then share the obtained resource fairly.

Specifically, based on the geographic locations, SUs form a cluster $\mathcal{N}$ with size N to share CSI. Then, the best SUs can be selected for each channel, which perform cooperation with PUs, in order to achieve the maximum aggregate rewarding access time of different channels.

This problem corresponds to a maximum weight matching problem, which can be represented by the bipartite graph in Fig. 4.4. Particularly, the vertices correspond to SUs and PUs, while the weight on each edge represents the rewarding access time $1 - \alpha_i(j)T$ when SU_i and PU_j cooperate with each other. Finding the best SUs for cooperation to maximize the aggregate rewarding time is equivalent to finding the maximum weight matching in Fig. 4.4. The well known Hungarian algorithm can be performed to find the matching such that the sum of the weights can be maximized [111].

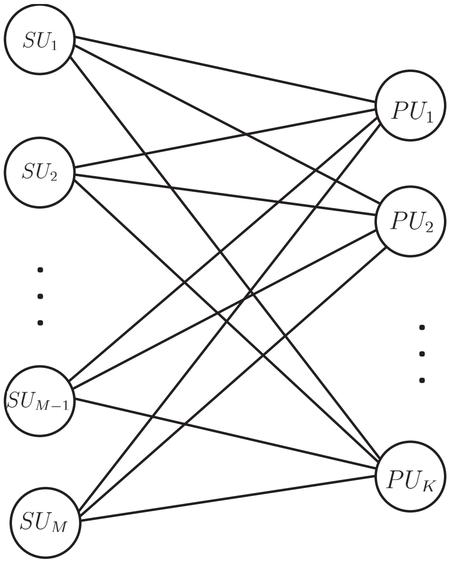


Figure 4.4: Maximum weight matching

Then, the selected SUs cooperate with the corresponding PUs over different channels using Stackelberg Equilibrium strategy to obtain the rewarding access time. After that, the SUs in the cluster start to share the obtained rewarding time fairly. For this purpose, SUs are divided into two classes: active SUs (i.e., the selected SUs to perform cooperation with PUs as relays) and inactive SUs (the rest SUs with the size of M). Considering that the active SUs spend the transmission power during cooperation, they should have a larger share of the rewarding time. To this end, two classes of users first share the channels using quadrature signaling, i.e., the active SUs stay in the current operating channels and use the in-phase component of

QAM for transmission, while each inactive SUs selects one channel to access and transmit by employing the quadrature component of QAM. By leveraging quadrature signaling, the active and inactive SUs can transmit concurrently without interference with each other. For each inactive SU, they also have to decide which channel to access to maximize their own utilities, i.e., the shares of rewarding time for accessing the channels. The decision-making process is modeled by a congestion game and the Nash Equilibrium (NE) strategy can be found. The share that each inactive SU can obtain is determined by the NE. With the SCC scheme, each SU can be guaranteed to gain certain access time. Moreover, the average access time obtained using the SCC scheme is longer than that using the random channel access approach, which will be shown in the numerical results.

Each inactive SU selects a access channel among the multiple channels with different rewarding time, aiming to maximize its own utility. The congestion game is leveraged to model this process, which is defined by the tuple $\{\mathcal{M}, \mathcal{K}, (\sum i)_{i\in\mathcal{M}}, (U_j^i)_{i\in\mathcal{M}, j\in\mathcal{K}}\}$, where $\mathcal{M} = \{1, 2, ..., M\}$ is the set of inactive SUs, $\mathcal{K} = \{1, 2, ..., K\}$ denotes the set of channels, $\sum i$ represents the strategy space of SU_i, and U_i^j is the utility function of SU_i when selecting channel j. Note that U_i^j is a decreasing function of the total number of SUs selecting the channel j, because of the competition or congestion. In other words, when more SUs select the same channel, each SU can obtain a less share. Each SU tries to maximize its utility by deciding which channel to access. The utility function of SU_i can be defined as follows:

$$U_i^j = \Psi_j \zeta(n_j), \tag{4.16}$$

where Ψ_j is the length of the rewarding access time of channel j, $\zeta(n_j)$ is the share of the rewarding access time which SU_i obtains over channel j, and n_j is the total number of inactive SUs selecting channel j. Therefore, U_j^i represents the access time that SU_i can have. For simplicity, the inactive SUs selecting the same channel share the rewarding time equally using TDMA, and then $\zeta(n_i) = 1/n_i$.

In the congestion game, if each one has chosen a strategy and no one can increase its utility by changing strategy unilaterally, the current strategy profile constitutes an NE.

Definition 3: A strategy profile $S^* = (s_1^*, s_2^*, \ldots, s_M^*)$ is an NE if and only if

$$U_i(s_i^*, s_{-i}^*) \geq U_i(s_i', s_{-i}^*), \forall i \in \mathcal{M}, s_i' \in S_i, \tag{4.17}$$

where s_i and s_{-i} are the strategies selected by SU_i and the other SUs, respectively. NE means no one can increase its utility unilaterally.

It is known that the congestion game always exists pure NE. The condition for NE in the congestion game is given as follows:

$$n_i = \lceil \frac{\Psi_i M - \sum_{j \neq i, j \in \mathcal{K}} \Psi_j}{\sum_{j \in \mathcal{K}} \Psi_j} \rceil + n', \tag{4.18}$$

where $n' \in \{0, 1, 2, \ldots, \lceil \frac{\Psi_i M + \Psi_i (K-1)}{\sum_{k \in \mathcal{K}} \Psi_k} \rceil - \lceil \frac{\Psi_i M - \sum_{k \neq i, k \in \mathcal{K}} \Psi_k}{\sum_{k \in \mathcal{K}} \Psi_k} \rceil - 1\}$. The detailed proof can be found in the Appendix C. Since any strategy profile which satisfies the above condition in (4.18) will constitute an NE, there exist multiple NEs in the proposed congestion game. In order for the SUs to select an NE strategy, procedure 2 in algorithm 5 can be used for SUs to determine which channel to access.

The whole procedure of SCC scheme is presented in Algorithm 1, which consists of two main parts: the best SUs selection and rewarding access time sharing.

4.4.2 Numerical Results

To evaluate the performance of the SCC scheme, similar to [86], we set up the simulation scenario as follows: the base station is placed at the origin (0, 0) and PUs are randomly located between $(0, d_{p,min})$ and $(0, d_{p,max})$; while SUs are randomly located between $(0, d_{s,min})$ and

Algorithm 3

```
// **Initialization**: Form the cluster based on geographic locations
// **Procedure 1**: Best SUs Selection
for each $SU_i \in \mathcal{N}$ do
    for $PU_j$ on channel $j$, $j \in \mathcal{K}$ do
        Calculate access time allocation $\alpha_{i,j}$ using (4.12)
        Calculate rewarding periods $\Psi_{i,j} = 1 - \alpha_{i,j}$.
    end for
end for
Run Hungarian algorithm to find the best SUs for cooperation
// **Procedure 2**: Rewarding Access Time Sharing
Set congestion vector $n(S) = (n_1, ..., n_K) = (0, 0, ..., 0)$.
Order the rewarding periods on each channel $[\Psi_1, \Psi_2, \ldots, \Psi_K]$ decreasingly according to
    the length.
for each $SU_i \subseteq \mathcal{N}$ do
    if $SU_i$ is active SU then
        $SU_i$ stays in the current operating channel.
        $SU_i$ employs the in-phase component for transmission.
    else
        for each $\Psi_j$, where $j \subseteq \mathcal{K}$ do
            Calculate $\Psi_j \zeta(n_j + 1)$.
        end for
        $SU_i$ selects the channel with maximum $\Psi_j \zeta(n_j + 1)$.
        $SU_i$ employs the quadrature component for transmission.
        $n_j = n_j + 1$.
    end if
end for
return
```

$(0, d_{s,max})$. The number of PUs is set to 5. The distances between nodes are normalized by $d_{p,max}$ and the previous path loss model is utilized to calculate average power gains.

Fig. 4.5 shows the impact of the number of inactive SUs (M) on the NE of the congestion game. Define channel selection indicator of channel i as the number of inactive SUs choosing channel i divided by the total number of inactive SUs, i.e., n_i/M, which reflects the popularity of the channel. When M is small, some channel(s) may not be chosen by any SU. For example, there is no inactive SU choosing channel 1 when $M = 8$. When M becomes higher, all

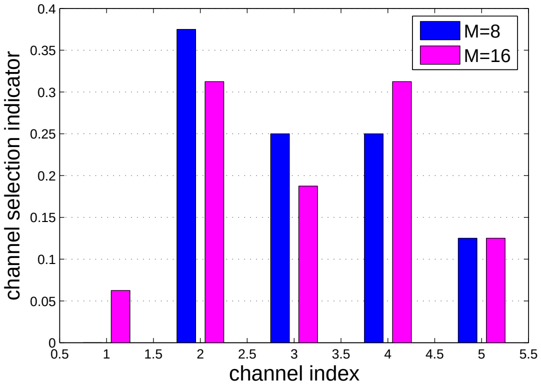


Figure 4.5: Impact of the number of inactive SUs on Nash Equilibrium

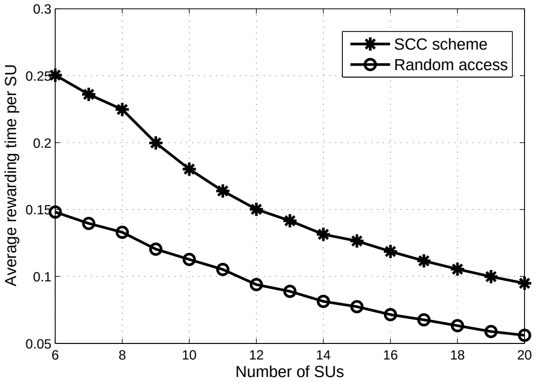


Figure 4.6: Average access time per SU averaged over fading for SCC scheme and random channel access

channels are selected by at least one SU and the selection indicator of each channel also changes to satisfy the NE condition.

Fig. 4.6 shows the average access time per user, averaged over fading, versus the size of the cluster. We compare the proposed scheme with the random channel access approach. It can be seen that each SU can obtain longer access time using the proposed scheme, compared with the random channel access approach. The reason is that the best SUs are selected to obtain the maximum aggregate time, which is fairly shared by all the SUs.

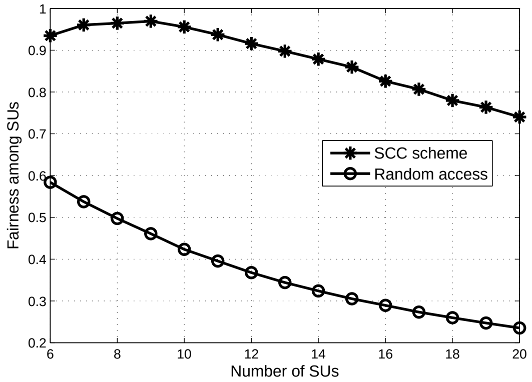


Figure 4.7: Fairness among SUs versus the number of SUs

Similar to [112], we define fairness as $\frac{(\sum_i U_i)^2}{N \sum_i U_i^2}$, where U_i is the access time obtained by SU_i. Fig. 4.7 shows the fairness among SUs. It can be seen that the fairness of the SCC scheme outperforms the random access approach. This is because each SU can obtain a certain share of access time using the SCC scheme, while only a few SUs can exclusively access the channel using the random channel access approach.

4.5 Summary

In this chapter, we have studied cooperative cognitive radio networking in multi-channel s-cenario, considering trustworthiness of SUs. We have investigated cooperation over a single channel by Stackelberg game. Based on the results of the single channel scenario, we have proposed a SCC scheme for the cooperation over multiple channels. In the SCC scheme, SUs form a cluster to maximize the total utility of the secondary network and share the obtained resources based on congestion game and quadrature signaling. Numerical results have demonstrated that, with the proposed schemes, the PUs can achieve higher throughput, while the SUs can obtain longer average access time, compared with the random channel access approach.

Chapter 5

Cooperation for Credits

In this chapter, we study the user cooperation to enhance the PU's security when SUs have no traffic, where the PU cooperates with SUs to transmit message securely in presence of multiple eavesdroppers [113]. To stimulate the cooperation of SUs, the PUs grant credits to them. The earned credits can be utilized by SUs for spectrum leasing in the future when they have traffic. In other words, the SUs can earn credits through cooperation with PUs and consume credits in spectrum trading market when needed. In this study, we mainly focus on the following issues: i) with whom to cooperate; ii) how to determine and share the credits. To address those issues, a cooperative framework is proposed, whereby the PU selects multiple SUs and stimulates them by granting an amount of rewards. Specifically, multiple SUs acting as cooperative relays and jammers are selected by the PU using greedy or cross-entropy based approaches. Then, the PU and the SUs negotiate for the payment and transmission power, which is modeled as a two-layer game. At the top layer, a buyer-seller game is utilized, where the PU pays to buy the service provided by the SUs. At the bottom layer, all the SUs share the reward by determining their transmission powers in a distributed way, which is formulated as a non-cooperative power selection game. By analyzing the game, the SUs can determine the transmission powers for cooperation, while the PU can select the best payment. To further improve the utility of the

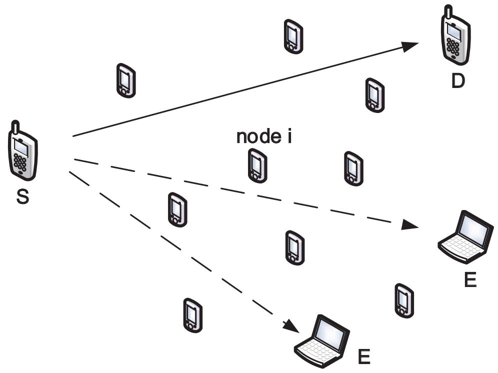


Figure 5.1: Cooperation for credits.

PU, a set of reward allocation coefficients are introduced and optimized using particle swarm optimization approach.

5.1 System Model

As depicted in Fig. 5.1, the system consists of a primary transmitter as the source (S), a primary receiver as the destination (D), M intermediate SUs ($i = 1, 2, ..., M$), and one or multiple eavesdroppers (E) who aim to decode the source's information [92]. It is known that when the channel between S and D is worse than that between S and E, the secrecy rate is zero. To transfer information securely, S requests the SUs for cooperation, which are all considered friendly[1]. For cooperation, it may not be the best for all the friendly nodes to participate. Moreover, the SUs can act as relay or jammer in cooperation. To maximize the secrecy rate, S has to select the suitable cooperative SUs and their roles (relay or jammer).

A slow, flat, block Rayleigh fading environment is considered, where the channel remains static in one time slot and changes independently over different time slots. The channel coeffi-

[1] The work in [114, 115] consider user cooperation with untrusted nodes.

cients from S to D and S to a specific E are denoted by h_{sd} and h_{se}, respectively. The channel coefficient from S to SU $i \in \mathcal{M}$ is denoted by h_s^i. Similarly, the channel coefficients from SU $i \in \mathcal{M}$ to D and E are h_d^i and h_e^i, respectively. The global CSI is assumed available for the system, including D-related CSI (D-CSI) and E-related CSI (E-CSI), which is a common assumption in PHY layer security literature [86, 87, 89, 90]. E-related CSI (E-CSI) can be obtained in the scenarios where the eavesdroppers are active in the network and their transmission can be monitored [86]. In addition, additive white Gaussian noise is assumed with zero mean and the one-side power spectral density is N_0. Moreover, each node is equipped with a single antenna and communicates with each other in a half-duplex mode.

5.2 Partner Selection

We use secrecy rate as a measure for secure communication, which is defined as the difference between the transmission rate at D and that at E. In what follows, we will first analyze the secrecy rate through cooperation and then select the suitable partners.

At the destination D, the SNR γ_{sd} from the direct link (S to D) is given by

$$\gamma_{sd} = \frac{P_s \left|h_{sd}\right|^2}{N_0}, \tag{5.1}$$

where P_s is the transmission power of the source.

Suppose that SU i is in the relay set $\mathbb{R}$, then the SNR from relay i using Amplify-and-Forward (AF) cooperative protocol can be given as follows [102]:

$$\gamma_d^i = \frac{1}{N_0} \frac{P_s \left|h_s^i\right|^2 P_i \left|h_d^i\right|^2}{P_s \left|h_s^i\right|^2 + P_i \left|h_d^i\right|^2 + N_0}, i \in \mathbb{R}, \tag{5.2}$$

where P_i is the transmission power of node i.

Suppose that SU j is in the jammer set $\mathbb{J}$, the interference γ_d^j caused by jammer j can be given as follow:

$$\gamma_d^j = \frac{P_j \left|h_d^j\right|^2}{N_0}, j \in \mathbb{J}. \tag{5.3}$$

Using maximal ratio combining (MRC), the achievable rate at D can be expressed as follows:

$$R_d = \frac{W}{2}\log_2(1 + \frac{\gamma_{sd} + \sum_{i\in\mathbb{R}} \gamma_d^i}{1 + \sum_{j\in\mathbb{J}} \gamma_d^j}). \tag{5.4}$$

At a generic eavesdropper, e.g., k-th E, the SNR γ_{se} from the source can be given as follows:

$$\gamma_{se} = \frac{P_s \left|h_{se}\right|^2}{N_0}. \tag{5.5}$$

The SNR γ_e^i from relay i, where $i \in \mathbb{R}$, can be given as follows:

$$\gamma_e^i = \frac{1}{N_0}\frac{P_s \left|h_s^i\right|^2 P_i \left|h_e^i\right|^2}{P_s \left|h_s^i\right|^2 + P_i \left|h_e^i\right|^2 + N_0}, i \in \mathbb{R}. \tag{5.6}$$

The interference γ_e^j caused by jammer j, where $j \in \mathbb{J}$, can be given as follow:

$$\gamma_e^j = \frac{P_j \left|h_e^j\right|^2}{N_0}, j \in \mathbb{J}. \tag{5.7}$$

Similarly, the achievable rate at the k-th E can be expressed as follows:

$$R_e^k = \frac{W}{2}\log_2(1 + \frac{\gamma_{se} + \sum_{i\in\mathbb{R}} \gamma_e^i}{1 + \sum_{j\in\mathbb{J}} \gamma_e^j}). \tag{5.8}$$

According to the definition of secrecy rate, the secrecy rate is given by

$$R_{sec}^k = R_d - R_e^k, \tag{5.9}$$

where R_d and R_e^k are given in (5.4) and (5.8), respectively.

Considering the presence of multiple eavesdroppers, the overall secrecy rate R_{sec} is given by

$$R_{sec} = \max\{0, \min_k\{R_d - R_e^k\}\}, \tag{5.10}$$

where R_e^k is the achievable rate at the k-th eavesdropper.

In the first step, the source selects the cooperative relays and jammers to maximize the secrecy rate, assuming that the transmission power of the potential participants is fixed. This problem can be formulated as follows:

$$\begin{aligned} &\max_{X_{i,j}, \forall i \in \{1,2,...,M\}} \quad R_{sec} \\ \text{s.t.} \quad &\sum_{j \in \{R,J,N_u\}} X_{i,j} = 1, \forall i \in \{1,2,...,M\} \\ &X_{i,j} \in \{0,1\}, \forall i \in \{1,2,...,M\} \text{ and } \forall j \in \{R,J,N_u\} \end{aligned}$$

Specifically, the binary variable $X_{i,j}$ indicates the role of SU i, where j can be $\{R, J, N_u\}$, which correspond to act as a relay (R), a jammer (J), or keep silent (N_u). For example, when $X_{i,R} = 1$, SU i acts as a relay. The secrecy rate $R_{sec} = \frac{W}{2}\log_2(1 + \frac{\gamma_{sd}+\sum_{i\in\mathbb{R}}\gamma_d^i}{1+\sum_{j\in\mathbb{J}}\gamma_d^j}) - \frac{W}{2}\log_2(1 + \frac{\gamma_{se}+\sum_{i\in\mathbb{R}}\gamma_e^i}{1+\sum_{j\in\mathbb{J}}\gamma_e^j})$, where the relay and jammer set can be determined by $\mathbb{R} = \{i, X_{i,R} = 1\}$ and $\mathbb{J} = \{i, X_{i,J} = 1\}$. Exclusive search can obtain the optimal solution. However, the complexity is high since the search space is exponential to the number of intermediate nodes. Instead, two heuristical algorithms are proposed in the following.

5.2.1 Greedy-based Partner Selection Algorithm

Based on the above formula, a greedy partner selection algorithm is developed, as shown in Algorithm 1. The main idea is to select the best cooperative SU at each round until the overall secrecy rate cannot be improved.

Algorithm 4 Greedy Parter Selection Algorithm

```
Input: $\mathcal{M}, h_s^i, h_d^i, h_e^i, \forall i \in \mathcal{M}$.
Output: Partner selection results $\mathbb{R}$ and $\mathbb{J}$
(Initialization): Set $R_{sec} = 0, \forall i \in \mathcal{M}$.
for $i \leftarrow 1$ to $M$ do
    for $j \in \{R, J, N_u\}$ do
        $X_{i,j} = 1$
        Calculate $R^{'}_{sec}$
    end for
    Find the maximum $R'_{sec}$
    if $R'_{sec} > R_{sec}$ then
        $R_{sec} = R'_{sec}$
        $X_{i,j} = arg \max R'_{sec}$
    end if
end for
return $\mathbb{R} = \{i, X_{i,R} = 1\}$ and $\mathbb{J} = \{i, X_{i,J} = 1\}$
```

5.2.2 Cross-Entropy based Partner Selection Algorithm

The partner selection problem can also be solved using the Cross-entropy (C-E) method, which is more efficient in searching the optimal solution [116]. In C-E method, ”deterministic” optimization problem should be translated into a related ”stochastic” optimization problem, where the rare event simulation techniques similar to [77] can be utilized. In other words, the main idea behind the C-E method is to define for the original optimization problem an associated stochastic problem (ASP) and then efficiently solve the ASP by an adaptive scheme. It sequentially generates random solutions which converge stochastically to the optimal or near-optimal one.

Typically, the C-E method involves an iterative procedure where each iteration comprises of the following two phases: i) Generate a random data sample according to a specified stochastic policy; ii) Update the stochastic policy based on the outcome of the sample to produce a ”better” sample in the next iteration.

C-E algorithm: Algorithm 2 represents the detailed procedure of channel selection, which consists of five main steps as follows.

Define the strategy space $\mathbb{S}$ for all the SUs as follows:

$$\mathbb{S} := \{R, J, N_u\}. \tag{5.11}$$

The probability vector associated with the strategy space is given as follows:

$$\mathbb{P}_t^i := \{p_{R,t}^i, p_{J,t}^i, p_{N_u,t}^i\}, \sum_{j\in\{R,J,N_u\}} p_{j,t}^i = 1, \tag{5.12}$$

where $\mathbb{P}_t^i$ denotes the stochastic policy of SU i on the strategy space $\mathbb{S}$ at t-th iteration, and $p_{j,t}^i$ denotes the probability that SU i chooses strategy j at t-th iteration.

1. (Initialization). Set the iteration counter $t := 1$. Set the initial stochastic policy $\mathbb{P}_0^i$ of all SUs to be the uniform distribution on the strategy space $\mathbb{S}$. In other words, for each intermediate node, it picks the strategy from the strategy space uniformly, with equal probability $1/3$.

2. (Generation samples). Based on the initial stochastic policy of all nodes, the Z samples of the strategy vector are generated, which can be given as follows:

$$\mathbb{S}^i(z) := \{I_R^i(z), I_J^i(z), I_{N_u}^i(z)\}, \tag{5.13}$$

Algorithm 5 C-E Partner Selection Algorithm

```
Input: $\mathcal{M}, T, Z, \rho, h_s^i, h_d^i, h_e^i, \forall i \in \mathcal{M}$.
Output: Partner selection results $\mathbb{R}$ and $\mathbb{J}$
(Initialization): Set $R_{sec} = 0$ and $p_{j,t}^i = 1/3, j \in \{R, J, N_u\}, \forall i \in \mathcal{M}$.
for $t \leftarrow 1$ to $T$ do
    for $z \leftarrow 1$ to $Z$ do
        for $i \leftarrow 1$ to $M$ do
            Generate samples of the strategy vector.
        end for
    end for
    for $z \leftarrow 1$ to $Z$ do
        Calculate the utilities $U(z)$ according to (5.9).
    end for
    Order the utilities $U(z)$ in a nonincreasing manner.
    for $i \leftarrow 1$ to $M$ do
        for $j \leftarrow \{R, J, N_u\}$ do
            Update $\mathbb{P}_t^i$ using (5.15)
        end for
    end for
end for
return $\mathbb{R} = \{i, p_{R,T}^i = 1\}$ and $\mathbb{J} = \{i, p_{R,J}^i = 1\}$
```

where $\mathbb{S}^i(z)$ is the z-th strategy vector of node i with only one element to be ”1” and the rest are ”0”. The probability for I_j^i to be ”1” is $p_{j,t}^i$.

3. (Performance evaluation). Substitute the samples into (5.11) to calculate the utilities $U(z)$. Arrange the $U(z)$ in a nonincreasing order according to the values, i.e., $U^1 > U^2 > ... > U^Z$. Let υ be the $(1-\rho)$ sample quantile of the performances: $\upsilon = U_{\lceil (1-\rho)Z \rceil}$, where $\lceil \cdot \rceil$ is the ceiling function.

4. (Stochastic policy update). Based on the same sample, calculate $\mathbb{P}_t^i := \{p_{R,t}^i, p_{J,t}^i, p_{N_u,t}^i\}$, using the following equation:

$$p_{j,t}^i = \frac{\sum_{z=1}^{Z} X_{U^n \geq \upsilon} I_j^i(z) = 1}{\sum_{z=1}^{Z} X_{U^z \geq \upsilon}}, \tag{5.14}$$

where $X_{U^z \geq \upsilon}$ is defined as follows:

$$X_{U^z \geq \upsilon} = \begin{cases} 1 & U^z \geq \upsilon \\ 0 & \text{otherwise} \end{cases} \tag{5.15}$$

5. If the stopping criterion is met (e.g., the maximum iteration number is reached), stop; otherwise increase the iteration counter t by 1, and reiterate from step 3.

5.3 Incentive Mechanism for Cooperative Secure Communications

To motivate the SUs to participate in cooperation for security enhancement, the source announces an amount of reward to all the participants. Then, all the participants, which is competitive with each other, maximize their utilities by determining the transmission power for cooperation, given the announced reward. This process is modeled as a two-layer game, which can be illustrated in Fig. 5.2. On the top layer, a buyer-seller game is utilized to model the payment selection process, based on the framework of two-stage Stackelberg game. On the bottom layer, all the partners share the reward by determining their transmission powers in a distributed way, which is formulated as a non-cooperative power selection game. By analyzing the game, the best payment and transmission power can be determined. In the following, we first define the utilities of players and then analyze the game to find the best strategies for the players.

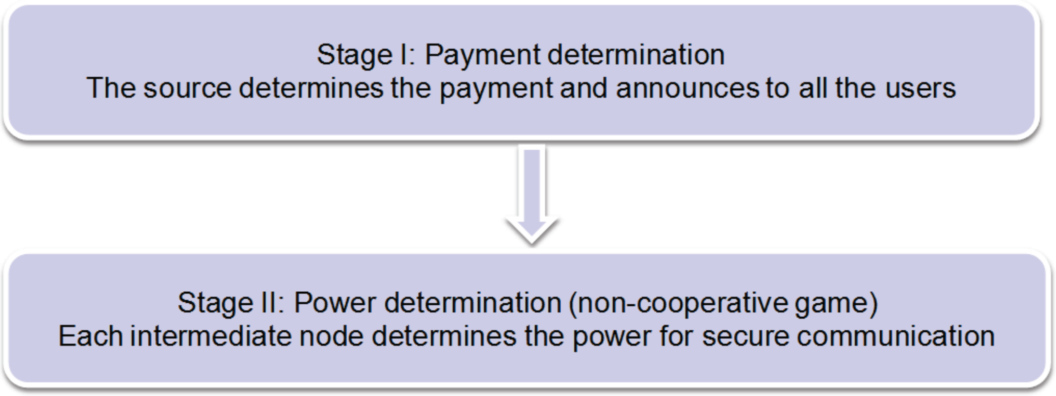

Stage I: Payment determination
The source determines the payment and announces to all the users
Stage II: Power determination (non-cooperative game)
Each intermediate node determines the power for secure communication

Figure 5.2: Two layer game.

5.3.1 Utility Functions

The utility of the source node (i.e., the primary transmitter) is given by

$$U_s = \lambda_1 R_{sec} - R_m \tag{5.16}$$

where λ_1 is the profit per secrecy rate, while $0 \leq R_m \leq R_{max}$ is the payment it grants to the cooperative relays and jammers.

The cooperative relays and jammers share the payment according to their contribution to the secrecy rate. In other words, the payment the cooperative participant can obtain is proportional to the contribution it makes in the cooperation. Since the relay is leveraged to increase the perfect secrecy of the relaying link compared with that of the eavesdropper link, the contribution can be approximately given by $\frac{P_r^i \left|h_{rd}^i\right|}{\left|h_{re}^i\right|}$. While the jammer is leveraged to increase more artificial noise at eavesdropper than at the destination node, the contribution the jammer makes can be approximately given by $\frac{P_j^i \left|h_{je}^i\right|}{\left|h_{jd}^i\right|}$.

The utility of the selected SU i is given by

$$U_i = \frac{P_i r_i}{\sum_{j \subseteq \mathbb{C}} P_j r_j} R_m - \lambda_2 P_i.$$

where $\mathbb{C} := \mathbb{R} \uplus \mathbb{J}$ is the set of selected nodes with the size N, λ_2 is the cost rate for transmission power, and the contribution factor r_i is defined as follows:

$$r_i = \begin{cases} \frac{|h_d^i|}{|h_e^i|}, & i \in \mathbb{R} \\ \frac{|h_e^i|}{|h_d^i|}, & i \in \mathbb{J} \end{cases} \tag{5.17}$$

As a two-stage game, the buyer-seller game can be analyzed by the backward induction method. First, the optimal strategies (i.e., the transmission powers) of the partners are analyzed, assuming the strategy of the source node (i.e., the payment) is fixed. Second, based on the results of the first step, the source node decides the optimal strategy, being aware of the effects of its decision on the strategies selected by the partners. By doing so, the best strategies of both the source node and the partners are obtained such that the corresponding utilities can be maximized.

5.3.2 No-cooperative Power Selection game

In order to stimulate the cooperation of the SUs, the source node pays for their service. Each SU gets a certain amount of payment according to its contribution in the service. For a given reward, each cooperative node tries to maximize its own utility by selecting a suitable transmission power, which is modeled as a non-cooperative power selection game.

Definition 5.3.1. *Non-cooperative power selection game is defined by $G = \{\mathbb{C}, \{\mathbb{S}_i\}, \{U_i\}\}$, where $\mathbb{C}$ is the set of players, $\mathbb{S}_i$ is the strategy set of SU i, and U_i is the utility function of SU i.*

Note that $\mathbb{S}_i$ is the transmission power that SU i can choose and the utility function of SU i is given as follows:

$$U_i = \frac{P_i r_i}{\sum_{j \subseteq \mathbb{C}} P_j r_j} R_m - \lambda_2 P_i.$$

Theorem 3. *There exists a Nash equilibrium in the non-cooperative power selection game $G = \{\mathbb{C}, \mathbb{S}_i, \{U_i\}\}$.*

Proposition 1. *An NE exists in the non-cooperative power selection game $G = \{\mathbb{C}, \{\mathbb{S}_i\}, \{U_i\}\}$, if for all node $i \in \mathbb{C}$: i) S_i is a nonempty, convex, and compact subset of some Euclidean space R^N; and ii) U_i is continuous in P and concave in P_i, where P is the set of $P_i, i \in \mathbb{C}$.*

The strategy space $\mathbb{S}_i$ is defined as the transmission power $0 \leq P_i \leq P_{max}$. Therefore, the strategy space is a nonempty, convex, and compact subset of some Euclidean space R^n.

Since the utility U_i is given by

$$U_i = \frac{P_i r_i}{\sum_{j \subseteq \mathbb{C}} P_j r_j} R_m - \lambda_2 P_i. \tag{5.18}$$

which is continuous in P. Taking the first derivative of U_i with respect to P_i yields

$$\frac{\partial U_i}{\partial P_i} = \frac{r_i R_m \sum_{j \neq i, j \subseteq \mathbb{C}} P_j r_j}{\left(\sum_{j \subseteq \mathbb{C}} P_j r_j\right)^2} - \lambda_2 \tag{5.19}$$

Then, taking the second derivative of U_i with respect to P_i, we have

$$\frac{\partial^2 U_i}{\partial^2 P_i} = -2 \frac{{r_i}^2 R_m \sum_{j \neq i, j \subseteq \mathbb{C}} P_j r_j}{\left(\sum_{j \subseteq \mathbb{C}} P_j r_j\right)^3} < 0 \tag{5.20}$$

The second derivative of U_i with respect to P_i is always negative, which means U_i is concave in P_i. Therefore, the non-cooperative power selection game G exists an NE.

Theorem 4. *The non-cooperative power selection game G has an unique Nash equilibrium.*

Definition 5.3.2. *A weighted sum of $U_i(P)$ is given by $\sigma(P,\mu) = \sum_{i=1}^{N} \mu_i U_i(P)$, where $\mu = \{\mu_1, \mu_2, ..., \mu_N\}$ with $\mu_i \geq 0$ and $P = \{P_1, P_2, ...P_i, ...P_N\}$. The pseudogradient of $\sigma(P,\mu)$ is defined by $\varphi(P,\mu)$, which is given by*

$$\varphi(P,\mu) = \begin{bmatrix} \mu_1 \nabla_1 U_1(P) \\ \mu_2 \nabla_2 U_2(P) \\ \vdots \\ \mu_N \nabla_N U_N(P) \end{bmatrix} \tag{5.21}$$

Define $\Psi(P,\mu)$ be the Jacobian matrix of $\varphi(P,\mu)$ with respect to P.

Proposition 2. *If $\sigma(P,\mu)$ is diagonally strict concave in P for some positive μ, the non-cooperative power selection game has a unique Nash equilibrium [117].*

Proposition 3. *$\sigma(P,\mu)$ is diagonally strict concave if the symmetric matrix $[\Psi(P,\mu), \Psi'(P,\mu)]$ is negative definite for P [117].*

Proposition 4. *The symmetric matrix $[\Psi(P,\mu), \Psi'(P,\mu)]$ is negative definite for P if the following conditions are satisfied: i) $U_i(P)$ is concave with respect to P_i; ii) $U_i(P)$ is convex with respect to P_i^-, where P_i^- is the transmission power of other nodes rather than SU i; iii) $\sigma(P,\mu)$ is concave with respect o P for some positive μ [117].*

As proved before, $U_i(P)$ is concave with respect to P_i. In the following, we prove the last two propositions. Taking the first derivative of $U_i(P)$ with respect to P_j, $j \neq i$, yields

$$\frac{\partial U_i}{\partial P_j} = -\frac{r_i R_m r_j}{\left(\sum_{j \subseteq \mathbb{C}} P_j r_j\right)^2} \tag{5.22}$$

The second derivative of $U_i(P)$ with respect to P_j $(j \neq i)$ is given by

$$\frac{\partial^2 U_i}{\partial^2 P_j} = \frac{2 r_i R_m r_j^2}{\left(\sum_{j \subseteq \mathbb{C}} P_j r_j\right)^3} > 0 \tag{5.23}$$

Therefore, $U_i(P)$ is convex with respect to P_i^-. According to the rule that $\frac{\partial \sum_i f(x)}{\partial x} = \sum_i \frac{\partial f(x)}{\partial x}$, based on (5.20) and (5.32), the second derivative of $\sigma(P, \mu)$ with respect to P_i is given by

$$\frac{\partial^2 \sigma(P,\mu)}{\partial^2 P_i} = \mu_i \frac{-2{r_i}^2 R_m \sum_{j \neq i, j \subseteq \mathbb{C}} P_j r_j}{\left(\sum_{j \subseteq \mathbb{C}} P_j r_j\right)^3} + \sum_{j \neq i, j \subseteq \mathbb{C}} \mu_j \frac{2 r_j R_m r_i^2}{\left(\sum_{j \subseteq \mathbb{C}} P_j r_j\right)^3} \tag{5.24}$$

It is obvious that for some positive μ, $\frac{\partial^2 \sigma(P,\mu)}{\partial^2 P_i} > 0$. Therefore, the non-cooperative power selection game has a unique NE.

Since U_i is concave with respect to P_i, the best response correspondence can be obtained by setting the first derivative of U_i with respect to P_i to 0, as follows:

$$\frac{\partial U_i}{\partial P_i} = -\frac{-r_i R_m A_i + \lambda_2 {A_i}^2 + 2\,\lambda_2 A_i P_i r_i + \lambda_2 {P_i}^2 {r_i}^2}{\left(\sum_{j \subseteq \mathbb{C}} P_j r_j\right)^2} = 0 \tag{5.25}$$

where $A_i = \sum_{j \neq i, j \subseteq \mathbb{C}} w_j P_j r_j$. By solving it, the solutions are given by

$$P_i^* = \begin{cases} 0 & \text{if } \sum_{j \neq i, j \subseteq \mathbb{C}} P_j r_j \geq \frac{R_m P_i r_i}{\lambda_2} \\ \frac{1}{r_i}(\sqrt{\frac{R_m P_i r_i A_i}{\lambda_2}} - A_i) & \text{if } \sum_{j \neq i, j \subseteq \mathbb{C}} P_j r_j < \frac{R_m P_i r_i}{\lambda_2} \text{ and } \frac{1}{r_i}(\sqrt{\frac{R_m P_i r_i A_i}{\lambda_2}} - A_i) < P_{max} \\ P_{max} & \text{otherwise} \end{cases} \tag{5.26}$$

The detailed procedure can be found in the Appendix D.

By solving the equations set (5.25), we can find the unique equilibrium as follows:

$$P_i^* = [\min\{\frac{R_m r_i B_i}{\lambda_2 (r_i + B_i)^2}, P_{max}\}]^+ \tag{5.27}$$

where $B_i = \frac{(N-1)r_i}{\sum_{j=1}^{N} \frac{r_i}{r_j} - N + 1}$. The detailed procedure can be found in the Appendix D.

5.3.3 Source Node Utility Maximization

Based on the analytical results of the power selection game, the source determines its strategy (the payment) to maximize its utility, aware of the effects of its strategy on the results of the power selection game. It can be formulated as the following problem:

$$\begin{aligned} &\max_{R_m} \ U_s = \lambda_1 R_{sec} - R_m \\ &s.t. \ 0 \le R_m \le R_{max}. \end{aligned} \tag{5.28}$$

where R_{sec} is obtained when the partners adopt the transmission power given by (5.27), which is a function of R_m. Therefore, the utility function of the source becomes a function of one single parameter R_m. To find the best R_m, the classic approach is to find the extremum by setting the first derivative of U_s with respect to R_m equal to 0 and then compare the extremum with the boundary to find the best payment R_m^*. Finally, we can obtain the best strategy of partners by substituting R_m^* into (5.27).

5.4 Weighted Payment Allocation Approach

In the previous section, the source can only determine the amount of payment to the cooperative partners. To further improve the utility of the source, it can actively affect the way how the partners share the payment by means of introducing a set of weights for the partners, which are relevant to the CSI of the partners. Specifically, the source introduces the weights $W := \{w_1, w_2, ..., w_i, ..., w_N\}$ as the allocation coefficients, associated with the selected SUs, where N is the total number of selected SUs for cooperation, $0 \leq w_i \leq 1$ is the allocation coefficient for SU i and $\sum_i w_i = 1$. With the allocation coefficient posed by the source, the interaction between the source and SUs are modeled using the similar game as before.

5.4.1 Utility Functions

The utility function of the source node is the same as before, which is given as follows:

$$U_s = \lambda_1 R_{sec} - R_m. \tag{5.29}$$

Different from the previous case, the utility of the cooperative SU i is given by

$$U_i = \frac{P_i w_i r_i}{\sum_{j \subseteq C} P_j w_j r_j} R_m - \lambda_2 P_i. \tag{5.30}$$

where w_i is the payment allocation coefficient for SU i and r_i is the contribution factor defined in (5.17).

5.4.2 Non-cooperative Power Selection Game

Given the payment R_m and the allocation coefficients $W := \{w_1, w_2, ..., w_i, ..., w_N\}$, the selected SUs determine their own strategies, i.e., the transmission power, to maximize their utilities, given by (5.30).

Taking the first derivative of U_i with respect to P_j, $j \neq i$, yields

$$\frac{\partial U_i}{\partial P_j} = -\frac{w_i r_i R_m w_j r_j}{\left(\sum_{j \subseteq \mathbb{C}} w_j P_j r_j\right)^2} \tag{5.31}$$

The second derivative of U_i with respect to P_j $(j \neq i)$ is given by

$$\frac{\partial^2 U_i}{\partial^2 P_j} = \frac{2 w_i r_i R_m (w_j r_j)^2}{\left(\sum_{j \subseteq \mathbb{C}} w_j P_j r_j\right)^3} > 0 \tag{5.32}$$

Similar to the proof for the existence of NE and the uniqueness in the previous case, the new power allocation game can be proved to have a unique NE.

Since U_i is concave with respect to P_i, the best response correspondence can be obtained by setting the first derivative of U_i with respect to P_i equal to 0, i.e.,

$$\frac{\partial U_i}{\partial P_i} = -\frac{-w_i r_i R_m A_i + \lambda_2 {A_i}^2 + 2\,\lambda_2 A_i w_i P_i r_i + \lambda_2 {w_i}^2 {P_i}^2 {r_i}^2}{\left(\sum_{j \subseteq \mathbb{C}} w_j P_j r_j\right)^2} = 0 \tag{5.33}$$

where $A_i = \sum_{j \neq i, j \subseteq \mathbb{C}} w_j P_j r_j$.

By solving the equations set (5.33), we can find the unique equilibrium as follows:

$$P_i^* = [\min\{\frac{R_m w_i r_i B_i}{\lambda_2 (w_i r_i + B_i)^2}, P_{max}\}]^+ \tag{5.34}$$

where $B_i = \frac{(N-1) w_i r_i}{\sum_{j=1}^{N} \frac{w_i r_i}{w_j r_j} - N + 1}$.

5.4.3 Source Node Utility Maximization

In the previous section, we present how the weight coefficient W affects the power allocation of the cooperative partners, as shown in (5.34). Different transmission power selection in turn changes the utility function of the source. Therefore, there exists an implicit relationship between the utility function U_s and the weight coefficient W. In this section, we aim to find the optimal W such that U_s can be maximized, which can be formulated as the following optimization problem:

$$\begin{aligned} &\max_{w_1,w_2,...,w_N} U_s \\ s.t.\ \ &0 \leq w_i \leq 1, i = 1,2,...,N \\ &\textstyle\sum_i w_i = 1 \end{aligned} \tag{5.35}$$

Since it is difficult to derive an explicit equation to express the relation between U_s and W, regular optimization methods may not be applicable. Bio-inspired and swarm intelligence optimal method, as an important branch of optimization theory, provides an effective way to address such complex problems. Genetic algorithm (GA) is the most successful one in this area and has been applied to solve many practical problems. However, due to the inherent encoding structure and iteration rule, GA is not appropriate for continuous variable optimization. In this section, we adopt a relatively new swarm intelligence method, named Particle Swarm Optimization (PSO) to solve the above problem [20, 118]. Compared with GA, PSO has better global searching ability, especially in the continuous space, and a local searching ability near the end of the run.

The standard PSO algorithm typically involves the following steps: 1) Construct particle structure to map the solution of interest problem; 2) Create initial topology for particle swarm and parameters; 3) Evaluate fitness value of each particle; 4) Update particle position; 5) Repeat step (2) to (4) until the solution satisfies the terminating condition.

Following this framework, we first construct a root particle $\mathbf{Pa}_{\mathrm{r}}$, which is a vector of allocation coefficients, i.e., $\mathbf{Pa}_{\mathrm{r}} = \{w_1, w_2, ..., w_n\}$. The n-th element of $\mathbf{Pa}_{\mathrm{r}}$ indicates the allocation coefficient for n-th partner (i.e., w_n). In other words, $\mathbf{Pa}_{\mathrm{r}}$ implies an initial allocation, as well as a start point for the optima searching. In this chapter, an equal weight distribution strategy are adopted, i.e. $\mathbf{Pa}_{\mathrm{r}}(n) = 1/N$.

Based on the given $\mathbf{Pa}_{\mathrm{r}}$, we initialized the particle swarm with the size of N^{PSO}. The i-

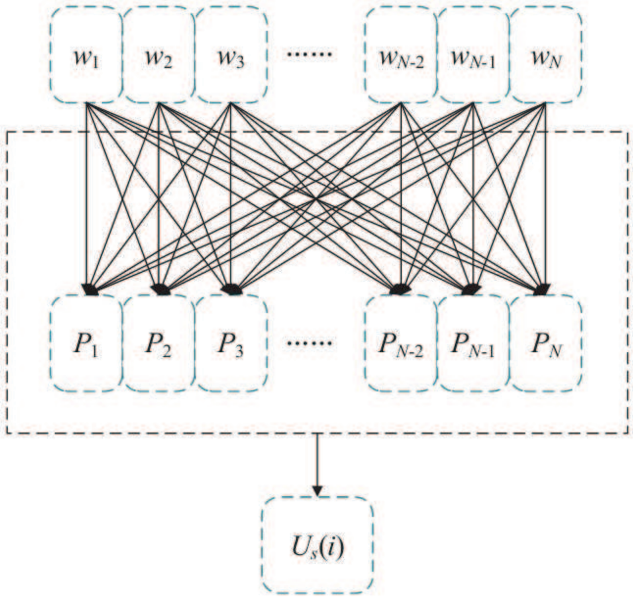


Figure 5.3: Illustration of calculating the fitness for a given particle.

th particle can be expressed as an N-dimensional vector $\mathbf{Pa}_i$ and denote its n-th element by $\mathbf{Pa}_i(n)$, which is given as follows:

$$\mathbf{Pa}_i(n) = \mathbf{Pa}_{\mathrm{r}}(n) + \omega, \tag{5.36}$$

where ω follows the uniform distribution in $[-\mathbf{Pa}_{\mathrm{r}}(n), 1 - \mathbf{Pa}_{\mathrm{r}}(n)]$.

$$\mathbf{Pa}_i(n) = \frac{\mathbf{Pa}_i(n)}{\sum_n \mathbf{Pa}_i(n)}, \forall i \in [1, N^{\mathrm{PSO}}], n \in [1, N] \tag{5.37}$$

The fitness value of the i-th particle is denoted as $\mathbf{Fi}_i$, which actually is the utility of the source. In other words, $\mathbf{Fi}_i$ is the utility function U_s of source that can be obtained by using (5.16). Fig. 5.3 illustrates the process for calculating the fitness for a given particle. In addition, denote by $\mathbf{Pa}^{\mathrm{Gopt}}$ the global best particle of the swarm, i.e. the particle with the highest fitness value $Gopt$; denote by $\mathbf{Pa}_i^{\text{Gopt}}$ the best historical position of i-th particle with the corresponding fitness value Popt_i. The position variation for i-th particle is denoted as $\mathbf{Ve}_i^t$. At the t-th iteration, the particle position can be updated by the following equations:

$$\mathbf{Ve}_i^{t+1} = \lambda \left(\mathbf{Ve}_i^t + c\gamma_1(\mathbf{Pa}_i^{\text{Gopt}} - \mathbf{Pa}_i^t) + c\gamma_2(\mathbf{Pa}^{\text{Gopt}} - \mathbf{Pa}_i^t) \right) \tag{5.38}$$

$$\mathbf{Pa}_i^{t+1} = \mathbf{Pa}_i^t + \mathbf{Ve}_i^t \tag{5.39}$$

where λ is inertia coefficient in PSO algorithm and the random variables γ_1 and γ_2 are uniformly distributed within [0,1]. In this chapter, these parameters are set as follows:

$$\lambda = \frac{1}{|1 - c - \sqrt{c^2 - 2c}|} \tag{5.40}$$

where $c = 2.05$ and $\lambda = 0.729$. Algorithm 3 represents the detailed procedure of the PSO based weight selection.

5.5 Simulation Results

In this section, simulation results are provided to evaluate the performance of the proposed scheme. The simulation is set up as follows. In a 1 km× 1 km area, the source, the destination, and two eavesdroppers are located at the origin, (1 km, 0.5 km), (1 km, -0.5 km), and (0.8 km, -0.4 km), respectively, while a set of SUs are located in between. The maximum transmission power of all nodes are set to 1 W, while the noise power is set to -70 dB. The average power gains between nodes is calculated by the path loss with exponent $\mu = 3.5$. The maximum power is set to 10 W.

To evaluate the average performance of the proposed partner selection algorithms with respect to the number of intermediate SUs, Monte Carlo simulation is carried out, which consists

Algorithm 6 PSO based weight selection algorithm

```
Input: Number of partners, number of particle swarm $N^{\text{PSO}}$
Output: Weight Coefficient $W$
// Step1: Initialization
Generate root particle particle$_{\text{root}}$ with equal weight distribution,
for $i \leftarrow 1$ to $N^{\text{PSO}}$ do
    Generate searching particle particle$_i$
end for
// Step2: Find particle$^{\text{Gopt}}$, $Gopt$
Calculate the Fitness$_i$ of source node, $i = 1, 2, ..., N^{\text{PSO}}$
Find the global best particle$^{\text{Gopt}}$ and $Gopt$
Find the local best particle$_i^{\text{Gopt}}$ and Popt$_i$
// Step3: Update
for $i \leftarrow 1$ to $N^{\text{PSO}}$ do
    Update particle$_i$ using (5.38) and (5.39)
    Run Step 2
    if particle$^{\text{Gopt}}$ and particle$_i^{\text{Gopt}}$ stay unchanged then
        Stop
    else
        Continue
    end if
end for
Return particle$^{\text{Gopt}}$
```

of 500 trials. At each trial, a number of intermediate SUs are uniformly distributed in the area. Fig. 5.4 shows the average secrecy rate using the exhaustive search algorithm, the proposed greedy algorithm, C-E algorithm, and single relay and jammer selection algorithm in [119]. The exhaustive search algorithm has the best performance and it provides a performance benchmark. It can be seen that the C-E algorithm can achieve almost the same performance as the exhaustive search algorithm does. Moreover, it can be seen that the proposed algorithms can achieve higher secrecy rate, compared with the single relay and jammer selection algorithm. This is because they can fully exploit the benefits of cooperation by leveraging multiple relays and jammers.

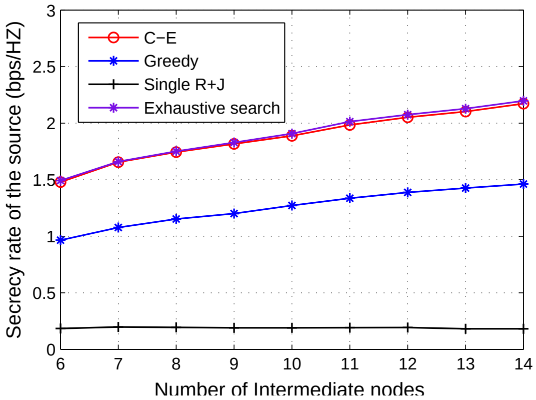


Figure 5.4: Comparison among different partner selection algorithms.

In the following simulation, we validate the incentive mechanism in the network scenario, as shown in Fig. 5.5. The source, destination, eavesdroppers are fixed at the same location as before, while 15 intermediate SUs are distributed at the locations marked in the figure. The source can choose the reward from the range between 0 and 100. Fig. 5.6 shows the utility of the source, averaged over fading distribution, versus the amount of reward, for different λ_1 and λ_2. It can be seen that the overall utility first increases and then decreases as the reward increases. The reason is that, at the beginning, with increasing reward, the partners are willing to devote more transmission power during cooperation, which leads to an increase in the secrecy rate.

However, when the reward keeps rising, the cost also increases, which will lower the overall utility. It can also be seen that there exists an optimal value of the reward, with which the utility can be maximized. It can also be seen that a larger λ_1 leads to a greater utility and payment because the source node cares more about the secrecy rate and is willing to pay more reward to increase the secrecy rate. Moreover, a larger λ_2 leads to a lower utility, since the intermediate SU cares more about their energy consumption and it will devote less power to cooperate given the same payment.

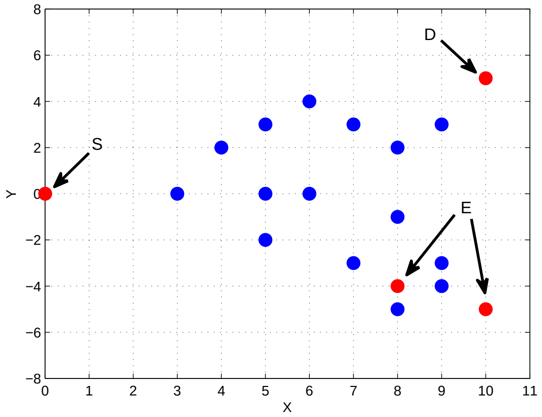


Figure 5.5: The network scenario for simulation.

Fig. 5.7 shows the utilities of intermediate SUs, averaged over fading distribution. It can be seen that the partners, who contribute to increase the secrecy rate of the source, can receive a certain amount of reward through cooperation, which implies that all the partners have the incentive for cooperation. Moreover, the node located at (0.9 km, -0.4 km) act as a jammer (node 13), while other nodes receiving non-zero rewards act as relays.

Fig. 5.8 shows the average utility of the source using PSO with respect to the number of intermediate SUs, using Monte Carlo simulation. It can be seen that with PSO algorithm, the source can achieve higher utility than that using only C-E partner selection algorithm when the proposed incentive mechanism is applied. That is because the source can actively affect

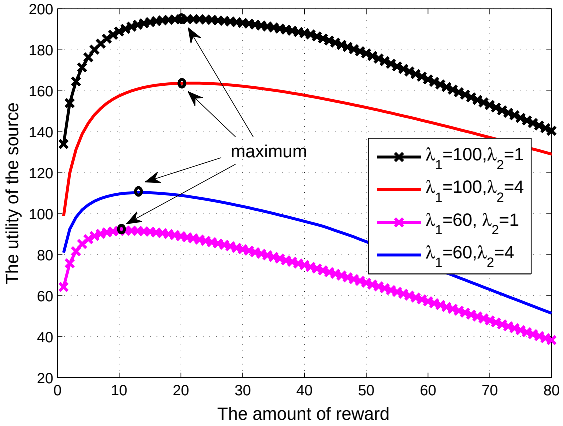


Figure 5.6: Utility of the source versus the amount of rewards.

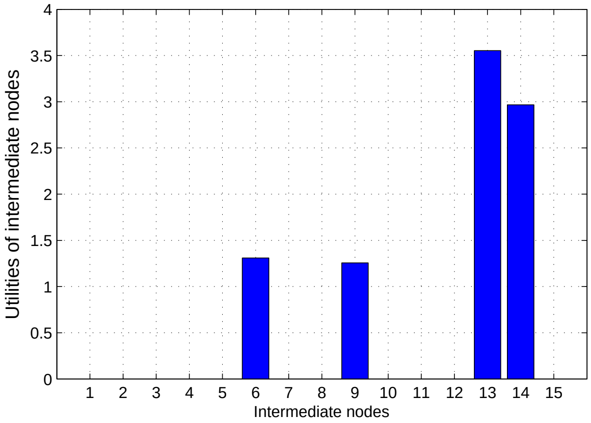


Figure 5.7: Utilities of intermediate nodes averaged over fading when $\lambda_1 = 60$ and $\lambda_2 = 1$.

the power allocation of the intermediate SUs by introducing the reward allocation weights. Through adjusting the weights, the intermediate SUs can be better stimulated to further improve the secrecy rate.

Fig. 5.9 shows the utilities of intermediate SUs, averaged over fading distribution using the same network scenario in Fig. 5.5. Compared with Fig. 5.7, it can be seen that more intermediate SUs are encouraged/stimulated to contribute to increase the secrecy rate when PSO algorithm is applied.

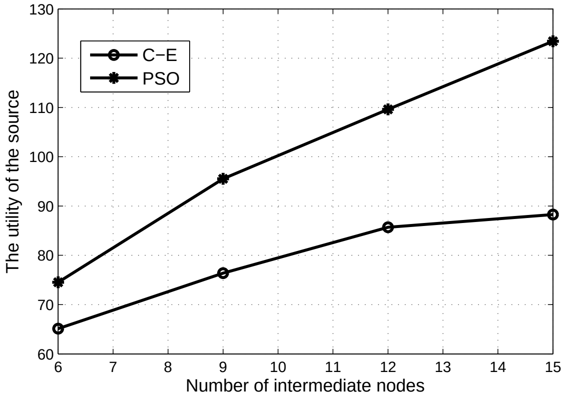


Figure 5.8: Utilities of the source with PSO when $\lambda_1 = 100$ and $\lambda_2 = 1$.

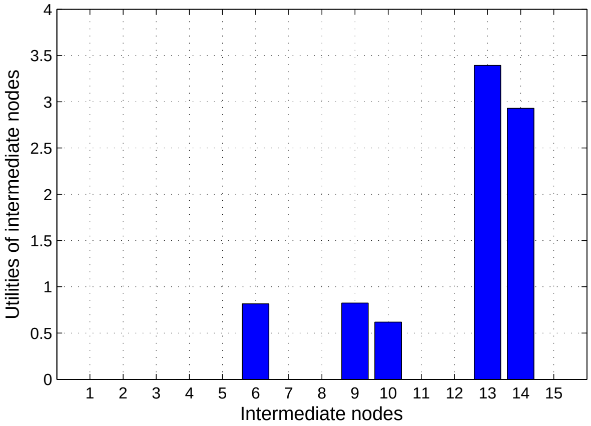


Figure 5.9: Utilities of intermediate nodes averaged over fading using PSO when $\lambda_1 = 60$ and $\lambda_2 = 1$.

5.6 Summary

In this chapter, we have proposed a cooperative framework to enhance the PU's security in present of multiple eavesdroppers through cooperation with SUs who have no traffic requirement. Two partner selection algorithms have been devised, which can select suitable SUs, acting as relays or jammers to maximize the secrecy rate. A game-theoretic incentive mechanism has been proposed to stimulate the SUs to participate into cooperation. With the proposed cooperative scheme, all the cooperative SUs can gain a ceratin amount of credits, which can be used in the future when needed. In addition, the security of the PU can be significantly enhanced by preventing eavesdroppers from decoding the message transmitted. The proposed scheme can be applied in a network without infrastructure for secure information transfer, or for key exchange. Moreover, the proposed scheme can combine with the upper layer cryptographic schemes to provide enhanced security.

Chapter 6

Conclusion and Future Works

In this chapter, we summarize the major research contributions and discuss future research works.

6.1 Major Research Contributions

This research aims at developing security-aware cooperation schemes for dynamic spectrum access. We are working on different cooperation scenarios, including cooperative spectrum sensing, secure communications in CCRN, risk-aware cooperation in CCRN, and cooperation with PUs for credits. Particularly, in this thesis, we have

- investigated dynamic spectrum access in a multi-channel CRN. A cooperative framework integrating spectrum sensing and spectrum sharing has been proposed, considering both the diverse channel usage characteristics and the diverse sensing performance of individual SUs. For spectrum sensing, to maximize the expected available time of all the channels, a cross-entropy based approach has been proposed to schedule SUs for selecting sensing channels. For spectrum sharing, an channel access algorithm has been proposed to achieve NE. The proposed cooperative framework can achieve higher throughput per user, which provides incentive to SUs to participate into cooperative spectrum sensing.

- investigated cooperation in the CRN, taking the physical layer security into consideration. With the proposed cooperation schemes, the PU enhances the security of communications and SUs can gain transmission opportunities. Particularly, the PU can either cooperate with two individual SUs or a cluster of SUs. For the former (R-J cooperation scheme), the two SUs act as one relay and one friendly jammer to increase the secrecy rate of the PU in the presence of one eavesdropper. For the latter (C-B cooperation scheme), a cluster of SUs enhances the secrecy of the PU's communication via collaborative beamforming. Two different scenarios with single eavesdropper and with multiple eavesdroppers are studied, respectively. To maximize the secrecy rate, joint time and transmit power allocation is considered in R-J cooperation scheme, while time allocation and weight selection are jointly optimized in C-B cooperation schemes. Numerical results have demonstrated that, with the proposed schemes, the secrecy of PU's communications can be significantly enhanced through cooperation with SUs.

- studied risk aware cooperation in cooperative cognitive radio networking, whereby multiple primary users (PUs) operating over different channels choose trustworthy secondary users (SUs) as relays to improve throughput, and in return SUs gain transmission opportunities. We have investigated cooperation over a single channel by Stackelberg game, in which the trustworthiness of SUs is integrated. Based on the results of the single channel scenario, we have proposed a SCC scheme for the cooperation over multiple channels, where SUs form a cluster to maximize the total utility of the secondary network and share the obtained resources based on congestion game and quadrature signaling.

- proposed a cooperative framework to gain credits when the SUs have no traffic. The

SUs earn credits through cooperation to enhance the security of the PUs in present of multiple eavesdroppers. The earned credits can be utilized for spectrum leasing when they have traffic in the future. Specifically, two partner selection algorithms have been devised, which can select suitable SUs, acting as relays or jammers to maximize the secrecy rate. A game-theoretic incentive mechanism has been proposed to stimulate the SUs to participate into cooperation. With the proposed cooperative scheme, all the cooperative SUs can gain ceratin amount of credits security, which can be used in the future when needed. In addition, the security of the PU can be significantly enhanced by preventing eavesdroppers from decoding the message transmitted. The proposed scheme can be applied in a network without infrastructure for secure information transfer, or for key exchange. Moreover, the proposed scheme can combine with the upper layer cryptographic schemes to provide enhanced security.

6.2 Future Research Directions

The research directions for further study are listed as follows:

- In the current work, we only consider the cooperation between one PU and multiple SUs for secure communication when SUs have no traffic. A more general scenario is that there exist multiple PUs requesting for cooperation and grant different payments. In such a case, SUs have more choices to choose with whom to cooperation for credit accumulation. Different SUs can form coalitions automatically to perform cooperation with different PUs to maximize their utilities, e.g., the earned credits. Each SU makes the decision to join or leave a coalition to pursue its own utility. The issue of how to group SUs into different coalitions needs to be studied.
- For risk-aware cooperation in CCRN, we integrate trust values into the partner selection

phase. Considering that the failure of transmission might be caused by other factors such as channel impairment, how to distinguish misbehavior from other factors needs to be considered. In addition, different misbehavior might have different levels of damage. Therefore, when calculating the trust values, different weights should be put on different misbehavior. Therefore, an efficient misbehavior detection method and a more accurate trust value model are needed.

- Cooperative sensing is a promising approach to detect the presence of the PUs by exploiting the spatial diversity of the secondary users. Such a spatial diversity might be exploited by a malicious attacker or untrusted fusion center to achieve involuntary geolocation of a secondary user by linking his location-dependent sensing report to his physical position. This kind of threat might stop legitimate SUs to participate in cooperative sensing, if they are privacy-sensitive. Thus, a privacy preservation cooperation scheme is crucial for cooperative spectrum sensing. In the literature, only one recent work studied the privacy preserving framework in cooperative spectrum sensing [120], in which a privacy preserving cooperative sensing framework was proposed. Although the privacy of SUs can be protected using the proposed framework in [120], when there exist some malicious SUs misbehaving during cooperation, it is difficult to track them. Thus, the malicious SUs can misbehave without being traced. It motivates us to investigate the conditional privacy-preserving cooperative sensing framework, whereby not only the location privacy of SUs can be protected but also the misbehaving SU can be traced. Specifically, we will focus on a centralized cooperative sensing system, where there exists a fusion center (FC). We will make an effort to propose a conditional privacy-preserving framework for cooperative sensing system so that the privacy of participants can be protected from being leaked to malicious users while the abnormal participants can be detected and traced by the FC.

Bibliography

[1] I. Akyildiz, W. Lee, M. Vuran, and S. Mohanty, “A survey on spectrum management in cognitive radio networks,” *IEEE Communications Magazine*, vol. 46, no. 4, pp. 40–48, 2008.

[2] Cisco, “Cisco visual networking index: Global mobile data traffic forecast,” *White Paper*, 2014.

[3] Nokia Siemens Networks, “2020: Beyond 4g radio evolution for the gigabit experience,” *White Paper*, 2011.

[4] N. Zhang, N. Cheng, A. T. Gamage, J. W. Mark, and X. Shen, “Cloud assisted hetnets toward 5g wireless networks,” *IEEE Communization Magazine*, 2015, to apprear.

[5] N. Lu, N. Zhang, N. Cheng, X. Shen, J. W. Mark, and F. Bai, “Vehicles meet infrastructure: Toward capacity–cost tradeoffs for vehicular access networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, pp. 1266 – 1277, 2013.

[6] URL: http://www.qualcomm.com/media/documents/wireless-networks-1000x-more-small-cells.

[7] Q. Zhao and B. M. Sadler, “A survey of dynamic spectrum access,” *IEEE Signal Processing Magazine*, vol. 24, no. 3, pp. 79–89, 2007.

[8] I. Akyildiz, W. Lee, M. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Computer Networks*, vol. 50, no. 13, pp. 2127–2159, 2006.

[9] J. Mitola III and G. Maguire Jr, "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.

[10] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, 2005.

[11] F. C. Commission *et al.*, "Notice of proposed rule making and order: Facilitating opportunities for flexible, efficient, and reliable spectrum use employing cognitive radio technologies," *ET docket*, no. 03-108, p. 73, 2005.

[12] Y.-C. Liang, Y. Zeng, E. C. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1326–1337, 2008.

[13] A. Ghasemi and E. Sousa, "Spectrum sensing in cognitive radio networks: requirements, challenges and design trade-offs," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 32–39, 2008.

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

[15] H. Zhou, B. Liu, L. Gui, X. Wang, and Y. Li, "Fast spectrum sharing for cognitive radio networks: A joint time-spectrum perspective," in *Proceedings of IEEE GLOBECOM*, 2011.

[16] T. Han, T. Xing, N. Zhang, K. Liu, B. Tang, and Y. Liu, “Wireless spectrum sharing via waiting-line auction,” in *Proceedings of 11th IEEE Singapore International Conference on Communication Systems*, 2008.

[17] Y. Xing, R. Chandramouli, S. Mangold *et al.*, “Dynamic spectrum access in open spectrum wireless networks,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 3, pp. 626–637, 2006.

[18] Y. Wang, Y. Zhang, Q. Zhang, and S. Wu, “Optimal selection of false alarm probability for dynamic spectrum access,” *IEEE Communications Letters*, vol. 17, pp. 844–847, 2013.

[19] N. Cheng, N. Zhang, N. Lu, X. Shen, and J. W. Mark, “Opportunistic spectrum access for cr-vanets: A game theoretic approach,” *IEEE Transactions on Vehicular Technology*, to appear.

[20] Y. Wang, Q. Zhang, Y. Zhang, and P. Chen, “Adaptive resource allocation for cognitive radio networks with multiple primary networks,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, no. 1, pp. 1–18, 2012.

[21] J. Wang, M. Ghosh, and K. Challapali, “Emerging cognitive radio applications: A survey,” *IEEE Communications Magazine*, vol. 49, no. 3, pp. 74–81, 2011.

[22] D. Scaperoth, B. Le, T. Rondeau, D. Maldonado, C. W. Bostian, and S. Harrison, “Cognitive radio platform development for interoperability,” in *Proc. of IEEE MILCOM*. IEEE, 2006, pp. 1–6.

[23] I. Akyildiz, W. Lee, and K. Chowdhury, “Crahns: Cognitive radio ad hoc networks,” *Ad Hoc Networks*, vol. 7, no. 5, pp. 810–836, 2009.

[24] Y. Zeng, Y. Liang, A. Hoang, and R. Zhang, “A review on spectrum sensing for cognitive radio: challenges and solutions,” *EURASIP Journal on Advances in Signal Processing*, vol. 2010, 2010.

[25] T. Yucek and H. Arslan, “A survey of spectrum sensing algorithms for cognitive radio applications,” *IEEE Communications Surveys & Tutorials*, vol. 11, no. 1, pp. 116–130, 2009.

[26] W. Zhang, R. Mallik, and K. Letaief, “Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks,” *IEEE Transactions on Wireless Communications*, vol. 8, no. 12, pp. 5761–5766, 2009.

[27] H. Kim and K. G. Shin, “In-band spectrum sensing in cognitive radio networks: energy detection or feature detection?” in *Proc. of ACM Mobicom*. ACM, 2008, pp. 14–25.

[28] Y. Zeng, Y. C. Liang, and R. Zhang, “Blindly combined energy detection for spectrum sensing in cognitive radio,” *IEEE Signal Processing Letters*, vol. 15, pp. 649–652, 2008.

[29] Z. Ye, G. Memik, and J. Grosspietsch, “Energy detection using estimated noise variance for spectrum sensing in cognitive radio networks,” in *Proc. of IEEE WCNC*. IEEE, 2008, pp. 711–716.

[30] K.-L. Du and W. H. Mow, “Affordable cyclostationarity-based spectrum sensing for cognitive radio with smart antennas,” *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1877–1886, 2010.

[31] Z. Ye, J. Grosspietsch, and G. Memik, “Spectrum sensing using cyclostationary spectrum density for cognitive radios,” in *2007 IEEE Workshop on Signal Processing Systems*. IEEE, 2007, pp. 1–6.

[32] I. Akyildiz, B. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical Communication*, 2010.

[33] N. Zhang, H. Zhou, K. Zheng, N. Cheng, J. W. Mark, and X. Shen, "Cooperative heterogeneous framework for spectrum harvesting in cognitive cellular network," *IEEE Communization Magazine*, 2015, to apprear.

[34] E. Peh and Y.-C. Liang, "Optimization for cooperative sensing in cognitive radio networks," in *Proceedings of IEEE WCNC 2007.* IEEE, pp. 27–32.

[35] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio networks," in *Proceedings of IEEE DySPAN*, 2005.

[36] D. Cabric, S. Mishra, and R. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Proceedings of the 38th. Asilomar Conference on Signals, Systems, and Computers,*, pp. 772–776, 2004.

[37] A. Ghasemi and E. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on.* Ieee, 2005, pp. 131–136.

[38] S. Mishra, A. Sahai, and R. Brodersen, "Cooperative sensing among cognitive radios," in *Proc. of IEEE ICC*, vol. 4. IEEE, 2006, pp. 1658–1663.

[39] W. Lee and I. Akyildiz, "Optimal spectrum sensing framework for cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 10, pp. 3845–3857, 2008.

[40] J. Zhang and Q. Zhang, "Stackelberg game for utility-based cooperative cognitiveradio networks," in *Proceedings of the tenth ACM international symposium on Mobile ad hoc networking and computing*, 2009.

[41] 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, 2008.

[42] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. Shen, “Cooperative spectrum access towards secure information transfer for crns,” *IEEE Journal on Selected Areas in Communications*, to appear.

[43] T. Elkourdi and O. Simeone, “Spectrum leasing via cooperation with multiple primary users,” *IEEE Transactions on Vehicular Technology*, vol. 61, no. 2, pp. 820–825, 2012.

[44] S. Hua, H. Liu, M. Wu, and S. Panwar, “Exploiting mimo antennas in cooperative cognitive radio networks,” in *Proceedings IEEE INFOCOM*, Shanghai, China, April, 2011.

[45] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. Shen, “Towards secure communications in cooperative cognitive radio networks,” in *Proceedings of IEEE ICCC’13*, 2013.

[46] Y. Han, A. Pandharipande, and S. Ting, “Cooperative decode-and-forward relaying for secondary spectrum access,” *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 4945–4950, 2009.

[47] Y. Yi, J. Zhang, Q. Zhang, T. Jiang, and J. Zhang, “Cooperative communication-aware spectrum leasing in cognitive radio networks,” in *Proceedings of IEEE DySPAN 2010*. IEEE, pp. 1–11.

[48] N. Zhang, N. Cheng, N. Lu, H. Zhou, J. W. Mark, and X. Shen, “Risk-aware cooperative spectrum access for multi-channel cognitive radio networks,” in *IEEE Journal on Selected Areas in Communications*, 2013.

[49] I. Stanojev, O. Simeone, U. Spagnolini, Y. Bar-Ness, and R. Pickholtz, “Cooperative arq via auction-based spectrum leasing,” *IEEE Transactions on Communications*, vol. 58, no. 6, pp. 1843–1856, 2010.

[50] N. Zhang, N. Cheng, N. Lu, H. Zhou, J. W. Mark, and X. Shen, “Cooperative cognitive radio networking for opportunistic channel access,” in *Proceedings of IEEE GLOBECOM’13*, 2013.

[51] Y. Zou, Y. Yao, and B. Zheng, “A selective-relay based cooperative spectrum sensing scheme without dedicated reporting channels in cognitive radio networks,” *IEEE Transactions on Wireless Communications*, vol. 10, no. 4, pp. 1188–1198, 2011.

[52] G. Ganesan and Y. Li, “Cooperative spectrum sensing in cognitive radio, part i: Two user networks,” *IEEE Transactions on Wireless Communications*, vol. 6, no. 6, pp. 2204–2213, 2007.

[53] Y. Zou, Y. Yao, and B. Zheng, “Cooperative relay techniques for cognitive radio systems: Spectrum sensing and secondary user transmissions,” *IEEE Communications Magazine*, 2012.

[54] Z. Yuan, D. Niyato, H. Li, J. B. Song, and Z. Han, “Defeating primary user emulation attacks using belief propagation in cognitive radio networks,” *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 10, pp. 1850–1860, 2012.

[55] L. Duan, A. W. Min, J. Huang, and K. G. Shin, “Attack prevention for collaborative spectrum sensing in cognitive radio networks,” *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 9, pp. 1658–1665, 2012.

[56] Y. Han, S. Ting, and A. Pandharipande, “Cooperative spectrum sharing protocol with secondary user selection,” *IEEE Transactions on Wireless Communications*, vol. 9, no. 9, pp. 2914–2923, 2010.

[57] B. Cao, L. Cai, H. Liang, J. Mark, Q. Zhang, H. Poor, and W. Zhuang, "Cooperative cognitive radio networking using quadrature signaling," in *Proceedings of IEEE INFOCOM*, Orlando, USA, March 2012.

[58] A. Alshamrani, X. Shen, and L. Xie, "QoS provisioning for heterogeneous services in cooperative cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 819–830, 2011.

[59] N. Zhang, H. Liang, N. Cheng, Y. Tang, J. W. Mark, and X. Shen, "Dynamic spectrum access in multi-channel cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 11, pp. 2053–2064, 2014.

[60] Y. Zou, Y. Yao, and B. Zheng, "Cooperative relay techniques for cognitive radio systems: Spectrum sensing and secondary user transmissions," *IEEE Communications Magazine*, 2012.

[61] Q. Zhao and J. Ye, "Quickest detection in multiple on–off processes," *IEEE Transactions on Signal Processing*, vol. 58, no. 12, pp. 5994–6006, 2010.

[62] L. Husheng, "Restless watchdog: Selective quickest spectrum sensing in multichannel cognitive radio systems," *EURASIP Journal on Advances in Signal Processing*, vol. 2009, 2009.

[63] W. Wang, B. Kasiri, J. Cai, and A. S. Alfa, "Channel assignment of cooperative spectrum sensing in multi-channel cognitive radio networks," in *Proceedings of IEEE ICC*, 2011.

[64] R. Fan and H. Jiang, "Optimal multi-channel cooperative sensing in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 9, no. 3, pp. 1128–1138, 2010.

[65] H. Yu, W. Tang, and S. Li, “Optimization of cooperative spectrum sensing in multiple-channel cognitive radio networks,” in *Proceedings of IEEE GLOBECOM*, 2011.

[66] R. Fan, H. Jiang, Q. Guo, and Z. Zhang, “Joint optimal cooperative sensing and resource allocation in multichannel cognitive radio networks,” *IEEE Transactions on Vehicular Technology*, vol. 60, no. 2, pp. 722–729, 2011.

[67] N. Zhang, N. Cheng, H. Liang, Y. Tang, J. W. Mark, and X. S. Shen, “Efficient channel assignment for cooperative sensing based on convex bipartite matching,” in *Proceedings of IEEE ICC’14*, 2014.

[68] X. Wang, Z. Li, P. Xu, Y. Xu, X. Gao, and H.-H. Chen, “Spectrum sharing in cognitive radio networksłan auction-based approach,” *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics,*, vol. 40, no. 3, pp. 587–596, 2010.

[69] X. Hao, M. Cheung, V. Wong, and V. Leung, “Hedonic coalition formation game for cooperative spectrum sensing and channel access in cognitive radio networks,” *IEEE Transactions on Wireless Communications*, vol. 11, pp. 3968 – 3979, 2012.

[70] K. Cohen, A. Leshem, and E. Zehavi, “Game theoretic aspects of the multi-channel aloha protocol in cognitive radio networks,” *IEEE Journal on Selected Areas in Communications*, 2013.

[71] A. Leshem, E. Zehavi, and Y. Yaffe, “Multichannel opportunistic carrier sensing for stable channel access control in cognitive radio systems,” *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 1, pp. 82–95, 2012.

[72] M. Liu and Y. Wu, “Spectum sharing as congestion games,” in *Proceedings of IEEE Allerton*, 2008.

[73] L. Law, J. Huang, and M. Liu, “Price of anarchy for congestion games in cognitive radio networks,” *IEEE Transactions on Wireless Communications*, vol. 11, pp. 3778 – 3787, 2012.

[74] H. Kim and K. G. Shin, “Optimal online sensing sequence in multichannel cognitive radio networks,” *IEEE Transactions on Mobile Computing*, vol. 12, no. 7, pp. 1349–1362, 2013.

[75] G. Ganesan, Y. Li, B. Bing, and S. Li, “Spatiotemporal sensing in cognitive radio networks,” *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 5–12, 2008.

[76] Z. Quan, S. Cui, and A. H. Sayed, “Optimal linear cooperation for spectrum sensing in cognitive radio networks,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, no. 1, pp. 28–40, 2008.

[77] R. Y. Rubinstein, “Optimization of computer simulation models with rare events,” *European Journal of Operational Research*, vol. 99, pp. 89–112, 1997.

[78] R. W. Rosenthal, “A class of games possessing pure-strategy nash equilibria,” *International Journal of Game Theory*, vol. 2, no. 1, pp. 65–67, 1973.

[79] D. Monderer and L. S. Shapley, “Potential games,” *Games and economic behavior*, vol. 14, no. 1, pp. 124–143, 1996.

[80] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, “Grs: The green, reliability, and security of emerging machine to machine communications,” *IEEE Commun. Magazine*, vol. 49, pp. 28–35, 2011.

[81] H. V. Poor, “Information and inference in the wireless physical layer,” *IEEE Wireless Communications*, vol. 19, no. 2, pp. 40–47, 2012.

[82] N. Anand, S. Lee, and E. Knightly, “Strobe: Actively securing wireless communications using zero-forcing beamforming,” in *Proc. of IEEE INFOCOM’12*, 2012.

[83] L. Ozarow and A. Wyner, “Wire-tap channel ii,” in *Advances in Cryptology*. Springer, pp. 33–50, 1985.

[84] J. Huang and A. Swindlehurst, “Robust secure transmission in miso channels based on worst-case optimization,” *IEEE Transactions on Signal Processing*, vol. 60, no. 4, pp. 1696–1707, 2012.

[85] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, “Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks,” *IEEE J. Select. Areas of Commun.*, vol. 29, no. 10, pp. 2067–2076, 2011.

[86] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” *IEEE Trans. Sign. Proces.*, vol. 58, no. 3, pp. 1875–1888, 2010.

[87] H. Wang, Q. Yin, and X. G. Xia, “Distributed beamforming for physical-layer security of two-way relay networks,” *IEEE Transactions on Signal Processing*, vol. 60, pp. 3532–3545, 2012.

[88] L. Lai and H. El Gamal, “The relay–eavesdropper channel: Cooperation for secrecy,” *IEEE Trans. Inf .Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.

[89] G. Zheng, L. Choo, and K. Wong, “Optimal cooperative jamming to enhance physical layer security using relays,” *IEEE Trans. Sign. Proces.*, vol. 59, no. 3, pp. 1317–1322, 2011.

[90] J. Li, A. Petropulu, and S. Weber, “On cooperative relaying schemes for wireless physical layer security,” *IEEE Trans. Sign. Proces.*, no. 99, pp. 1–1, 2011.

[91] K. Lee, O. Simeone, C. Chae, and J. Kang, “Spectrum leasing via cooperation for enhanced physical-layer secrecy,” in *Proc. of IEEE ICC’11*, 2011.

[92] Z. Gao, Y. Yang, and K. Liu, “Anti-eavesdropping space-time network coding for cooperative communications,” *IEEE Trans. Wirel. Commun.*, vol. 10, no. 11, pp. 3898–3908, 2011.

[93] L. Dong, Z. Han, A. Petropulu, and H. Poor, “Secure wireless communications via cooperation,” in *Annual Allerton Conference on Communication, Control, and Computing*, 2008.

[94] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. Shen, “Cooperative networking towards secure communications for crns,” in *Proc. of IEEE WCNC’13*, 2013.

[95] N. Zhang, N. Lu, R. Lu, J. W. Mark *et al.*, “Energy-efficient and trust-aware cooperation in cognitive radio networks,” in *Proc. of IEEE ICC’12*, 2012.

[96] H. Ochiai, P. Mitran, H. Poor, and V. Tarokh, “Collaborative beamforming for distributed wireless ad hoc sensor networks,” *IEEE Transactions on Signal Processing*, vol. 53, no. 11, pp. 4110–4124, 2005.

[97] L. Tang, X. Gong, J. Wu, and J. Zhang, “Secure wireless communications via cooperative relaying and jamming,” in *Proc. of IEEE GLOBECOM’11*, 2011.

[98] M. Gursoy, “Secure communication in the low-snr regime: A characterization of the energy-secrecy tradeoff,” in *Proc. of IEEE ISIT’09*. IEEE, pp. 2291–2295.

[99] G. Kim, *Scheduling in wireless ad hoc networks: algorithms with performance guarantees*. ProQuest, 2008.

[100] A. Wiesel, Y. C. Eldar, and S. Shamai, “Zero-forcing precoding and generalized inverses,” *IEEE Transactions on Signal Processing*, vol. 56, no. 9, pp. 4409–4418, 2008.

[101] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wirel. Commun.*, vol. 7, no. 6, pp. 2180–2189, 2008.

[102] J. Laneman, D. Tse, and G. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3062–3080, 2004.

[103] A. Boukerche and Y. Ren, "A trust-based security system for ubiquitous and pervasive computing environments," *Computer Communications*, vol. 31, no. 18, pp. 4343–4351, 2008.

[104] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," *Proceedings of the IEEE*, vol. 98, no. 10, pp. 1755–1772, 2010.

[105] S. Ganeriwal, L. Balzano, and M. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 4, no. 3, pp. 1–37, 2008.

[106] A. Jøsang and R. Ismail, "The beta reputation system," vol. 160, 2002.

[107] Y. Mao and M. Wu, "Tracing malicious relays in cooperative wireless communications," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 2, pp. 198–212, 2007.

[108] T. Khalaf and S. Kim, "Error probability in multi-source, multi-relay networks under falsified data injection attacks," pp. 1–4, 2008.

[109] S. Dehnie, H. Senear, and N. Memon, "Detecting malicious behavior in cooperative diversity," in *Proceedings of the Conference on Information Science and Systems (CISS) 2007.* IEEE, 2007, pp. 895–899.

[110] S. Dehnie and N. Memon, “Detection of misbehavior in cooperative diversity,” in *Proceedings of IEEE MILCOM 2008*. IEEE, 2008, pp. 1–5.

[111] D. B. West *et al.*, *Introduction to graph theory*. Prentice hall Englewood Cliffs, 2001, vol. 2.

[112] R. Jain, D.-M. Chiu, and W. R. Hawe, *A quantitative measure of fairness and discrimination for resource allocation in shared computer system*. Eastern Research Laboratory, Digital Equipment Corporation, 1984.

[113] N. Zhang, N. Lu, N. Cheng, X. Zhang, J. W. Mark, and X. Shen, “Partner selection and incentive mechanism for physical layer security,” *IEEE Transactions on Wireless Communications*, 2015, to apprear.

[114] R. Zhang, L. Song, Z. Han, and B. Jiao, “Physical layer security for two-way untrusted relaying with friendly jammers,” *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3693–3704, 2012.

[115] N. Zhang, N. Cheng, N. Lu, H. Zhou, J. W. Mark, and X. Shen, “Risk-aware cooperative spectrum access for multi-channel cognitive radio networks,” *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 3, pp. 516–527, 2014.

[116] M. G. Damavandi, A. Abbasfar, and D. G. Michelson, “Peak power reduction of ofdm systems through tone injection via parametric minimum cross-entropy method,” *IEEE Transactions on Vehicular Technology*, vol. 62, no. 4, pp. 1838–1843, 2013.

[117] J. B. Rosen, “Existence and uniqueness of equilibrium points for concave n-person games,” *Journal of the Econometric Society Econometrica*, pp. 520–534, 1965.

[118] Q. Xu, X. Li, H. Ji, and X. Du, “Energy-efficient resource allocation for heterogeneous services in ofdma downlink networks: Systematic perspective,” *IEEE Transactions on Vehicular Technology*, vol. 63, no. 5, pp. 2071–2082, 2014.

[119] I. Krikidis, J. Thompson, and S. McLaughlin, “Relay selection for secure cooperative networks with jamming,” *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 5003–5011, 2009.

[120] S. Li, H. Zhu, Z. Gao, X. Guan, K. Xing, and X. Shen, “Location privacy preservation in collaborative spectrum sensing,” *Proceedings of of INFOCOM12*.

[121] L. M. Law, J. Huang, and M. Liu, “Price of anarchy of wireless congestion games,” *IEEE Transactions on Wireless Communications*, to appear.

Appendices

Appendix A:

Proof of Nash Equilibrium

For an NE, it should satisfy the following requirement:

$$w_i \zeta_{j \in s_i}(W_j) \geq w_i \zeta_k(W_k + w_i), \forall k \in \mathcal{K}, j \neq k, i = 1, ..., N. \tag{6.1}$$

To constitute an NE, for any two arbitrary users i and k, according to (6.7), we have

$$w_i \zeta_{j \in s_i}(W_j) \geq w_i \zeta_{j \in s_k}(W_j + w_i) \text{ and}$$
$$w_k \zeta_{j \in s_k}(W_j) \geq w_k \zeta_{j \in s_i}(W_j + w_k)$$

Suppose that SU_1 chooses channel k with the maximum $w' \zeta_k(W_k + w')$, since $w' \zeta_k(W_k + w') > w' \zeta_m(W_m + w')$, $m \neq k, m \in K$. For SU_2, it chooses channel l with the maximum $w' \zeta_l(W_l + w')$, since $w' \zeta_l(W_l + w') > w' \zeta_s(W_s + w')$, $s \neq l, s \in K$. Since $w' \zeta_k(W_k + w') > w' \zeta_l(W_l + w')$, we have $w' \zeta_k(W_k + w') > w' \zeta_l(W_l + w' + w')$. Also, we have $w' \zeta_l(W_l + w') > w' \zeta_k(W_k + w')$. Thus, none of them are willing to change their strategies, and hence their strategies constitute an NE.

For the subsequent users in U_{G1}, they choose their best strategies and then all the strategy files constitute an NE for the new users and existing users. For a new user SU_n, it chooses channel q with the maximum $w'\zeta_q(W_q + w')$, since $w'\zeta_q(W_q + w') > w'\zeta_m(W_m + w')$, $m \neq q, m \in K$. Before SU_n joining, all the former users's strategies constitute an NE. i.e., for SU_p choosing channel j, $w'\zeta_j(W_j) > w'\zeta_m(W_m + w')$,$m \neq j, m \in K$. Then, we have $w'\zeta_j(W_j) > w'\zeta_q(W_q + w') > w'\zeta_q(W_q + w' + w')$. It also holds that $w'\zeta_q(W_q + w') > w'\zeta_m(W_m + w')$, $m \neq q, m \in K$. Thus, the strategies of all the users constitute an NE.

For the user set U_{G2}, each user is assigned a weight of w. For a new user SU_j, it chooses channel x with the maximum $w\zeta_x(W_x + w)$, since $w\zeta_x(W_x + w) > w\zeta_m(W_m + w)$, $m \neq x, m \in K$. Before SU_j joining, all the former users are in NE. Taking an arbitrary user SU_i as an example, if SU_i has chosen channel j rather than channel x, $w_i\zeta_j(W_j) > w_i\zeta_m(W_m + w_i)$, $m \neq j, m \in K$. Then, we have $w_i\zeta_j(W_j) > w_i\zeta_x(W_x + w_i) > w\zeta_x(W_x + w_i + w_i)$. Therefore, for those SUs choosing channel j rather than channel x, they should stay in their current channel and do not change their strategies. If SU_i has chosen channel x, since $w_i\zeta(W_x + w) > w_i\zeta(W_m + w)$, $m \neq x, m \in K$, $w_i\zeta(W_x + w) > w_i\zeta(W_m + w) > w_i\zeta(W_m + w + w)$, $m \neq x, m \in K$. Then, we have $\Psi_x\zeta(W_x + w) > \Psi_j\zeta(W_j + w + w')$. Those users do not have the motivation to change their strategies. Therefore, for all users, their strategies constitute an NE.

Appendix B:

When $\alpha(1-\beta)R_R \geq \alpha\beta R_D$, we have $\beta \leq \frac{R_R}{R_R+R_D}$. Then, the secrecy rate in (3.6) can be given by $[\alpha\beta R_D - \alpha\beta R_E]^+ = \alpha\beta[(R_D - R_E)]^+$, which is a monotonically increasing function with respect to β. To maximize the secrecy rate, β should take the maximum value $\frac{R_R}{R_R+R_D}$. Substituting $\beta = \frac{R_R}{R_R+R_D}$ into (3.6), the secrecy rate can be rewritten as follows: $\bar{R}_{SEC} = \alpha[\frac{R_R(R_D-R_E)}{R_R+R_D}]^+$. When $\alpha(1-\beta)R_R \leq \alpha\beta R_D$, we have $\beta \geq \frac{R_R}{R_R+R_D}$. Then, the secrecy rate in (3.6) can be given by $[\alpha(1-\beta)R_R - \alpha\beta R_E]^+$. which is a monotonically decreasing function of β. To maximize the secrecy rate, β should take the minimum value $\frac{R_R}{R_R+R_D}$. Substituting $\beta = \frac{R_R}{R_R+R_D}$ into (3.6), the secrecy rate can be rewritten as follows: $\bar{R}_{SEC} = \alpha[\frac{R_R(R_D-R_E)}{R_R+R_D}]^+$. As shown above, for the two cases, to maximize the $\bar{R}_{SEC}$, β always equals to $\frac{R_R}{R_R+R_D}$. Moreover, when β takes the optimal value, it holds that $\alpha(1-\beta)R_R = \alpha\beta R_D$. Thus, $\bar{R}_{SEC} = \alpha[\frac{R_R(R_D-R_E)}{R_R+R_D}]^+ = \alpha[R_R - \frac{R_R(R_R+R_E}{R_R+R_D})]^+$.

Appendix C:

Proof of Property 1

Taking the first order partial derivative of the utility function with respect to P_s yields

$$\frac{\partial U_s}{\partial P_s} = \frac{(1-\alpha)W\left|h_s\right|^2}{(1+\frac{P_s h_s^2}{N_0})N_0 \ln 2} - c(1-\frac{\alpha}{2}). \tag{6.2}$$

Then, we have

$$\frac{\partial U_s^2}{\partial P_s^2} = -\frac{(1-\alpha)W\left|h_s\right|^4}{(1+\frac{P_s h_s^2}{N_0})^2 N_0^2 \ln 2}. \tag{6.3}$$

From the above equation, we can see that $\frac{\partial U_s^2}{\partial P_s^2} < 0$. Therefore, the utility function U_s^i of SU_i is concave in its own power level P_s^i when the time allocation is fixed.

Proof of Property 2

For a given SU, the optimal transmission power is given by

$$P_s^*(\alpha) = \frac{(1-\alpha)W}{c(1-\frac{\alpha}{2})\ln 2} - \frac{N_0}{\left|h_s\right|^2}. \tag{6.4}$$

Taking the first derivative of P_s^* with respect to α, we have

$$\frac{\partial P_s^*}{\partial \alpha} = \frac{-\alpha W}{\left(-2+\alpha\right)^2 c \ln 2}. \tag{6.5}$$

The denominator is always positive, while the numerator is negative. Then, $\frac{\partial P_s^*}{\partial \alpha} < 0$. Therefore, the optimal transmission power P_s^* decreases with α.

Proof of Property 3

Since P_s^* is continuous with α, the utility function U_p of the PU is also continuous with α. Substituting $P_s^*(\alpha) = \frac{(1-\alpha)W}{c(1-\frac{\alpha}{2})\ln 2} - \frac{N_0}{\left|h_s\right|^2}$ into U_p, the utility can be given by (4.13), which is a function of α. Taking first order derivative of (4.13) withe respect to α yields (4.14). Then, taking second order derivative of (4.13) with respect to α yields

$$\frac{\partial^2 U_p}{\partial \alpha^2} = 2 \cdot A\alpha + B. \tag{6.6}$$

Since $A > 0$, $B = -2A$, and $0 < \alpha < 1$, we have $\frac{\partial^2 U_p}{\partial \alpha^2} < 0$. Therefore, the utility function of the primary user is concave in the time allocation coefficient α.

NE Condition

A strategy profile is a set of strategy of all inactive SUs and is denoted by $S = s_1, s_2, \ldots, s_M$, where s_i is the strategy of SU_i, Denote by $n(S) = (n_1, ..., n_K)$ the congestion vector corresponding to the strategy profile S, where n_i represents the total number of SUs choosing channel i. For an NE, according the definition of NE, it holds that

$$\Psi_i \zeta(n_i) \geq \Psi_k \zeta(n_k + 1), \forall k \in \mathcal{K}, k \neq i. \tag{6.7}$$

Similar to the work in [121] where uniform MAC is considered, $\zeta(n_i) = 1/n_i$. To constitute an NE, for any two arbitrary channels i and j, according to (6.7), we have

$$\frac{\Psi_i}{n_i} \geq \frac{\Psi_j}{n_j + 1} \text{ and } \frac{\Psi_j}{n_j} \geq \frac{\Psi_i}{n_i + 1},$$

which can be further written as

$$\frac{\Psi_j}{\Psi_i} n_i - 1 \leq n_j \leq \frac{\Psi_j}{\Psi_i} n_i + \frac{\Psi_j}{\Psi_i}, j \neq i. \tag{6.8}$$

For any channel $k \in \mathcal{K}$, $k \neq i, j$, it also holds that

$$\frac{\Psi_k}{\Psi_i} n_i - 1 \leq n_k \leq \frac{\Psi_k}{\Psi_i} n_i + \frac{\Psi_k}{\Psi_i}, k \neq i, j. \tag{6.9}$$

Combining (6.8) and (6.9), we have

$$\sum_{j\neq i, j\in\mathcal{K}} (\frac{\Psi_j}{\Psi_i}n_i - 1) \leq \sum_{j\neq i, j\in\mathcal{K}} n_j \leq \sum_{j\neq i, j\in\mathcal{K}} (\frac{\Psi_j}{\Psi_i}n_i + \frac{\Psi_j}{\Psi_i}), \tag{6.10}$$

which can be further written as

$$\frac{\sum_{j\neq i, j\in\mathcal{K}} \Psi_j}{\Psi_i} n_i - (K-1) \leq \sum_{j\neq i, j\in\mathcal{K}} n_j \leq \tag{6.11}$$

$$\frac{\sum_{j\neq i, j\in\mathcal{K}} \Psi_j}{\Psi_i} n_i + \frac{\sum_{j\neq i, j\in\mathcal{K}} \Psi_j}{\Psi_i}, \tag{6.12}$$

Since $\sum_{j\neq i, j\in\mathcal{K}} n_j = M - n_i$, we have

$$\frac{\Psi_i M - \sum_{j\neq i, j\in\mathcal{K}} \Psi_j}{\sum_{j\in\mathcal{K}} \Psi_j} \leq n_i \leq \frac{\Psi_i M + \Psi_i(K-1)}{\sum_{j\in\mathcal{K}} \Psi_j}. \tag{6.13}$$

Let the right side of (6.13) minus the left side, and we have

$$\frac{\Psi_i M + \Psi_i(K-1)}{\sum_{j\in\mathcal{K}} \Psi_j} - \frac{\Psi_i M - \sum_{j\neq i, j\in\mathcal{K}} \Psi_j}{\sum_{j\in\mathcal{K}} \Psi_j} > 1.$$

Moreover, for the left side of (6.13), it holds that

$$-1 < \frac{\Psi_i M - \sum_{k\neq i, k\in\mathcal{K}} \Psi_k}{\sum_{k\in\mathcal{K}} \Psi_k} < M$$

Therefore, the proposed congestion game has the following solution:

$$n_i = \lceil \frac{\Psi_i M - \sum_{j\neq i, j\in\mathcal{K}} \Psi_j}{\sum_{j\in\mathcal{K}} \Psi_j} \rceil + n', \tag{6.14}$$

where $n' \in \{0, 1, 2, \ldots, \lceil \frac{\Psi_i M + \Psi_i(K-1)}{\sum_{k\in\mathcal{K}} \Psi_k} \rceil - \lceil \frac{\Psi_i M - \sum_{k\neq i, k\in\mathcal{K}} \Psi_k}{\sum_{k\in\mathcal{K}} \Psi_k} \rceil - 1\}$.

Appendix D

Derivation of (5.26) The objective function can be rewritten as follows:

$$\begin{aligned} &\frac{\partial U_i}{\partial P_i} = \frac{r_i P_m \sum_{j \neq i, j \subseteq \mathbb{C}} P_j r_j}{\left(\sum_{j \subseteq \mathbb{C}} P_j r_j\right)^2} - \lambda_2 = 0 \\ \Longrightarrow &\sum_{j \subseteq \mathbb{C}} P_j r_j = \sqrt{\frac{r_i \sum_{j \neq i, j \subseteq \mathbb{C}} P_j r_j}{\lambda_2}} \\ \Longrightarrow &P_i = \frac{1}{r_i}\left(\sqrt{\frac{r_i P_m \sum_{j \neq i, j \subseteq C} P_j r_j}{\lambda_2}} - \sum_{j \neq i, j \subseteq \mathbb{C}} P_j r_j\right) \end{aligned} \tag{6.15}$$

Considering the physical meaning and the maximum power constraint, we have

$$P_i^* = \begin{cases} 0 & \text{if } \sum_{j \neq i, j \subseteq \mathbb{C}} P_j r_j \geq \frac{P_m P_i r_i}{\lambda_2} \\ \frac{1}{r_i}\left(\sqrt{\frac{P_m P_i r_i A}{\lambda_2}} - A\right) & \text{if } \sum_{j \neq i, j \subseteq \mathbb{C}} P_j r_j < \frac{P_m P_i r_i}{\lambda_2} \text{ and } \frac{1}{r_i}\left(\sqrt{\frac{P_m P_i r_i A}{\lambda_2}} - A\right) < P_{max} \\ P_{max} & \text{otherwise} \end{cases} \tag{6.16}$$

Derivation of (5.27) To solve the optimal transmission power of the selected partners, we have

$$\begin{aligned} &\frac{\partial U_i}{\partial P_i} = 0 \\ \Longrightarrow &\frac{r_i P_m \sum_{j \neq i, j \subseteq \mathbb{C}} P_j r_j}{\left(\sum_{j \subseteq \mathbb{C}} P_j r_j\right)^2} = \lambda_2 \end{aligned} \tag{6.17}$$

Then, we have

$$\begin{gathered}\frac{r_1 P_m \sum_{j\neq 1, j\subseteq \mathbb{C}} P_j r_j}{\left(\sum_{j\subseteq \mathbb{C}} P_j r_j\right)^2} = \lambda_2 \\ \vdots \\ \frac{r_i P_m \sum_{j\neq i, j\subseteq \mathbb{C}} P_j r_j}{\left(\sum_{j\subseteq \mathbb{C}} P_j r_j\right)^2} = \lambda_2 \\ \vdots \\ \frac{r_n P_m \sum_{j\neq n, j\subseteq \mathbb{C}} P_j r_j}{\left(\sum_{j\subseteq \mathbb{C}} P_j r_j\right)^2} = \lambda_2\end{gathered} \tag{6.18}$$

Therefore,

$$\begin{gathered}\sum_{j\neq 1, j\subseteq \mathbb{C}} P_j r_j = \frac{r_i}{r_1} \sum_{j\neq i, j\subseteq \mathbb{C}} P_j r_j \\ \vdots \\ \sum_{j\neq n, j\subseteq \mathbb{C}} P_j r_j = \frac{r_i}{r_n} \sum_{j\neq i, j\subseteq \mathbb{C}} P_j r_j\end{gathered} \tag{6.19}$$

Since the summation of the left side equal to the summation of the right side, we have,

$$\left(\frac{r_i}{r_1} + \frac{r_i}{r_2} + ... + \frac{r_i}{r_n}\right) \sum_{j\neq i, j\subseteq \mathbb{C}} P_j r_j = (n-1)\left(\sum_{j\neq i, j\subseteq \mathbb{C}} P_j r_j + P_i r_i\right) \tag{6.20}$$

We also have

$$P_i = \frac{1}{r_i}\left(\sqrt{\frac{r_i P_m \sum_{j\neq i, j\subseteq \mathbb{C}} P_j r_j}{\lambda_2}} - \sum_{j\neq i, j\subseteq \mathbb{C}} P_j r_j\right) \tag{6.21}$$

Then, we can calculate P_i as follows:

$$P_i = \frac{P_m r_i B_i}{\lambda_2 (r_i + B_i)^2} \tag{6.22}$$

where $B_i = \frac{(n-1)r_i}{\sum_{j=1}^{n} \frac{r_i}{r_j} - n + 1}$.

Considering the physical meaning of P_i and the maximum power constraint, we have

$$P_i^* = [\min\{\frac{P_m r_i B_i}{\lambda_2 (r_i + B_i)^2}, P_{max}\}]^+ \tag{6.23}$$