



저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

**Reliable Spectrum Sensing and Physical Layer Security for
Cognitive Radio Networks**

for the Degree of

Doctor of Philosophy

(Electrical Engineering)

Hurmat Ali Shah

November 2018

**Reliable Spectrum Sensing and Physical Layer Security for
Cognitive Radio Networks**

Dissertation

Submitted in partial fulfillment of the requirements
for the degree of

Doctor of Philosophy
(Electrical Engineering)

at the

University of Ulsan

by

Hurmat Ali Shah

November 2018

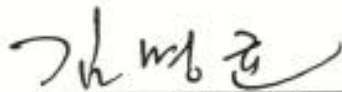
Publication No. _____

©2018 – Hurmat Ali Shah

All rights reserved

Reliable Spectrum Sensing and Physical Layer Security for Cognitive Radio Networks

Approved by supervisory committee:



Prof. Myung-Kyun Kim, Chair



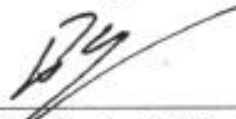
Prof. In-Soo Koo, Supervisor



Prof. Hyung-Yun Kong



Prof. Young-Tae Noh



Prof. Vifadimir V. Shakhov

Department of Electrical Engineering

Ulsan, Republic of Korea

Date: November 2018

VITA

Hurmat Ali Shah was born in Swat, Pakistan in 1987. He received his B.Sc and M.Sc in Computer Systems Engineering from University of Engineering and Technology, Peshawar in 2010 and 2013 respectively. His interests in Masters were reconfigurable computing and bioinformatics. He worked as an entrepreneur before joining his doctoral program.

Since Feb. 2014 he has been involved with School of Electrical Engineering in the doctoral program in electrical engineering, under the supervision of Prof. In-Soo Koo. His research interests span over spectrum sensing and resource allocation in cognitive radio networks, inter-disciplinary approach to problems in wireless communications, machine learning, IoTs and next generation wireless communication technologies.

Dedicated

To the sadness and quiet of dusk at the sea; to the first drop of rain after a sizzling hot day and the first ray of sun in a long gloomy winter; to the breeze at top of the mountain and warmth of the fireplace; to melancholy, to hope, to beauty and to future.

ACKNOWLEDGMENTS

This has been a long journey with stumbles and rejuvenation, despair and hope, joy and trepidation, a sense of achievement and a sense of not being good enough have walked together, often hand in hand. But in the end it was all worth it. But in this entire journey one thing has remained constant: the total guidance by my supervisor Prof. Insoo Koo and his timely interventions in the research work to keep it on track. Without his help the vision of both this research work and the arc of the research direction would be hazy or to be apt short-sighted. I thank Prof. Koo for all his guidance, trust and support in this long journey of my studies. I am also thankful to my Ph.D. supervisory committee for taking out the time to invest in the improvement of my thesis.

I have to thank my family, my elder brother especially, who all have been a source of constant support, love and care to make me go in life. They have focused all their attention and resources on me and understandably all their hopes. I wish to be able to meet up to their hopes soon.

I am thankful to my friends here in Korea and back home and spread throughout the world who have been my anchors in the hardest of my times. The beautiful part of my life is the days I have spent with my group of friends in Korea. It will not be possible to name and thank all of my friends but I will name two friends for personal reasons. I thank Mr. Saeed Ahmad for constant support and lending an ear to listen to my troubles all the time. I am more than obliged to my friend Yousaf Anwar Khan who despite being away at thousands of kms has been a constant source of motivation and cheering up.

I am very thankful to BK 21+ program for financing my studies. My colleagues at MCSL have been more than fellow-travelers. Other than the apt and much required critique and feedback of my work they have come with possible solutions and we have brainstormed together to solve different research problems. I am in particular thankful to my senior Dr. Muhammad Usman for his help and collaboration in initial phase of my research. I am thankful to Dr. Vu Van Hiep for his valuable feedback and recommendation throughout the research seminars and always available when asked for help. I am thankful to all of my other lab-mates and especially my dear friend Sanullah Jan for providing me with a cordial environment all this time.

ABSTRACT

Reliable Spectrum Sensing and Physical Layer Security for Cognitive Radio Networks

by

Hurmat Ali Shah

Supervisor: Prof. Insoo Koo

Submitted in partial fulfillment of the requirements for the Degree of Philosophy (Electrical
Engineering)

November, 2018

The need for spectrum is ever-growing as the use of data services is becoming pervasive. With the onset of new services like smart cities and internet of things (IoTs), and infotainment services in next generation of vehicles, the demand for data and thus for the limited spectrum is increasing. Wireless networks and services supported by wireless technology have been around for ages but because of the revolution in mobile computing brought by smart phones and other such devices the need and desire to stay connected 24/7 has put a unique demand on wireless networks. The services and the devices which need to be served are raising exponentially but the wireless spectrum is a physically limited spectrum. So, to meet all the demands the onus comes on managing the spectrum efficiently.

There is a focus for the last decade or so to come up with techniques which can exploit the loopholes in the present management of the spectrum and also in some ways to radically shift the ways in which the spectrum is accessed. One of such approaches is cognitive radio network (CRN) which aims to exploit the underutilization of the allocated spectrum to fixed and dedicated nodes and services. CRN is a

secondary network which has an unlicensed access the spectrum under certain conditions. CRN is faced with architectural as well as management issues because it has to meet not only the constraints of the primary network and the primary user (PU) but also it has to meet the service demands of the CR users. This dissertation focuses on two of the architectural issues, reliable spectrum sensing and physical layer security. The CR user has to first ascertain that the PU is absent before it can access the channel. This process is known as spectrum sensing. There are myriad of issues in spectrum sensing including the reliability of the spectrum sensing data and learning the changing behavior of the PU. These are addressed in the first part of the dissertation. In the second part of the dissertation the need for secure communication among the CR users is considered. As the CR users are mobile devices so they have limited computing power. The channel codes and encryption techniques used in conventional wireless communications cannot be used in a CRN because of the ad-hoc nature of the CRN and also because of exhaustive demands for computing power of the encryption techniques. Physical layer security which employs digital signal processing techniques to ensure secrecy is suitable for CRN because rather than taking exhaustive computational power it uses the features of channels for providing information secrecy.

In the first part of the dissertation applying bioinformatics inspired techniques to be spectrum sensing is studied. String matching algorithms used in bioinformatics can be applied to scenarios in cognitive radios where reports of cooperative spectrum sensing nodes need to be compared with each other. Cooperative spectrum sensing is susceptible to security risks where malicious users who participate in the process falsify the spectrum sensing data, thus affecting cognitive radio network performance. In this work, an efficient spectrum sensing system is developed where each CR user senses the spectrum multiple times within an allocated sensing period. Each CR user quantizes its decision to predefined levels so as to achieve a trade-off between bandwidth utilization and decision reporting accuracy. The reports for all the CR users are compared at the fusion center using Smith-Waterman algorithm (SWA), an optimal algorithm for aligning biological sequences used in bioinformatics, and similarity indices are computed. Robust mean and robust deviation of the similarity indices are calculated and a threshold is determined by these values. The CR users who have similarity index below the given threshold are declared malicious and their reports are discarded. The local decisions of the remaining CR users are combined using the modified rules of decision combination to take a global decision. Simulation results show that our proposed scheme performs better than conventional schemes with and without malicious users.

The study is extended for investigating optimal quantization schemes for spectrum sensing next. Cooperative spectrum sensing can be made more reliable by excluding the reports of unreliable CR users from the final decision combination at the fusion center (FC). Hard decision combination provides

bandwidth efficiency but the results produced are unreliable while on the other hand soft decision combination has better results but at the expense of much consumption of bandwidth. If instead of hard decision or soft decision combination, quantized information is sent by the CR users to the FC, an acceptable trade-off is achieved. In this paper an optimal quantization scheme is proposed in which the local sensing information is quantized in such a way which ensures that the maximum detection probability is met while the false alarm probability remains under a certain constraint. The proposed optimal scheme works on the basis of energy detection and the local quantization thresholds are found through iterative search. A method inspired from bioinformatics, Smith-Waterman algorithm (SWA) is used to compare the local sensing reports of the CR users and on the basis of comparison similarity indexes are found for the CR users. On the basis of robust mean and robust standard deviation a threshold is calculated for the cooperative spectrum sensing. The local sensing decisions of the CR users below the calculated threshold are rejected and are not included in the final decision combination at the FC. As quantized information is used so the conventionally used rules of decision combination are modified to work on the quantized information and the FC combines the local sensing decisions of rest of the CR users through the modified rules. For detailed analysis, SWA-based rules of decision combination with optimal quantization thresholds are compared with a scheme that employs SWA-based rules of decision combination with heuristically selected quantization thresholds and a conventional majority combination scheme based on heuristically selected quantization thresholds. Simulation results show that the proposed scheme performs better than the other two schemes.

After that a reliable spectrum sensing scheme is proposed, which uses K-nearest neighbor, a machine learning algorithm. In the training phase, each CR user produces a sensing report under varying conditions, and based on a global decision, either transmits or stays silent. In the training phase the local decisions of CR users are combined through a majority voting at the fusion center and a global decision is returned to each CR user. A CR user transmits or stays silent according to the global decision and at each CR user the global decision is compared to the actual primary user activity, which is ascertained through an acknowledgment signal. Based on this comparison, the sensing report is assigned to a sensing class. In the training phase enough information about the surrounding environment i.e. the activity of PU and the behavior of each CR to that activity is gathered. In the classification phase, each CR user compares its current sensing report to existing sensing classes, which are formed in the training phase, and distance vectors are calculated. Based on quantitative variables, the posterior probability of each sensing class is calculated and the sensing report is declared to represent either the absence or presence of a primary user at the CR user level. The quantitative variables used for calculating the posterior probability are calculated

through K-nearest neighbor algorithm. These local decisions are then combined at the fusion center using a novel decision combination scheme, which takes into account the reliability of each CR user. The CR users then transmit or stay silent according to the global decision. Simulation results show that our proposed scheme outperforms conventional spectrum sensing schemes, both in fading and non-fading environments, where performance is evaluated using metrics such as the probability of detection, total probability of error and the ability to exploit data transmission opportunities.

The first part of the dissertation is concluded by investigating a joint spectrum sensing and transmission framework. Actor-Critic algorithm is employed to get the optimal policy and value function and the algorithm is trained through all possible actions and states. In transmission the CR user is constrained by the residual energy. So, energy harvesting is used to harvest energy and then to transmit with transmission energy which meets the long term requirement of the CR user. Given a state which is composed of the remaining energy, the belief and the local and global spectrum decisions an action is selected on the basis of optimal value function and optimal policy function after the training phase is done with. Simulation result show the occurrence of each action selected which points to the probability of the occurrence of the particular state and action combination. The average rate achieved is also shown and is compared with an exhaustive search scheme which acts as the upper bound for the scheme.

The second part of the dissertation deals with physical layer security. First, a physical layer-security scheme for an underlay relay-based CRN that uses OFDM as the medium access technique is proposed. Resource allocation in relay-aided CRNs becomes a hard problem especially if it is under security threat. Different from conventional relay-based OFDM schemes, in the paper we consider the relay network which has two dedicated relay nodes; One relay which is capable of subcarrier mapping forwards the received signal to the destination and the other sends a jamming signal to add noise to the signal received by the eavesdropper. Optimization is performed under a unified framework where power allocation at the source node, power allocation and subcarrier mapping in the relay network are optimized to maximize the secrecy rate of the CRN while satisfying the maximum transmission power constraints and the interference threshold of the PU. The power allocation problem at the forwarding relaying node is a non-convex optimization problem. Therefore, at first the optimization problem is simplified and a closed form solution is obtained which satisfies the maximum PU interference constraint. Afterwards, the optimization problem is solved for satisfying the maximum transmission power constraint. An algorithm is also proposed for subcarrier mapping at the forwarding relaying node. The proposed power allocation method and subcarrier mapping scheme have low complexity, compared to the baseline schemes. Finally, simulation results are

provided for different parameters to show the performance improvement of the proposed scheme in terms of secrecy rate.

Physical layer security is further explored by proposing a physical layer security-based scheme for an underlay CRN that has energy-constrained relay nodes. In the scheme, the cooperative diversity of multiple relays is exploited to provide physical layer security against an eavesdropping attack. Different from conventional relay schemes, relay-based CRN faces other issues, such as the maximum interference-constraint with the PU, and takes into consideration leakage to eavesdroppers in case of an eavesdropping attack. For a CRN to be practical, the energy constraint should be taken into consideration because ad-hoc networks cannot have a fixed power supply all the time. If the nodes in a CRN are able to harvest energy and then spend less energy than the total energy available, we can ensure a perpetual lifetime for the network. In this paper, an energy-constrained CRN is considered where relay nodes are able to harvest energy. A cooperative, diversity-based relay and subchannel-selection algorithm is proposed, which selects a relay and a subchannel to achieve the maximum secrecy rate while keeping the energy consumed under a certain limit. A transmission power factor is also selected by the algorithm, which ensures long-term operation of the network. The power allocation problem at the selected relay and at the source also satisfies the maximum-interference constraint with the PU. The proposed scheme is compared with a variant of the proposed scheme where the relays are assumed to have an infinite battery capacity (so maximum transmission power is available in every time slot), and is compared with a scheme that uses jamming for physical layer security. The simulation results show that the proposed scheme closely follows the infinite battery capacity scheme, which works as the upper bound for the proposed scheme. The infinite battery-capacity scheme outperforms the jamming-based physical layer security scheme, thus validating that cooperative diversity-based schemes are suitable to use when channel conditions are better employed, instead of jamming for physical layer security.

Contents

Supervisory committee	Error! Bookmark not defined.
VITA	viii
Dedication	ix
Acknowledgment	x
Abstract	xi
Contents	xvi
List of Figures	xix
Chapter 1 Introduction	1
1.1 Spectrum Sensing and Physical Layer Security Context	1
1.2 Motivation and Objective.....	5
1.3 Thesis Outline	6
Chapter 2 Bioinformatics-inspired quantized hard combination based abnormality detection for cooperative spectrum sensing in cognitive radio networks	9
2.1 Introduction.....	9
2.2 Related Work	10
2.3 System Model	11
2.4 Malicious Users Detection	14
2.4.1 Spectrum sensing in mini-slots	14
2.4.2 Alignment of the mini-slots	15
2.4.3 Computing similarity index.....	15
2.4.3.1 Smith Waterman Algorithm.....	17
2.4.4 Detecting Malicious Users by Robust Statistics	22
1) Sample median and sample median absolute deviation	22
2) Test for malicious users	23
2.4.5 Decision Combination.....	24
2.5 Simulation Results and Discussion	27
2.5 Conclusion	32
Chapter 3 Optimal multi-threshold quantization scheme for bioinformatics inspired cooperative spectrum sensing in cognitive radio networks	33
3.1 Introduction.....	33
3.2 System Model	37

3.3 Spectrum Sensing.....	41
3.3.1 Optimal Quantization Parameters Selection	41
3.3.2 Computing Similarity Index for CR Users.....	45
3.4 Decision Combination.....	46
3.5 Results and Discussion.....	47
3.6 Conclusion	53
Chapter 4 Reliable machine-learning based spectrum sensing in cognitive radio networks	54
4.1 Introduction.....	54
4.2 System Model	57
4.3. Spectrum Sensing.....	61
4.3.1 Training Phase.....	62
4.3.2 Classification Phase	69
4.3.3 Cooperative Spectrum Sensing	72
4.4. Results and Analysis	75
4.5. Conclusion	83
Chapter 5 Actor-Critic algorithm based accurate multi-bit quantization sensing and transmission framework in energy constrained CRN	84
5.1 Introduction.....	84
5.2 System Model	85
5.3 System Constraints and Definitions	86
5.3.1 Energy Harvesting Process	86
5.3.2 Markovian process	87
5.4 Actor-critic algorithm.....	89
5.5 Simulation Results	92
5.6 Conclusion	95
Chapter 6 A novel physical layer security scheme in OFDM-based cognitive radio networks.....	96
6.1 Introduction.....	96
6.2 System Model and Problem Formulation	99
6.2.1 System Model	100
6.2.2 System Constraints Definitions.....	103
6.2.3 Problem Formulation	104
6.3 Power Allocation and Subcarrier Mapping Scheme	105
6.4 Results and Discussion.....	114
6.5 Conclusion	121

Chapter 7 Improving physical layer security via cooperative diversity in energy-constrained cognitive radio networks with multiple eavesdroppers	123
7.1 Introduction.....	123
7.2 System Model and Problem Formulation	127
7.2.1 System Model	127
7.2 System Constraints Definitions.....	130
7.2.3 Problem Formulation	133
7.3 Relay and subchannel selection under energy constraints and a power allocation scheme	133
7.3.1 Representing the OP through a graph	134
7.3.2 Relay and subchannel selection algorithm.....	138
7.3.3 Power Allocation.....	142
7.4 Results and Analysis	142
7.5 Conclusions.....	149
Chapter 8 Summary of Contributions and Future Work	150
8.1 Introduction.....	150
8.2 Summary of Contributions.....	150
8.3 Future Work	152
Publications	155
References	157

List of Figures

Figure 2.1. Basic system model. CR users sense spectrum and report their results to fusion center.....	12
Figure 2.2. Slotted frame structure. The sensing slot is further divided into mini-slots.....	14
Figure 2.3. System flowchart.....	16
Figure 2.4 Different number of mini-slots due to different SNR for CR users.....	19
Figure 2.5. Alignment of mini-slots with best performing CR user, i.e., $CR^*=CR1$. (a) Aligning CR2 with CR^* , (b) Aligning CR3 with CR^* and (c) Aligning CR4 with CR^*	19
Figure 2.6 Computation of similarity indexes.....	21
Figure 2.7. Similarity scores of CR users.....	26
Figure 2.8(a). ROC for our proposed scheme and the conventional rules of combination without malicious users....	29
Figure 2.8(b). ROC for our proposed scheme and the conventional rules of combination with malicious users.....	30
Figure 2.9. Performance comparison of the conventional (soft) MRC and our proposed (modified) MRC.....	30
Figure 2.10 Comparing the SWA schemes.....	31
Figure 2.11. The effect of SNR on probability of error.....	32
Figure 3.1 Basic system model.....	37
Figure 3.2 Slotted frame structure where the sensing slot is divided into mini-slots.....	40
Figure 3.3 Basic operation sequence.....	41
Figure 3.4. An example of sensing reports of CR users at the fusion center.....	45
Figure 3.5 Flow chart of the proposed scheme.....	48
Figure 3.6. System detection performance with Majority rule for schemes having optimal and heuristic thresholds.....	49
Figure 3.7. System error performance with Majority rule for schemes having optimal and heuristic thresholds.....	50
Figure 3.8. System detection performance with MRC rule for schemes having optimal and heuristic thresholds.....	51
Figure 3.9. System error performance with MRC rule for schemes having optimal and heuristic thresholds.....	52
Fig. 4.1. Basic system model.....	60
Fig.4. 2. Local sensing report and local decision during training phase.....	62
Figure 4.3 (a) Decision tree for the case that local decision is Z_1	66
Figure 4.3 (b) Decision tree for the case that local decision is Z_2	66
Figure 4.3 (c) Decision tree for the case that local decision is Z_3	67
Figure 4.3 (d) Decision tree for the case that local decision is Z_4	67
Fig. 4.4 (a). Time frame structure when the FC decision is Z_3 or Z_4 during the training phase.....	68
Fig. 4.4 (b). Time frame structure when the FC decision is Z_1 or Z_2 during the training phase.....	68
Fig. 4.5. Frame structure during classification phase.....	70
Fig. 4.6. System detection performance with non-fading channels.....	78
Fig. 4.7. System error performance with non-fading channels.....	79
Fig. 4.8. System probability of exploiting spectral holes.....	80
Fig. 4.9. System detection performance with fading channels.....	81
Fig. 4.10. System error performance with fading channels.....	82
Fig. 4.11. Effect of number of CR users.....	82
Figure 5.1 Basic system model.....	86
Figure 5.2 Markovian process.....	87
Figure 5.3 Average throughput of the system.....	93
Figure 5.3 Comparison of probability of error.....	94

Figure 6.1 The system model	100
Figure 6.2 Flowchart of the proposed scheme	109
Figure 6.3 Effect of number of subcarriers on the secrecy rate	116
Figure 6.4 Effect of maximum transmission power on secrecy rate	116
Figure 6.5 Effect of the distance between relay network and eavesdropper on the secrecy rate	117
Figure 6.6 Effect of channel gain between relay and CR receiver on secrecy rate	119
Figure 6.6 Comparison with reference scheme	121
Figure 7.1 Basic system model	128
Figure 7.2 Step 1 in graph matching	136
Figure 7.3 Step 2 in graph matching	136
Figure 7.4 Step 3 in graph matching	137
Figure 7.5 Step 4 in graph matching	137
Figure 7.6 Effect of the energy harvesting rate	144
Figure 7.7 Effect of the long-term energy constraint	146
Figure 7.8 Effect of the number of relays on the secrecy rate.....	146
Figure 7.9 Effect of the number of relays on secrecy rate	148
Figure 7.10 Comparison with the reference scheme	148

Chapter 1

Introduction

1.1 Spectrum Sensing and Physical Layer Security Context

Cognitive radio (CR) has been proposed to address the issue of spectrum scarcity resulting from inefficient utilization of spectrum resources [1, 2]. A CR user has unlicensed access to the spectrum under the constraint that primary user (PU) communication is not affected. To ensure this, the spectrum is continuously monitored for PU activity. Spectrum sensing can also be used to detect spectral holes and enable CR users to transmit opportunistically. The performance gain of a CR system is further improved by cooperative spectrum sensing (CSS), where multiple CR users cooperate to detect spectral holes.

While matched filtering outperforms other techniques such as cyclostationary detection and energy detection used for spectrum sensing, its complexity makes it impractical for most systems. Energy detection is the simplest technique, given the limited resources (e.g., energy and computational power) of most CR users. Common spectrum sensing problems such as multi-path fading and shadowing can be overcome by exploiting spatial diversity using CSS, thereby ensuring that PU constraints are met [3]. In CSS, individual CR users share their data with a fusion center (FC) that combines local reports to make a global decision. CR users can report the actual amount of received energy i.e. the not quantized into different levels and then reporting the quantized level which can be represented by fewer bits than the number of bits required for representing the actual amount of energy received. This is called soft decision combination and results in optimal detection performance, but theoretically requires infinite bandwidth [4]. Alternatively, CR users can make a hard decision based on the received energy and report a single bit representing either the presence or absence of the PU to the FC [5]. Hard reporting saves bandwidth, but

produces inferior results as compared to soft reporting. Linear soft combination has nearly the same performance as likelihood ratio tests [6].

Radio spectrum is scarce; however, the appetite for spectrum is boundless. The ever-increasing connectivity of huge arrays of today's devices and appliances as well as introduction of new ones, such as Internet of Things (IoT), put a strain on usage of precious radio spectrum resources. The traditional method of allocating fixed frequency band to a user or a system makes it hard to meet the demands for deploying new services or enhancing the present ones. Inflexible spectrum management rather than physical shortage of the resource is the reason for spectrum scarcity [7]. Alternative approaches that use the spectrum efficiently provide solutions for the growing demands and mitigating the spectrum scarcity issue. CR is the technology that utilizes the spectrum efficiently by dynamic spectrum access. It is critical to sense the presence of the PU reliably and vacate the band quickly.

Spectrum sensing is a daunting task; however, it is crucial to the performance of the cognitive radio network (CRN). Spectrum sensing of a single CR user becomes unreliable due to factors such as shadowing, fading and time-diversity of wireless channels. Cooperative spectrum sensing is used to reliably sense the spectrum in the above scenarios. In cooperative spectrum sensing, a slotted frame structure is used to sense the spectrum and transmit data [8]. Spectrum is sensed continuously by cooperating CR users in the first portion of the slotted frame-structure, which is known as sensing slot. The remaining time slot, known as transmission slot, is utilized to transmit data. As the sensing time increases, the spectrum sensing becomes more reliable; however, this occurs at the expense of less time for actual data transmission and vice versa. The optimal sensing time and transmission time tradeoff are investigated by researchers in [9]. Cooperative spectrum sensing adds space-diversity to the process; however, the wireless channels also vary with time. Therefore, to add time-diversity, a multi-slot spectrum sensing, where a sensing slot is divided into mini-slots, is considered in [9] and [3].

The benefits of cooperation aside, cooperation incurs potential security vulnerabilities. In addition to the traditional security threats in wireless communications, CRN brings its own set of security issues. The most potent among them, which can severely degrade performance of CRN, is the spectrum sensing data falsification (SSDF) attack. In SSDF, a CR user maliciously reports wrong result of a spectrum sensing to the common reporting center, called fusion center (FC), and affects the reliability of spectrum sensing. Authors in [4] show that presence of even a single malicious user (MU) can significantly affect the output of spectrum sensing at the FC. An MU can affect the performance in multiple ways. If the PU is absent and an MU reports its presence, this may result in the increased probability of false alarms, which

will increase the number of missed opportunities for transmission. Hence it reduces overall system throughput. In an opposite scenario, the detection probability will be reduced and it will cause interference to the PU. The CR users send their local information to the FC where it is combined with information from other CR users for decision-making. In a practical scenario, a large number of bits are required when a CR user transmits the real value of observed energy level and this results in wasting communication bandwidth. Although hard combination efficiently utilizes bandwidth, it produces inferior results as compared to soft combination due to the information loss. Hard combination may be practically inferior because control channels between CR users and FC are often considered to be perfect (i.e., error-free) while it may not be the case in reality. Therefore, it is easy to change or reverse the result of hard-combination by either noise or some malicious activity. To combine the performance gain and bandwidth efficiency of both hard and soft combination, quantized combination is used in [10] and [11]. In [11], the authors used an approach called softened hard combination scheme where the observed energy is quantized into four different regions and two bits, that represent an energy zone, are sent instead of one bit. This accomplishes an acceptable trade-off between the improved performance that is the result of soft reporting and the information loss during the process.

There are two methods to access the spectrum. The first method for accessing the spectrum is called overlay mode, and the second is called underlay mode. Spectrum sensing is necessary for the overlay mode as access to the spectrum is dependent upon knowing the state of PU. In underlay mode, because of the coexistence of two different kinds of communications, each with different levels of priority, power allocation in CR communications becomes a design issue on which the performance of the whole system depends. Orthogonal frequency division multiplexing (OFDM) has shown great promise in improving transmission efficiency. By minimizing inter-symbol interference, high-speed data transmission is made possible. If the concept of OFDM is integrated into cognitive radio, spectrum utilization will improve. OFDM-based cognitive radio can become an important future-generation wireless system. The key problem in relay-based cognitive radio networks that use OFDM as a spectrum access technique is power allocation on different hops. In a multi-hop network, the channel gain over different hops may be mutually independent for all subcarriers. So, the subcarriers that face deep fading over one hop may not experience deep fading over the other hops [12]. This fact allows a degree of freedom in resource allocation, which allows for properly matching subcarriers on different hops. This is called sub-carrier matching [13]. Compared with traditional single-hop OFDM systems, resource allocation in a relay-based multi-hop OFDM system becomes more challenging. Resource allocation is made more difficult by the interference

constraint in cognitive radio systems. In the context of a cognitive radio network (CRN), a subcarrier with the highest gain over one hop may also cause the most interference with the PU, and mapping this subcarrier to a carrier with the highest gain over the next hop may result in strong interference with the PU.

Wireless communications suffer from security issues where an eavesdropper overhears legitimate communications. Confidentiality of wireless communications is attracting much research interest. Traditionally, the security for communications systems is dealt with at higher layers. But because of the lack of infrastructure in ad-hoc networks, such as a CRN, security at higher layers in ad-hoc networks becomes infeasible. The encryption algorithms used in higher-layer security approaches can be compromised as computational power is becoming increasingly available to users that can be eavesdroppers [2]. This approach is also made complicated by the difficulty with secret key distribution. Thus, physical layer-security techniques have received greater interest of late to ensure security at the physical layer. Physical layer-security approaches exploit properties of the communications channel to ensure secrecy. It is an information-theoretic approach, and secrecy is achieved by using channel codes and signal processing techniques at the physical layer.

The work on exploiting cooperative diversity for physical layer security in wireless networks cannot be directly applied to CRNs. The CRN is presented as a solution to the spectrum scarcity problem, where spectrum is left unutilized by the PU. When the spectrum is underused by the PU, CR user can access it, or the CR user can access the spectrum simultaneously with the PU provided interference with the PU is under a certain limit (underlay mode). So, CRNs have special features: the PU always takes precedence in using the spectrum, and it is unreasonable to assume that the PU is willing to cooperate with CR users without any conditions. Along with the special features of a CRN, cooperative diversity cannot be directly exploited, as is done in traditional wireless networks, without any concern for security. In traditional cooperative diversity schemes, the channel state information (CSI) of a two-hop network (source to relay and relay to destination) is needed. While exploiting cooperative diversity for physical layer security, the CSI of the wiretap link with two-hop link CSI has to be taken into consideration.

To consider practical ad-hoc networks, taking the energy constraints into consideration is of paramount importance. When cooperative diversity-based schemes are considered, then the power used for generating artificial noise in jamming-based schemes can be directed towards transmission on the main link. The main restraint in energy-limited wireless networks is that the power spent in a time slot should be equal to, or less than, the total energy available. The harvested energy adds to the residual energy, and thus, the network can potentially operate for eternity, provided that the rate of energy harvesting is taken into

consideration. For an energy-constrained CRN, the constraints on maximum transmission power, interference with the PU, and residual energy have to be taken into consideration before transmission. To ensure long-term operation, there needs to be enough energy left in the battery for future transmissions. Thus, selecting a relay from among many in order to exploit spatial diversity is a problem to be solved in maximizing the secrecy rate, along with keeping to the PU's maximum-interference requirements and the energy budget

1.2 Motivation and Objective

CRN are emerging as an intriguing alternative to the conventional modes of wireless communications. The Spectrum Policy Task Force of the Federal Communications Commission of the US pointed out back in 2002 that the spectrum allocated is underutilized [2]. Thus the issues of spectrum scarcity which is result of the ever-growing needs for spectrum and the ubiquitous spread of wireless communication nodes is basically a spectrum management issue. According to the report mentioned the spectrum is unoccupied for 15% to 80% of the time. CR was proposed earlier by Mitola as software defined radio framework which is able to function intelligently [1]. CR has the capacity to change the operational parameters and transmitting behavior based on feedback from the environment. CR in terms of communications is employed for unlicensed access to the spectrum. There is a PU who has licensed access to the spectrum and given that the PU is absent or the interference caused to the PU is below a threshold the CR user can have access to the spectrum. The CR user has to vacate the spectrum at the earliest if the PU appears. As CR users are ad-hoc nodes and a CRN is an ad-hoc network the mobility along-with the energy available for transmission has to be taken into consideration. Wireless networks are always faced with security threats but in case of a CRN because of the ad-hoc nature of the network the security threat becomes both immediate and hard to detect.

So, in CRN there are many areas to be investigated in detail. The spectrum needs to be sensed reliably so that there is no interference to the communication of PU. Other than that the malicious activity in the process of sensing along with the reliability of the data regarding sensing has to be investigated in depth. Solutions to both detecting malicious activity and to gathering accurate sensing data have to be proposed. After spectrum sensing the data need to be transmitted securely. The cryptography technique requires complex channel codes and a lot of computational resources, so, they are not suitable for a CRN. As an alternative physical layer security is employed that relies on techniques of digital signal processing to

counter the security threats. The constraint on maximum transmission energy limits the performance of an ad-hoc network so the energy requirements during the transmission have also to be taken into consideration when optimizing the throughput for the current transmission slot. Based on this introduction the thesis will focus on having reliable spectrum sensing schemes which can detect malicious activity and also can reflect accurately the behavior of the PU in the sensing data. On the other end physical layer security scheme with optimization techniques for providing security while requiring low computational resources will be investigated.

The objective of this dissertation is to (i) investigate a multi-bit quantization based spectrum sensing scheme which detects the malicious activity for CRNs, (ii) investigate the optimal quantization thresholds for spectrum sensing as the result of spectrum sensing are based on the quantization scheme, (iii) investigate machine learning to learn the sensing environment and thus to enable the CR to gauge its behavior to the changing PU activity, (iv) investigate physical layers security scheme in a CRN which uses OFDM as media access technology, (v) to come up with a physical layer security scheme which works in an environment where there are multiple eavesdroppers and under awareness of the energy constraint, and (iv) to investigate a sensing and transmission framework for energy constrained CRN.

1.3 Thesis Outline

The thesis is divided into two parts. The first part is about spectrum sensing and is composed of chapter 2, 3, 4 and 5. The second part is focused on physical layer security and is composed of chapter 6 and 7. A brief description of each chapter is given below.

Chapter 2 explores the mechanism where bioinformatics inspired methods can be applied into CRN. In bioinformatics sequence matching is an important basic operation and is used to find similarities or dissimilarities between two biological sequences. When there are malicious users present in the process of spectrum sensing the sensing data cannot be accepted as it is. Rather there is a need to detect the malicious users and remove their sensing result in the final sensing decision combination. The methods in bioinformatics which are used for detecting similarity can be applied to this context in a CRN. A weight is also assigned to each CR user and it is taken into consideration before taking a global sensing decision. Robust statistics is employed to reach have stable data points for reliable sensing decision. The scheme proposed in this chapter is compared with conventional sensing schemes through parameters such as

detection performance and performance of false alarm probability. *This work was published in IEEE Sensors journal in 2015.*

Chapter 3 focuses on finding accurate quantization thresholds for multi-bit sensing. Quantizing the received energies at the CR user before taking a global decision is of crucial importance to the performance of the quantization based decision combination. Multi-bit quantization achieves a trade-off between the performance of soft decision combination and the bandwidth improvement of hard decision combination. The theoretical model of multi-bit quantization is analyzed and the metric for performance of detection and false alarm probability stated. Based on the probability of detection and probability of false alarm an algorithm for finding optimal thresholds for quantization is proposed. The optimal thresholds are compared with heuristically selected thresholds and conventional sensing schemes and the results show that the optimal quantization threshold outperforms the other schemes. *This study was published in International Journal of Electronics in 2018.*

Chapter 4 discusses the need for using machine learning techniques for reliable spectrum sensing. The wireless environment and spectrum is dynamic and thus always changing. The CR users are not able to know the changing behavior of the PU and its own behavior to that change in the environment. Implicit in the process of a continuous sensing is learning. Machine learning techniques can be applied to convert this learning into a meaningful data for future sensing. The sensing behavior of the CR users is learned and the sensing data is categorized into sensing classes based on the status of the ACK signal. The ACK signal determines the ground reality i.e whether the sensing decision taken in case of the PU being absent truly reflected the actual PU status or not. When the training phase is complete there is enough data to accurately take spectrum decision in the current sensing slot. The decision in current sensing slot is taken by computing a posterior probability based on K nearest neighbor machine learning method. The simulation results show the effect of different sizes of the training phases and also compare the proposed scheme to spectrum sensing methods not based on machine learning techniques. *This work was published in Wireless Communication and Mobile Computing in 2018.*

Chapter 5 discusses a joint spectrum sensing and transmission scheme. Actor-critic algorithm is used to take an action which is to stay silent or transmit with one of two levels of transmission energies in order to meet the long term operational requirements is selected. The current state at CR user determines the action to be taken. The state is composed by the combination of local and global sensing decision, the belief and the residual energy. The actor takes an action and based on the temporal difference the critic gives feedback to the actor. When the training phase is complete there is optimal value function and

optimal policy. The throughput performance of the actor-critic algorithm and the occurrence of each training instance are found via simulations.

In the second part of the thesis the physical layer security is discussed. In chapter 6 power allocation scheme for physical layer security for CRN when OFDM is used as the medium access technique is discussed. In the presence of eavesdroppers the power allocation at the relay has to take into account the interference caused by the jammer. The jammer has to transmit simultaneously with the forwarding relay node so that the leakage to the eavesdropper is at minimum. The power allocated to the subcarriers at the relay becomes a non-convex optimization problem which is NP hard and thus had to be converted into a convex optimization problem by solving for the maximum interference to the PU constraint and relaxing the maximum transmission power constraint. The revised optimization problem is solved through Cauchy-Shwartz inequality then. The simulation result show the secrecy rate achieved while varying different parameters like power, channel gain and distance. *This work was published in IEEE Access in 2018.*

In chapter 7 multiple eavesdroppers along-with multiple relays are taken into consideration for proposing a physical layer security scheme. The cooperative diversity of the relays is exploited to maximize the secrecy rate. Multiple subchannels are also considered in the system model for this chapter so selecting a relay with a subchannel becomes a non-trivial problem. Ad-hoc networks have limited amount of power available so energy harvesting is taken into consideration. An algorithm is proposed which selects the best relay and best subchannel for that relay to transmit over and select a transmission power factor for the relay-subchannel pair which will satisfy the long term energy requirements of the system. Graph theory is used to translate the complex problem of three way matching to a two way matching with multiple edges which represent the value of transmission power factor and the nodes represented relay and subchannel-eavesdropper pairs. The performance of the proposed system is shown through the effect of transmission power, number of relay, number of eavesdroppers and MER on the secrecy rate. *This work is under-review in International Journal of Communication Systems.*

Finally, chapter 8 concludes the thesis and presents a brief summary of the contributions and discusses future work.

Chapter 2

Bioinformatics-inspired quantized hard combination based abnormality detection for cooperative spectrum sensing in cognitive radio networks

2.1 Introduction

Bioinformatics is an integrated approach that combines multiples fields like mathematics, statistics, computer science and signal processing to model and answer crucial questions raised in molecular biology. One of the fundamental tasks in bioinformatics is DNA sequence alignment. Long strings of characters, representing DNA bases, are matched against each other in order to find regions of similarity, overall similarity, or dissimilarity. Simple though exact and powerful methods such as Smith-Waterman algorithm (SWA) are employed to perform sequence alignment. The insights gathered in bioinformatics can be easily migrated to a CRN. The techniques developed in biological sequence alignment (like protein sequences, DNA, and RNA sequences) can be applied in a CRN to identify malicious users because both processes are concerned with identifying anomaly among patterns of information.

In this chapter, a holistic approach to detect malicious users accurately and mitigate their adverse effects in cooperative spectrum sensing is presented. The approach combines an efficient spectrum sensing method, a quantized method for reporting sensing information, a well-used method in bioinformatics known as Smith-Waterman algorithm, and the modified rules of fusion at the fusion center. To add time-diversity to the spectrum sensing, the sensing slot is divided into mini-slots. The observed energy in each mini-slot is quantized into one of four quantized zones and is reported in two bits. Hence, it combines both the bandwidth efficiency and accurate information reporting. The reports of all CR users are compared with each other using the SWA to determine the similarity indices. Accurate mean and standard deviation of the similarity indices are found using the robust statistics. The CR users whose similarity indices are below a certain threshold, which is determined by the robust mean and robust standard deviation, are declared

malicious and their reported information is discarded. Different rules of combination are applied to combine evidences from the remaining CR users. Because of using quantized hard reporting, the conventional rules of combination, such as OR, AND, and Majority, cannot be applied directly. Therefore, conventional rules are modified as multi-level OR, AND, and Majority rules that can make multi-level decision. Similarly, the maximum ratio combination (MRC) rule is modified to support multi-level inputs.

This chapter is organized as follow; Section 2 presents the related work; Section 3 describes the system model in detail; Section 4 presents a method for detecting malicious users; Section 5 presents the results and discussion; and finally Section 6 concludes the paper.

2.2 Related Work

The factor of foremost consideration in slotted-cooperative spectrum sensing is the duration of each time slot. Authors in [3] have studied and proposed a polynomial complexity algorithm to optimize the duration of sensing. The sensing duration is divided into mini-slots and each mini-slot is used to sense one channel. Ref [10] shows that the presence of even a single misbehaving user will significantly affect the performance of cooperative spectrum sensing. Methods to detect malicious users can be generally divided into two categories: a passive method that apply the techniques of robust signal processing to mitigate the effect of a malicious user activity [14], and a proactive method that allows other users or a common reporting center to detect a malicious activity. Ref [15]-[17] provide a fusion center with MU detection capability. Authors in [14] and [12] consider special type of attackers, which are more complicated than the simple conventional attackers that only falsify data. Ref [14] introduces an intelligent and dependent attacker that has the capability to peek into other CR users' reports and can change its behavior accordingly. Ref [18] considers a specific type of attacker; "hit-and-run" attacker who knows the fusion rule used by the FC and estimates its suspicion level. It continues to send malicious reports while the suspicion level is below a threshold.

Methods ranging from recording of the reporting history of CR users to machine learning are used to detect such malicious users' anomalies. Ref [19] uses a non-uniform reliability and identification tag to detect unreliable and malicious users. Non-uniform reliabilities are computed using the correlation between the reports sent by CR users and the global decision taken by the FC. Ref [15] detects malicious users by computing different reputation metrics for a CR user. It declares a CR user to be honest or malicious based on the trust values derived from the metrics. Ref [20] also computes a reputation metric by comparing the

report of each user to the one generated by the FC. If a mismatch is found, the reputation metric is increased by one, and if the reputation metric is above a specified threshold, the CR user is declared to be malicious. Ref [21] adjusts for temporarily misbehaviors of the CR users which are caused by effects such as fading or shadowing. The reputation metric of a CR user is restored when the CR user starts behaving normally. Weighted Sequential Probability Ratio Test (WSPRT) is used in [22] to assign weights to each CR user. The weights are calculated by comparing each CR user's report with the FC decision. If both are the same, the reputation metric is increased by one; otherwise, it is decreased by one.

Ref [4] studies a softened hard combination scheme in which each CR user uses two bits to report its sensing information. These bits represent different regions in which the sensed energy falls. The presence or absence of the PU signal is decided based on the condition that whether one of the three specified thresholds is met or not. Authors in [23] have considered a uniform quantization scheme for cooperative sensing, which uses a global weight vector as a global decision function. Analytical expressions for one-bit hard combination and two-bit hard combination have been derived by [11].

2.3 System Model

We consider a single PU and a CRN that consists of N -CR users as shown in Fig. 1. The CR users perform spectrum sensing and report their results to the FC. We assume a slotted time frame-structure where each slot is divided into two slots: a sensing slot, which is used for spectrum sensing, and a transmission slot, which is used for actual data transmission. The sensing slot is further divided into sub-slots named mini-slots as shown in Fig. 2. In each mini-slot, the spectrum sensing is performed independently [3]. This process adds temporal diversity to the process of spectrum sensing. The number of mini-slots of the i -th CR user is denoted by m_i .

Each CR user employs the energy detection scheme for spectrum sensing. The signal received at the k -th mini-slot by the i -th CR user is given by Eq. (1)

$$y_{k,i} = \begin{cases} w(n); & H_0 \\ s(n) + w(n); & H_1 \end{cases} \quad (2.1)$$

where n represents the sample of the received signal, $w(n)$ is the additive white Gaussian noise and $s(n)$ is the received signal from the PU with mean μ and variance σ^2 . Energy of the received signal in the k -th mini-slot is given by

$$Y_{k,i} = \frac{1}{Z} \sum_{n=1}^Z |y_{k,i}(n)|^2 \quad (2.2)$$

where Z is the total number of samples received in the sensing duration of the k -th mini-slot. The received energy in each mini-slot is quantized into predefined energy zones. The energy zones are represented by A, C, T, and G. These are the same letters as are used in the DNA sequence alignment where each letter represents bases of a DNA sequence. The quantized energy zones are represented as

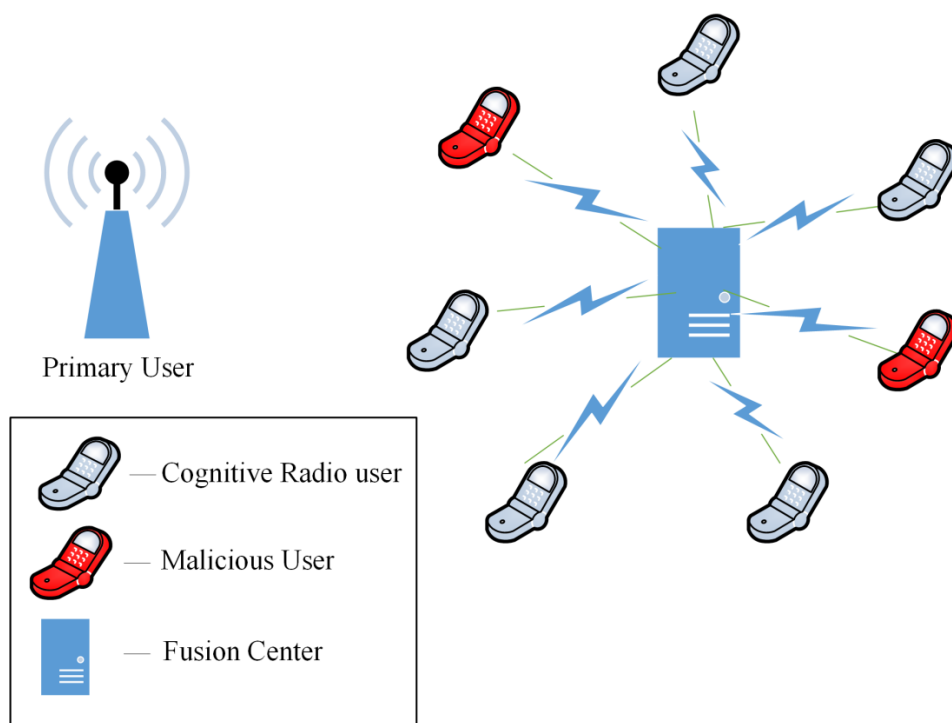


Figure 2.1. Basic system model. CR users sense spectrum and report their results to fusion center.

$$q_{k,i} = \begin{cases} A & ; Y_{k,i} \leq \lambda_A \\ C & ; Y_{k,i} \leq \lambda_C \end{cases} H_0 \\ \begin{cases} T & ; Y_{k,i} \leq \lambda_T \\ G & ; Y_{k,i} > \lambda_T \end{cases} H_1 \quad (2.3)$$

where λ_A , λ_C , and λ_T are the thresholds that differentiate different energy zones, and $q_{k,i}$ represents quantized energy for the k -th mini-slot of the i -th CR user. Sensing report of the i -th CR user is given by set

$\hat{q}_i = \{q_{1,i}, q_{2,i}, \dots, q_{m_i,i}\}$. Later, when comparing reports of different CR users, symbols that represent neighboring energy zones (A, C, or T, G) are assigned different weights from the ones far from each other (i.e., A and G). Each CR user takes a local decision by averaging the energy values obtained in mini-slots as given as

$$Y_i = \frac{\sum_{k=1}^{m_i} Y_{k,i}}{m_i} \quad (2.4)$$

The local decision of the i -th CR user is represented by D_i and is given by

$$D_i = \begin{cases} A & ; Y_i \leq \lambda_A \\ C & ; Y_i \leq \lambda_C \\ T & ; Y_i \leq \lambda_T \\ G & ; Y_i > \lambda_T \end{cases} \quad (2.5)$$

The detection probability and false alarm probability of the i -th CR user is given by Eq. (2.6) and Eq. (2.7), respectively as

$$P_{d,i} = \Pr(D_i = U | H_1) = \Pr(Y_i > \lambda_C | H_1) \quad (2.6)$$

and

$$P_{f,i} = \Pr(D_i = U | H_0) = \Pr(Y_i > \lambda_C | H_0) \quad (2.7)$$

where $U = \{T, G\}$ corresponds to H_1 .

The maximum allowable sensing duration of a mini-slot is T_s , which is the total duration of a sensing slot. The number of mini-slots, m_i , for the i -th CR user is given by

$$m_i = \frac{T_s}{t_{s,i}} \quad (2.8)$$

where $t_{s,i}$ is the duration of each mini-slot of the i -th CR user. For a given detection probability and false alarm probability, the sensing duration of a mini-slot of the i -th CR user is determined as [24]

$$t_{s,i} = \frac{Q^{-1}(P_{f,i}) - Q^{-1}(P_{d,i}\sqrt{2\gamma_i + 1})}{\sqrt{f_s \gamma_i}} \quad (2.9)$$

where γ_i is the received signal-to-noise ratio (SNR) at the i -th CR user, f_s is the sampling frequency and $Q^{-1}(\cdot)$ is the inverse Q -function.

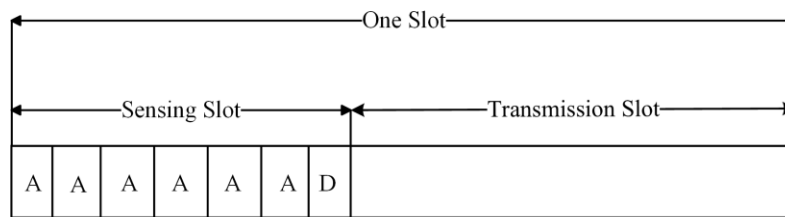


Figure 2.2. Slotted frame structure. The sensing slot is further divided into mini-slots.

Each CR user sends the quantized sensing reports of its mini-slots and local decision to the FC. After preprocessing, the FC compares reports of the CR users with each other to calculate similarity indices. The CR users having similarity indices below a threshold, which is determined by robust statistics, are declared malicious and their reports are discarded. Sensing reports of the honest CR users are considered for decision combination. Details of the MU detection and decision combination are described in the next section.

2.4 Malicious Users Detection

This section presents the proposed approach to detect malicious users using Smith-Waterman algorithm, a well-known algorithm in bioinformatics and other fields where string comparison is the primary required operation. The reports sent by MUs mainly deviate from the reports of legal CR users. Exploiting this property and applying efficient sequence matching technique, MUs can be detected and their evidences are excluded from decision combination process. Fig. 2.3 presents the system flowchart. Each process is explained in the following subsections.

2.4.1 Spectrum sensing in mini-slots

As described in Section 2.3, each CR user senses spectrum multiple times during a sensing slot. Energy of the signal measured in each mini-slot is quantized into predefined quantization levels. Fig. 2.4 illustrates an example of the spectrum sensing reports sent by four CR users. The number of mini-slots depends on SNR of the CR user. A better SNR results in better spectrum sensing; hence, the number of mini-slots increases for the CR user with better SNR.

2.4.2 Alignment of the mini-slots

A CR user with better SNR channel completes spectrum sensing in less time and is able to sense the channel multiple times within the allocated sensing slot, which is the maximum allowable sensing duration. This results in many sub-slots known as mini-slots. After receiving sensing reports from all CR users, alignment of these reports is required for the next step where they are compared with each other. The FC determines alignment factor for each CR user with respect to the best CR user and may further divide each mini-slot based on the alignment factor. The best CR user is the CR user that has the largest number of mini-slots and is denoted by CR*.

The alignment factor is denoted by Ω_i and is determined as follows:

$$\Omega_i = \left\lceil \frac{m_{\max}}{m_i} \right\rceil \quad (2.10)$$

where m_{\max} is the number of mini-slots for the best CR user and m_i is the number of mini-slots for the i -th CR user. Fig. 2.5 shows an example of the mini-slots alignment for four CR users. CR1 is the best CR user because it has the maximum number of mini-slots (i.e., six mini-slots) due to its received SNR. In Fig. 2.5(a), the alignment factor for CR2 (Ω_2) is two. This implies that each mini-slot for CR2 should be further divided into two sub-slots in order to be aligned with the mini-slots for CR1. Since the sensing result of CR2 is available at the 2nd mini-slot, the 1st mini-slot of each subdivision is marked with “-”, which denotes that the sensing result is not available in the particular mini-slot. Similarly, this process is repeated for the reports of CR3 and CR4 as shown in Fig. 2.5(b) and 2.5(c), respectively.

2.4.3 Computing similarity index

After the alignment process, reports of the CR users are compared with each other using the SWA to compute their similarity indices. The similarity index shows the degree of similarity that each CR user's report has with reports of other CR users. The SWA is briefly presented in the following sub-section.

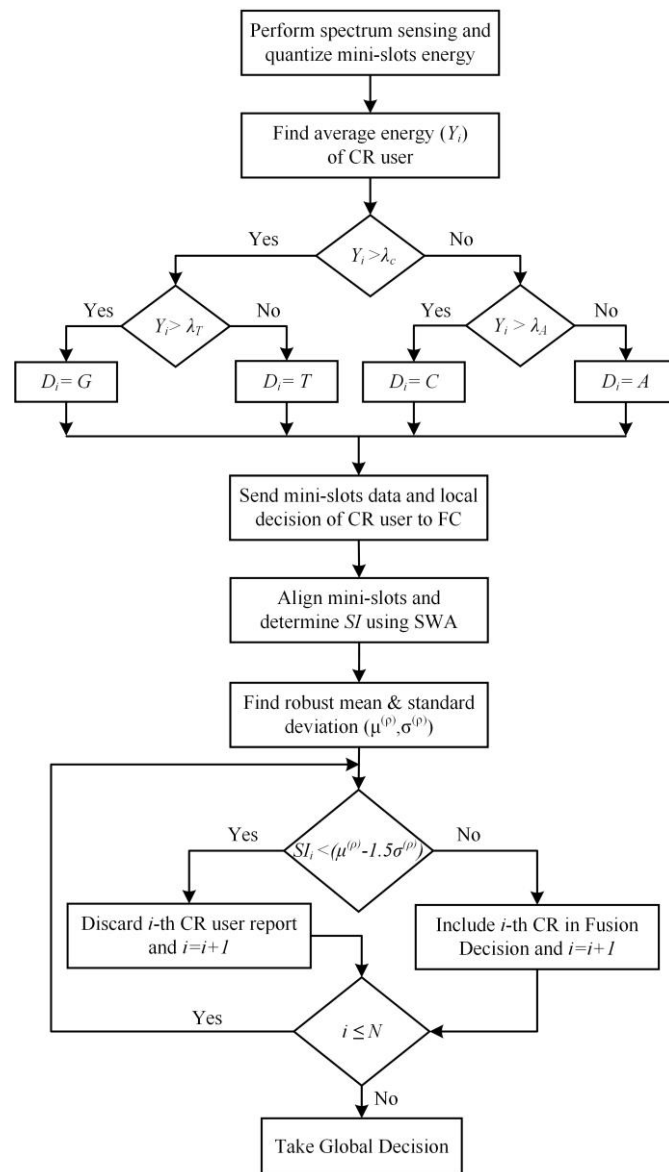


Figure 2.3. System flowchart.

2.4.3.1 Smith Waterman Algorithm

The Needleman and Wunsch presented an efficient algorithm [25] for the global alignment of two sequences. The Needleman-Wunsch algorithm (NWA) produces optimal results; however, it could not find relations between distantly related sequences as it performed global alignments. Global alignments perform well when the sequences to be aligned are closely related because they consider similarity between the whole sequences and ignore regions of similarity. Therefore, global alignment methods fail to perform optimally when the sequences to be aligned do not have large homology. Smith and Waterman presented a variant of the NWA in 1984, known as the Smith-Waterman algorithm (SWA) [26]. The SWA finds the local alignment and works well for sequences that are distantly related, because such sequences do not manifest overall similarity while they have regions that have concentrated local similarity.

Local alignments are carried out by making small changes to the equations that perform global alignments. Similar to the NWA, the SWA consists of three stages to perform the alignment: initialization, matrix fill, and trace back. The initialization and matrix fill stages resemble those of the NWA, while the trace back stage differs from the NWA. The three stages are briefly described as follows.

i. Initialization

The initialization step differs for the NWA and SWA. In the SWA, the top row and the leftmost column are initialized to 0, whereas in the NWA the upper-rightmost element (0, 0) is set to zero and the top row and leftmost column are initialized with the values of gap penalties.

ii. Matrix Fill

The sensing reports of two CR users are compared by arranging the report of a CR user (\hat{q}_i) vertically and report of the other CR user (\hat{q}_j) horizontally, as shown in Table 2.1. Each element of \hat{q}_i , i.e., $q_{k,i}$, is compared with every element of \hat{q}_j , i.e., $q_{l,j}$, and score ($F(k, l)$) is computed accordingly using the matrix fill equation as given below.

$$F(k, l) = \max \begin{cases} 0 \\ F(k-1, l-1) + s(q_{k,i}, q_{l,j}) \\ F(k-1, l) - d(q_{k,i}, q_{l,j}) \\ F(k, l-1) - d(q_{k,i}, q_{l,j}) \end{cases} \quad (2.11)$$

where $k, l = 1, 2, \dots, m_{max}$ and are indices of the elements of report \hat{q}_i and report \hat{q}_j , respectively, $q_{k,i}$ is the k -th element of report \hat{q}_i and $q_{l,j}$ is the l -th element of report \hat{q}_j , $s(q_{k,i}, q_{l,j})$ is the similarity reward between two characters and is selected on the basis of their similarity, and $d(q_{k,i}, q_{l,j})$ is the gap penalty (dissimilarity) that determines the degree of mismatch between $q_{k,i}$ and $q_{l,j}$ to be penalized. Values of the similarity reward and gap penalties for biological sequence alignment are derived from biological observations. Different reward and penalty values are defined for different types of sequences and applications. Here we use intuitive values based on experimental results. The value of a similarity reward shows how much reward is given to the match and the value of gap penalty shows how much penalty is given to the mismatch between two characters. Equation (2.12) is used for similarity reward and (2.13) is used for gap penalty as

$$s(q_{k,i}, q_{l,j}) = \begin{cases} 2, & (q_{k,i} = q_{l,j}; q_{k,i}, q_{l,j} \neq '-')$$

$$\begin{cases} 1, & (q_{k,i} = 'A', q_{l,j} = 'C') \text{ or} \\ & (q_{k,i} = 'T', q_{l,j} = 'G') \\ 0, & \text{otherwise} \end{cases} \quad (2.12)$$

and

$$d(q_{k,i}, q_{l,j}) = \begin{cases} 4, & (q_{k,i} = 'A', q_{l,j} = 'G') \text{ or } ('-', q_{l,j}) \text{ or } (q_{k,i}, '-')$$

$$\begin{cases} 3, & (q_{k,i} = 'A', q_{l,j} = 'T') \text{ or } (q_{k,i} = 'C', q_{l,j} = 'G') \\ 2, & (q_{k,i} = 'C', q_{l,j} = 'T') \\ 1, & (q_{k,i} = 'A', q_{l,j} = 'C') \text{ or } (q_{k,i} = 'T', q_{l,j} = 'G') \\ 0, & \text{otherwise} \end{cases} \quad (2.13)$$

It is important to note that $s(q_{k,i}, q_{l,j}) = s(q_{l,j}, q_{k,i})$ and $d(q_{k,i}, q_{l,j}) = d(q_{l,j}, q_{k,i})$, i.e., similarity reward and gap penalty hold commutative property. Similarity score between two CR users $F_{\hat{q}_i, \hat{q}_j}$ is obtained by taking the maximum element of score matrix (F). Similarity score of the i -th CR user when compared with the j -th CR user is given by

$$F_{\hat{q}_i, \hat{q}_j} = \max_{k, l=1, 2, \dots, m_{max}} \{F(k, l)\}. \quad (2.14)$$

Similarity score also holds commutative property like the similarity reward and gap penalty. Similarity

score of two CR users is shown as an example in Table 2.1, which is obtained using the matrix fill equation. Similarity score between CR_i and CR_j is obtained by selecting the maximum value in Table 2.1.

iii. Trace back

The third stage of the SWA is called trace back and is performed to align sequences based on the scores computed in “matrix fill” stage. Our objective is to get the maximum score of two sequences instead of aligning them; therefore, the trace back stage is not required in our work.

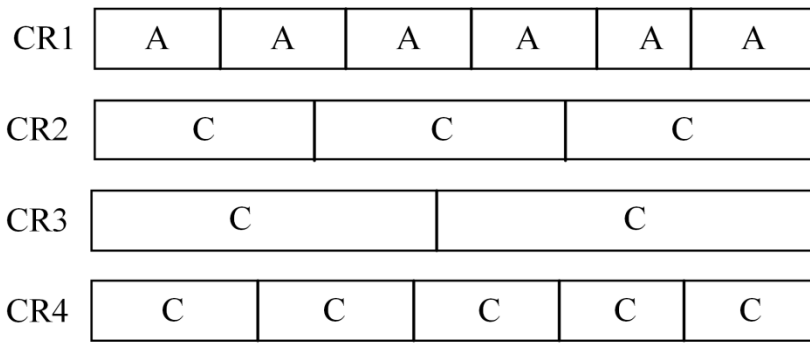


Figure 2.4 Different number of mini-slots due to different SNR for CR users.

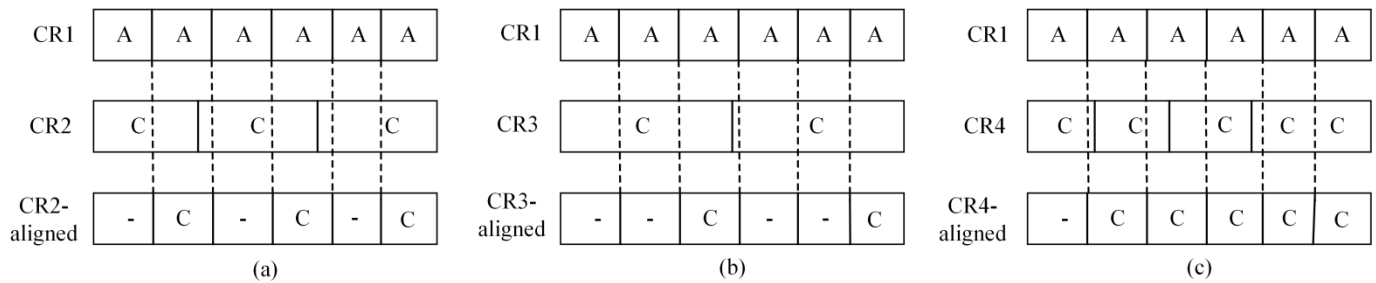


Figure 2.5. Alignment of mini-slots with best performing CR user, i.e., $CR^*=CR1$. (a) Aligning CR2 with CR^* , (b) Aligning CR3 with CR^* and (c) Aligning CR4 with CR^*

2.4.3.2 Similarity index

Similarity index of a CR user is computed by accumulating the similarity scores of a CR user obtained from comparison with the other CR users. The similarity index of the i -th CR user is computed by the following expression.

$$SI_i = \sum_{j=1, j \neq i}^N F_{\hat{q}_i, \hat{q}_j} \quad (2.15)$$

The flowchart in Fig. 2.6 summarizes computation of the similarity indices for CR users. Fig. 2.7 and Table 2.2 show an example of similarity indices computation for five CR users. Similarity index of CR1 is obtained by comparing its sensing report with CR2, CR3, CR4, and CR5 successively. Comparison of CR1 with CR2, CR3, CR4, and CR5 using the SWA produces the similarity scores; nine, six, eight, and zero, respectively. Similarity index of CR1 is the summation of all similarity scores and is 23 (9 + 6 + 8 + 0). Similarity index of CR2 is computed in a similar fashion. However, comparison of CR2 and CR1 is not required due to the commutative property of similarity scores. The process is repeated until similarity indices for all CR users are obtained.

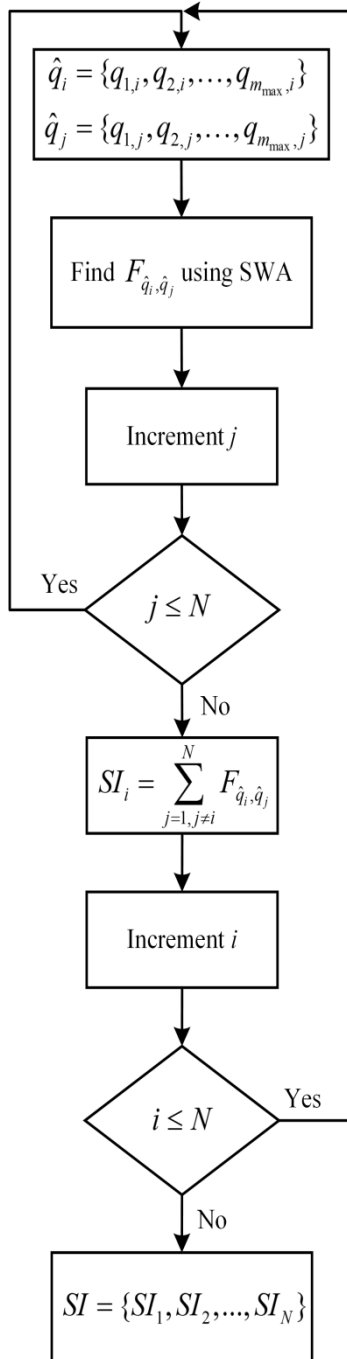


Figure 2.6 Computation of similarity indexes

2.4.4 Detecting Malicious Users by Robust Statistics

The robust statistics [27] guard against the stability threat by progressively adjusting the mean and standard deviation of data, similarity indices for all CR users in this case. This approach provides an alternative to statistical estimators such as mean and standard deviation and is more resilient in face of malicious activity; therefore, it is called “robust”. Other than sample mean and sample standard deviation, robust statistics define two other important parameters: the sample median and sample median absolute deviation.

1) Sample median and sample median absolute deviation

Let $SI = \{SI_{(1)}, SI_{(2)}, \dots, SI_{(N)}\}$ be the ordered set of similarity indices for all CR users arranged in ascending order. The sample median is defined by the following equation.

$$MED(SI) = \max \begin{cases} SI_{((N+1)/2)}, & \text{if } N \text{ is odd} \\ \frac{SI_{(N/2)} + SI_{(N/2+1)}}{2}, & \text{if } N \text{ is even} \end{cases} \quad (2.16)$$

Median is the point that bi-furcates the values into two sets when there is no outlier. The sample median absolute deviation is defined by

$$MAD(SI) = MED(|SI_i - MED(SI)|) \quad (2.17)$$

$MAD(SI)$ determines the distance in which observations lie away from $MED(SI)$. At least half of the observations lie at a distance $MAD(SI)$ or more on one side of the $MED(SI)$ and at least half are at a distance $MAD(SI)$ or more on the other side of the $MED(SI)$. We use Hubber’s method [27] to accurately estimate the variance and mean of the resulted data distribution. The original data is progressively transformed by an iterative process known as Winsorisation process, which makes use of deviating data instead of rejecting it altogether. The Winsorisation process is summarized in the following steps.

Step 1: Set initial value of mean and variance as

$$\begin{cases} \mu^{(0)} = MED(SI) \\ \sigma^{(0)} = 1.4826 \times MAD(SI) \end{cases} \quad (2.18)$$

The factor 1.4826 is a constant factor that makes the robust value correspond to the normal distribution.

Step 2: Test and adjust malicious users (outlier) data using the Winsorization process as

$$\hat{SI}_i = \begin{cases} \mu^{(0)} - 1.5\sigma^{(0)}, & \text{if } SI_i < \mu^{(0)} - 1.5\sigma^{(0)} \\ \mu^{(0)} + 1.5\sigma^{(0)}, & \text{if } SI_i > \mu^{(0)} + 1.5\sigma^{(0)} \\ SI_i, & \text{otherwise} \end{cases} \quad (2.19)$$

where 1.5 is chosen as multiplier value in the Winsorisation process.

Step 3: An improved estimated mean and an improved estimated standard deviation are calculated as $\mu^{(1)} = mean(\hat{SI}_i)$ and $\sigma^{(1)} = 1.134 \times stdev(\hat{SI}_i)$, respectively.

Step 4: Steps 2 and 3 are repeated until data values become stable, i.e., the estimated mean and estimated standard deviation no longer change. Let the number of iterations be ρ , then $\mu^{(\rho)}$ and $\sigma^{(\rho)}$ are the robust or stable estimated mean and standard deviation, respectively.

2) Test for malicious users

After accurate estimation of sample robust mean and sample robust standard deviation, test for malicious users is carried out using (19). CR users who have similarity indices below a threshold are declared malicious, because they have deliberately tampered with spectrum sensing data. The threshold value is determined by robust statistics which consists of a stable mean and a stable standard deviation. The spectrum sensing reports from malicious users are discarded before moving to the decision combination for the remaining honest CR users.

$$CR_i = \begin{cases} 0, & \hat{SI}_i < \mu^{(\rho)} - 1.5\sigma^{(\rho)} \\ 1, & \text{otherwise} \end{cases} \quad (2.20)$$

According to the above equation, malicious users (CR users whose similarity index is below the threshold)

are assigned zero value. The number of malicious users can be obtained using the following equation.

$$M = N - \sum_{i=1}^N CR_i \quad (2.21)$$

The number of honest CR users are $N - M$.

2.4.5 Decision Combination

After discarding reports from malicious users, local decisions of the remaining CR users need to be combined in order to decide about presence or absence of the PU signal. The conventional rules of combination are modified to multi-level rules of combination, because they are not applicable to the scenario in its original form. However, the logic of multi-level rules remains similar to the conventional rules. The working principle of multi-level OR rule defines that the input which represents the highest energy level is propagated as output. G is the highest energy level followed by T , C , and A . The truth table for OR rule is given in Table 2.3 and the multi-level OR rule is given by

$$OR(I_1, I_2) = \begin{cases} I_1; & \text{if } I_1 = I_2 \\ \max(I_1, I_2); & \text{if } I_1 \neq I_2 \end{cases} \quad (2.22)$$

where I_1 and I_2 are inputs, which may be one of the four symbols i.e., A , C , T and G . The global probability of detection and global false alarm probability of the OR-rule are given as

$$\begin{aligned} P_D &= 1 - \prod_{i=1}^{N-M} (1 - P_{d,i}) \\ P_F &= 1 - \prod_{i=1}^{N-M} (1 - P_{f,i}) \end{aligned} \quad (2.23)$$

In case of the AND rule, the lowest of inputs is produced as the output. The multi-level AND rule is given by (23) and its truth table is presented in Table 2.4.

$$AND(I_1, I_2) = \begin{cases} I_1; & \text{if } I_1 = I_2 \\ \min(I_1, I_2); & \text{if } I_1 \neq I_2 \end{cases} \quad (2.24)$$

The global detection probability and global false alarm probability of the AND-rule are given by

$$\begin{aligned}
 P_D &= \prod_{i=1}^{N-M} P_{d,i} \\
 P_F &= \prod_{i=1}^{N-M} P_{f,i}
 \end{aligned}
 \tag{2.25}$$

The multi-level Majority rule works similar to the conventional single bit Majority rule. The quantized symbol reported by majority of CR users is taken as the global decision and corresponds to the absence or presence of the PU signal. The global detection probability and global false alarm probability of the Majority-rule are given as

$$\begin{aligned}
 P_D &= \sum_{x=\lfloor \frac{N-M}{2} \rfloor}^{N-M} \binom{N-M}{x} P_{d,i}^x (1 - P_{d,i})^{N-M-x} \\
 P_F &= \sum_{x=\lfloor \frac{N-M}{2} \rfloor}^{N-M} \binom{N-M}{x} P_{f,i}^x (1 - P_{f,i})^{N-M-x}
 \end{aligned}
 \tag{2.26}$$

where $\lfloor \cdot \rfloor$ represents the floor operator.

Maximal Ratio Combination (MRC) is conventionally used in soft-decision combination where each CR user is assigned a weight and its report is evaluated accordingly. We propose a modified MRC rule as a decision combination of the quantized reports sent by CR users. The previously calculated similarity index is used as the weighting factor for the quantized local decision of a CR user. Weights of the same local decisions are accumulated according to the following equation;

$$P(r) = \sum_{i=1}^{N-M} \frac{SI_i}{S} 1(D_i = r); \quad r \in \{A, C, T, G\}
 \tag{2.27}$$

where $S = \sum_{i=1}^{N-M} SI_i$ and $1(D_i = r) = \begin{cases} 1; & D_i = r \\ 0; & D_i \neq r \end{cases}$.

If the combined cumulative weight of A and C is greater than the combined cumulative weight of T and G , then status of the PU signal is declared H_0 ; otherwise, H_1 . Global decision (D_G) using the modified MRC

rule can be expressed as follows:

$$D_G = \begin{cases} H_0; & P(r = 'A') + P(r = 'C') > \\ & P(r = 'T') + P(r = 'G') \\ H_1; & P(r = 'A') + P(r = 'C') \leq \\ & P(r = 'T') + P(r = 'G') \end{cases} \quad (2.28)$$

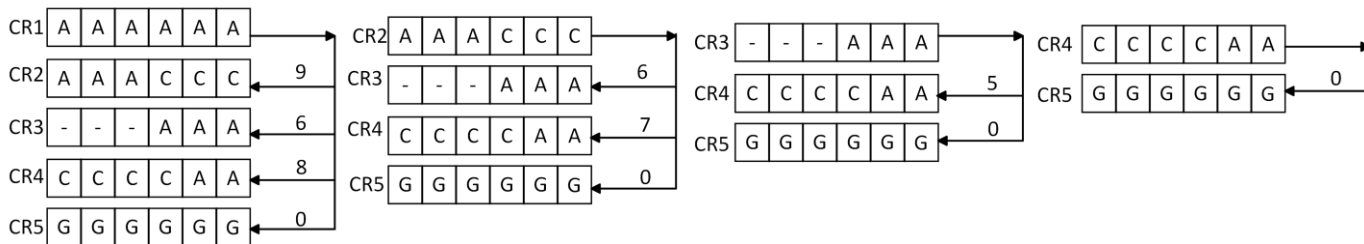


Figure 2.7. Similarity scores of CR users.

TABLE 2.1
COMPARING REPORT \hat{q}_j WITH \hat{q}_i

		\hat{q}_j					
		A	A	A	A	A	A
\hat{q}_i	A	2	2	2	2	2	2
	A	2	4	4	4	4	4
	A	2	4	6	6	6	6
	C	1	3	5	7	7	7
	C	1	2	4	6	8	8
	C	1	2	3	5	7	9

TABLE 2.2
SIMILARITY INDICES OF CR USERS

	CR1	CR2	CR3	CR4	CR5	SI
CR1	-	9	6	8	0	23
CR2	9	-	6	7	0	22
CR3	6	6	-	5	0	17
CR4	8	7	5	-	0	20
CR5	0	0	0	0	-	0

2.5 Simulation Results and Discussion

TABLE 2.3
MULTI-LEVEL OR RULE

I_1	I_2	OR
G	A,C,T,G	G
A,C,T,G	G	G
T	A,C,T	T
A,C,T	T	T
C	A,C	C
A,C	C	C
A	A	A

TABLE 2.4
MULTI-LEVEL AND RULE

I_1	I_2	AND
A	A,C,T,G	A
A,C,T,G	A	A
C	C,T,G	C
C,T,G	C	C
T	T,G	T
T,G	T	T
G	G	G

In this section, we present simulation results to show the effectiveness of our work. In simulations we have compared our results with the conventional cooperative spectrum sensing, employing one-bit conventional OR, AND, and Majority rules, with and without malicious users. We have shown performance improvement in our work by plotting the ROC curve. We have also shown the effect of SNR on detection probability and error probability. We have considered a CRN consisting of ten CR users. The duration of the sensing slot is considered to be 1 ms.

The number of iterations are 3000. The false alarm probability of CR users is 0.02. SNR of the CR users varies from -30 dB to -5 dB. The idle probability of PU, denoted by $P(H_0)$, is 0.5. We assume that the channel from PU to CR users suffer from log-normal shadowing. The CR users are assumed to be close enough to the source PU and far enough from other PUs; thus, the interference from other PUs is negligible.

Fig. 2.8(a) shows the detection performance of the conventional cooperative spectrum sensing scheme and our proposed approach when the system has no MUs. The conventional cooperative spectrum sensing which uses hard decision with conventional logical rules of decision combinations and no method for detection of malicious users are shown by the curves with “Conv” tags. Our proposed scheme uses modified logical rules for decision combination and the SWA for computing similarity indices for the CR users. It is represented by the curves with “SWA” tags. It is clear from the figure that our proposed scheme gives better detection performance than the conventional cooperative spectrum sensing scheme. This is because the CR users with low SNR are unable to detect the PU signal accurately and this misdetection leads to a degraded detection performance in the conventional scheme. On the other hand, our proposed scheme suppresses the reports of such CR users by assigning a low similarity index to them. The CR users with good SNR values are assigned high similarity indices accordingly, which results in an improved detection performance of the network.

Fig. 2.8(b) contrasts the performance of both schemes in the presence of MUs. Always busy (AB), always false (AF), and always opposite (AO) malicious users are modeled. The combined effect of these malicious activities and temporary misbehaviors affect the overall CRN system performance. It is clear from the figure that even the best performing conventional scheme has a worse performance than our worst performing proposed scheme in the presence of MUs. This is because the lowest similarity indices are assigned to MUs due to their deviant behavior from the honest CR users. In effect, the CR users with a similarity index below a threshold, determined by the robust statistics in Section 4.4, are declared malicious and their reports are discarded. Contribution of the honest CR users for global decision improves detection performance of the system. On the other hand, conventional schemes have no safeguard to detect temporary misbehavior or intentional misbehavior; therefore, any anomaly affects the global decision combination and leads the FC to make false decision.

In Fig. 2.9, we have compared MRC as conventionally used and our proposed modified MRC that works for the quantized hard decisions, with and without MUs respectively. It can be seen that the conventional soft decision based MRC outperforms our proposed scheme at the expense of considerable bandwidth

consumption. Our proposed approach uses two bits to represent the result of a CR user while soft-decisions take a large number of bits to send the exact value of its observation. When malicious users are introduced to the system, they drastically affect the performance of “MRCsoft”, which is the conventional MRC. However, the “MRCModif”, which is our proposed scheme shows resilience and closely follows the curve for the case of no malicious users. The conventional MRC scheme decides on distribution of energy values and is misled when the distribution is tilted to the false side. Hence, it affects the performance of conventional MRC scheme. Any temporary misbehavior as well as malicious users are detected by our proposed scheme; hence, the global decision combination is not affected.

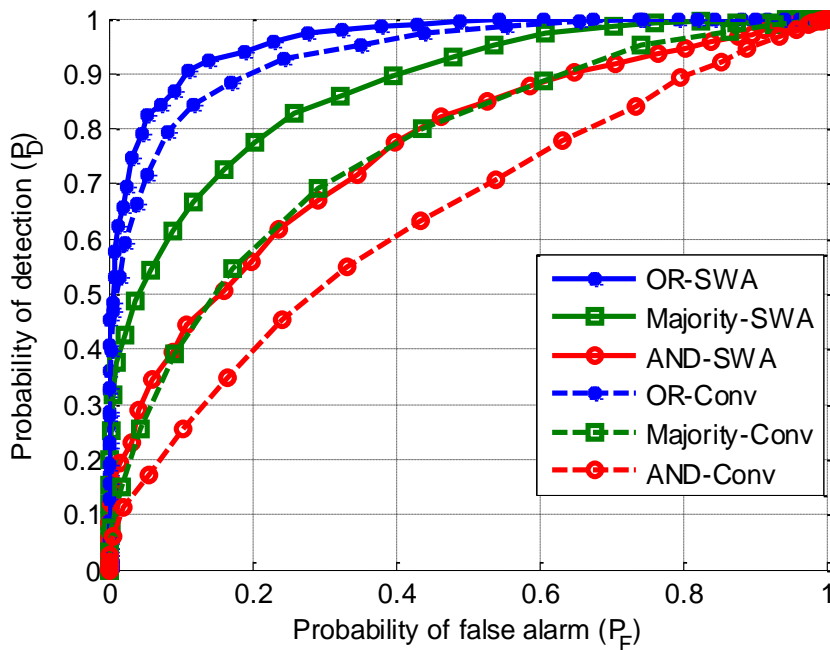


Figure 2.8(a). ROC for our proposed scheme and the conventional rules of combination without malicious users

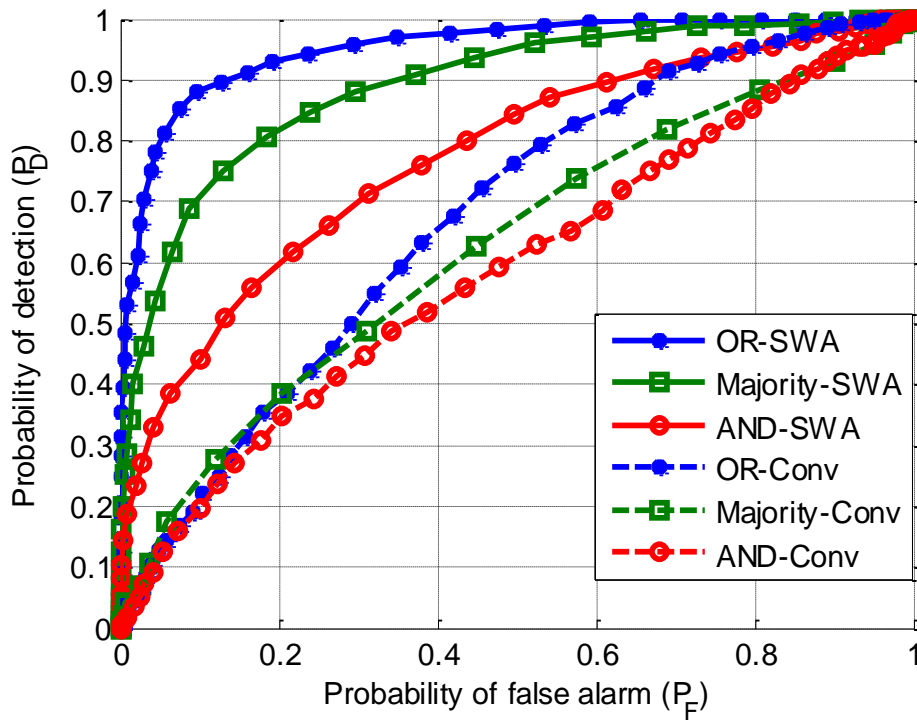


Figure 2.8(b). ROC for our proposed scheme and the conventional rules of combination with malicious users.

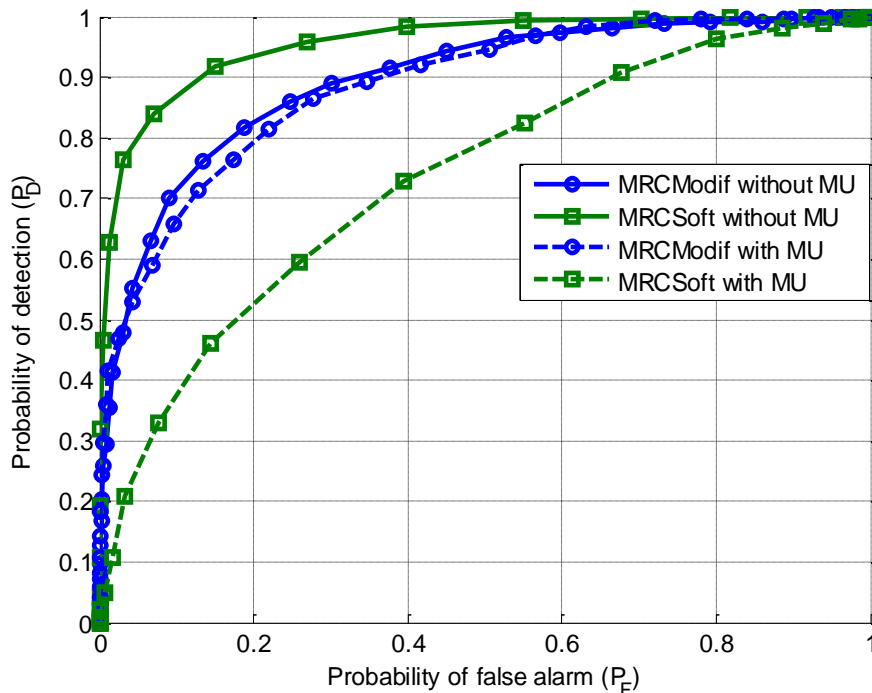


Figure 2.9. Performance comparison of the conventional (soft) MRC and our proposed (modified) MRC.

Fig.2.10 shows the effect of SNR on detection probability of the system. The detection probability matches with intuition. The detection probability of the system improves with the increasing values of SNR and quickly reaches to the convergent value. At low SNR values, the CR users may be unable to detect the PU signal, which results in a reduced detection probability. For high values of SNR, the chances of misdetection decreases and results in an improved detection probability.

Fig. 2.11 shows the probability of error in relationship to SNR. The error probability is defined by

$$P_E = P_F \times P(H_0) + (1 - P_D) \times P(H_1). \quad (2.29)$$

The figure demonstrates that increase of SNR decreases the error probability. The inverse relationship of error probability with the detection probability causes a decrease in the error probability as detection probability increases. As demonstrated in Fig. 10, the detection probability increases when SNR increases; hence, the increase of SNR ultimately makes the error probability to decrease.

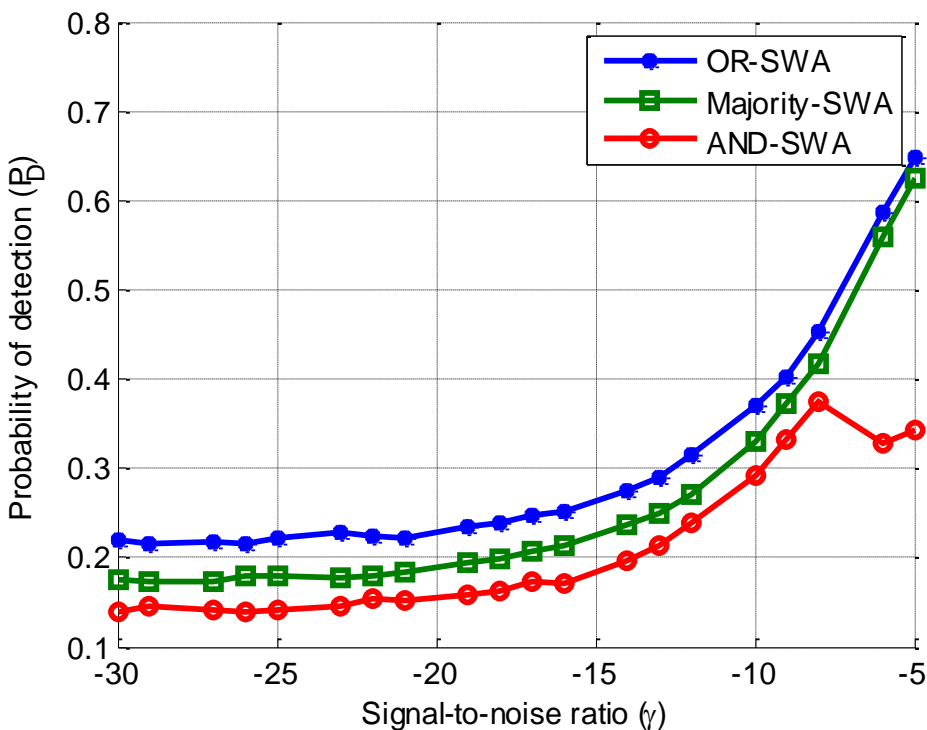


Figure 2.10 Comparing the SWA schemes

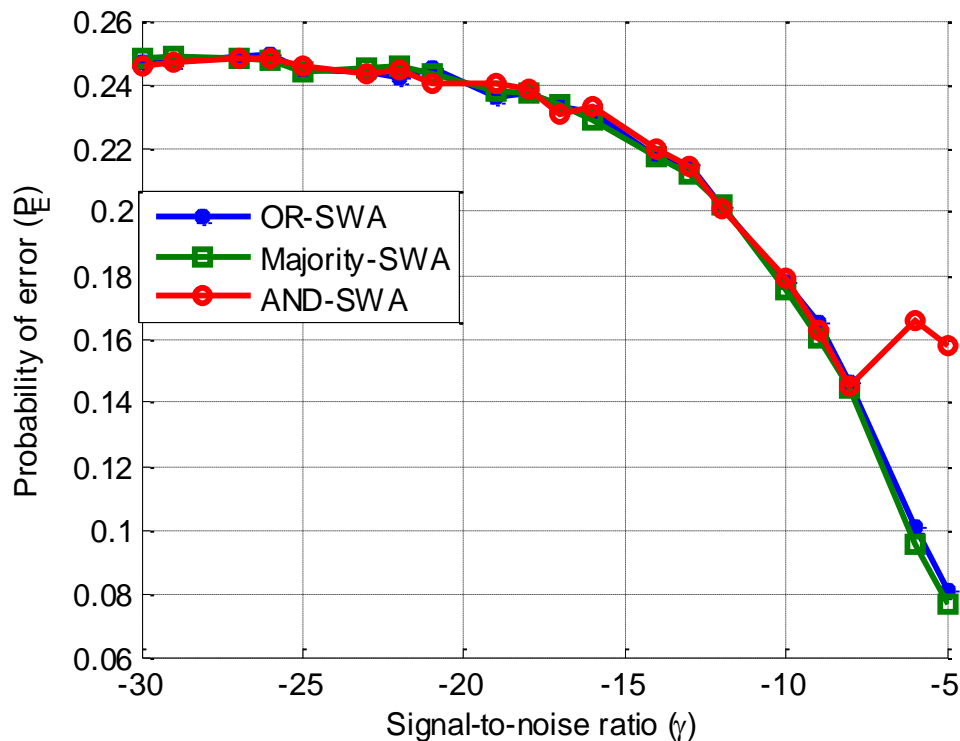


Figure 2.11. The effect of SNR on probability of error.

2.5 Conclusion

Smith-Waterman algorithm is extensively used in bioinformatics to accurately align biological sequences and identify similarities between biological sequences. The SWA can be easily used to find information that is dissimilar to others; thus malicious activity can be detected in cognitive radio network. In this paper, we devised a method to detect malicious users using the SWA. Spectrum sensing reports of CR users, who sensed spectrum multiple times in one allocated sensing time slot, were compared with each other using the SWA. Based on the comparison, a similarity index was computed for each CR user. CR users with similarity indices below a threshold that is determined by robust statistics were declared malicious and their reports were excluded from decision combination process. The reports of the remaining CR users were combined using the modified rules of combination to find the status of the PU.

Chapter 3

Optimal multi-threshold quantization scheme for bioinformatics inspired cooperative spectrum sensing in cognitive radio networks

3.1 Introduction

In cooperative spectrum sensing, a CR user sends its local information to the FC where it is combined with information from other CR users for decision-making. There are two ways to combine the local sensing information at the FC. The first one is soft decision combination in which the CR users send the actual value of received energy to the FC and the FC combines the information from all CR users to take a global decision. The second way is hard decision combination in which the CR users take local decisions based on the received energy and send one-bit local decisions to the FC. The FC combines the one-bit local decisions of all CR users to take a global decision. In a practical scenario, a large number of bits is required when a CR user transmits the real value of observed energy and this results in wasted communication bandwidth. Although a hard combination efficiently utilizes bandwidth, it produces inferior results compared to a soft combination due to the information loss. A hard combination may be practically inferior because control channels between CR users and FC are often considered to be perfect (i.e., error-free), while this may not be the case in reality. Therefore, it is easy to change or reverse the result of a hard combination through error or noise in the reporting channel.

To combine the performance gain and bandwidth efficiency of both soft and hard combinations, a quantized combination is used in [3] and [11]. In [3], the authors used an approach called softened hard combination scheme, where the observed energy is quantized into four different regions, and two bits, which represent an energy zone, are sent instead of one bit. This accomplishes an acceptable trade-off between the improved performance that is the result of soft reporting and the information loss during the

process.

The authors in [3] have studied a polynomial complexity algorithm to optimize the duration of the sensing slot as the duration of the sensing slot affects the performance of CSS employing slotted-frame structure.

The sensing time and scheduling of sensors are also considered by [28]. The authors in [23] have studied quantization schemes for multiple primary bands, while those in [29] proposed a scheme that involved an idle state where the CR users do not report any decision when they are unsure about the activity of the PU. Closed form expressions of cooperative false alarm probability and detection probability over fading channels when quantization is used have been derived in [30].

The authors in [3] studied a softened hard combination scheme in which each CR user uses two bits to report its sensing information. These bits represent different regions of sensed energy. The presence or absence of the PU signal is determined based on whether or not one of the three specified thresholds is met. The authors in [28] have considered a uniform quantization scheme for cooperative sensing, which uses a global weight vector as a global decision function. Analytical expressions for one-bit hard combination and two-bit hard combinations have been derived in [11].

In [28], the relationship between bit error probability and signal to noise ratio is established, and a new concept of BER wall is introduced. The weighted sequential probability ratio test (WSPRT) is used in [22] to assign weights to each CR user. The weights are calculated by comparing each CR user report with the FC decision. If these two are the same, the reputation metric is increased by one; otherwise, it is decreased by one.

For improving sensing performance in low signal-to-noise ratio (SNR) regimes, authors in [31] proposed a Markov model based adaptive double threshold energy detection method for spectrum sensing. The Markov model accounts for the time-varying characteristic of channel occupancy while the adaptive threshold overcomes the effect of noise uncertainty. Authors in [31] also used adaptive thresholds in low SNR regimes while [32] carried performance analysis of double thresholds in under different sensing channels. Energy efficiency is crucial in ad-hoc networks. Authors in [33] have solved the energy efficiency maximization problem in double-threshold based soft decision fusion cooperative spectrum sensing. The energy efficiency maximization is solved under multiple constraints by using an iterative algorithm. In [34] a double threshold was employed to reduce system overhead and to overcome noise uncertainty in cognitive vehicular networks. A user correlation and double threshold based cooperative spectrum sensing algorithm was used to achieve a trade-off between sensing performance and system overhead in cognitive radio based vehicular networks.

Authors in [35] have proposed an adaptive double-threshold scheme for fending off the sensing failure problem which results from the confused region phenomenon. If the received energy value falls in the confused region then instead of a binary decision, decimal values are generated and the decimal values are used for taking a binary decision in a second phase. In scheme presented in [36] the double thresholds were adapted to the fluctuations in the received energy based on fixed probability of false alarm and decimal values were generated for the confused region based on the double thresholds. Multiple antennas were used in [37] to improve the reliability of spectrum sensing and thus to reduce the interference to the PU and also the optimal number of CR users required for cooperation was found out based on total error rate. Authors in [38] found optimal local and global decision thresholds for soft combination by minimizing the total probability of error. The reporting channels may not be perfect in a given scenario. To overcome this problem, authors in [39] considered imperfect reporting channels while finding the optimal number of CR users required for cooperation and the optimal values of normalized thresholds.

In quantization based CSS, the CR users quantize the received energy into quantization zones based on quantization thresholds and send multiple bits instead of one bit to the FC. The performance of quantization based CSS is dependent upon the selection of quantization thresholds. If the quantization thresholds are not selected properly, energy zones will not reflect the actual status of the PU. This may either result in representing low received energies with higher quantization zones or representing high received energies with lower quantization zones. The first case results in higher probability of false alarm and the second case results in higher probability of misdetection. The quantization thresholds should thus be selected in a way that satisfies the criteria for probability of detection while restraining the probability of false alarm to the minimum.

Local decisions of CR users are combined at the fusion center (FC) to take a global decision. Local decisions of some CR users may be affected by fading and reports of such CR users are different from the rest of the CR users. Including the local decisions of such CR users in global decision combination may affect the performance of the overall cognitive radio network. Methods inspired from bioinformatics can be applied to scenarios where CR users with unreliable reports are identified to exclude their local decisions from global decision combination. In bioinformatics, string matching is a basic operation for biological sequence alignment. The techniques developed in biological sequence alignment (like protein sequences, DNA, and RNA sequences) can be applied in a CRN to identify such poor performing CR users because both processes are concerned with identifying anomalies among patterns of information.

Because of using non-optimal quantization thresholds the performance of quantized-hard combination

schemes is non-optimal. The CR users send quantized spectrum sensing information to the FC. Because of non-optimal thresholds, there is performance loss. In this paper, we propose an optimal quantization scheme which select optimal quantization thresholds. Due to consideration of the optimal algorithm, the total number of mini-slots of each CR user is fixed. To make possible the optimization of the whole CR system, the SNR of all CR users is also the same as it makes possible the computation of same quantization parameters for the whole system.

Our proposed quantization scheme selects optimal parameters for uniform quantization such that the criteria for probability of detection given a false alarm probability are satisfied. Our local quantization algorithm not only focuses on local quantization parameters, but also maximizes the global detection performance. The global detection performance is improved by excluding poor performing CR users from the final global decision combination. The Smith-Waterman algorithm is used for computing similarity indexes of CR users, and robust mean and robust standard deviation of the similarity indexes are calculated. CR users who have similarity indexes below a threshold determined by robust mean and robust standard deviation are excluded from the final decision combination. For the sake of optimizing the quantization thresholds, the received SNR is considered to be the same for all CR users but some CR users may have bad sensing performance because of hardware malfunctioning or sensing capabilities. Due to the use of quantized hard reporting, the conventional rules of combination, such as OR, AND, and Majority, cannot be applied directly. Therefore, the conventional Majority rule is modified to a multi-level Majority rule that can perform a multi-level decision. Similarly, the maximum ratio combination (MRC) rule is modified to support multi-level inputs. The performance of the proposed scheme has been shown through the Majority rule and MRC.

Our proposed scheme contributes to the optimization of energy detection thresholds by taking into consideration the probability of detection and probability of false alarm. The former is the basic requirement for cognitive radio operation while on the later the performance of the CR users is dependent upon. The resultant thresholds produce higher detection probability while keeping the false alarm under a strict constraint. Multi-slot sensing at each CR user level and then cooperative spectrum sensing adds spatial and temporal diversity to our optimized scheme which is not used before. Because of optimized thresholds, the sensing reports that are formed at each CR user are reliable depiction of activity of PU. But as some CR users may have bad sensing results because of reasons explained, the sensing decisions of those CR users has to be removed from final decision combination at the FC. SWA works as second part of the whole optimal spectrum sensing algorithm where bad sensing CR users are identified and their local

decisions excluded from final decision combination. SWA works on the assumption that the number of bad performing CR users is less than the number of good performing CR users.

The rest of the chapter is organized as; section 2 explains the system model in detail, section 3 expands on section 2 and presents the cooperative spectrum sensing, section 4 analyzes the results, and section 5 concludes the chapter.

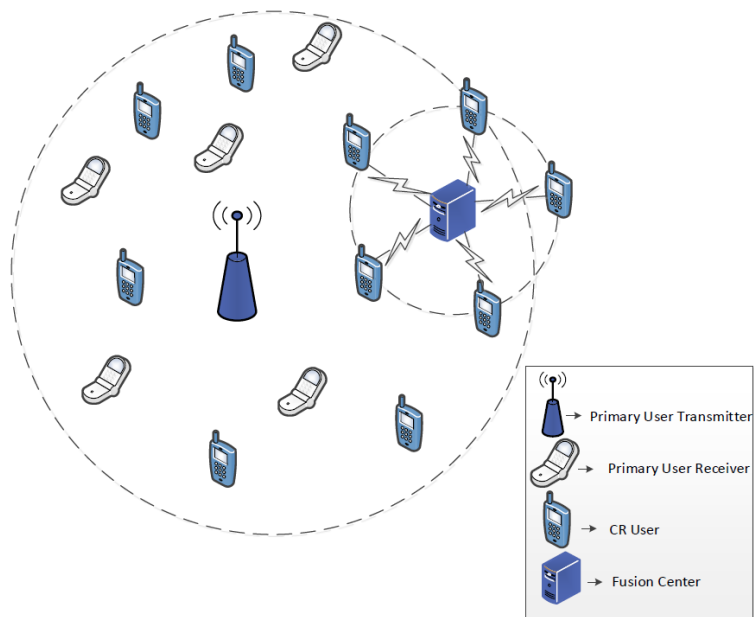


Figure 3.1 Basic system model

3.2 System Model

We consider a single PU and a CRN that consists of N_{CR} CR users, as shown in Fig. 3.1. The CR users perform spectrum sensing and report their results to the FC. The larger outer circle represents the range of PU, while the smaller circle represents the CRN. We assume a slotted time frame structure where each slot is divided into two slots: a sensing slot, which is used for spectrum sensing, and a transmission slot, which is used for actual data transmission. The sensing slot is further divided into sub-slots named mini-slots. The spectrum sensing results can change from one mini-slot to the other given a change in environment. In this case, the change is not significant as it is from a lower energy zone to the adjacent lower energy zone. In each mini-slot, spectrum sensing is performed independently, which adds temporal diversity to the process of spectrum sensing.

For spectrum sensing, each CR user employs an energy detection scheme. The energy received by the i -th CR user at the k -th mini-sensing slot, where $K \in \{1, 2, \dots, n\}$ and n is the total number of mini-slots, is $X_{k,i}$ and is given as

$$X_{K,i} = \sum_{j=1}^N x_j \quad (3.1)$$

where x_j is the j -th received energy sample, and N is the total number of samples and is given by $N=2TN$, and T and W are detection time and signal bandwidth in hertz, respectively. The received signal x_j is given under both hypothesis of absence and presence of PU signal, i.e. H_0 and H_1 , respectively by (3.2) where a represents the sample of the received signal, $w(a)$ is zero-mean additive white Gaussian noise, and $s(a)$ is the received signal from the PU with mean μ and variance σ^2

$$x_j = \begin{cases} w(a); & \text{hypothesis } H_0 \\ s(a) + w(a); & \text{hypothesis } H_1 \end{cases} \quad (3.2)$$

If the primary signal is absent, $X_{K,i}$ follows a central chi-square distribution with N degrees of freedom; otherwise $X_{K,i}$ follows a non-central Chi-square distribution with N degrees of freedom and a non-centrality parameter $\theta_i = N\gamma$ and is given by

$$X_{K,i} \sim \begin{cases} x_N^2 & H_0 \\ x_N^2(\theta_i) & H_1 \end{cases} \quad (3.3)$$

When N is large, the received energy signal, under both hypotheses of absence or presence of PU can be well approximated by a Gaussian random variable under both hypothesis. Under Rayleigh fading the probability distribution function of SNR under both hypothesis is given by

$$f(x_{K,i} / \gamma) \sim \begin{cases} \eta(N, 2N) & H_0 \\ \eta(N(1+\gamma), 2N(1+2\gamma)) & H_1 \end{cases} \quad (3.4)$$

where γ is the received SNR and $\eta(\cdot)$ represents a normal distribution. The received SNR under AWGN channel conditions is same for all CR users.

The energy received at each min-slot is quantized into predefined energy zones. The M-level quantizer of input variable x is represented by a set of quantization levels and a set of quantization thresholds. The

quantization thresholds determine the accuracy to which the quantization levels can represent the actual signal. Equation 3.5 gives the M-level quantization and also the set of quantization thresholds as,

$$q(x) = Z_m \text{ if } x_m \in (\lambda_{m-1}, \lambda_m) \quad (3.5)$$

whereas $-\infty = \lambda_0 \leq \lambda_1 \leq \dots \leq \lambda_{M-1} \leq \lambda_M = \infty$.

Each quantization zone B_m can be defined in terms of likelihood ratio (LR). The LR presents the ratio of distribution of the presence of PU signal to that of absence of PU signal. The LR of the m -th quantization zone can be determined using (3.6), where Q_0 and Q_1 are distribution of input signal x under H_0 and H_1 , respectively, and their distribution is F_{H_0} and F_{H_1} , respectively as,

$$L_{Q(x)} = \frac{dQ_1}{dQ_0} = \frac{\int_{\lambda_{m-1}}^{\lambda_m} dF_{H_1}}{\int_{\lambda_{m-1}}^{\lambda_m} dF_{H_0}}. \quad (3.6)$$

The number of quantization thresholds in this work is three, i.e., $M=3$. Thus the number of quantization levels is four. These levels or quantization zones are represented by A,C,T and G, the same letters as used for denoting bases of a DNA sequence. Zones ‘A’ and ‘C’ represent low energy or when PU is absent, while ‘T’ and ‘G’ represent high energy or when PU is present. The quantized energy zones are represented as,

$$q_{K,i} = \left\{ \begin{array}{l} H_0 \left\{ \begin{array}{l} A \quad X_{K,i} \leq \lambda_A \\ C \quad X_{K,i} \leq \lambda_C \end{array} \right\} \\ H_1 \left\{ \begin{array}{l} T \quad X_{K,i} \leq \lambda_T \\ G \quad X_{K,i} > \lambda_T \end{array} \right\} \end{array} \right\} \quad (3.7)$$

where λ_A , λ_C and λ_T are the thresholds that differentiate different quantization zones, and $q_{K,i}$ represents quantized energy for the K -th mini-slot of the i -th CR user. Thus, the set of quantization zones is $q \in \{A, C, T, G\}$, and the set of thresholds is $\lambda \in \{\lambda_A, \lambda_C, \lambda_T\}$. The optimal values of these thresholds are presented in section IV-A. Each CR user takes a local decision by averaging the energy values obtained in the mini-slots given as

$$X_i = \frac{\sum_{K=1}^n X_{K,i}}{n}. \quad (3.8)$$

The local decision of i -th CR user is represented by D_i and is given by

$$D_i = \left\{ \begin{array}{l} A; \quad X_i \leq \lambda_A \\ C; \quad X_i \leq \lambda_C \\ T; \quad X_i \leq \lambda_T \\ G; \quad X_i > \lambda_T \end{array} \right\}. \quad (3.9)$$

In Fig. 3.2, the first six mini-slots represent results of each mini-slot spectrum sensing, while the last mini-slot represents the local decision of the CR user. The detection probability and false alarm probability of the i -th CR user are given by (10) and (11) as

$$P_{d,i} = Pr(D_i = U | H_1) = Pr(X_i > \lambda_C | H_1), \quad (3.10)$$

and

$$P_{f,i} = Pr(D_i = U | H_0) = Pr(X_i > \lambda_C | H_0) \quad (3.11)$$

where $U = \{T, G\}$ corresponds to H_1 . The probability of detection and probability of false alarm are dependent upon the value of λ_C ; therefore the optimal value of λ_C is important for optimal performance in terms of probability of detection and probability of false alarm.

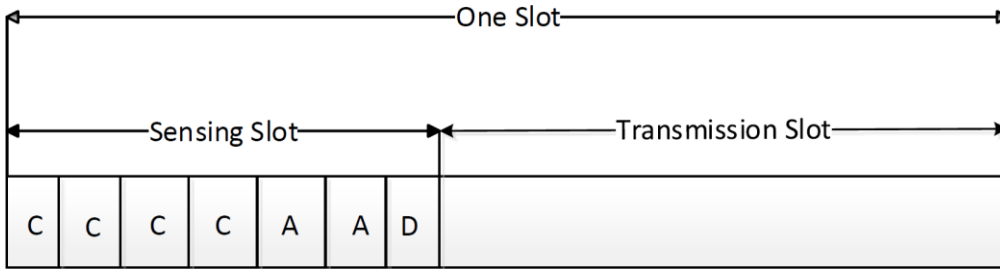


Figure 3.2 Slotted frame structure where the sensing slot is divided into mini-slots

The procedure for determining the optimal value of λ_C is given in section 3.1. First the optimal quantization parameters are selected. The proposed scheme is a uniform quantization scheme in which one threshold and the quantization distance are optimized. As long as the SNR remain the same, the system parameters remain unchanged. After this, each CR user sends the quantized sensing reports of its mini-slots and local decision to the FC. The number of mini-slots is the same for all CR users. The operations and procedure used for deciding the presence or absence of the PU are presented in section 3.2 and section 3.3, respectively.

3.3 Spectrum Sensing

To sense the spectrum, the optimal parameters for quantization are first selected. CR users quantize the energy received based on those parameters and report their information to the FC. The FC calculates the similarity index for each CR user using the SWA and determines the activity of the PU. Each step is explained in the following sub-sections.

3.3.1 Optimal Quantization Parameters Selection

The optimization problem at hand relates to finding a quantization threshold and quantization distance. The quantization distance is then used to find other quantization thresholds by combining it with the optimal threshold. A basic operational structure is given in Fig. 3.3.

The set of quantization thresholds and quantization zones was given in section 2. From (3.7), it

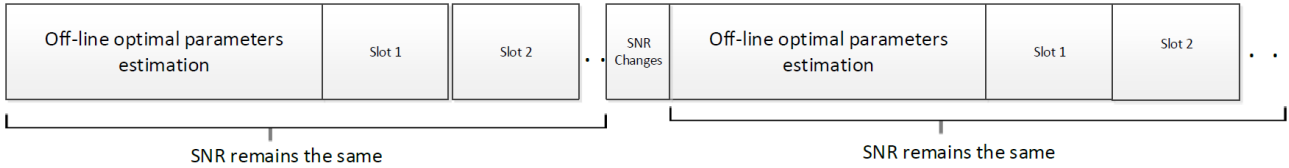


Figure 3.3 Basic operation sequence

can be seen that λ_c is the most important of the quantization thresholds; Δ is added to or subtracted from λ_c to find other quantization thresholds. Thus, these two parameters are to be optimized to find such distribution, as shown below

$$(\lambda_c, \Delta) = \arg \max_{\lambda_c, \Delta} \sum_{l=1}^M \frac{[F_{H_1}(a_{l+1}) - F_{H_1}(a_l)]^2}{F_{H_0}(a_{l+1}) - F_{H_0}(a_l)}. \quad (3.12)$$

These optimal parameters can be found by maximizing the probability of detection. The parameters that produce the maximum probability of detection are chosen to be the optimal parameters and are used to calculate the other thresholds. Based on these thresholds, the input energy distribution is quantized into the quantization zones. The optimization problem is formulated as,

$$Q_d^* - Q_d \leq \beta$$

$$\text{s.t. } Q_f = \prod_{m=1}^M \binom{N_{CR} - \sum_{j=1}^l N_{Bj}}{N_{Bm}} (P_f(B_m))^{N_{Bm}} < \alpha \quad (3.13)$$

where $Q_d = \prod_{m=1}^M \binom{N_{CR} - \sum_{j=1}^l N_{Bj}}{N_{Bm}} (P_d(B_m))^{N_{Bm}}$, $P_d(B_m)$ is the local probability of detection for quantization

zone B_m , N_{Bm} is the number of users who have local decision in zone m and l is the largest integer less than m . $P_f(B_m)$ is the local probability of false alarm for quantization zone B_m , Q_d and Q_f are probabilities of detection and false alarm of the overall system respectively, Q_d^* is the target detection probability, while α is the constraint on maximum probability of false alarm and β determines the degree of tolerance between the system detection probability and target detection probability. The equation determines that a target probability of detection should be achieved i.e the difference between the achieved probability of detection and a pre-set target probability should be below a predefined constraint given the probability of false alarm also is below a constraint.

Changing λ_c and Δ changes the number of users in each quantization bin. This change in quantization parameters thus affects the overall system detection probability. If Δ is fixed at a certain value, then increasing λ_c results in higher values of Q_m , which is the overall system probability of misdetection. Fixing λ_c and increasing Δ result in the same behavior. Similarly, keeping λ_c and Δ at low values will result in higher values of Q_f . Δ is important as it determines values of other quantization thresholds. Based on these thresholds the symbol for each mini-slot is determined. If the quantization zone is misrepresented, it will lead to higher degree of dissimilarity in the next phase i.e. when SWA is applied to find bad performing CR users. So the other quantization thresholds should be optimized so that the sensing report accurately reflects the PU activity. Thus, to improve the overall system performance the quantization parameters should be selected optimally. The thresholds are given as

$$\lambda_A^* = \lambda_C^* - \Delta^*$$

$$\lambda_T^* = \lambda_C^* + \Delta^* \quad (3.14)$$

where λ_A^* , λ_C^* and λ_T^* are the optimal quantization thresholds and Δ^* is the optimal quantization distance. The local probability of detection for each zone is given as

$$P_d(B_m) = \begin{cases} \mathbf{1} - Q_{TW}(\gamma, \lambda_m) & \mathbf{If } m = \mathbf{1} \\ Q_{TW}(\gamma, \lambda_{m-1}) & \mathbf{If } m = M \\ Q_{TW}(\gamma, \lambda_{m-1}) - Q_{TW}(\gamma, \lambda_m) & \mathbf{otherwise} \end{cases} \quad (3.15)$$

where $Q_{TW}(\gamma, \lambda_m) = Q_{TW}(\sqrt{2\gamma}, \sqrt{\lambda_m}) = P(X_i > \lambda_m | H_1)$, $Q_u(a, b)$ is the generalized Marcum Q-function

given by $Q_u(a, b) = \frac{a}{a^{u-1}} \int_{-\infty}^{\infty} t^u e^{-\frac{t^2+u^2}{2}} I_{u-1}(at) dt$ and $I_{u-1}(\cdot)$ is the modified Bessel function of the first kind and order $u-1$. The local probability of false alarm is given as

$$Pf(B_m) = \begin{cases} \mathbf{1} - G_{TW}(\lambda_m) & \mathbf{If } m = \mathbf{1} \\ G_{TW}(\lambda_{m-1}) & \mathbf{If } m = M \\ G_{TW}(\lambda_{m-1}) - G_{TW}(\lambda_m) & \mathbf{otherwise} \end{cases} \quad (3.16)$$

where $G_{TW} = \frac{\Gamma(TW, \lambda_m / 2)}{\Gamma(TW)} = P(X_i > \lambda_m / H_0)$ and M is the total number of quantization zones, $\Gamma(a, x)$

is the incomplete gamma function and is given by $\Gamma(a, x) = \int_{-\infty}^{\infty} t^{a-1} e^{-t} dt$, while $\Gamma(a)$ is the gamma function.

In this chapter, we propose an iterative algorithm that determines the optimal quantization parameters by iteratively checking the optimization criteria given in (3.14) for different values of λ_c and Δ . Different values of λ_c and result in different values for N_{B_m} , and this affects the overall system detection performance. So, the optimal values λ_c and can be found through an iterative algorithm. Our proposed iterative algorithm is given in Algorithm 1. The values of λ_c and Δ with which the criteria in the problem formulation given in (3.13) can be satisfied are the optimal quantization parameters. Based on these optimal quantization parameters, the CR users quantize their received energies according to (3.7) into quantization zones and report to the FC. The received energy distributions under both hypothesis are given in step 1, while in step 2, the initial values of λ_c and Δ are given. If the optimal values of λ_c and Δ are not found yet, will be increased and Q_d and Q_f will be calculated. If Q_d and Q_f satisfy the conditions given in step 6 then the algorithm is terminated and the optimal values λ_c and Δ are returned, otherwise Δ is checked for all possible values of F_{H_0} and F_{H_0} . If Δ is checked for all possible and still λ_c^* and Δ^* are not found then λ_c is increased and step 4 is repeated until λ_c is checked for all possible values under F_{H_0} and F_{H_0} .

Algorithm 1 Algorithm to find optimal quantization thresholds

1. Given F_{H_0} and F_{H_0}
2. Given initial values of λ_C and Δ
3. while $\lambda_C^* \neq \lambda$ and $\Delta^* \neq \Delta$
4. Increase Δ to all possible values of F_{H_0} and F_{H_0} for a fixed values of λ_C
5. Find

$$Q_d = \prod_{m=1}^M \binom{N_{CR} - \sum_{j=1}^l N_{Bj}}{N_{Bm}} (P_d(B_m))^{N_{Bm}}$$

and

$$Q_f = \prod_{m=1}^M \binom{N_{CR} - \sum_{j=1}^l N_{Bj}}{N_{Bm}} (P_f(B_m))^{N_{Bm}}$$

6. if $Q_d^* - Q_d \leq \beta$ and $Q_f < \alpha$

$$\lambda_C^* = \lambda, \Delta^* = \Delta$$

else

Increase λ_C until all possible values of F_{H_0} and F_{H_0} are checked and go to Step 4.

endif

endwhile

3.3.2 Computing Similarity Index for CR Users

An example of the reports received from CR users at FC are as shown in Fig. 3.4. Some CR users have good sensing performance compared to other CR users. The difference in the sensing reports can be used to identify good performing CR users and bad performing CR users. The bad performing CR users have low similarity with the rest of the CR users, and the Smith-Waterman algorithm is employed to identify such bad performing CR users. In Fig. 3.4, the first five mini-slots represent the spectrum sensing result of each mini-slot of each user, while the last slot represents the local decision of each CR user.

By using the SWA and the methods for finding the outliers as detailed in section 2.4.3 and 2.4.3 respectively the reliable CR users are found as

$$CR_i = \begin{cases} \mathbf{0}, & SI_i < \mu^p - 1.5\sigma^p \\ \mathbf{1}, & otherwise \end{cases} \quad (3.17)$$

and ultimately

CR1	A	A	A	A	A	D ₁
CR2	A	A	A	C	C	D ₂
CR3	C	C	C	A	A	D ₃
CR4	C	C	C	C	A	D ₄
CR5	G	G	G	G	G	D ₅

Figure 3.4. An example of sensing reports of CR users at the fusion center

$$R = N_{CR} - \sum_{i=1}^N CR_i \quad (3.18)$$

whereas SI_i is given by 2.14.

3.4 Decision Combination

After discarding reports from unreliable users, local decisions of the remaining CR users need to be combined in order to determine the presence or absence of the PU signal. The conventional rules of combination are modified to multi-level rules of combination because they are not applicable to the scenario in its original form. However, the logic of multi-level rules remains similar to the conventional rules. We used Majority rule and the maximal ratio combination (MRC) scheme at the FC to analyze performance of our proposed sensing scheme.

The multi-level Majority rule works similar to the conventional single-bit Majority rule. The quantized symbol reported by majority of the CR users is taken as the global decision and corresponds to the absence or presence of the PU signal. The global detection probability and global false alarm probability of the Majority-rule can be found in [27]. The Maximal Ratio Combination (MRC) is conventionally used in soft-decision combinations where each CR user is assigned a weight, and its report is evaluated accordingly. We propose a modified MRC rule as a decision combination of the quantized reports sent by CR users. The previously calculated similarity index as calculated in Eqn. \ref{eq18} is used as the weighting factor for the quantized local decision of a CR user. Weights of the same local decisions are accumulated as

$$P(b) = \sum_{i=1}^R \frac{SI_i}{S} I_0(D_i = b); \quad b \in \{A, C, T, G\} \quad (3.19)$$

where $S = \sum_{i=1}^R SI_i$ and $I_0(D_i = b) = \begin{cases} \mathbf{1}; & D_i = b \\ \mathbf{0}; & D_i \neq b \end{cases}$.

If the combined cumulative weight of A and C as calculated in (3.19) is greater than the combined cumulative weight of T and G , then the status of the PU signal is declared H_0 ; otherwise, H_1 . The global decision D_G using the modified MRC rule can be expressed as follows:

$$D_G = \begin{cases} H_0 & \text{Condition 0} \\ H_1 & \text{Condition 1} \end{cases} \quad (3.20)$$

where $\text{Condition 0} = P(b = A) + P(b = C) > P(b = T) + P(b = G)$ and $\text{Condition 1} = P(b = A) + P(b = C) \leq P(b = T) + P(b = G)$.

Finally, 3.5 shows the overall flow chart of the proposed scheme. The mean and variance of energies received by all CR users are used to calculate the probability distributions under both hypotheses in the first step according to (4). Initial values for λ_c and Δ are fixed. The algorithm proceeds as is explained in section 3.3.1.

In the second phase the CR users will use the optimal thresholds found in the previous stage to take a local decision according to (9). As our proposed scheme has three thresholds, there is a two-level decision making as shown in the figure. After the local decisions are taken, the local sensing decisions as well as the sensing reports are sent to the FC. The FC combines the local decision according to (3.20).

3.5 Results and Discussion

In this section, we present simulation results to show the effectiveness of our work in terms of Q_d and Q_e which respectively, are the system detection probability and the system error probability. Q_e is defined as

$$Q_e = Q_f \times P(H_0) + (1 - Q_d) \times P(H_1). \quad (3.21)$$

In simulations, we compare our results with those of the conventional cooperative spectrum sensing (Conventional Quantized Maj), employing two-bit quantization with heuristically selected thresholds, while the Majority rule is used at the FC. The majority rule uses a modified logical rule of majority combination, in which the quantization symbol with the largest count is selected as the global decision. We also compared two SWA-based cooperative spectrum sensing schemes, one scheme uses SWA with optimal quantization thresholds (Maj-SWA with Opt. threshold) as computed by our algorithm, and the other uses heuristic thresholds (Maj-SWA with heuristic threshold). Both the schemes use Majority rule for decision combination at the FC. The conventional majority rule and ‘‘Maj-SWA with heuristic thresholds’’ have the following setting for quantization thresholds. For the heuristic scheme, λ_A is the mean of probability

distributions of the received energy when PU is absent, λ_T is the mean of probability distributions of received energy when PU is present and λ_C is the average of the two means.

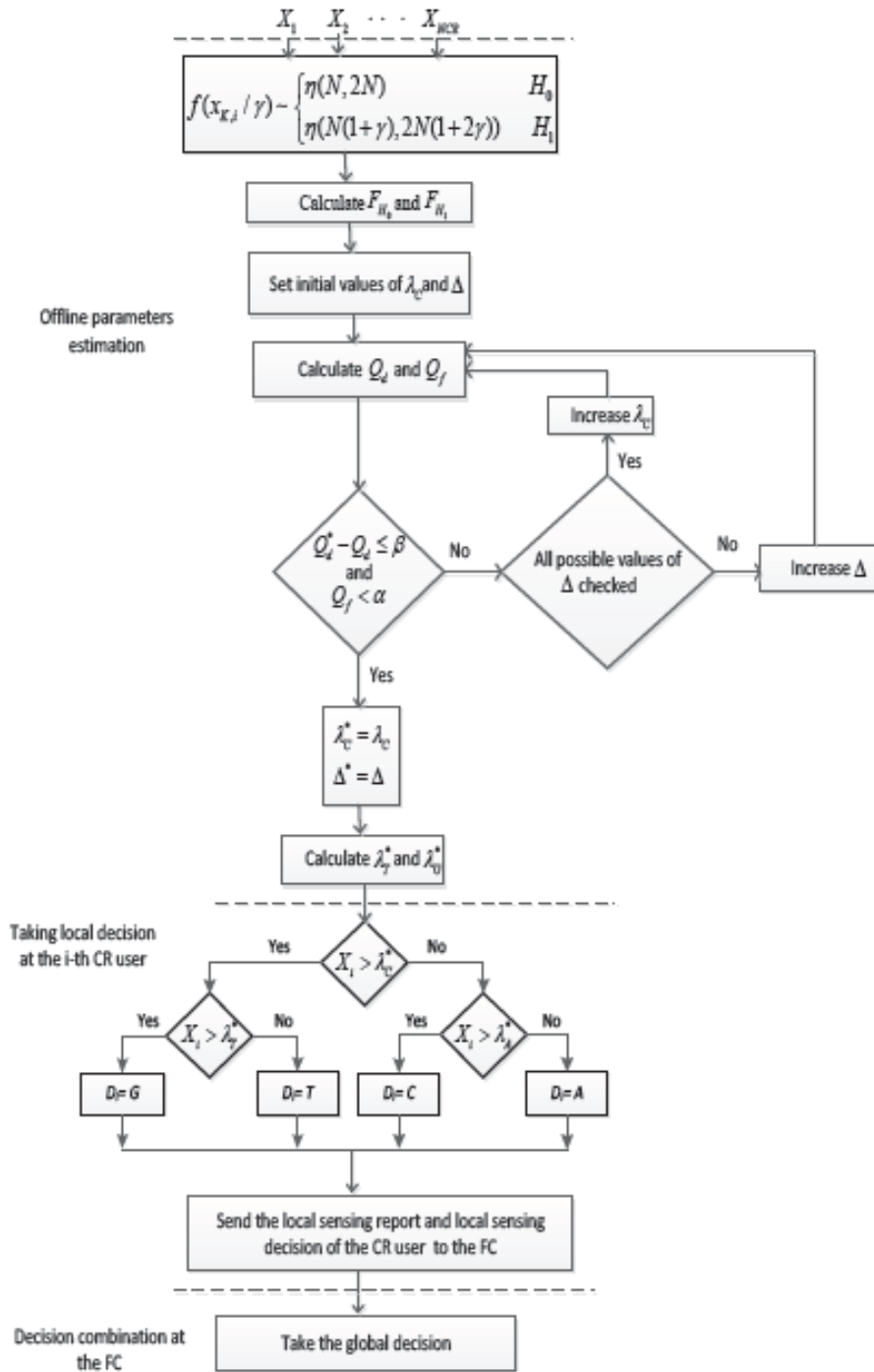


Figure 3.5 Flow chart of the proposed scheme

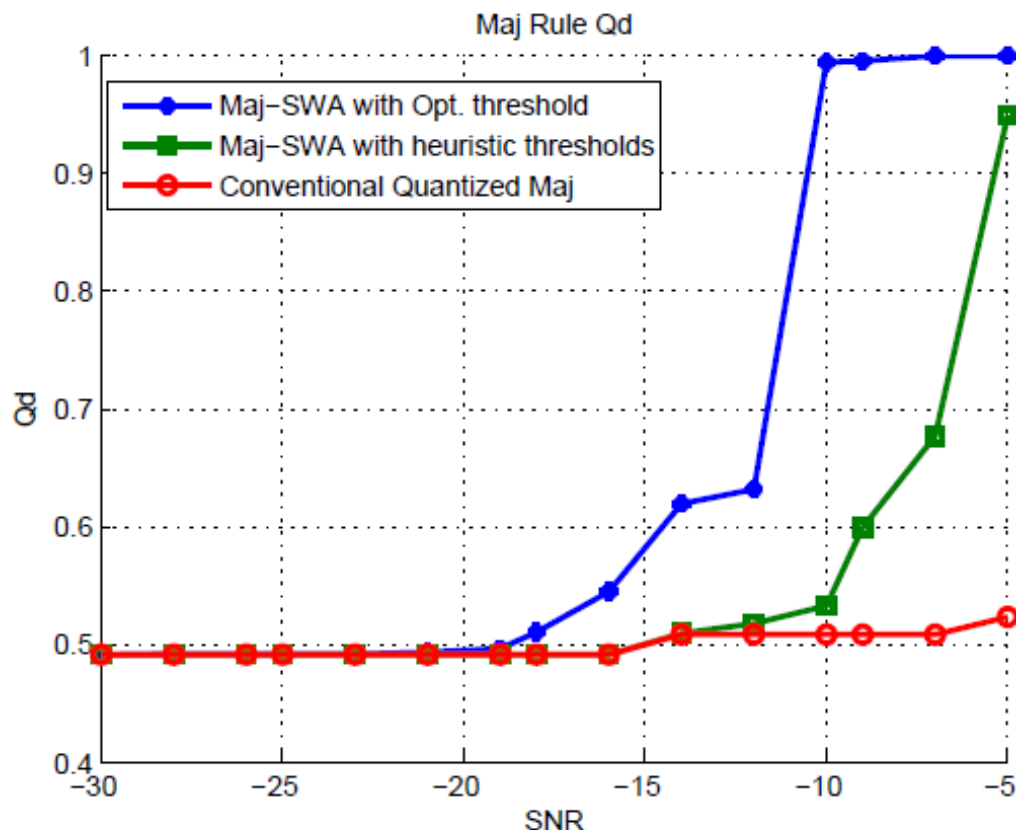


Figure 3.6. System detection performance with Majority rule for schemes having optimal and heuristic thresholds.

For simulation, we consider a CRN consisting of 10 CR users. The duration of the sensing slot is considered to be 1 ms. The number of iterations is 2000. The false alarm probability of CR users is 0.02. SNR of the CR users varies from -30 dB to -5 dB. The idle probability of PU, denoted by $P(H_0)$, is 0.5. We assume that the channel from PU to CR users suffer from log-normal shadowing. The CR users are assumed to be close enough to the source PU and far enough from other PUs; thus, the interference from other PUs is negligible.

Figure 3.6 presents the detection performance of the schemes discussed above. Conventional Quantized Maj has the worst performance of all. The SWA-based majority rule with heuristic quantization thresholds has worse performance than the SWA majority scheme based on optimal quantization thresholds. The reason is that unreliable users are unable to successfully detect PU when their faulty

decisions are included in the final decision combination, it skews the global detection performance to the lower side. This is visible in both SWA-based schemes. The reason the SWA-based majority schemes outperform the one with heuristic thresholds is because of the inaccurate quantization. PU activity may be reported to belong to the wrong quantization zone, and the accumulated effect of this lowers the overall system detection performance.

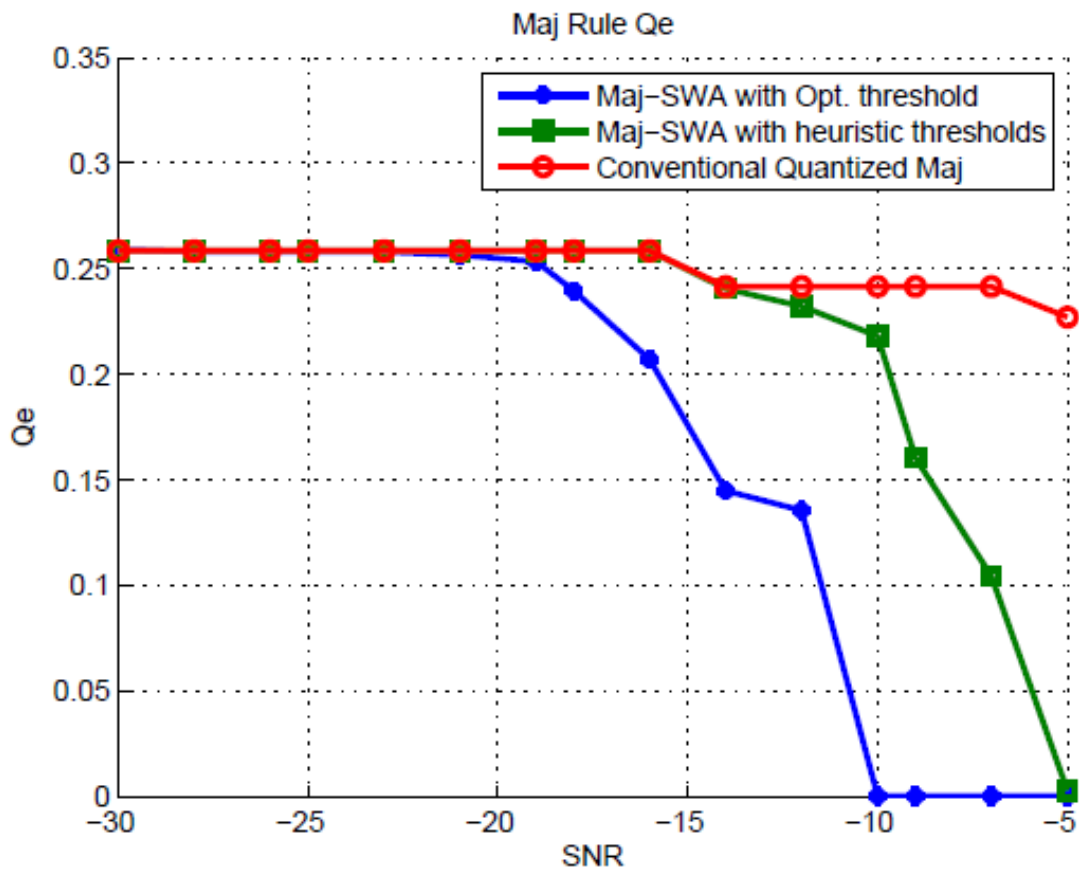


Figure 3.7. System error performance with Majority rule for schemes having optimal and heuristic thresholds

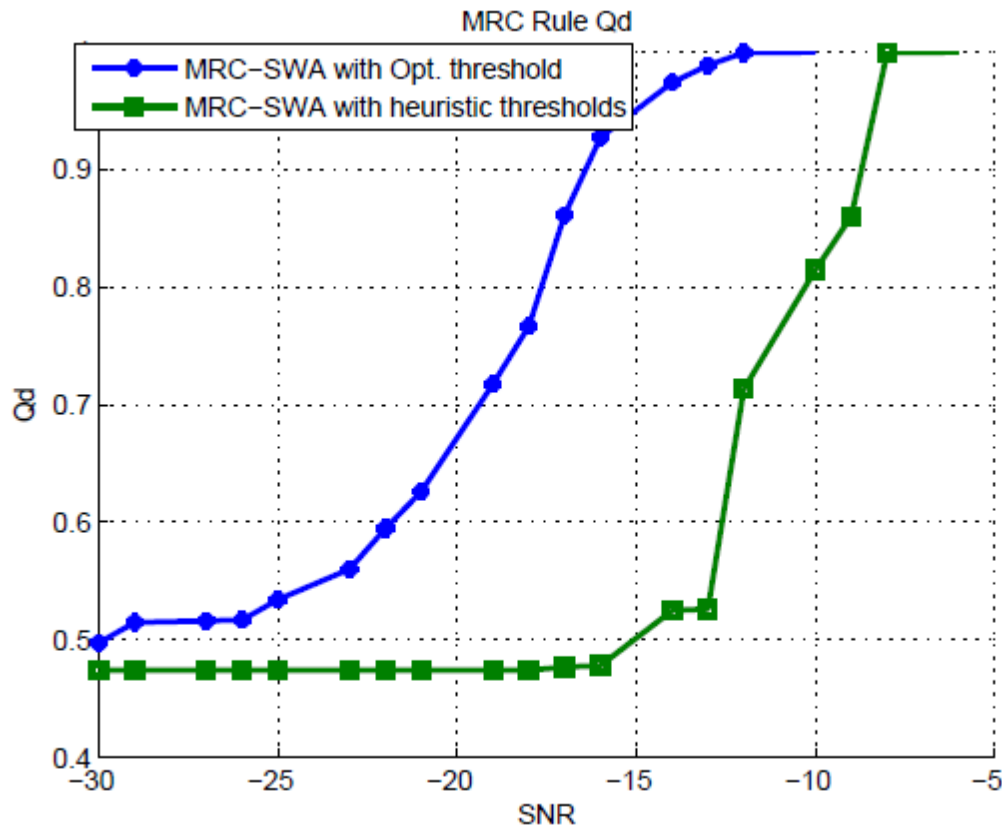


Figure 3.8. System detection performance with MRC rule for schemes having optimal and heuristic thresholds

Figure 3.7 shows the error performance of the three schemes. The same reasoning as is applied to the system detection performance can be applied here. The inaccurate quantization increases the probability of error. The error calculation takes into account both probability of false alarm and probability of misdetection. The inaccurate quantization thresholds may represent high PU signal energy with lower quantization zones and low PU signal energy with higher quantization zones. These result in higher values of misdetection and higher values of false alarm respectively. Accurate quantization combined with local reports of reliable CR users allows the optimal quantization-based SWA majority scheme to outperform the other two in terms of good error performance.

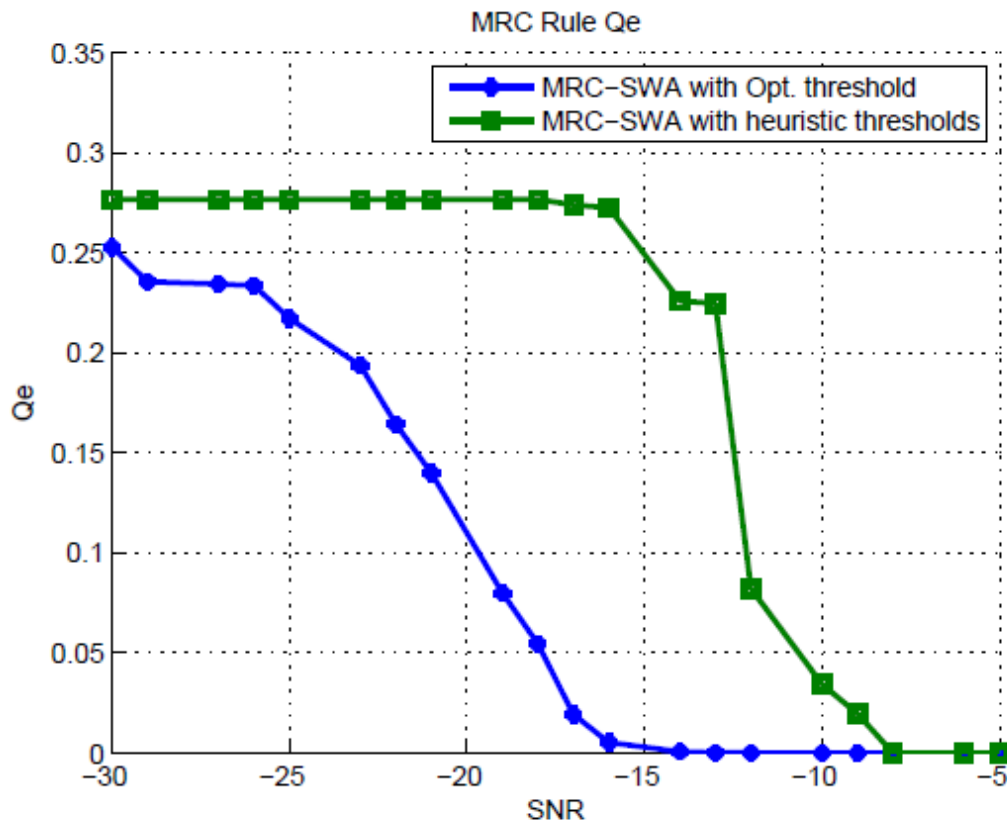


Figure 3.9. System error performance with MRC rule for schemes having optimal and heuristic thresholds

Figure 3.8 shows the detection performance of the optimal quantization threshold based MRC scheme. Here, the similarity indexes of CR users as calculated in (18) are used as weight for each CR user even after the removal of unreliable CR users. The CR users with higher similarity indexes are given more consideration in the global decision combination than the ones with lower similarity scores. Thus, in this scheme, only the most reliable CR users affect the global decision.

Figure 3.9 gives the error performance of SWA-based MRC schemes. SWA-based MRC scheme with optimal quantization thresholds outperforms the SWA-based MRC scheme with heuristic quantization thresholds. The reason is that even after discarding reports of unreliable CR users, the inaccurate quantization process may result in increase in false alarms or misdetections or both. SWA-based MRC schemes with optimal quantization thresholds ensure that the PU signal energy is accurately reported, and that the most reliable CR users are taken into account for the global decision combination.

3.6 Conclusion

The Smith-Waterman algorithm is extensively used in bioinformatics to accurately align biological sequences and identify similarities between biological sequences. The SWA can be used to find information that is dissimilar to others; thus, reliable combinations of CR user local sensing results can be ensured. In this paper, we developed a novel sensing scheme in which optimal quantization thresholds were found. The PU signal energy was quantized by each CR user, based on these optimal quantization thresholds. The local reports of each CR user which consist of multi-slot quantized values and average PU signal energy as received by each CR user are reported to the FC. The FC calculates similarity indexes for each CR user through SWA; based on these similarity indexes, only sensing reports from the most reliable CR users are combined in the final decision combination. Simulation result showed that SWA schemes with optimal quantization thresholds outperform the schemes with heuristic thresholds.

Chapter 4

Reliable machine-learning based spectrum sensing in cognitive radio networks

4.1 Introduction

Along with other factors such as the number of participating CR users, the sensing environment, and sensing capabilities of CR users, the FC's global decision combination rule determines the detection performance of the CR system. For instance, an OR rule results in good protection for the PU but has the lowest spectral hole exploration capability [23], whereas an AND rule improves spectral hole detection but lowers the PU protection capacity. Likewise, poor sensing and/or malicious CR users reduce the performance of the k-out-N decision combination rule. More sophisticated combination rules such as Bayesian analysis and the sequential probability ratio test (SPRT) have better PU protection and spectral hole exploration, but require prior information which may not always be available in a given CR environment [22].

The notion of learning from the environment is embedded in the concept of cognitive radios. CR users are meant to monitor the environment and adapt their operating characteristics (operating frequency, transmitting power, etc.) to the changing conditions. To enable CR users to learn from the environment, several authors have considered machine learning algorithms [40-45]. Machine learning in spectrum sensing becomes a task of extracting a feature vector from a pattern and classifying it into a hypothesis class corresponding either to the absence or presence of PU activity. Fading and shadowing can make estimating the channel condition difficult, and hence spectrum sensing cannot reliably determine the PU status based on the current sensing slot only [7]. However, machine-learning-based spectrum sensing is capable of implicitly learning the surrounding environment. Another advantage of machine-learning-based

spectrum sensing is that it can reliably detect PU activity without requiring any prior knowledge of the environment.

Machine learning algorithms are classified into two types: supervised and unsupervised. K-nearest neighbor (KNN) is a supervised machine learning algorithm. In KNN, training instances (spectrum sensing feature vectors) are used to form K neighborhood classes. A test instance is then classified into one of K neighbors based on majority voting. The voting is based on statistical information gained from finding the distance between the test instance and the training instances. The distance should be calculated accurately as to truly reflect the classifying class [46]. KNN is the simplest of machine learning algorithms, suitable for the low-complexity requirements of CR users. KNN is also the most stable machine learning algorithm [47].

Authors in [48-50] have considered KNN for spectrum sensing. In [48] the authors have considered a binary hypothesis testing and have proposed to optimize the distance between the two classes. The drawback of their scheme is that they have considered soft-decision combination and have used a one-time spectrum sensing which cannot be checked against ground reality. In [49], KNN is used in conventional way as a counting mechanism to fill the spaces in building a TV white space database. The use of KNN is limited to reconstruction of the missing spectrum sensing points and thus, the full capacity of KNN as a classifier is not exploited. In [50], authors have found a global energy detection threshold for different conventional rules of decision combination. These rules are used in conjunction with different classification schemes to classify a test instance which takes the signal strength as a feature vector. The authors in [50], also have used KNN as a counting mechanism and, moreover, the global decision combination rule does not take into consideration the weight of individual CR users and their performance history.

Authors in [51] used multiple antennas for centralized spectrum sensing while in [52] a scheme based on multiple energy detectors and adaptive multiple thresholds for cooperative spectrum sensing was presented. For regional area networks, some improved energy detectors were presented in [53-54]. Authors in [53] proposed a two stage energy detector where decisions of both the detectors are fused at a decision device while in [54] multiple antennas were used for spectrum sensing in regional area networks. In [55] both a fixed energy detector and adaptive double threshold were used for cooperative spectrum sensing. In [56] multiple antennas based energy detector utilizing adaptive double-threshold for spectrum sensing was proposed while in [57] a comparison between cyclostationary detection technique and adaptive double threshold based energy detection scheme was carried out.

In this paper, we propose a machine-learning-based reliable spectrum sensing algorithm in which the FC uses a weight-based decision combination rule. In the training phase, CR users perform spectrum sensing,

and based on an acknowledgment signal (ACK) and the global decision; the sensing report is assigned to a sensing class. The sensing class corresponds to the behavior of a CR user in a changing environment which is due to the changing activity of the PU. These sensing classes reliably reflect the activity of the PU and the CR user's behavior in response to it. After enough information is gathered about the surrounding environment, the classification phase begins. In the training phase the CR users form a local decision. The local decision is in quantized hard form. The local decisions of the CR users are sent to the FC and the FC takes a global decision. The CR users stay silent or transmit according to the global decision. If the CR users transmit and ACK is received in the next time slot then the transmission was successful. Based on the global decision and the status of ACK signal sensing classes are formed. The training phase is over when enough training data for the sensing classes is gathered. In the classification phase, the KNN algorithm is used, where the sensing classes obtained in the training phase are treated as neighbors for the test instance, which is the current sensing report. The Smith-Waterman algorithm (SWA) is used to accurately find the distance between the current sensing report and the neighboring classes. Based on quantitative variables like the conditional probability and posterior probability, which are calculated through KNN, the current sensing report is classified into one of the sensing classes, corresponding to either the absence or presence of the PU. The local decision is then reported to the FC, where the local decisions of all CR users are combined to make a global decision, taking into consideration the reliability of each CR user.

The proposed scheme uses the quantized information as opposed to the soft decision combination scheme that is proposed in [58]. The spectrum is sensed multiple times in a sensing slot, which makes the proposed scheme more reliable since temporal diversity to the spectrum sensing process is added as wireless channel changes rapidly. The scheme proposed in [30] was based on one-time spectrum sensing while we add a verification mechanism in case that the spectrum sensing decision is absence of PU activity. The classification problem in the proposed scheme is a multi-label one where the current spectrum sensing report is classified into eight different classes. These eight different classes belong to either hypothesis. But the division of the binary hypothesis into sub-classes makes the proposed scheme more accurately analyze the PU activity. In addition, the scheme proposed in [58] used the KNN in the traditional way as a counting mechanism. On the other hand, we in the proposed scheme use posterior probability to find the nearest neighbor, and utilize KNN to calculate the conditional and prior probabilities.

In the reference of [59], KNN was simply used for data recovery in white space database as a mechanism for majority voting. The classification problem in [59] is also a binary one and the KNN decides a label based on majority labels of the neighboring data points. The proposed spectrum sensing scheme is different from that of [59] in that quantized energy levels are used to train the classifier and then

the sensing reports are used to find the class label of the current sensing report by finding the distance between them. Instead of majority voting, we have used an efficient distance measuring algorithm, Smith-Waterman algorithm (SWA) to calculate the similarity of the current sensing report and the training reports.

Mikaeil et al. proposed different classification schemes which work on thresholds calculated through different fusion rules [60]. In the paper, we utilize a different fusion rule at the fusion center which takes into consideration the weight of different CR users before taking a global decision. The focus of [60] is to find the thresholds for different schemes and KNN is used as one of the classifications schemes. On the other hand, in the proposed scheme, the fusion rule utilizes the distance between the test report and the training reports intrinsically at the CR user level and at the FC the historical accuracy of each CR user is also taken into consideration. In this way, the global fusion rule at the FC makes use of the training reports as well as the history of performance of each CR user. Therefore, the global fusion rule is more robust as well as reliable.

The rest of the paper is organized as follows: section 2 describes the system model; section 3 describes the spectrum sensing scheme which consist of KNN algorithm, SWA, the training phase, and the classification phase in detail; section 4 describes the cooperative spectrum sensing and the global decision combination in detail; section 5 discusses the results; and section 6 concludes the paper.

4.2 System Model

In this section the energy detection method used and the quantization method which is employed are discussed. This section deals with forming of sensing report which is used both in training phase and classification phase of the spectrum sensing scheme. We consider N CR users that continuously sense the spectrum, report their local decisions to the FC through a dedicated control channel [4]. The CR user transmit information if a spectral hole exists which is determined by the FC. CR users can either transmit or receive at a given time, i.e., they operate in half-duplex mode. CR users are assumed to be close to the PU and outside the range of other PUs. The system model is presented in Fig. 4.1.

CSS introduces spatial diversity, while temporal diversity is introduced by dividing the sensing slot into mini-slots. We consider a slotted time-frame structure, where the first slot is used for spectrum sensing and the second slot is used for transmitting CR user data. The authors in [61] investigated the optimal sensing slot duration. In this work a sub-optimal sensing slot duration is considered. The sensing result may change when fading and shadowing phenomena are present. Temporal diversity counters these effects by sensing the spectrum n times in the sensing slot. In this work, the sensing-slot is further divided into mini-

slots. In each mini-slot, the spectrum is sensed independently. The sensing performance can be improved if the number of mini-slots and hence the sensing duration is increased but that results in lesser duration for the transmission slot. The authors in [61] investigated the optimal number of mini-slots for sensing-throughput trade-off in CRNs. According to [61], diversity reception is introduced in the sensing process by sensing the channel independently in mini-slots within the same sensing phase. In our proposed scheme the results of these mini-slots are combined to form a sensing report which later is used in the classification phase as given in section 3.2. The sensing reports were previously used in section 2.4 to calculate trust of each CR user in a CRN which is under-attack by malicious users. In this work the sensing reports are used to train the classifiers and then later used for classifying the current sensing report. A half-duplex CR user system is considered in which in the sensing slot the CR users remain silent. If in the sensing slot it is decided that the PU is absent then the CR users transmit in the transmission slot, otherwise the CR users remain silent. When the duration of one time frame, which consists of a sensing slot and a transmission slot, is over the CR users sense the spectrum again. Energy detection is used in each mini-slot. The energy received in the w -th sensing slot by the i -th CR user at the k -th mini-slot, $X_{k,w,i}$, can be expressed as

$$X_{k,w,i} = \sum_{j=1}^{N_0} |e_{k,w,i}(j)|^2 \quad (4.1)$$

where $k \in \{1,2,3, \dots, n\}$, n is total number of mini-slots, $e_{k,w,i}(j)$ is the j -th energy sample received at the k -th mini-slot of the w -th sensing slot by the i -th CR user, and N_0 is the total number of samples, given by $N_0 = 2TB$. T and B are the detection time and signal bandwidth in Hertz, respectively. The number of samples received in a particular mini-slot is dependent upon the bandwidth of the sensed spectrum and the sensing time. The received signal $e_{k,w,i}(j)$ in the absence of PU (H_0) and presence of PU (H_1) is given as follows

$$e_{k,w,i}(j) = \begin{cases} v_{k,w,i}(j); & H_0 \\ s_{k,w,i}(j) + v_{k,w,i}(j); & H_1 \end{cases} \quad (4.2)$$

where $v_{k,w,i}(j)$ is zero-mean additive white Gaussian noise (AWGN) and $s_{k,w,i}(j)$ is the j -th sample of the PU signal received at the k -th mini-slot of the of the w -th sensing slot by the i -th CR user.

It was shown in [62] that if the primary signal is absent the probability density function of the energy of the received signal at the i -th CR user ($X_{k,w,i}$) follows a central chi-square distribution with mean μ_0 and variance σ_0^2 ; otherwise it follows a non-central chi-square distribution with mean μ_1 and variance σ_1^2 , which can be estimated as,

$$\begin{cases} \mu_0 = N_0 & \sigma_0^2 = 2N_0 \\ \mu_1 = N_0(\gamma_i+1) & \sigma_1^2 = 2N_0(2\gamma_i+1) \end{cases} \quad (4.3)$$

where γ_i is the signal to noise ratio (SNR) of the received signal at the i -th CR user.

When the total number of samples, N_0 , is large, the energy signal received, $X_{k,w,i}$, under both hypotheses H_0 and H_1 can be approximated by a Gaussian random variable. In our scheme, the energy signal at each mini-slot is quantized into discrete zones. Multiple bits representing the corresponding zone are transmitted to the FC, rather than transmitting a continuous energy variable (a soft decision) or a single bit (a hard decision). An M -level quantizer of an input variable is represented by a set of quantization levels and a set of quantization thresholds. These quantization thresholds determine the accuracy to which the quantization levels represent the actual received signal.

In the paper, the slotted-frame structure is considered where a frame is one unit of accessing the spectrum. The first slot, called the sensing slot, in each frame is used to sense the spectrum to decide whether the PU is active or not. If it is decided in the sensing slot that the PU is absent, the CR users transmit in the transmission slot. Otherwise, they remain silent for the duration of the transmission slot. When the duration of transmission slot is over, the CR users will start sensing the spectrum again.

Because wireless channel changes rapidly, the spectrum is sensed multiple times instead of only once so as to consider the changing behavior of the channel. To do this, in the paper, the sensing slot is divided into mini-slots. In each mini-slot, the spectrum is sensed independently and based on the result, a sensing report is formed. A sensing report is formed according to the quantized decision of each mini-slot, which is expressed by eq. (4) and will be used in the classification phase later. For spectrum sensing, the energy detection is utilized where samples of received energy are summed and compared with a threshold and based on the comparison result it is decided that whether PU is present or absent.

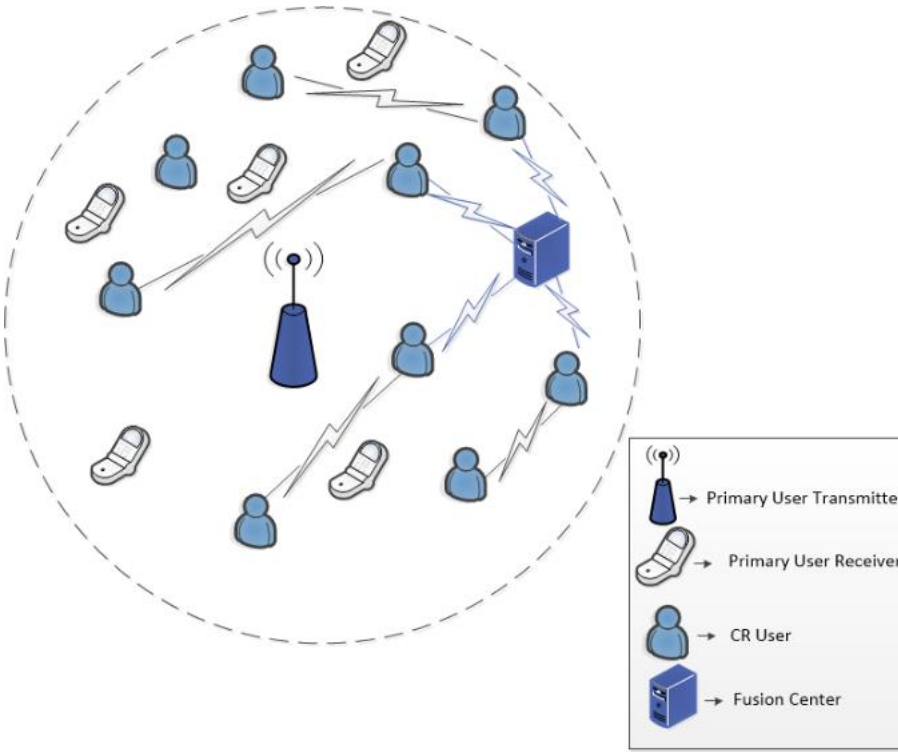


Fig. 4.1. Basic system model

In this work the number of quantization levels is four, i.e. $M = 4$. These levels or quantization zones are represented by Z_1, Z_2, Z_3 and Z_4 . Zones Z_1 and Z_2 represent low energy or the absence of the PU, while Z_3 and Z_4 represent high energy or the presence of the PU. The quantized energy zones are given as

$$u_{k,w,i} = \begin{cases} H_0 & \begin{cases} Z_1 & ; X_{k,w,i} \leq \lambda_{Z_1} \\ Z_2 & ; \lambda_{Z_1} < X_{k,w,i} \leq \lambda_{Z_2} \end{cases} \\ H_1 & \begin{cases} Z_3 & ; \lambda_{Z_2} < X_{k,w,i} \leq \lambda_{Z_3} \\ Z_4 & ; X_{k,w,i} > \lambda_{Z_3} \end{cases} \end{cases} \quad (4.4)$$

where $u_{k,w,i}$ represents the quantized energy for the k -th mini-slot of the w -th sensing slot of the i -th CR user, $\lambda_{Z_1}, \lambda_{Z_2}$, and λ_{Z_3} are the thresholds that differentiate different quantization zones. The set of quantization zones is $q \in \{Z_1, Z_2, Z_3, Z_4\}$ and the set of thresholds is $\lambda \in \{\lambda_{Z_1}, \lambda_{Z_2}, \lambda_{Z_3}\}$. Eq. (4) signifies that in case of H_0 , the average received energy at i -th CR user at the k -th sensing slot ($X_{k,w,i}$) can be quantized into either Z_1 or Z_2 and in case of H_1 , $X_{k,w,i}$ is quantized into either Z_3 or Z_4 . According to our quantization scheme Z_1 and Z_2 represent H_0 , and Z_3 and Z_4 represent H_1 .

At each sensing slot, a sensing report is formed that consists of symbols belonging to q . The report for the i -th CR user at the w -th sensing slot is called sensing report and is represented by $R_{i,w}$, which contains n elements belonging to q (the sensing report formation is further explained in section 4.3). This report is used as a feature vector for the machine learning algorithm. During the training phase, this report is assigned to a sensing class based on ACK and the global decision, which will be discussed in detail in section 4.3. The next section describes the spectrum sensing algorithm at the CR user level.

4.3. Spectrum Sensing

The proposed spectrum sensing scheme aims to improve PU detection capability under varying environments to improve spectral hole detection. The first goal protects the PU's data from harmful interference, and is the foremost constraint specified by IEEE 802.21 which is the standard for accessing TV white spaces [63]. The second goal efficiently exploits spectrum access opportunities, enabling the CR user to transmit data. For the i -th CR user at the w -th sensing slot, channel availability is decided on the basis of the energy vector ($R_{i,w}$). To correctly map $R_{i,w}$ to PU activity, the behavior of the PU has to be learned. Thus the energy vector in our case is analogous to a feature vector in the context of machine learning.

To construct a classifier, i.e., to classify the current sensing report into channel available (H_0) or channel busy (H_1) classes, a training phase is needed. Each CR user stores energy vectors of size W , where W is the length of the training or training phase. In training phase, the slotted frame structure is used as explained in section 2. As explained in section 2, a one time slot has a sensing phase and a transmission phase. There are W slots in the training phase. These vectors are input of a classifier in the classification phase, where the current sensing report is compared with previously stored sensing reports to decide between H_0 and H_1 .

In our proposed scheme, first the CR users learn the behavior of the PU by mapping the generated quantized energy vectors, which are called sensing reports, to the accurate status of the PU. The true status of the PU is found through ACK and a reliable combination of local decisions of CR users determined by the FC. The function of the CR user in the training phase is different from its function in the classification phase. In the training phase, sensing reports are assigned to sensing classes according to the actual activity of the PU and the corresponding behavior of the CR user. In the classification phase, sensing reports are sorted into one of the sensing classes using KNN. To accurately calculate the distance between the current sensing report and existing members of the sensing classes, SWA is used. Section 3.1 describes the training phase, while section 3.2 describes the classification phase.

4.3.1 Training Phase

In this phase, the operating environment is learned by gauging the behavior of the CR user to the changing activity of the PU. The i -th CR user generates a sensing report $R_{i,w}$, makes a local decision on the basis of the average received energy in the current sensing slot, sends the local decision to the FC, and based on the result of FC and the status of ACK assigns the sensing report to a sensing class. This section will explain these steps in detail.

Let the energy received in the w -th sensing slot at the i -th CR user be represented by $Y_{i,w}$ which is given as

$$Y_{i,w} = \frac{\sum_{k=1}^n X_{k,w,i}}{n} \quad (4.5)$$

where $X_{k,w,i}$ is given by (4.1).

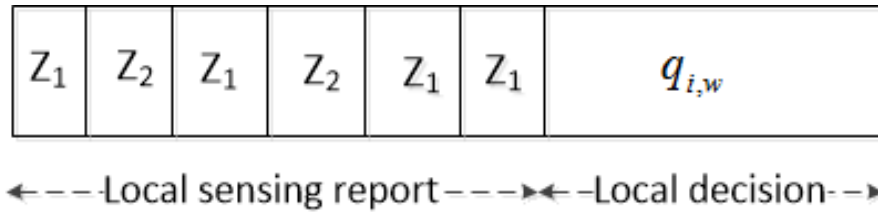


Fig.4. 2. Local sensing report and local decision during training phase.

The local decision for the i -th CR user at the w -th sensing slot in the training phase is represented by $q_{i,w}$ and is given by

$$q_{i,w} = \begin{cases} H_0 \begin{cases} Z_1 & ; Y_{i,w} \leq \lambda_{Z_1} \\ Z_2 & ; \lambda_{Z_1} < Y_{i,w} \leq \lambda_{Z_2} \end{cases} \\ H_1 \begin{cases} Z_3 & ; \lambda_{Z_2} < Y_{i,w} \leq \lambda_{Z_3} \\ Z_4 & ; Y_{i,w} > \lambda_{Z_3} \end{cases} \end{cases} \quad (4.6)$$

The local decision is sent to the FC, which combines local decisions from all CR users and renders a global decision. In the training phase, the simple majority rule is used as the rule of decision combination. The symbol (quantization zone) reported by the majority of CR users determines the global decision at the FC. As can be seen from (4.6), the local decision during the training phase is in the quantized-hard form, so the global decision at the FC is also in the quantized-hard form. The sensing report of a CR user is as shown in figure 2. The local sensing report was explained above in the previous section. In figure 2, the

first six mini-slots constitute a local sensing report. As can be seen every element of the report belongs to q . For every CR user, at every sensing slot a sensing report (the current sensing report is represented by $R_{i,w}$) is formed, and the local decision is taken according to (4.6).

Next, the global decision is returned to the CR users. The CR users either transmit or remain silent based on the global decision. If the CR global decision is H_0 then this can be verified by the ACK signal which is sent by the CR receiver to the CR sender after the CR receiver receives the transmission. As overlay cognitive radio network is considered, so, there is no interference to the PU communications. The ACK signal is affected by the PU communication only when the spectrum sensing result is wrong and in fact the ground reality is H_1 . Based on the local decision and the global decision, there are eight possible cases for the CR user and the sensing classes according to our system model. These possible cases called observations are given below.

Observation 1: The local decision ($q_{i,w}$) is Z_1 and the global decision is also Z_1 . The CR user transmits its data. If ACK is received, it means the sensing result was correct and the actual status of the PU was H_0 . Through the ACK signal, the true status of the PU is known. The sensing report corresponding to this decision ($R_{i,w}$) is stored in a class labelled as R_1 while in case of absence of ACK signal it is stored in R_2 .

Observation 2: Both the local decision ($q_{i,w}$) and the global decision are Z_1 , or the global decision is Z_2 and the local decision is Z_1 . The CR user will transmit, but ACK is not received, meaning that the sensing decision was wrong and the PU was available. The CR user will store $R_{i,w}$ in a class labelled R_2 . If ACK signal is received it will be stored in R_1 . If the local decision is Z_1 and the global decision is Z_3 or Z_4 , then $R_{i,w}$ will also be stored in this class.

Observation 3: The local decision ($q_{i,w}$) is Z_2 and the global decision is also Z_2 . The CR users follow the procedure as explained in observation 1. If ACK is received, the sensing decision is correct and the PU is not present. $R_{i,w}$ is stored in a class labelled R_3 , otherwise it is stored in R_4 .

Observation 4: The local decision is Z_2 and the global decision is Z_1 or Z_2 . The CR user transmits, and if ACK is not received, $R_{i,w}$ is assigned to the class with label R_4 , otherwise in R_3 . If the local decision is Z_2 and the global decision is either Z_3 or Z_4 , then again $R_{i,w}$ will be stored in the class labelled as R_4 .

Observation 5: The local decision is Z_3 and the global decision is also Z_3 . There will be no transmission in this case. The true status of the PU thus cannot be known. $R_{i,w}$ will be assigned to a class

which is labelled as R_5 . The sensing report will also be stored in class R_5 if the global decision is Z_4 and the local decision is Z_3 .

Observation 6: The local decision is Z_3 but the global decision is either Z_1 or Z_2 . The CR user will transmit. If ACK is received, $R_{i,w}$ will be stored in a class labelled R_6 , otherwise it will be stored in R_5 .

Observation 7: Both the local and global decisions are Z_4 . There will be no transmission and $R_{i,w}$ will be stored in the class labelled as R_7 . $R_{i,w}$ will also be stored in R_7 if the local decision is Z_4 and global decision is Z_3 .

Observation 8: The local decision is Z_4 , but the global decision is either Z_1 or Z_2 . The CR user will transmit. If ACK is received, $R_{i,w}$ will be stored in class R_8 . If no ACK is received, $R_{i,w}$ will be stored in R_7 .

In the observations above it can be seen that ACK signal is used when the global decision is H_0 . When the global decision is H_1 the CR users do not transmit and thus ACK signal cannot be used to ascertain ground reality. So, in the case when H_1 is the global decision at the FC the CR users store the current sensing report in the classes R_5 and R_7 as the current sensing decision cannot be verified in any other way than at the risk of causing interference to the PU transmission.

The observations are given in decision tree form in figure 3. As the observations do not stem from one set of decisions, there is no unified root of the decision tree. The decision trees are given in four partitions depending on the local decision. The local decision is abbreviated as LD and the global decision as GD in figure 3. Figure 4.3(a) corresponds to the case that the local decision is Z_1 and observation 1 and observation 2 are obtained. Figure 4.3(b) corresponds to the case that the local decision is Z_2 and the observation 3 and observation 4 are obtained. Figure 4.3(c) and figure 4.3(d) respectively corresponds to the cases that the local decisions are Z_3 and Z_4 and the observation 5 and observation 6 and observation 7 and observation 8 are obtained.

These observations help learn the CR user about the surrounding environment and its behavior in response to the environment, and also give CR users historical data that can be used in conjunction with the current sensing behavior to more reliably predict the PU status. This process can be seen as cooperative learning where not only the individual CR user is taken into account, but also the impact of other CR users is incorporated through the global decision. This adds spatial diversity to the learning process, where a receiver with better signal to noise ratio (SNR) conditions can drive the behavior of CR users with poorer SNR conditions.

The training phase is run until the CR user is sufficiently trained in the behavior of the surrounding environment, including changing the SNR conditions and changing the behavior of the PU. Fading can also temporarily affect the signal and thus the energy received due to the continuously changing sensing environment. The training scheme developed takes into consideration the presence of fading and thus store sensing reports that may have been the results of either fading or bad sensing in their corresponding categories. As the learning is based on the ACK and reliable decision combination at the FC, classes based on training more reliably reflect the sensing environment and PU activity. The results of either fading or bad sensing at the CR user level are found in the above observations, where the local decision is different from the global decision or when ACK is not received.

The training data is collected locally at each CR user in the training phase. The performance of machine learning techniques is dependent upon the size of the training phase. As the training size increase, the performance also improves. With an increase in the number of CR users a larger area under the PU is covered. Because our training model incorporates the global decision by acting according to it and also through the ACK signal the ground reality is known, the training phase can accurately know the behavior of CR users to the PU activity. With a large number of CR users, each CR user can reflect the ground reality in its training classes through the global decision. With a large training phase, the behavior of CR users to varying nature of the PU activity also can be accurately known. In conventional machine learning techniques, the training phase can gather adequate amount of training data to know the environment. Knowing the exact nature of PU activity is practically not feasible because of the random nature both of wireless channel and of the PU activity. But as will be shown in simulations, given a sufficiently large size of the training phase, the system detection performance can converge even at a very low SNR.

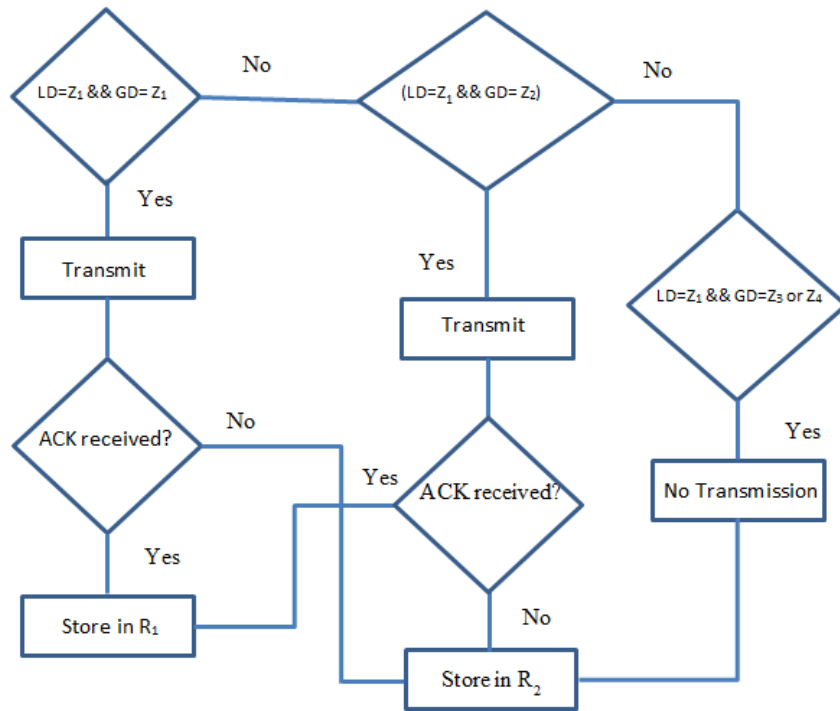


Figure 4.3 (a) Decision tree for the case that local decision is Z_1

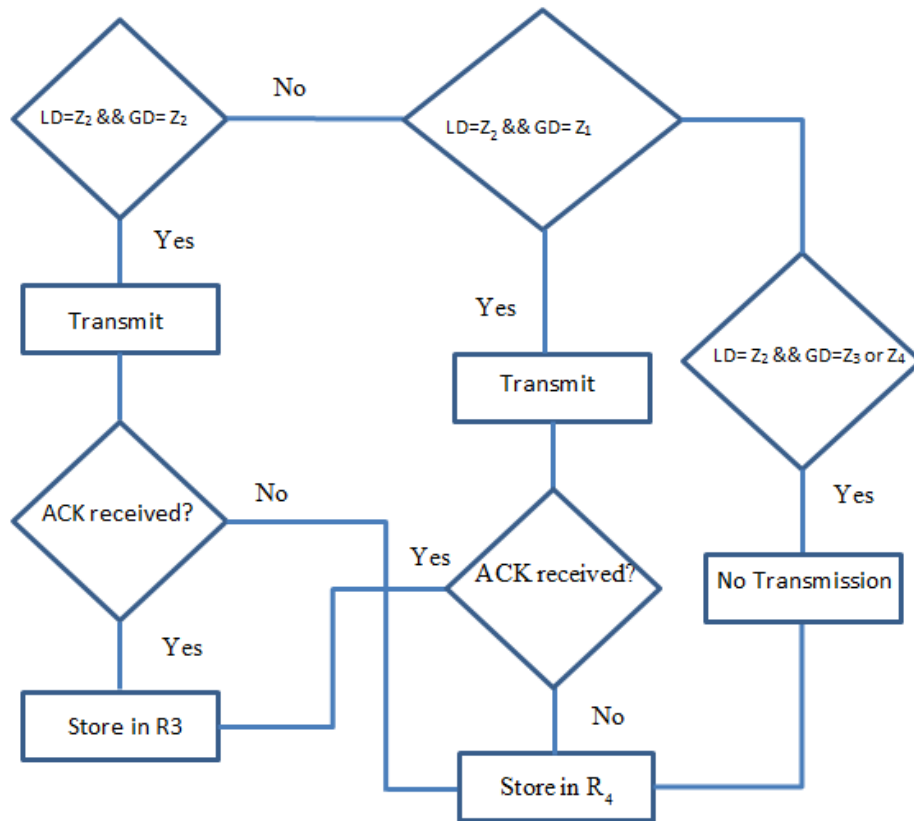


Figure 4.3 (b) Decision tree for the case that local decision is Z_2

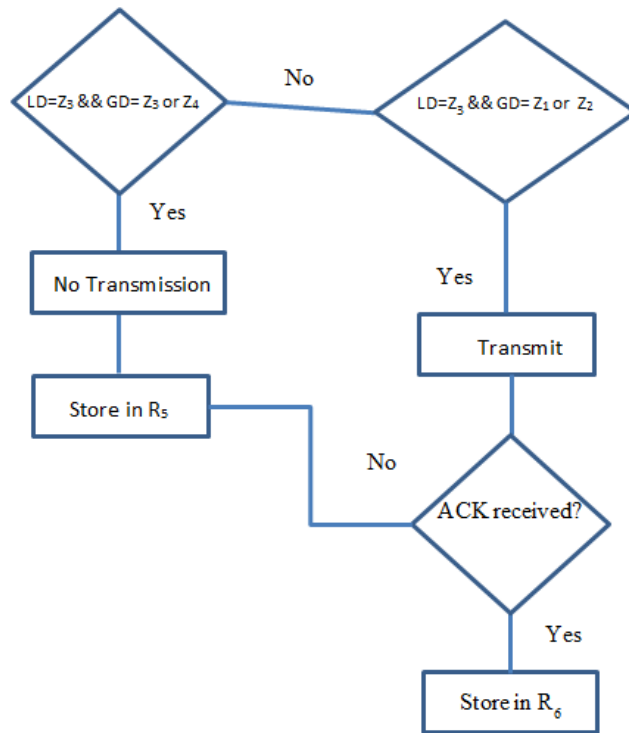


Figure 4.3 (c) Decision tree for the case that local decision is Z_3

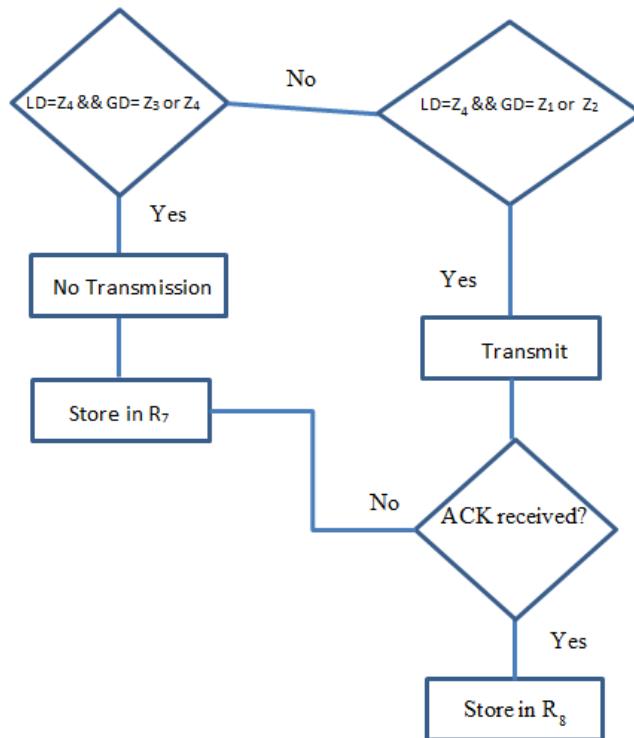


Figure 4.3 (d) Decision tree for the case that local decision is Z_4

Fig. 4.4 (a) presents the frame structure when the FC decides that the PU is present during training phase. The CR users remain silent during the transmission phase in this case. Different operations in the sensing phase happen as first the local decision is made then the local sensing decision is sent to the FC through a CCC. The FC combines the local sensing decisions and decides whether the PU is present or absent. If the FC decides that the PU is absent then the CR users transmit and hear for the ACK signal over the same channel on which transmission has been done. The CCC is not used for establishing links between the CR users. Rather it the communications happen between the CR user through the spectrum which is licenced to the PU and which is accessed by the CR users if the PU is absent. Fig. 4.4 (b) presents the time frame for the case when PU is absent during training phase. On the basis of the ACK signal the sensing report of the sensing slot is assigned into the classes as defined by the observations above. The frame structure is different for training phase from classification phase. In the training phase the sensing classes are updated on the basis of status of the ACK signal which helps in training the CR user to accurately reflect the ground reality.

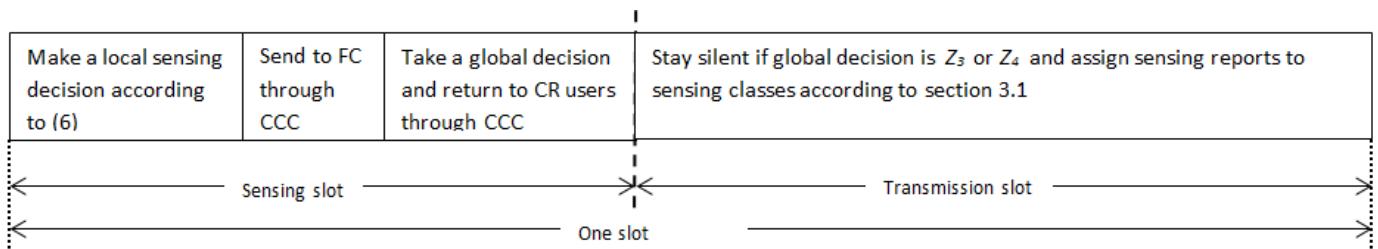


Fig. 4.4 (a). Time frame structure when the FC decision is Z_3 or Z_4 during the training phase

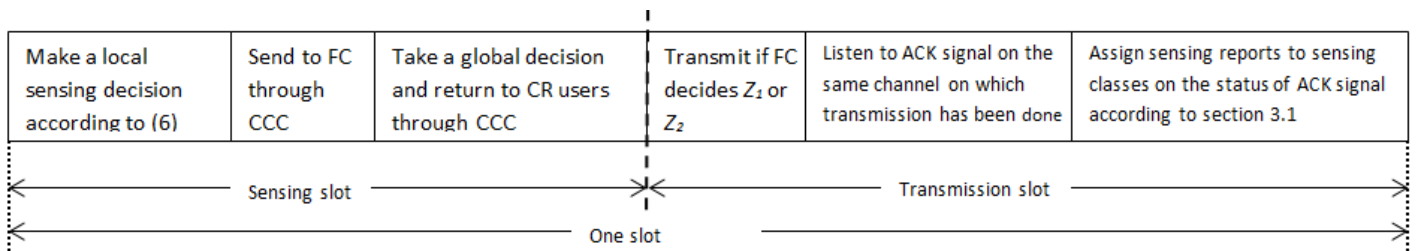


Fig. 4.4 (b). Time frame structure when the FC decision is Z_1 or Z_2 during the training phase

4.3.2 Classification Phase

In the previous phase, information was gathered regarding the operating environment and the CR user behavior in response to the changing environment. Learning the environment is made especially difficult by the nature of CR networks. Because of the noisy sensing environment, CR users only obtain partial observations of the environment variables. In addition, CR users must also transmit data. This results in a trade-off between sensing time and throughput: the higher the sensing time, the more accurate the sensing result and thus the more efficient the learning. Therefore, partial observability and capping the sensing time complicate the learning process. A third limitation is that a PU is considered to be autonomous. A CR user may not have any prior information about PU behavior, its operating characteristics, the RF environment, interference levels, or noise power distribution.

Our learning scheme addresses these issues. Partial observability is addressed by incorporating the behavior of other CR users into the learning process through the global decision. The ACK enables CR users to better learn the operating environment and divide the sensing observations into their respective classes more accurately. Our learning scheme requires no prior information and can efficiently map sensing performance to the changing activity of the PU, thus enabling the CR user to more reliably detect the PU.

A frame structure during the classification phase is presented in figure 5. In the local decision making phase, the spectrum is sensed and a sensing report is created. The first six mini-slots in the local decision making part of figure 5 represent the local sensing report. The second part is the classification phase discussed in section 4.3.2. The last part of the local decision making slot is the reporting phase, where the local decision is reported to the FC, the global decision is returned and the CR user takes action accordingly. The transmission phase follows the local decision making phase.

In this section, we will present in detail how the current sensing report is classified into one of the training classes. KNN, a machine learning algorithm, is used to accurately classify the current instance into one of the sensing classes and thus reliably detect PU activity. The next section presents the KNN algorithm.

4.3.2.1 K-Nearest Neighbor Algorithm

KNN is a distribution-free machine learning algorithm that classifies observations into one of several classes based on quantitative variables. KNN, being a distribution-free method, is suitable for the context of cognitive radios. KNN classifies a test instance, in our case the current sensing report as described in section 4.3.1, into one of several neighboring classes by majority voting. The voting can be

modified to calculate the distance between any two sensing reports. In the context of CR networks, it is highly improbable that any two sensing reports are exactly the same, so we have to measure the similarity between them.

The classification plane is divided into a number of neighbors and the distance of the current sensing report to each of those neighbors is found. For the sake of notational simplicity let's denote the sensing report of the current sensing slot at the i -th CR user by x_i onwards. Let $d(x_i, y)$ be the distance, where y represents the neighbors, or the sensing classes obtained in section 4.3.1, given by $y \in \{R_1, R_2, R_3, R_4, R_5, R_6, R_7, R_8\}$. The distance is calculated to each of the neighbors representing either H_0 or H_1 . Based on the calculated distance, the current sensing report is classified either to H_0 or H_1 . Section 4.3.2.2 shows how the distance is calculated and section 4.3.3 shows the procedure for using KNN for classification.

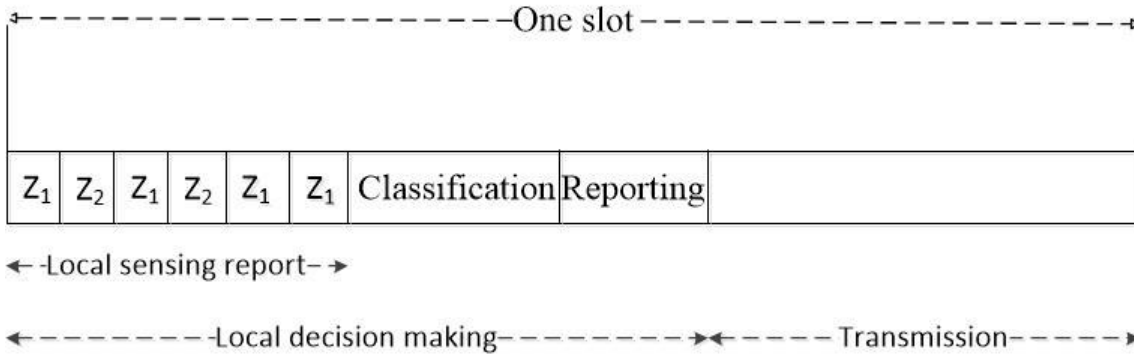


Fig. 4.5. Frame structure during classification phase.

4.3.2.2 Smith-Waterman Algorithm

The similarity score for each report is calculated through SWA as is given in section 2.4.3. The equations for calculating the similarity score according to the method discussed in section 2.4.3 are given below;

$$F(p, l) = \max \begin{cases} 0 \\ F(p-1, l-1) + o(q_{p,m}, q_{l,j}) \\ F(p-1, l) - t(q_{p,m}, q_{l,j}) \\ F(p, l-1) - t(q_{p,m}, q_{l,j}) \end{cases} \quad (4.7)$$

$$t(q_{p,m}, q_{l,j}) = \begin{cases} 4, & (q_{p,m} = 'Z_1', q_{l,j} = 'Z_4') \\ 3, & (q_{p,m} = 'Z_1', q_{l,j} = 'Z_3') \\ & \text{or } (q_{p,m} = 'Z_2', q_{l,j} = 'Z_4') \\ 2, & (q_{p,m} = 'Z_2', q_{l,j} = 'Z_3') \\ 1, & (q_{p,m} = 'Z_1', q_{l,j} = 'Z_2') \\ & \text{or } (q_{p,m} = 'Z_3', q_{l,j} = 'Z_4') \\ 0, & \text{otherwise} \end{cases} \quad (4.8)$$

$$o(q_{p,m}, q_{l,j}) = \begin{cases} 2, & (q_{p,m} = q_{l,j}) \\ 1, & (q_{p,m} = 'Z_1', q_{l,j} = 'Z_2') \text{ or} \\ & (q_{p,m} = 'Z_3', q_{l,j} = 'Z_4') \\ 0, & \text{otherwise} \end{cases} \quad (4.9)$$

$$F_{\hat{q}_m, \hat{q}_j} = \max_{p,l=1,2,\dots,n} \{F(q_{p,m}, q_{l,j})\}. \quad (4.10)$$

4.3.2.3 Classification

As is explained a sensing report have n elements belonging to q . The sensing report (x_i) has to be classified into one of the sensing classes, which are treated as neighbors for x_i . The candidate set of neighbors for x_i is denoted by $N(x_i)$ and contains all classes as found in section 4.3.1 such that $N(x_i) \in \{R_1, R_2, R_3, R_4, R_5, R_6, R_7, R_8\}$ and each CR user has its own version of sensing classes.

The current sensing report is compared with every member of each of the sensing classes belonging to $N(x_i)$. The membership counting vector is represented by $\vec{y}_{x_i}(l)$. Each element of $\vec{y}_{x_i}(l)$ is the result of comparing x_i with the j -th member of the l -th sensing class which is computed by (10). Let h_1^l be the event that sensing report x_i belongs to class l , and h_0^l be the event that sensing report x_i does not belong to class l . Furthermore, let E_ω^l be the event that ω elements in $\vec{y}_{x_i}(l)$ are greater than a threshold. Then the posterior probability ($P_{x_i}(l)$) that the current sensing report x_i belongs to class l is found as

$$\begin{aligned}
P_{x_i}(l) &= P(h_1^l / E_\omega^l) \\
&= P(h_1^l)P(E_\omega^l / h_1^l) / \sum_{b \in \{0,1\}} P(h_b^l)P(E_\omega^l / h_b^l) \\
&= P(h_1^l)P(E_\omega^l / h_1^l).
\end{aligned} \tag{4.11}$$

In (4.11) the posterior probability for the current sensing report that it belongs to the class l is found out by Bayes rule. The prior probability is given by $P(h_1^l)$ and the probability of likelihood by

$P(E_\omega^l / h_1^l) / \sum_{b \in \{0,1\}} P(h_b^l)P(E_\omega^l / h_b^l)$ and as binary result is possible i.e. the current sensing either belong to the

class or does not so it is summed over the both classes. Based on the posterior probability, the local decision for the i -th CR user at the r -th sensing slot, represented by $q_{i,r}$, is given as

$$q_{i,r} = \begin{cases} H_0 & P_0 > P_1 \\ H_1 & \text{otherwise} \end{cases} \tag{4.12}$$

where P_0 is the sum of posterior probabilities of sensing classes representing H_0 and is given as

$$P_0 = P_{x_i}(R_1) + P_{x_i}(R_3) + P_{x_i}(R_6) + P_{x_i}(R_8) \tag{4.13}$$

and P_1 is the sum of posterior probabilities of sensing classes representing H_1 and is given as

$$P_1 = P_{x_i}(R_2) + P_{x_i}(R_4) + P_{x_i}(R_5) + P_{x_i}(R_7). \tag{4.14}$$

4.3.3 Cooperative Spectrum Sensing

The FC receives the local decisions as D_i where $i = 1, 2, 3, \dots, N$. In CSS, the sensing capabilities of CR users are different from each other which results in different local sensing results [64]. In the proposed scheme, we use a weight-based decision combination at the FC. Each CR user is assigned a weight based on its effectiveness.

A partial global decision at FC, represented by $L_{G,i}$ is made by excluding the result of the i -th CR user as

$$L_{G,i} = \begin{cases} H_0 & N_{H_0}^i > N_{H_1}^i \\ H_1 & \text{otherwise} \end{cases} \tag{4.15}$$

where $N_{H_0}^i$ is the number of CR users reporting H_0 excluding the local decision of the i -th CR user and is given as

$$N_{H_0}^i = \sum_{j=1, j \neq i}^N I_0(D_j = H_0) \tag{4.16}$$

where $I_0(D_i = H_0)$ is indicator function for H_0 and is given by

$$I_0(D_i = H_0) = \begin{cases} 1; & D_i = H_0 \\ 0; & D_i \neq H_0 \end{cases}. \quad (4.17)$$

On the other hand, $N_{H_1}^i$ is the number of CR users reporting H_1 excluding the local decision of the i -th CR user and is given as

$$N_{H_1}^i = \sum_{i=1, i \neq i}^N I_0(D_i = H_1) \quad (4.18)$$

where $I_0(D_i = H_1)$ is indicator function for H_1 and is given by

$$I_0(D_i = H_1) = \begin{cases} 1; & D_i = H_1 \\ 0; & D_i \neq H_1 \end{cases}. \quad (4.19)$$

Partial global decisions are found for all CR users. The local decisions are then combined through a majority rule as $L_{G,all}$ and can be expressed as

$$L_{G,all} = \begin{cases} H_0 & N_{H_0} > N_{H_1} \\ H_1 & \text{otherwise} \end{cases} \quad (4.20)$$

where N_{H_0} is the number of CR users reporting H_0 and N_{H_1} is the number of CR users reporting H_1 . Based on (15) and (20), the weight for each CR user, α_i , is calculated as

$$\alpha_i = \begin{cases} \alpha_i + 1 & L_{G,i} \neq L_{G,all} \\ \alpha_i & L_{G,i} = L_{G,all} \end{cases}. \quad (4.21)$$

The cumulative weight for each hypothesis, β_a where $a \in \{H_0, H_1\}$ is then calculated as

$$\beta_a = \sum_{i=1}^N \alpha_i I_0(D_i = a) \quad a \in \{H_0, H_1\} \quad (4.22)$$

where $I_0(D_i = a)$ is given by

$$I_0(D_i = a) = \begin{cases} 1; & D_i = a \\ 0; & \text{otherwise} \end{cases}. \quad (4.23)$$

The final global decision is denoted by L_G and is calculated as

$$L_G = \begin{cases} H_0 & \beta_{H_0} > \beta_{H_1} \\ H_1 & \text{otherwise} \end{cases}. \quad (4.24)$$

The global decision is returned to CR users and the CR users then transmit or stay silent according to the global decision.

Let $\beta = \sqrt{2\gamma \sum_{k=1}^n |h_k|^2 + 1}$ where h_k is the channel gain between the primary user and the i -th CR user

during the k -th mini-slot and γ is the mean SNR as received from the PU. If it is assumed that the system's coefficients are known then the system probability of false alarm under non-fading channels is given as [61]

$$P_f^S = Q\left(\beta Q^{-1}(\bar{P}_d) + \sqrt{N_0} \gamma \sum_{k=1}^n |h_k|^2\right) \quad (4.25)$$

where $Q(\cdot)$ is the complimentary distribution function of the standard Gaussian i.e.

$Q(\chi) = \frac{1}{2\pi} \int_{\chi}^{\infty} \exp(-\frac{t^2}{2}) dt$ and \bar{P}_d is the system target probability of detection. The probability of detection

and probability of false alarm of the proposed scheme depend both on the probability of the sensing report falling into a particular quantization zone and on the number of mini-slots in the sensing slot. The target probability of detection and target probability of false alarm are depended upon the number of quantization zones, the portability that under a particular hypothesis the sensing decision will fall in a particular quantization zone and the weight of each quantization zone. The quantization thresholds are adjusted such that the optimal quantization thresholds are found. On the basis of quantization parameters the target probabilities of detection and false alarm are optimized. For cooperative spectrum sensing the target probability of detection, if the weight of the quantization zones is considered the same i.e. that each quantization zone contribute the same to the final decision combination, can be given as [65]

$$\bar{P}_d = \prod_{m=1}^M \left\{ \binom{N - \sum_{s=1}^l N_{Z_s}}{N_{B_m}} (P_{H_1}(Z_m))^{N_{Z_m}} \right\} \quad (4.26)$$

where N_{Z_m} is the number of CR users having the local sensing decision in zone Z_m , l is the largest integer less than m , $P_{H_1}(Z_m)$ is the probability of having the local sensing decision in quantization zone Z_m under H_1 . The system probability of detection can be given as [61]

$$P_d^S = Q\left(\beta Q^{-1}(\bar{P}_f) + \sqrt{N_0} \gamma \sum_{k=1}^n |h_k|^2\right) \quad (4.27)$$

where \bar{P}_f is the system target probability of false alarm and is given by [65]

$$\bar{P}_f = \prod_{m=1}^M \left\{ \binom{N - \sum_{s=1}^l N_{Z_s}}{N_{B_m}} \left(P_{H_0}(Z_m) \right)^{N_{Z_m}} \right\} \quad (4.28)$$

and $P_{H_1}(Z_m)$ is the probability of having the local sensing decision in quantization zone Z_m under H_0 .

4.4. Results and Analysis

In this section we observe the behavior of our proposed scheme and compare it to other schemes through system parameters such as probability of detection, probability of error, and probability of spectral holes exploitation. In chapter 1, the effect of introducing multiple bits for reporting and sensing the spectrum multiple times within the same sensing phase was investigated where the scheme utilizing reporting multiple bits and multiple mini-slots was shown to be robust against all kind of attacks. Authors in [3] and [61] have also shown the reliability gain which is brought by using multiple mini-slots. The number of CR users is 5, the number of iterations is 1000, the sensing slot duration is 1 ms, the sampling frequency is 300 kHz and the number of energy samples in each sensing slot is 600. The idle probability of PU is 0.5. The SNR range is from -25 to -10 dB. When the number of CR users is large, clusters are formed for spectrum sensing to reduce the overhead. Authors in [66] considered clusters to sense the spectrum where the number of CR users in each cluster was five. That is, when cluster is considered, the CR users send their local decisions to a cluster-head to reduce the number of direct reports sent to the FC. To consider a higher number of CR users, the concept of cluster needs to be adopted. However, it is beyond the scope of the paper. However, according to [66] as the number of clusters and thus the number of CR users increase the sensing performance also improves. The idle probability is used as 0.5 in literature for the sake of fairness ([66]). If the idle probability of PU is increased, it will provide higher opportunities of transmission to the CR user. Therefore, the idle probability of PU in the paper is taken as 0.5 for maintaining fairness among CR and PU systems. As the idle probability of PU is considered equal to that of probability of activity of the PU, the target detection probability for channel without fading is set to be 0.8 at SNR of -20 dB. The detection probability as is set in this paper with a higher active probability of the PU of 0.5 (the authors in [61] considered a low active probability of PU of 0.3) guarantees the protection of the

PU data. We measure the performance of our proposed scheme in both the AWGN channels and also in fading channels by observing our scheme's behavior and also of other schemes behavior through varying SNR conditions for different system parameters. The training phase strongly impacts the system performance, as through this phase, the sensing classes are developed. The larger this phase, the greater the number of training instances, which means the current sensing report has more similar reports to match with. We plot the proposed scheme with two variants. In one, the training phase is 100 iterations and in the other it is 330 iterations. These schemes are compared with a scheme in which the CR users make a one-bit local decision and the local decisions are combined at the FC by using a conventional OR rule.

In this paper, the probability of error (Pe) is given as

$$Pe = Pf \times P(H_0) + (1 - Pd) \times P(H_1) \quad (4.29)$$

where Pd is the probability of detection, Pf is the probability of false alarm, $P(H_0)$ is the prior probability of H_0 , and $P(H_1)$ is the prior probability of H_1 . The probability of detection (Pd) is defined as

$$Pd = \frac{n_{(D_G=1 \ \&\& \ H=1)}}{n_{(D_G=1 \ \&\& \ H=1)} + (n_{(D_G=0 \ \&\& \ H=1)})} \quad (4.30)$$

and the probability of false alarm (Pf) is defined as

$$Pf = \frac{n_{(D_G=1 \ \&\& \ H=0)}}{n_{(D_G=1 \ \&\& \ H=1)} + (n_{(D_G=0 \ \&\& \ H=1)})} \quad (4.31)$$

where H is the real status of the PU and is equal to a randomly generated stream of ones and zeroes with size equal to the total number of iterations. A one represents the presence of the PU, while a zero represents absence of the PU. The notation $n_{(x \ \&\& \ y)}$ means the number of times the condition in the subscript is satisfied. The probability of spectral hole exploitation is represented by Pnf and can be expressed as

$$Pnf = 1 - Pf . \quad (4.32)$$

Soft decision combination gives the optimal sensing performance [4]. In [4], it is also shown that hard decision combination gives inferior results but only has one-bit overhead while soft combination incurs a lot of overhead. In one-bit hard combination scheme, sensing information was lost during local decision making because of using only one threshold. By using multiple thresholds, the sensing information loss can be reduced, which leads to better performance, and more overhead. In [11], it is also shown that using two bits for reporting the local decision can significantly improve the sensing performance. The effectiveness of using two bits (four quantization levels) was shown for both perfect and imperfect

reporting channels. In [67], *H. Sakran et al.* utilized three bits to report the local decision to the FC. The performance improvement was shown to be better than using two bits for reporting local decision. In summary, it is obvious that tradeoff exists between spectrum sensing performance and overhead when we design the quantization levels. Therefore, in the paper we mainly focus on applying machine-learning algorithm into Smith-Waterman Algorithm-based soft-decision spectrum sensing by considering the case of four quantization levels. To consider more quantization levels than 4 levels, the whole problem formulation such as the observations in section 3.1 and the classification classes have to be changed and re-designed. Therefore, simulation results are bounded to the case of four quantization levels.

In the training phase the probability of detection of the proposed scheme is equal to that of Majority rule which uses quantization. In machine learning technique, the performance of the proposed scheme is dependent upon the classification phase. In the simulations, the probability of detection is composed of those of both the training and classification phase. Similarly, training data in the proposed scheme is required to train the KNN classifier, and the performance of the classifier is depended on the training size of the data. The proposed scheme utilizes the Majority rule to get training data. Since malicious users or anomalies are not considered in the paper, the Majority rule works by majority voting and corresponding performance will be dependent upon local sensing decisions of the CR users. When the training phase is over, the classifier will have ample data available to the changing behavior of PU, and will be trained.

Fig. 4.6 shows the system detection performance in an AWGN channel. The proposed scheme with the larger training phase outperforms the other two schemes. The proposed scheme with a smaller training phase has the same detection performance as an OR rule in the low SNR regime. The reason is that the sensing reports in low SNR regimes do not have large distances from each other. The energies received under both hypotheses in the low SNR regime vary little from each other and thus, the scheme with fewer training instances fails to learn the environment more reliably. As the SNR improves, the proposed scheme with the smaller training phase results in more reliable spectrum sensing than conventional schemes. Figure 4.7 shows the error performance as calculated by 4.32. In this figure, it can also be seen that the proposed scheme with the larger training phase has a low probability of error even in the low SNR regime. The scheme with the smaller training phase converges to one with a larger training phase in better SNR conditions, which shows that even with a smaller training size the proposed scheme can result in more reliable spectrum sensing than conventional schemes.

Figure 4.8 shows the capability of the proposed scheme to exploit spectral holes which is defined by (4.28). Exploiting available opportunities for transmitting data is the highest priority from the perspective of a CR user. Even in bad SNR conditions our proposed scheme enables CR users to exploit data

transmission opportunities. The proposed scheme with the smaller training phase lags behind the one with the larger training phase in bad SNR conditions, but converges to the scheme with the larger training phase in good SNR regimes.

In the region of high SNR, the sensing reports which are formed are better reflections of the PU's activity. The sensing performance can be improved under the region of high SNR regimes since the PU signal will take larger portion of the received signal, compared to the added noise. That is to say, when SNR gets larger, a smaller number of training samples and further a smaller size of the training window are required to train the classifier. Therefore, when the SNR improves, a smaller training size results in the same performance. On the other hand, in the region of lower SNR, a larger training size and a higher training size are needed to accurately reflect the PU's activity. All the three schemes show same performance trend but at different SNR levels. The OR rule has the best detection performance among conventional schemes, as it uses the most relaxed criteria for declaring, whether the PU is present or not out of all the conventional rules. However, this means that the OR rule cannot efficiently exploit data transmission opportunities. These figures show that our proposed scheme can protect PU data more effectively as well as provide more data transmission opportunities.

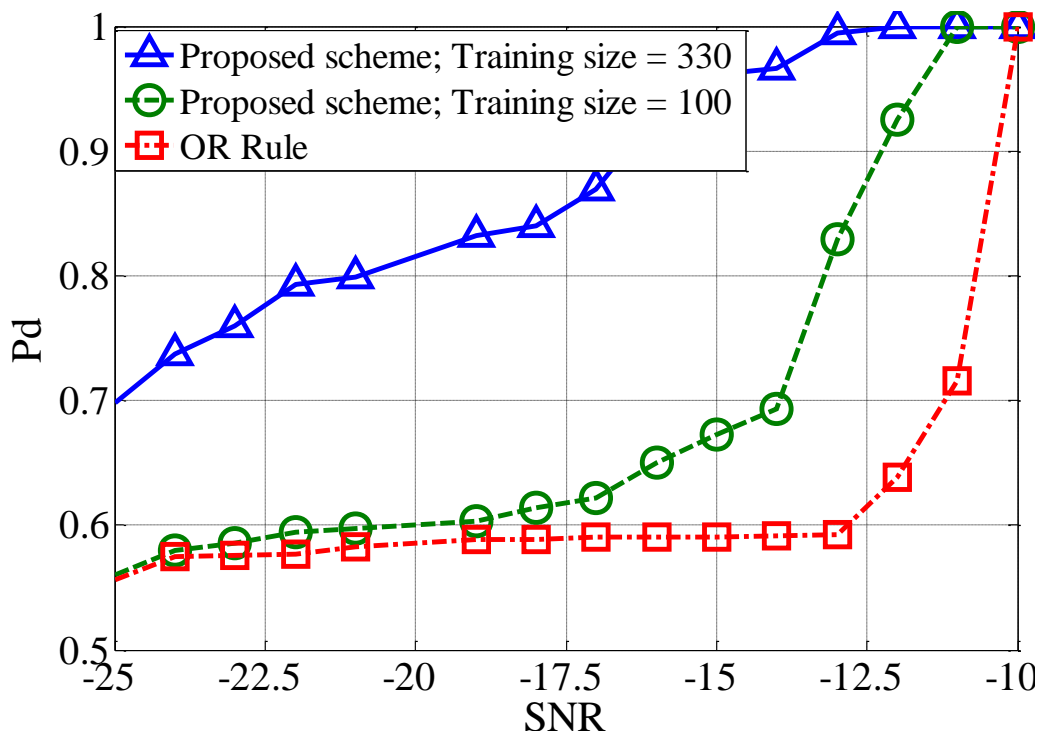


Fig. 4.6. System detection performance with non-fading channels.

Fig. 4.9 shows the detection performance of the proposed scheme in a fading environment. Fading affects the power of the received signal and thus the number of energy samples required to efficiently decide the

status of the PU. In non-fading environment the amplitude gain of the channel is deterministic while in the fading channels the amplitude gain of the channel varies [17]. Thus the probability of detection is dependent upon the instantaneous SNR. The effect of fading on performance of spectrum sensing was investigated in detail by [7]. Instead of following (2) and (3) for setting up a simulation environment, we have followed a path-loss model to incorporate fading as presented in [68]. We assume a path-loss model where the signal goes fading proportional to d^α , where d is the distance between the PU and the CR users and $\alpha = 3$. The average distance between the PU and CR users is assumed to be 20 m. The performance of our proposed scheme with the larger training phase outperforms the OR rule by 5% when the SNR is -23 dB, but when the SNR improves to -16 dB, the improvement is about 20%. The detection performance of the proposed scheme outperforms the OR rule by a larger margin when SNR conditions improve. As can be seen from the figure, the OR rule has a very poor detection performance in a fading environment despite the fact that it has the best detection performance among conventional fusion rules. Fig. 4.10 shows the error performance of the proposed scheme in a fading environment. It can be seen that with increasing SNR, the error reduces. At -25 dB, the error probability is just above 0.1. Due to fading, the error probability of the OR rule is 0.35, which is very high compared to our proposed scheme.

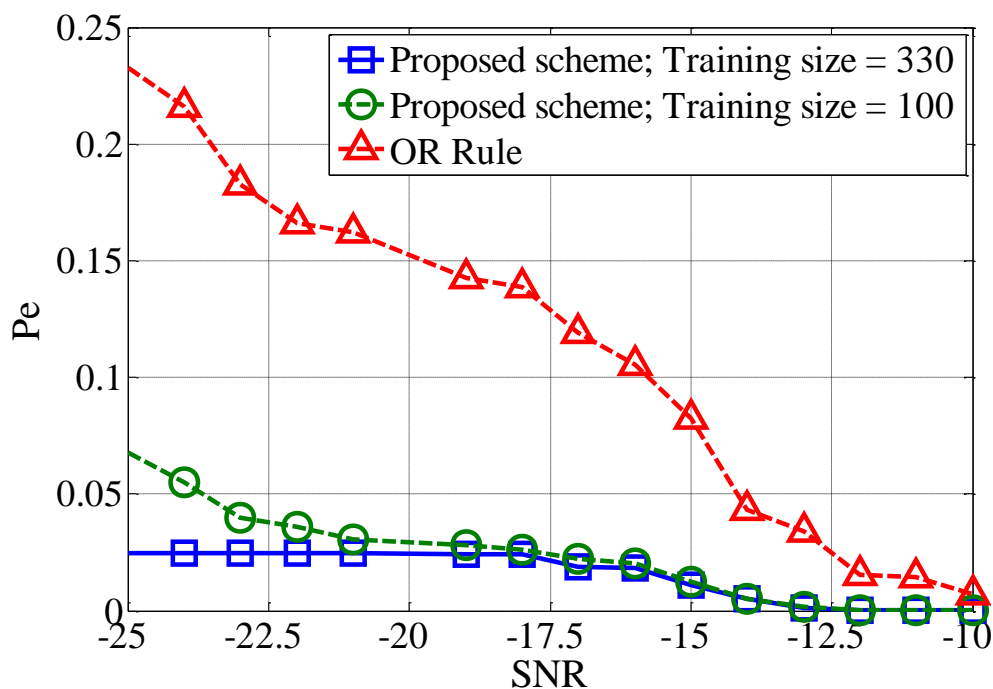


Fig. 4.7. System error performance with non-fading channels.

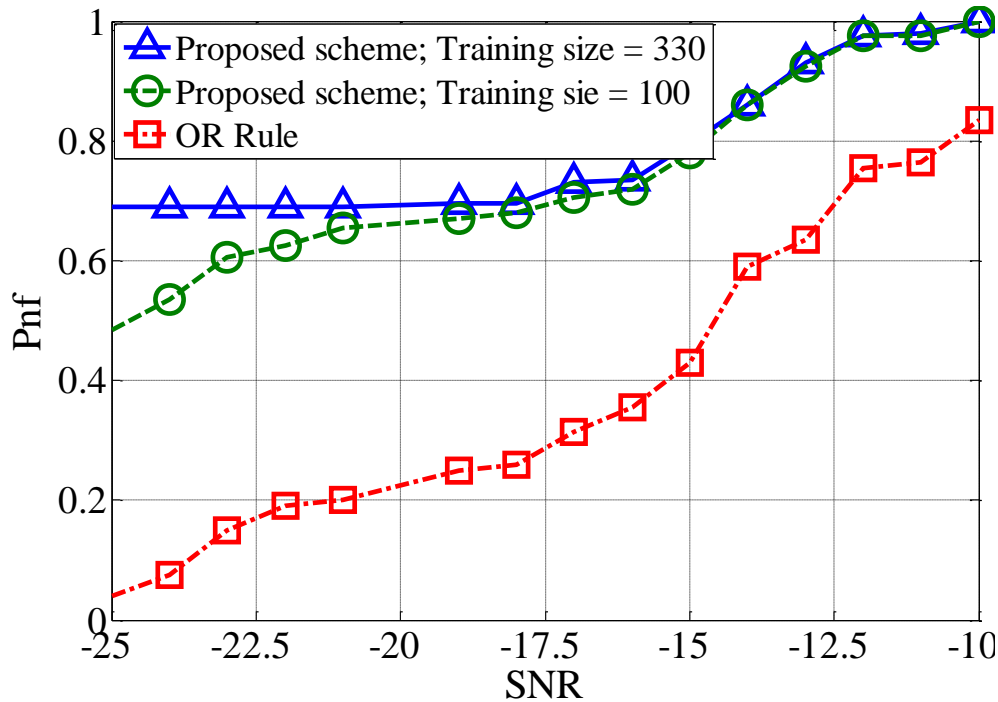


Fig. 4.8. System probability of exploiting spectral holes.

Fig. 4.11 shows the effect of the number of CR users on the performance of cooperative spectrum sensing under fading channels where some CR users undergo deep fading and thus have unreliable training data. To reflect the effect of increasing number of CR users fading conditions are required as in non-fading channels the performance with increasing the number of CR users remains the same because the training data of less CR users is also reliable and reflect the PU activity accurately. In the figure for each number of CR users the SNR is varied from -25 to -10 and then the mean of probabilities of detection is found. For instance, when the number of CR users is 6 the probability of detection for a multiple values of SNR varying between -25 and -15 is calculated and then the mean of the computed probabilities is the mean probability of detection. The mean probability of detection is represented by Pmd . As the values shown are mean values so the Pmd cannot converge to 1. For each values of SNR the system is run 1,000 time for the proposed scheme having training size of 100 and 300 times for the proposed scheme having training size of 100.

As can be seen as the number of CR users increases beyond a limit, in this case beyond 10 the improvement in mean probability of detection is not abrupt. That is because of the reasons explained in first paragraph of this section that to utilize the gain which can be introduced by increasing the number of CR users clusters need to be formed. When instead of cluster-heads the FC combines the sensing decisions of all CR users then the sensing decisions of many CR users may fall outside of the similarity distances range as calculated in section 3.2.2 and thus their reports will be rejected. From figure (11) it can be seen that the

mean probability of detection of the proposed scheme with a larger training size surpasses the performance of the other schemes. A mean probability of detection when the number of users equals to 20 reaches 0.8 which is target detection probability as we consider in this paper at SNR of -20 dB for non-fading channels when the number of CR users is 5 as we have considered in this paper. The proposed scheme reaches highest mean probability of detection of near 0.7 and the OR can achieve highest mean probability of detection of less than 0.6.

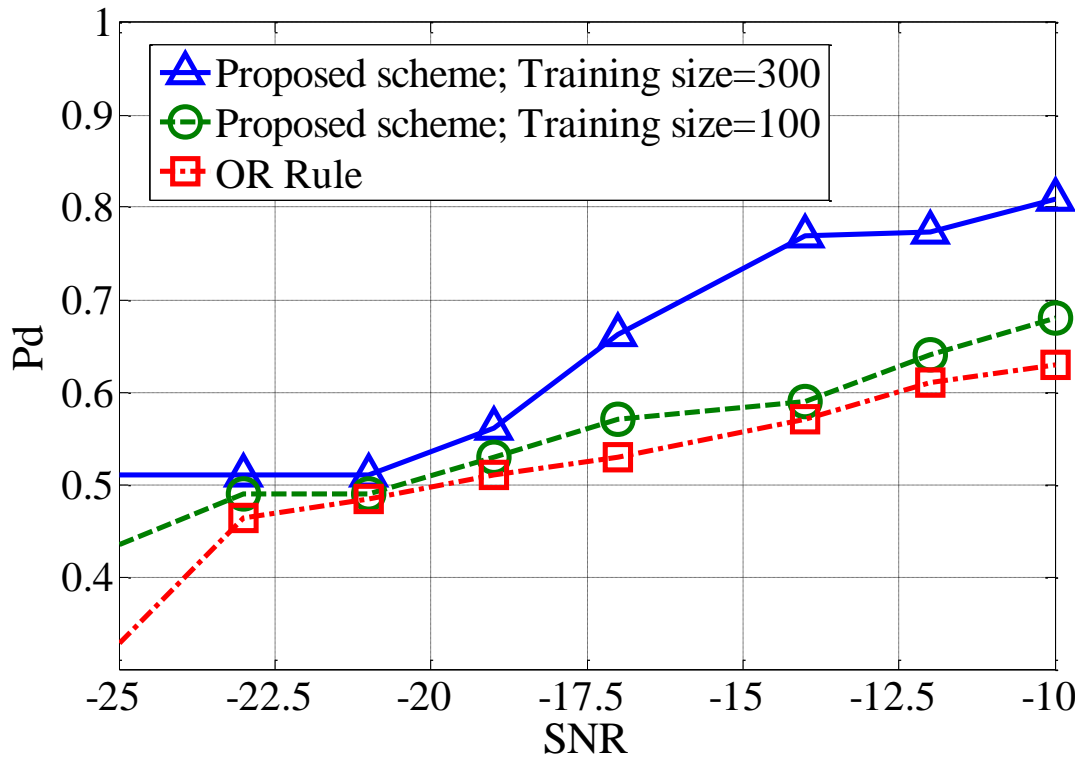


Fig. 4.9. System detection performance with fading channels.

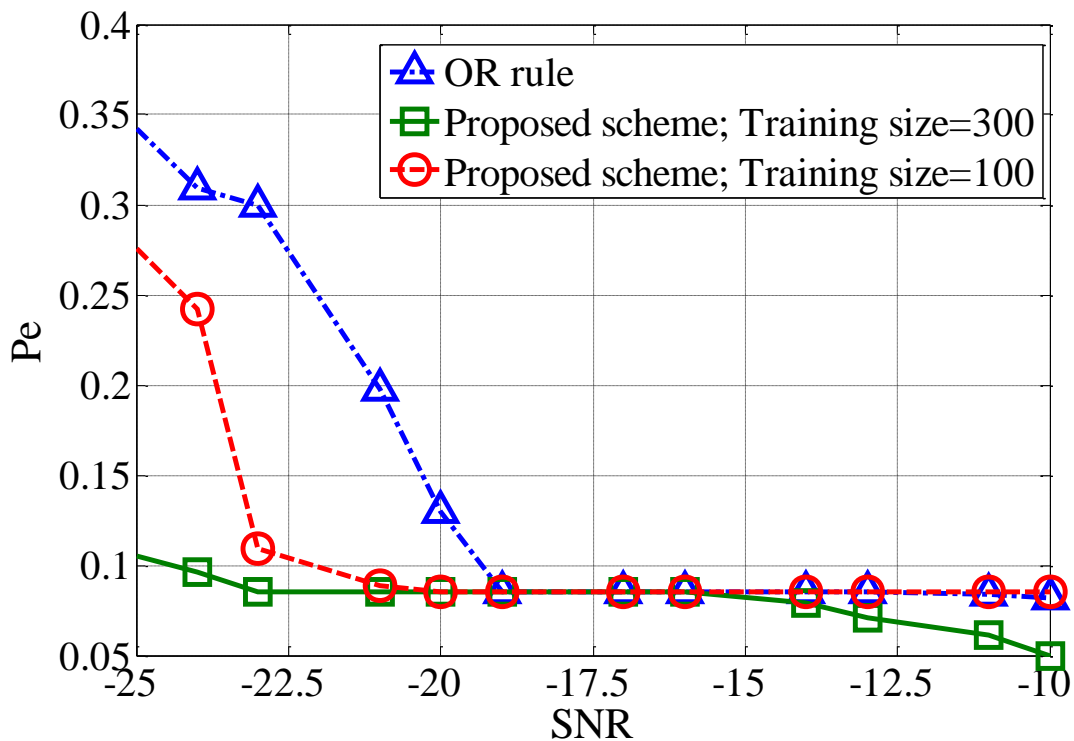


Fig. 4.10. System error performance with fading channels.

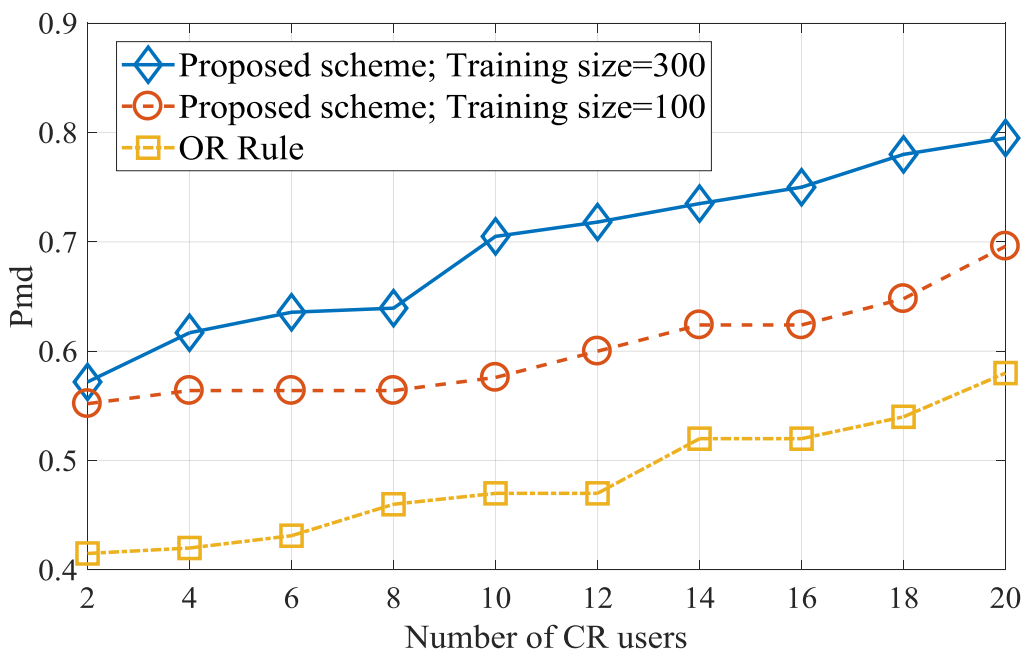


Fig. 4.11. Effect of number of CR users.

4.5. Conclusion

In this paper, a machine-learning-based reliable spectrum sensing scheme is proposed. The proposed scheme learns from the environment by taking into account the true status of the PU. Sensing reports are stored in appropriate sensing classes and then the current sensing report is classified into one of the sensing classes. Based on the result of classification, the PU is declared present or absent. Local decisions are combined at the FC by a novel decision combination scheme that takes into account the reliability of the CR users. Mechanisms at both the CR level and the FC level ensure reliable spectrum sensing. Simulation results show that our proposed scheme has better detection performance and better spectral hole exploitation capability than the conventional OR rule. Fading affects detection performance, but our scheme detects successfully 80% of the times at -10 dB SNR even in a fading environment.

Chapter 5

Actor-Critic algorithm based accurate multi-bit quantization sensing and transmission framework in energy constrained CRN

5.1 Introduction

In chapter 3, 4 and 5 methods for reliable and accurate spectrum sensing were proposed and the literature regarding spectrum sensing was studied in detail. In this chapter a transmission framework which is based on the sensing decision is explained. After the sensing decision is made the CR users either has to transmit or stay silent. The decision to transmit is based on the current state and the transition probability to the next state and the remaining energy if energy constrained networks are considered. The states to transition to are limited by the current state. The set of actions is also determined by the current state which may be a combination of spectrum sensing decision, the belief function and the remaining energy. In the Markovian decision systems the state-transition should strictly follow the Markovian chain. So, all the possible states and possible actions for those states will have to be computed. In this case the computation becomes complex and expensive.

In this chapter a model free reinforcement learning algorithm called actor-critic algorithm [69-70]. The advantage of actor-critic algorithm is that it is not as computationally complex as POMDP approaches and it does not need all of the state transition information to make a decision. In the training phase the critic updates the approximation to state information on the basis of simulation parameters and feed this information to the actor to update the policy parameters. The actor-critic algorithm may converge to a local optimal policy but it generates the policy directly from training so much less computation complexity and formulation is required.

In this chapter energy constrained CRN is considered. The CR users take a local sensing decision, send it to the FC to take a global decision and these two form part of the local state. The belief function and

the remaining energy form the rest of the state. The action space is formed of silent mode, or transmits with a level of energy that is able to fulfil the long term energy requirements of the system. The CR users are able to harvest energy and the transmission energy in the current slot also has to take into consideration the long-term energy requirement. On the basis of transmission and ACK signal a reward is assigned to each action. The critic evaluates the reward brought by the action and updates the policy function. At the end of the training phase the optimal value function and the optimal policy function are obtained.

Rest of the chapter presents the system model in section 2, in section 3 the system energy constraints, energy harvesting process and Markovian process are explained, in section 4 the actor-critic algorithm is presented, section 5 presents simulation results while section 5 concludes the chapter.

5.2 System Model

We consider a single PU and a CRN that consists of N -CR users as shown in Fig. 5.1. The CR users perform spectrum sensing and report their results to the FC. We assume a slotted time frame-structure where each slot is divided into two slots: a sensing slot, which is used for spectrum sensing, and a transmission slot, which is used for actual data transmission.

Each CR user employs the energy detection scheme for spectrum sensing. The signal received by the i -th CR user is given as

$$y_i = \begin{cases} w(n); & H_0 \\ s(n) + w(n); & H_1 \end{cases} \quad (5.1)$$

where $w(n)$ is additive white Gaussian noise and $s(n)$ is the energy received of the PU's signal. The received energy is quantized as

$$l_i = \begin{cases} H_0 \begin{cases} Z_1 & ; Y_i \leq \lambda_{Z_1} \\ Z_2 & ; Y_i \leq \lambda_{Z_2} \end{cases} \\ H_1 \begin{cases} Z_3 & ; Y_i \leq \lambda_{Z_3} \\ Z_4 & ; Y_i > \lambda_{Z_3} \end{cases} \end{cases} \quad (5.2)$$

where λ_{Z_1} , λ_{Z_2} and λ_{Z_3} are the quantization thresholds. The global decision is taken on the basis of majority rule i.e. the majority of the reported symbols is considered to be the global decision. Let's denote it by D_i . The combination of local and global decisions determine the state of the CR at the current slot.

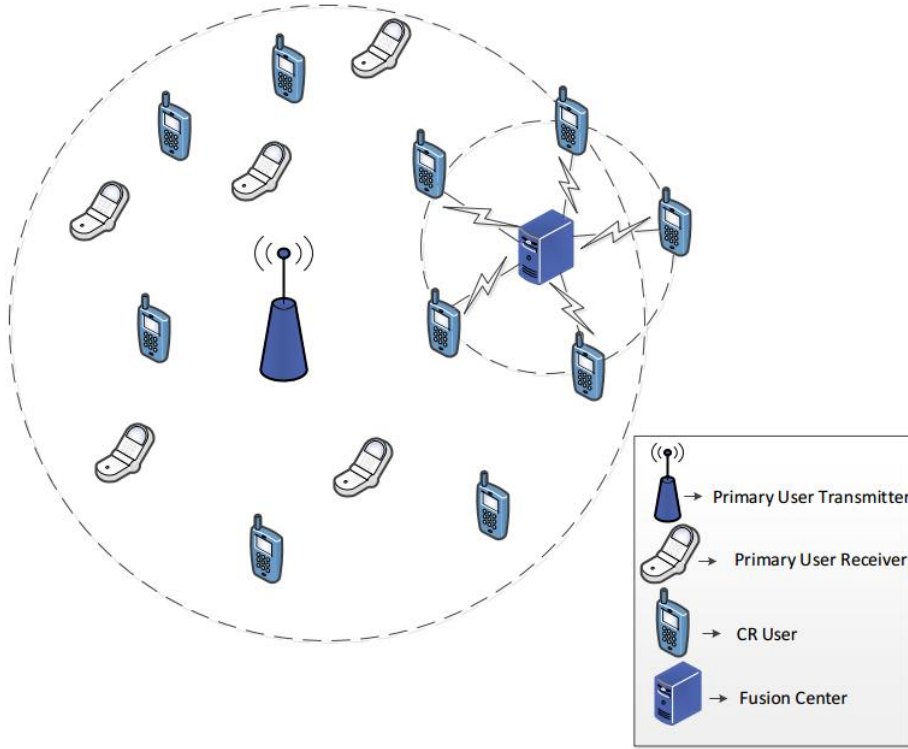


Figure 5.1 Basic system model

5.3 System Constraints and Definitions

In the section below the system model, the system constraints and processes are explained in detail.

5.3.1 Energy Harvesting Process

The CR users are able to harvest energy. If the energy arrival process $e_h^t \subset \mathbf{R}^+$ is assumed to be an i.i.d sequences of variables then $\mathbf{E}\{e_h^t\} = e_h$. It is also assumed that the energy harvested in time slot t is immediately available in slot $t+1$.

The total energy spend in the current slot, t , if the CR user transmit is given as

$$e_c(t) = e_s + \alpha_t e_r \quad (5.3)$$

where e_s is the sensing energy, e_r is the transmission energy and α_t is given as

$$\alpha_t = \begin{cases} 1 & \text{If the CR user transmits} \\ 0 & \text{otherwise.} \end{cases} \quad (5.4)$$

The residual energy for the next time slot, if the CR user transmit in the current time slot is

$$e_{rem}(t+1) = \min\{e_{cap}, e_{rem}(t) - e_c(t) + e_h\} \tag{5.5}$$

where e_{cap} is the maximum battery capacity

To ensure long term operation of the network the remaining energy of the current time slot has to satisfy energy requirements for some future time slots. As the transmission is dependent upon the sensing decision so its value cannot be estimated. The sensing energy for the future time slots remains fixed and on its basis the constraint can be formulated as;

$$e_{rem} \geq N(e_s - e_h) \tag{5.6}$$

5.3.2 Markovian process

Let the PU activity follow a two state Markovian process as;

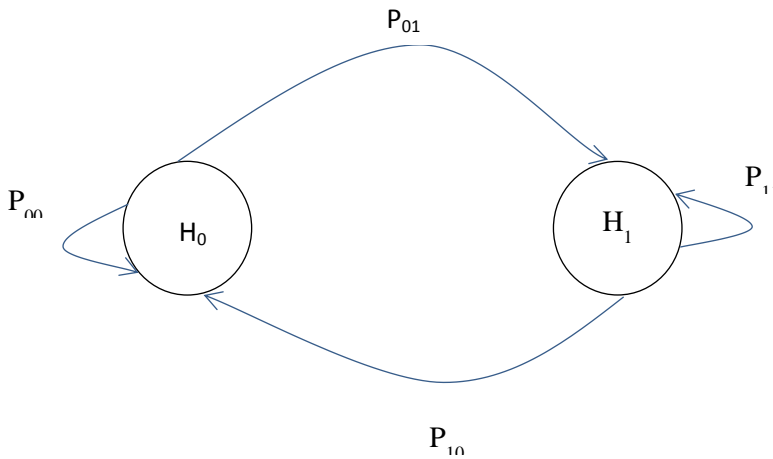


Figure 5.2 Markovian process

In Fig. 5.2 the Markovian process is presented where the CR user either transition to another state or remain in the same state. On the edges the transition probabilities are given. For the sake of simplicity ‘H’ is not written in the subscript of P.

The sensing and transmission framework is formulated as a Markov Decision process. The Markov decision process tuple is defined as $\langle \mathbf{S}, \mathbf{A}, \mathbf{P}, \mathbf{R} \rangle$.

The state is composed of the local and global sensing decisions, the remaining energy and the transition probability. For simplicity let's denote the combination of local and sensing decision as Q_{ld} . The state at time t is given as

$$s(t) = \{Q_{ld}, e_{rem}(t), \mu(t)\}. \quad (5.7)$$

The transition probabilities are dependent upon the current local and global sensing decisions. They will be presented in detail later.

The CR user after sensing can either be silent, transmit with Z_1 or Z_2 with different level of transmission energies to meet the long term energy requirements. Two transmission energies are considered. There can be many level of transmission energy but the formulation and the solution will become untenable. The action space is defined as

$$A = \{\text{SIL}, e_r^1(t), e_r^2(t)\} \quad (5.8)$$

where $e_r^1(t)$ representing transmitting with transmission energy e^1 and $e_r^2(t)$ is transmitting with energy level e^2 while SIL represents no transmission.

The reward is based on the ACK signal. The rewards are assigned as;

$$\begin{aligned} R((Q_{l1}, e_{rem}(t), \mu(t)), e_r^1(t) / \text{ACK}) &= T^{\{Q_{l1}, e_{rem}(t), \mu(t), e_r^1(t)\}} \\ R((Q_{l1}, e_{rem}(t), \mu(t)), e_r^2(t) / \text{ACK}) &= T^{\{Q_{l1}, e_{rem}(t), \mu(t), e_r^2(t)\}} \\ R((Q_{l2}, e_{rem}(t), \mu(t)), e_r^1(t) / \text{ACK}) &= T^{\{Q_{l2}, e_{rem}(t), \mu(t), e_r^1(t)\}} \\ R((Q_{l2}, e_{rem}(t), \mu(t)), e_r^2(t) / \text{ACK}) &= T^{\{Q_{l2}, e_{rem}(t), \mu(t), e_r^2(t)\}} \end{aligned}$$

$$R(s(t), e_r^i / \overline{\text{ACK}}) = 0$$

where $i = 1, 2$ and $l \in (Z_1, Z_2)$

(5.9)

The first part of the reward function i.e., $(Q_{li}, e_{rem}(t), \mu(t))$ represents the state, while the second part i.e., $e_r^i(t)$ represents the transmission energy. $T^{\{ \cdot \}}$ represents the throughput achieved with the given state and transmission energy.

5.4 Actor-critic algorithm

The CR user can take an action given a particular state and transition to another state in the current time slot as;

$$P(s' / s(t), a(t)) = \begin{cases} \mathbf{1}, & \text{if } s' = s(t + \mathbf{1}) \\ \mathbf{0}, & \text{otherwise.} \end{cases} \quad (5.10)$$

The reward associated with each state is given in (5.9).

The total discounted reward in the t -th time slot is given by value function when the current state is $s(t)$ and is compute as [70]

$$V(s(t)) = \sum_{k=t}^{\infty} \gamma^k R(s(t), a(t)). \quad (5.11)$$

The policy function is given by [70]

$$\pi(a(t) / s(t)) = P(a(t) \in A / s(t)) = \frac{e^{\phi(a(t), s(t))}}{\sum_{a \in A} e^{\phi(a(t), s(t))}} \quad (5.11)$$

where $e^{\phi(a(t), s(t))}$ is the tendency to select action $a(t)$ in state $s(t)$.

After the action is taken, the reward will be calculated. After calculation of the reward the temporal difference is found out as

$$\delta(t) = [R(s(t), a(t)) + \gamma V(s(t + \mathbf{1})) - V(s(t))]. \quad (5.12)$$

On the basis of the temporal difference, the value function is updated by the critic as

$$V(s(t)) = V(s(t)) + \beta \cdot \delta(t) \quad (5.13)$$

where β is the positive parameter of the critic. The tendency to selection an action given a state is updated as

$$\varphi(s(t), a(t)) = \varphi(s(t), a(t)) + \chi \cdot \delta(t) \quad (5.14)$$

where χ is a positive step-size parameter.

The decision in the current time slot is based on the summation of reward in the current time slot and the expected future reward in the next time slot. In the current time slot, in case the CR user decides to transmit, it can either send Z_1 or Z_2 . For Z_1 the reward in the current and future time slot on the basis of status of ACK signal is

$$B_{Z_1}^i = P_{ACK} \times \{R(Q_{l1}, e_{rem}(t), \mu(t), e_r^i(t))\} + P_{ACK} \times \sum_{\substack{t=t+1 \\ \{e_{rem}(t+1)\}}} P[*]V(s(t)) + P_{ACK} \times \sum_{\substack{t=t+1 \\ \{e_{rem}(t+1)\}}} P[*]V(s(t)) \quad (5.15)$$

and for Z_2 it is given as

$$B_{Z_2}^i = P_{ACK} \times \{R(Q_{l2}, e_{rem}(t), \mu(t), e_r^i(t))\} + P_{ACK} \times \sum_{\substack{t=t+1 \\ \{e_{rem}(t+1)\}}} P[*]V(s(t)) + P_{ACK} \times \sum_{\substack{t=t+1 \\ \{e_{rem}(t+1)\}}} P[*]V(s(t)) \quad (5.16)$$

where $P[*]$ gives the probability that (5.6) will be satisfied and $i \in (1, 2)$. The decision function for the current time slot can then be formulated as

$$B_0(e_{rem}(t+1), \mu(t), Q_{ld}) = Arg \max_A \{B_{Z_1}^i, B_{Z_2}^i\} \quad (5.17)$$

where $l, d \in (Z_1, Z_2)$ and A is given by (5.8).

The training process is meant to find the set of policy and the optimal value function corresponding to each state. The CR user take a local decision and send the quantized energy zone to the FC. The FC takes a global decision and send it to the CR users. Based on the local decision and the global decision the CR users can stay silent or transmit one of two quantized symbols with one of two level of transmission energy. At the beginning of each time slot a CR user take an action $a(t) \notin A$ according to policy $\pi(a(t)/s(t))$ in a given state. There will be transition to another state or the current state will be retained and the next state will be $s(t+1)$ based on the residual energy and the feedback. The rewards will be calculated according to (5.9). The temporal difference is calculated according to (5.12) after the calculation of reward. On the basic of temporal difference updating the value function in (5.13) and the tendency to select an action $a(t)$ in state $s(t)$ is updated in (5.13). After the training is complete there will be an optimal value function $V(s)$ and an optimal set of policy π .

The following are the possible cases for the CR users in the training phase

Case 1: $D_i = Z_1$ or Z_2 & $l_1 = Z_1$ then stay silent. The belief that the PU is absent in the current time slot is updated using Bayes' rule [70] as

$$\mu^*(t) = \frac{\mu(t)P_f^{Z_1}}{\mu(t)P_f^{Z_1} + (1 - \mu(t))P_d^{Z_1}} \quad (5.18)$$

where $P_f^{Z_i}$ is the local probability of false alarm for zone Z_i and $P_d^{Z_i}$ is local probability of detection for zone Z_i and $i \in (1, 2, 3, 4)$. The belief for next time slot is given as

$$\mu(t+1) = \mu^*(t)P_{11} + (1 - \mu^*(t))P_{01}. \quad (5.19)$$

The residual energy for the next time slot is updated as

$$e_{rem}(t+1) = \min\{e_{cap}, e_{rem}(t) - e_s + e_h\}. \quad (5.20)$$

Case 2: $D_i = Z_1$ or Z_2 & $l_i = Z_2$ then stay silent. The belief that the PU is absent in the current time slot is updated using Bayes' rule as

$$\mu^*(t) = \frac{\mu(t)P_f^{Z_2}}{\mu(t)P_f^{Z_2} + (1 - \mu(t))P_d^{Z_2}}. \quad (5.21)$$

The belief for next time slot is given is as in (5.18) and the residual energy for next time slot is the same as in (5.19).

Case 3: $D_i = Z_1$ or Z_2 & $l_i = Z_3$ then stay silent. The belief that the PU is absent in the current time slot is updated using Bayes' rule as

$$\mu^*(t) = \frac{\mu(t)P_f^{Z_3}}{\mu(t)P_f^{Z_3} + (1 - \mu(t))P_d^{Z_3}}. \quad (5.22)$$

The belief for next time slot is given is as in (5.18) and the residual energy for next time slot is the same as in (5.19).

Case 4: $D_i = Z_1$ or Z_2 & $l_i = Z_4$ then stay silent. The belief that the PU is absent in the current time slot is updated using Bayes' rule as

$$\mu^*(t) = \frac{\mu(t)P_f^{Z_4}}{\mu(t)P_f^{Z_4} + (1 - \mu(t))P_d^{Z_4}}. \quad (5.23)$$

The belief for next time slot is given is as in (5.18) and the residual energy for next time slot is the same as in (5.19).

Case 5: $D_i = Z_1$ or Z_2 & $l_i = Z_1$ then transmit. The belief that the PU is truly absent in the current time slot is given by Bayes' rule as

$$\mu^*(t) = \frac{\mu(t)(1 - P_f^{Z_1})}{\mu(t)(1 - P_f^{Z_1}) + (1 - \mu(t))(1 - P_d^{Z_1})}. \quad (5.24)$$

The residual energy at the CR user for the next time slot is given as

$$e_{rem}(t+1) = \min\{e_{cap}, e_{rem}(t) - e_r^j - e_s + e_n\} \quad (5.25)$$

where $j \in (1,2)$

The belief that the PU will be absent in the next time slot is given as

$$\mu(t+1) = P_{01}. \quad (5.26)$$

Case 6: $D_t = Z_2$ or Z_2 & $l_1 = Z_1$ then transmit. The belief that the PU is truly absent in the current time slot is given by Bayes' rule as

$$\mu^*(t) = \frac{\mu(t)(1 - P_f^{Z_2})}{\mu(t)(1 - P_f^{Z_2}) + (1 - \mu(t))(1 - P_d^{Z_2})}. \quad (5.27)$$

The residual energy at the CR user for the next time slot and the belief are given in (5.23) and (5.24).

Based on the ACK signal, the rewards are assigned if case 5 and 6 occur on the basis of (5.9).

5.5 Simulation Results

In this section the performance of the proposed actor-critic algorithm based sensing and transmission framework is calculated through simulations. In the simulation the proposed scheme is compared with an exhaustive search scheme where the reward brought by each action in each state is calculated and the best is selected rather than finding the transition probabilities for each state to another state. This scheme also supposes infinite battery capacity where the maximum transmission power is available in each transmission slot. This scheme can be considered as an upper bound for the proposed scheme.

For simulating the proposed scheme the maximum battery capacity is assumed to be 110 packets, the initial value of residual energy is 50 packets, the energy spend on spectrum sensing is 3 packets, e^1 is considered to be the available energy divided by the 10 and e^2 is the available energy divided by 5. The time slot duration is 200 ms and the sensing duration is eight of the total slot duration. The probability of detection is 0.9 and false alarm probability is 0.1 while the initial belief for PU is 0.5. The state transition probabilities of the channel are 0.2. γ is considered 0.4 while χ is 0.3.

Figure 5.3 presents the comparison of the proposed scheme with the exhaustive search scheme. It can be seen from the figure that the proposed scheme closely follows the exhaustive search scheme which acts as the upper bound for the proposed scheme. At a very low SNR of -9 dB the proposed scheme starts to converge and the behavior is the same as the upper bound. The exhaustive search scheme rather than taking an optimized decision search the subspace of available actions and thus the one selected is the global optimum. The proposed scheme on the other hand may at best converge to a locally optimal policy and thus there always is a gap even after the training converges to an optimal value function and policy. As the subspace of all available actions are checked through and all the reward brought by all possible next states is calculated in the exhaustive search scheme it is computationally expensive. The proposed scheme on the other hand has less computational complexity but gives a performance closely following the upper bound.

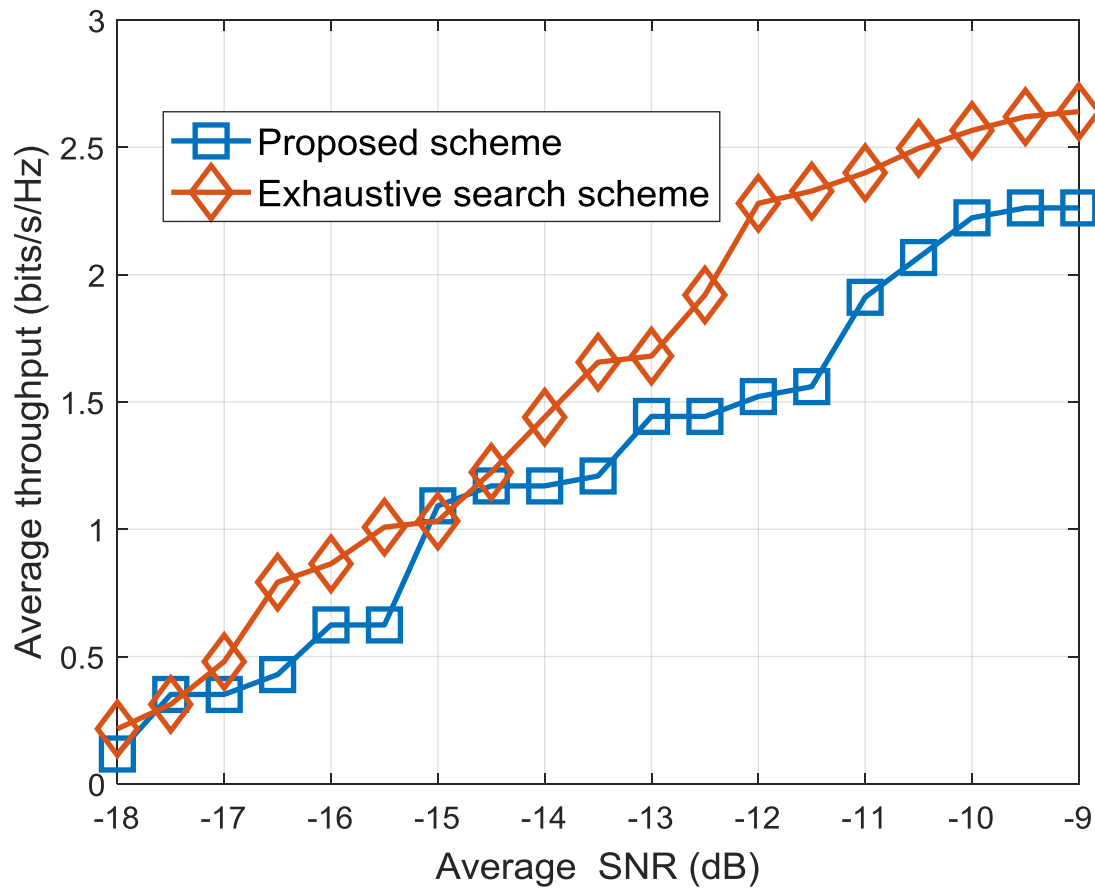


Figure 5.3 Average throughput of the system

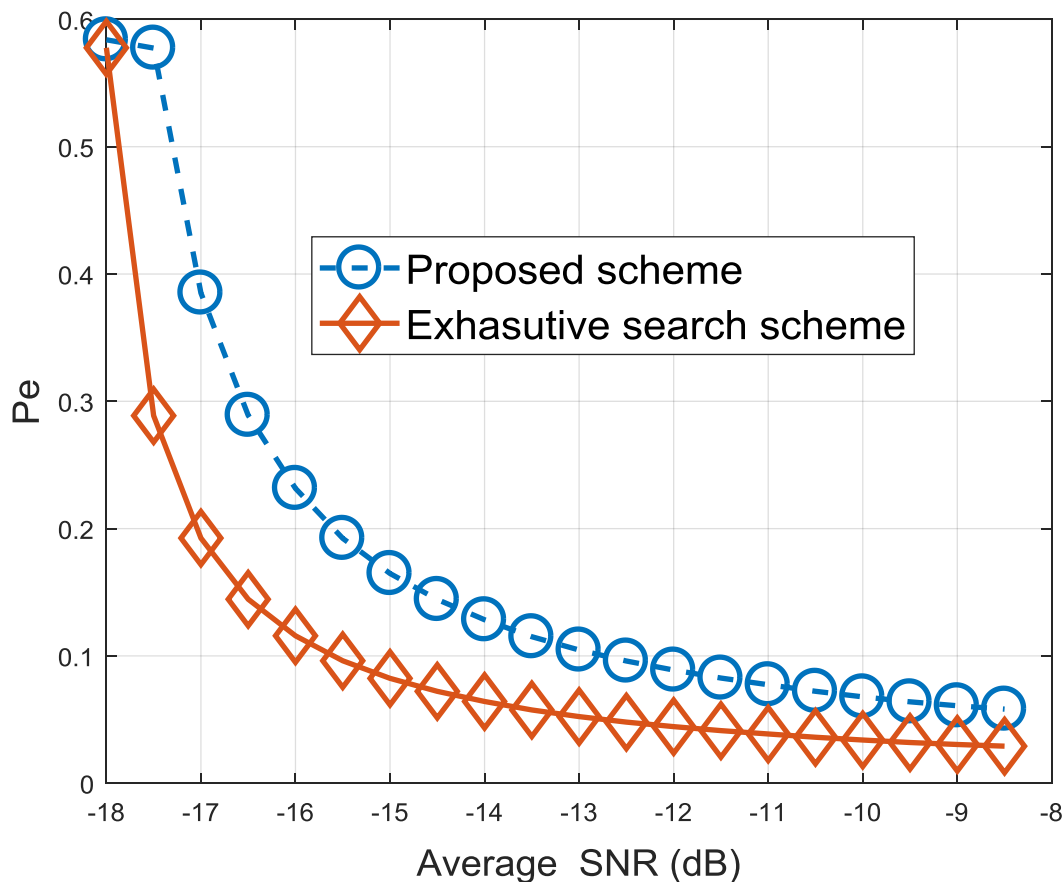


Figure 5.3 Comparison of probability of error

Figure 5.4 presents the probability of error which is represented by Pe . It consists of both the false alarm error and the errors which are result of misdetection. Though both the scheme follows the same quantization based sensing scheme the error performance of the exhaustive search scheme is better than the proposed scheme because the proposed scheme is based on estimating the next state while the exhaustive search scheme checks the reward brought by all the next possible states and select the best one. In that scenario the exhaustive search scheme assumes knowledge of all the possible states. Moreover, for both the results presented exhaustive search schemes assumes infinite battery capacity. While the CR users in the proposed scheme will not be able to sense and thus will miss on sensing and transmission opportunities the exhaustive search scheme can sense and if possible transmit in every time slot. The infinite battery capacity results in higher throughput as it is possible to transmit with the maximum transmission power each time. It also results in a good error performance because of never running out of sensing energy. Even after the

proposed scheme having energy constraint is closely following the upper bound and converges to it in the case of error performance of as low SNR as -9 dB.

5.6 Conclusion

In this chapter a joint sensing and transmission framework was considered. The state transition probabilities from one state to the other and the set of available actions are determined through the sensing result and the residual energy. This allows for a robust framework where the CRN ensures that there is energy available for future slots while achieving throughput in the current slot. Actor-critic algorithm is formulated to decide the next state and the transmission energy if there is transmission. The value function takes care to come up with an optimal policy which is to associate an optimal action with each state. After the training is complete there is an optimal policy function as the environment is learnt through interplay of actor and critic functions.

Chapter 6

A novel physical layer security scheme in OFDM-based cognitive radio networks

6.1 Introduction

Ozarow and Wyner [71] showed that perfectly secure information can be communicated at a nonzero rate from source to destination, while leaving the eavesdropper unable to learn anything about the information being communicated, referred to as secrecy rate. It is defined as the difference between the transmission rate of the source–destination link and the source–eavesdropper link. A simple but efficient way to increase the secrecy rate in communications systems is with the use of artificial noise [72]. The decoding capability of the eavesdropper is degraded by introducing controlled interference into the eavesdropper link. When users in a communication are restricted to having one antenna, then an array of external relays can be employed where some relays forward the received information to the destination and others send a jamming signal against the eavesdropper. The power of the relay that forwards the received information, combined with the jamming power of the relay that functions as a jamming relay node, causes interference with PU communications. In the context of an OFDM-based CRN, providing physical layer security becomes a hard problem. Along with subcarrier mapping over different hops, power allocation at the source, the forwarding relaying node, and the jamming relay node becomes crucial for the secrecy rate of the system under a maximum interference constraint.

Optimal power allocation schemes for minimizing symbol error rates and outage probability, respectively, for a multi-node relay transmission were carried out by Sadek et al. [73] and Seddik et al. [6]. But these schemes are not applicable in the context of a CRN, as the schemes designed by Sadek et al. [73] and Seddik et al. [74] may violate the interference constraints that safeguard the communications of primary users. We are investigating physical layer security for an OFDM-based CRN. The transmitter embeds artificial noise in its transmission, which is designed to avoid interference with the legitimate

receiver and only harm the eavesdropper [75]-[77]. However, those various schemes [75]-[77] consider multiple antennas, and artificial noise cannot be used in a system where the nodes have only one antenna. In ad-hoc networks and CRNs, the nodes are assumed to be of low complexity with fewer computational resources. So, to provide physical layer security in a CRN, external relays that act as jammers can be employed. This approach is referred to as cooperative jamming.

Authors in [78] considered physical layer security in underlay full duplex cognitive radio system while the secrecy performance of full duplex multi-antenna wiretap networks in presence of a jammer was analyzed by [79]. Some other works [80]-[82] have also discussed basic schemes using multiple external relays for cooperative jamming. The optimal design of cooperative jamming relay weights to maximize the secrecy rate was investigated by Zheng et al. [83]. A combination of two relays, where one relay forwards the transmitted signal while the other relay acts as a cooperative jammer, was discussed by Krikidis et al. [84]. Ding et al. [85] combined cooperative jamming with interference alignment. Beamforming for improving secrecy capacity was investigated by Wang et al. [86]. The schemes and works discussed here cannot be directly applied to CRNs because of their different contexts. CRNs have special features: (1) the PU always has first priority when using the spectrum in a CRN, and (2) it is unreasonable to assume that the PU always cooperates with CR users unconditionally. Lee et al. [87] studied a cooperation-based access strategy that improves the secrecy rate of the primary link but at the cost of employing multiple antennas. A low-complexity but efficient solution needs to be investigated, where a minimum number of relays with a single antenna are employed.

Subcarrier assignment and power allocation to subcarriers are the most important parameters on which the capacity and performance of OFDM systems depend. Mu et al. [88] studied joint subcarrier assignment and power allocation for decode-and-forward multi-relay OFDM systems. The problem was formulated as joint optimization of three types of resources (subcarrier, power, and relay) and was solved through dividing the optimization problem into sub-problems with dual relations. In a study by Ho et al. [89] each node was constrained by the maximum power allowed, and a power-allocation scheme was proposed for an OFDM-based two-way relay link. Interference with the PU is the foremost design constraint in a CRN. Jitvanichphaibool et al. [90] proposed a scheme that suppresses interference with the primary user by employing multi-antenna relay nodes. Bansal et al. [91] studied power allocation in an OFDM-based CRN, and Yan and Wang [92] extended the work to a relay-aided transmission scenario, and proposed a sub-optimal algorithm that optimizes both source and relay power. Relay assignment also affects the performance of OFDM-based multi-relay systems. Jia et al. [93] proposed an optimal strategy for spectrum allocation and relay assignment. As described earlier, a new degree of freedom is allowed for

resource allocation in multi-hop OFDM networks as the subcarriers that face deep fading over one hop may not experience deep fading over another hop. The concept of subcarrier-mapping was first introduced by Herdin [94], who showed that system throughput can be enhanced if the subcarriers of two hops are coupled in order of magnitude. Hammerstrom and Wittneben [95] and Li et al. [96] considered joint power allocation and subcarrier matching in amplify-and-forward, and decode-and-forward networks, respectively.

In underlay cognitive radios managing the interference caused to legitimate transmissions is of utmost importance. Interference alignment based strategies are employed to zero-cross the interference caused to the CR receiver. Interference alignment is the concept where multiple interfering signals are consolidated into a small subspace at the receiver so that the number of interference-free dimensions remaining for the desired signal can be maximized [97]. Interference alignment (IA) is adopted to analyze the precise secure degree of freedom of many kinds of wireless networks based on information theoretic aspect [98]-[100]. Nevertheless the physical layer security aspects of IA-based wireless networks have received very little attention in the literature. Zhao et al. [81] studied the systematic analysis of physical layer security of IA-based networks. The concept of artificial noise (AN) can be used together with the idea of IA in low signal to noise ratio (SNR) regimes in underlay cognitive radio networks to improve to increase the secrecy throughput. Introducing AN and aligning the interference caused by the AN can degrade the throughput performance of the wireless networks which is rectified by using the spectrum opportunistically.

As explained earlier, abiding by the interference threshold and the co-existence of CR user and PU on the same spectrum band are hard problems, which become harder when secrecy of the communication is considered. In this paper, we consider physical layer security and formulate a novel physical layer–security scheme for OFDM-based CRNs under maximum interference constraints and total power constraints. Power and subcarrier mapping optimization is carried out to maximize the secrecy rate. An optimal power allocation algorithm is proposed that maximizes the CR system secrecy capacity under maximum interference and power constraints. The interference constraint protects the PU communications from harmful interference, and thus, guarantees co-existence in the same spectrum of both the PU and CR users. The interference constraint can be seen as a way of interference alignment. The interference caused is such that it causes maximum damage to the external eavesdropper’s signal while the interference caused by the jamming signal to the legitimate transmissions is managed by aligning the level of power allocated at the forwarding relaying node and the jamming relay node. The maximum power constraint is motivated by the fact that in sensor networks and ad-hoc systems like a CRN, long-term power consumption is a major

concern; so, restricting the total transmission power is an effective way to satisfy the long-term power constraint. In our proposed scheme, one relay, known as forwarding relaying node, forwards the source information, and the other, known as jamming relay node, sends a jamming signal against the eavesdropper. On the forwarding relaying node which forwards the source information, subcarrier mapping is also performed so as to reduce the total interference with the PU and to maximize the secrecy rate. Using maximum interference and power constraints, optimal power allocation (PA) is formulated at the forwarding relaying node, which maximizes the CR system secrecy rate. Since the optimal PA problem is non-convex, it is difficult to find a global optimal solution. First the maximum transmission power constraint is relaxed to simplify the PA problem, and a closed form solution is obtained. The maximum transmission power constraint is satisfied after the closed-form solution is derived for the simplified optimization problem by using the Cauchy-Shwartz inequality. Finally, based on the closed-solution of the simplified optimization problem, a sub-optimal PA scheme is proposed that satisfies both the maximum interference constraint and the maximum transmission power constraint. PA is also performed at the source and at the jamming relay node in order to satisfy the maximum interference constraint and the maximum transmission power constraint.

Our proposed scheme seamlessly combine AN with IA. The power allocation scheme at both jamming relay node and the forwarding relaying node takes into consideration the effect of interference caused. The power allocated at source implicitly takes into consideration the interference caused to the PU. The power allocation scheme at the forwarding relaying node takes into consideration the power allocated at the jamming relay node and thus the level of interference which the jamming relay node can cause to the legitimate destination is managed. This can be seen as interference alignment at the forwarding relaying node. The subcarrier mapping done at the forwarding relaying node is meant to reduce leakage of useful information to the eavesdropper. The interference caused by jamming signal is aligned at the forwarding relaying node implicitly and thus the AN generated is made to affect to eavesdropper only.

The rest of this chapter is divided as follows. Section 2 presents the system model and the problem formulation. Section 3 discusses the problem in detail and presents our proposed solution. Section 4 deals with results and analysis of our proposed scheme, while Section 5 concludes the chapter.

6.2 System Model and Problem Formulation

Section 6.2.1 presents our proposed system model, Section II-B presents the constraints on our optimization problem, and Section II-C formulates our given problem.

6.2.1 System Model

We consider a CR system with one CR sender (known as the source), one CR destination, and two relays, as shown in Fig. 6.1. We assume that the destination is located far outside the transmission range of the source, and thus, cannot directly receive the source communication. A relay network consisting of two relays is proposed. The forwarding relaying node forwards the received signal to the destination, and the jamming relay node, sends a jamming signal to affect the signal received by an eavesdropper. We assume that the forwarding relaying node is a dedicated relay node which has more and computational resources as compared to ad-hoc nodes.

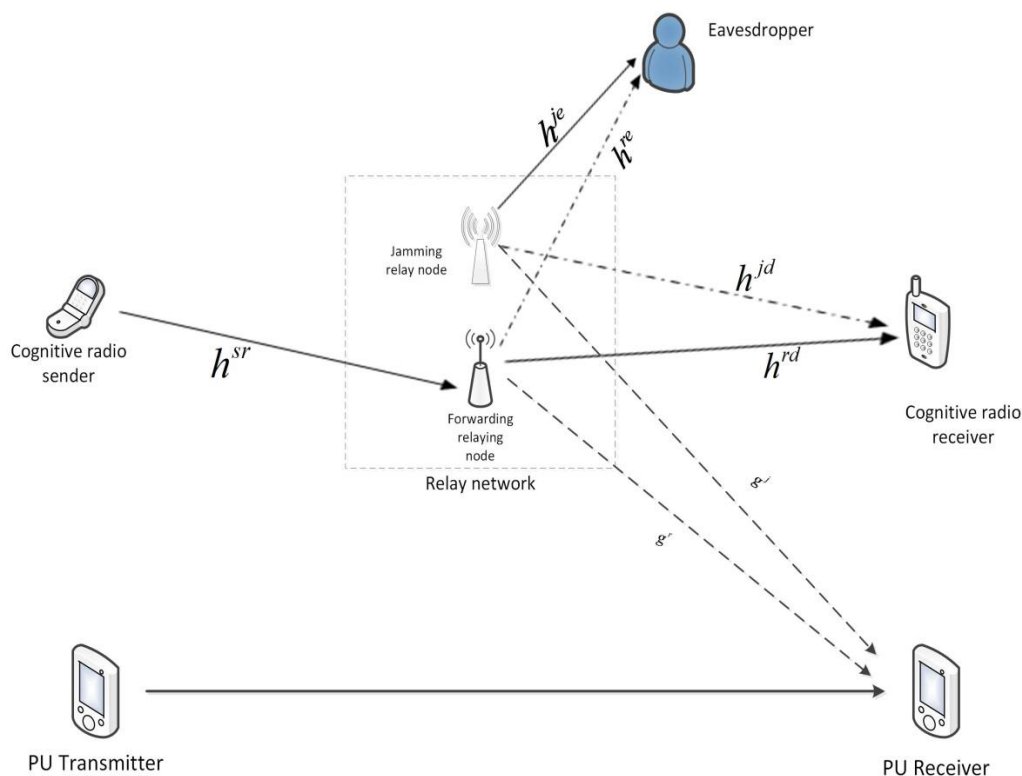


Figure 6.1 The system model

In the first phase of communication, the source transmits to the relay network. In the second phase, the forwarding relaying node sends the received data using amplify-and-forward protocol to the destination, and the jamming relay node broadcasts an artificial jamming signal. The power allocated to the subcarriers at the forwarding relaying node and the jamming relay node is optimized so the secrecy rate of the CR system is maximized. In the first phase, interference with the PU's communications is caused by transmission of the source. In the second phase, interference with the PU is caused by both the forwarding relaying node's transmission and the jamming relay node's transmission. Power is allocated in both the first phase and the second phase such that interference with the PU is below the interference threshold.

We assume an underlay CR transmission where the whole PU spectrum is accessible to the CR system, given that interference with the PU system is less than the interference threshold. The interference caused to the PU as well as the interference caused to the CR receiver is managed through interference alignment in power allocation at the source and forwarding relaying node. The overall power allocation at the jamming relay node and forwarding relaying node is designed in a way to align the interference caused to the legitimate transmission is taken into consideration at forwarding relaying node. We assume that instantaneous channel information is available, and channel coefficients for all links are known a priori. Practical considerations, like using statistical channel knowledge or erroneous channel knowledge and finding the gain of the eavesdropper, are outside the scope of this work. PU communications is not considered in this work other than that the interference caused by the CR transmission should be less than an interference constraint. The physical medium is accessed via OFDM, and thus, all the links have multiple orthogonal subcarriers.

In the first phase, the CR source transmits to the relay network, and the transmission rate at the forwarding relaying node, denoted by R_r , is given by [13]

$$R_r = \log_2(1 + \gamma) \quad (6.1)$$

where $\gamma = \frac{\sum_{i=1}^N P_i^s |h_i^{sr}|^2}{N_0}$. P_i^s is the power allocated at the source to the i -th subcarrier, h_i^{sr} is the channel gain between source and forwarding relaying node for the i -th subcarrier, N is the total number of subcarriers, and N_0 is additive white Gaussian noise (AWGN).

In the second phase, the forwarding relaying node forwards the received message to the destination. The transmission rate at the CR receiver, R_d , is given by [13][101]

$$R_d = \frac{1}{2} \log \left[I + \frac{P_s}{N_0} \frac{\left(\frac{\sum_{i=1}^N |h_i^{sr} h_i^{rd}| \sqrt{P_i^r}}{\sqrt{P_i^s} |h_i^{sr}|^2 + N_0} \right)^2}{I + \sum_{i=1}^N \left(\frac{|h_i^{rd}| \sqrt{P_i^r} |h_i^{je}| \sqrt{P_i^j}}{\sqrt{P_i^s} |h_i^{sr}|^2 + N_0} \right)^2} \right] \quad (6.2)$$

where P_s is the combined power as allocated to all subcarriers at the source, h_i^{rd} is the channel gain for the i -th subcarrier between the forwarding relaying node and destination, P_i^r is the power allocated to the i -th subcarrier at the forwarding relaying node, h_i^{je} is the channel gain between the jamming relay node and the eavesdropper for the i -th subcarrier, P_i^j is the power allocated to the i -th subcarrier at the jamming relay node, and the factor $\frac{1}{2}$ is due to two time slots taken for a complete transmission from source to destination.

The eavesdropper also receives the signal from the forwarding relaying node along with the jamming signal. The eavesdropper may be able to extract some useful information from the received signal. The transmission rate or throughput at the eavesdropper is represented by R_e and is given as [13] [101]

$$R_e = \frac{1}{2} \log \left[I + \frac{P_s}{N_0} \frac{\left(\frac{\sum_{i=1}^N |h_i^{sr} h_i^{re}| \sqrt{P_i^r}}{\sqrt{P_i^s} |h_i^{sr}|^2 + N_0} \right)^2}{I + \sum_{i=1}^N \left(\frac{|h_i^{re}| \sqrt{P_i^r} |h_i^{je}| \sqrt{P_i^j}}{\sqrt{P_i^s} |h_i^{sr}|^2 + N_0} \right)^2} \right] \quad (6.3)$$

where h_i^{re} is the channel gain of the link between the forwarding relaying node and the eavesdropper for the i -th subcarrier. The secrecy rate is denoted by R_{sec} and by definition is given as [13]

$$R_{\text{sec}} = [R_d - R_e]^+ \quad (6.4)$$

where $[\cdot]^+$ identifies that the secrecy rate cannot be negative i.e. $R_{\text{sec}} = \max[R_d - R_e, 0]$.

Our main objective is to maximize the secrecy rate of the CR system, as given in (4). In the next section, the constraints on the maximization problem are explained.

6.2.2 System Constraints Definitions

Each subcarrier from the first hop is mapped to one subcarrier from the other hop. As explained earlier, channel condition for a subcarrier over one hop may change over the next hop. So, instead of forwarding the data received at the forwarding relaying node using the same subcarrier, the channel conditions of the link from forwarding relaying node to destination and forwarding relaying node to eavesdroppers can be taken into consideration in subcarrier mapping at the forwarding relaying node. We exploit this phenomenon to maximize the secrecy rate of the CR system. Let us define a binary mapping variable as

$$\ell_{(k,m)} = \begin{cases} 1, & \text{if } k\text{-th subcarrier of the first hop is} \\ & \text{assigned to } m\text{-th subcarrier of the} \\ & \text{second hop} \\ 0, & \text{otherwise.} \end{cases} \quad (6.5)$$

Another form of subcarrier mapping function can be given as

$$\sum_{k=1}^N \ell_{(k,m)} = 1, \quad \forall m, \quad \sum_{m=1}^N \ell_{(k,m)} = 1, \quad \forall k. \quad (6.6)$$

To ensure long-term power availability, the transmission power at the source, the forwarding relaying node, and the jamming relay node should satisfy a maximum power constraint. The maximum power constraint also takes into account the current amount of power available when determining the optimal transmit power. The power constraint at the source is given as

$$0 \leq P_i^s \leq P_s^{\max} \quad (6.7)$$

where P_s^{\max} is the maximum power available at the CR source. The power constraint at the forwarding relaying node and jamming relay node, respectively, are given as

$$0 \leq P_i^r \leq P_r^{\max} \quad (6.8)$$

and

$$0 \leq P_i^j \leq P_j^{\max} \quad (6.9)$$

where P_r^{\max} is the maximum power available at the forwarding relaying node, and P_j^{\max} is the maximum power available at the jamming relay node.

Under our system model, interference with the PU transmission is caused in both the first phase and the second phase of communications. The interference caused in the first phase is because of the source transmission, and so, the transmission should satisfy the maximum interference limit, which is given as

$$\sum_{i=1}^N |g_i^s|^2 P_i^s \leq I_{max} \quad (6.10)$$

where I_{max} is the maximum allowable interference threshold, and g_i^s is the channel gain between the source and PU transmitter for the i -th subcarrier. In the second phase, the interference is caused by both forwarding relaying node and jamming relay node transmissions. The combined interference caused in the second phase should satisfy the maximum allowable interference threshold as

$$\sum_{i=1}^N |g_i^r|^2 P_i^r + \sum_{i=1}^N |g_i^j|^2 P_i^j \leq I_{max} \quad (6.11)$$

where g_i^r is the channel gain for the i -th subcarrier between the forwarding relaying node and the PU transmitter, and g_i^j is the channel gain for the link between the jamming relay node and the PU transmitter for the i -th subcarrier.

6.2.3 Problem Formulation

Our aim is to optimize the source power, forwarding relaying node power, and jamming relay node power, and to map subcarriers of the two hops so as to maximize the secrecy rate of the CR system. Power allocation in our system model is not a trivial problem. In traditional OFDM systems and in overlay CRNs, where the CR users access the spectrum if it is not used by the PU, the increase in power allocation increases the system throughput. But in our system model, increasing the power at the source may cause an increase in interference with the PU transmission. An increase in power at the forwarding relaying node may increase interference with the PU as well, and may result in higher leakage to the eavesdropper; and increasing the transmission power at the jamming relay node may result in higher interference with the CR receiver, as well as increase interference with the PU transmission.

The optimization variables for the subcarriers on the first hop (i.e. for source-forwarding relaying node link and for the second hop (i.e. for forwarding relaying node-destination link) can be given mathematically as $\mathbf{P}^s = \{P_i^s \geq 0\}$, $\mathbf{P}^r = \{P_i^r \geq 0\}$, $\mathbf{P}^j = \{P_i^j \geq 0\}$ and $\ell = \{\ell_{(k,m)} \in \{0,1\}\}$ where \mathbf{P}^s is a vector representing the power allocated to the subcarriers at the CR sender, \mathbf{P}^r is a vector representing power allocated to the subcarriers at the forwarding relaying node while \mathbf{P}^j is a vector representing power

allocated to the subcarriers at the jamming relay node. With these optimization variables, the optimization problem (OP) is given as

$$OP: \max_{\mathbf{P}^s, \mathbf{P}^r, \mathbf{P}^j, \ell} \sum_{k=1}^N \sum_{m=1}^N \ell_{(k,m)} R_{\text{sec}}(k, m) \quad (6.12)$$

s. t. (6) - (11).

6.3 Power Allocation and Subcarrier Mapping Scheme

The OP as presented in (6.12) is divided into four sub-problems. The first sub-problem is to allocate optimal power to the subcarriers at the forwarding relaying node, the second sub-problem is to allocate optimal power at the jamming relay node, the third sub-problem becomes optimal power allocation at the source, and the fourth sub-problem is optimal subcarrier mapping. Since the logarithm in (6.12) is a monotonically increasing function of power, the power allocation parts can be separated, and the OP in terms of power allocation can be given as

$$\mathbf{P}^* = \max_{\mathbf{P}^s, \mathbf{P}^r, \mathbf{P}^j} \sum_{k=1}^N \sum_{m=1}^N R_{\text{sec}}(k, m) \quad (6.13)$$

s. t. (7) - (11).

where $\mathbf{P}^* = \{\mathbf{P}_s^*, \mathbf{P}_r^*, \mathbf{P}_j^*\}$. \mathbf{P}_s^* is the optimal source power vector, \mathbf{P}_r^* is the optimal power at the forwarding relaying node vector, and \mathbf{P}_j^* is the optimal power vector at the jamming relay node as allocated to the subcarriers.

We consider optimal power allocation at the forwarding relaying node the first sub-problem. The optimal power at the forwarding relaying node is given by

$$\mathbf{P}_r^* = \arg \max_{\mathbf{P}_r} \left\{ \frac{\mathbf{P}_s}{N_0} \frac{\left(\frac{\sum_{i=1}^N |h_i^{sr} h_i^{rd}| \sqrt{\mathbf{P}_i^r}}{\sqrt{\mathbf{P}_i^s |h_i^{sr}|^2 + N_0}} \right)^2}{1 + \sum_{i=1}^N \left(\frac{|h_i^{rd}| \sqrt{\mathbf{P}_i^r} |h_i^{je}| \sqrt{\mathbf{P}_i^j}}{\sqrt{\mathbf{P}_i^s |h_i^{sr}|^2 + N_0}} \right)^2} \right\} \quad (6.14)$$

s. t. (8) and (11).

For the sake of simplicity, let $\alpha_i = |h_i^{sr}|^2$, $\beta_i = |h_i^{rd}|^2$, $\lambda_i = |h_i^{jd}|^2$, $w_i = |g_i^r|^2$, $v_i = |g_i^j|^2$, $\sigma_i = \frac{P_i^j}{P_i^r}$, $u_i = \frac{v_i P_i^j}{\sigma_i}$ and

$\gamma_i = \frac{\beta_i}{\alpha_i P_i^s + N_0}$. Equation (14) can be expressed in terms of α_i , β_i , λ_i , w_i , v_i and γ_i as

$$\mathbf{P}_r^* = \arg \max_{\mathbf{P}^r = \{P_1^r, P_2^r, \dots, P_N^r\}} \frac{\left(\sum_{i=1}^N \left(\sqrt{\alpha_i \gamma_i} \sqrt{P_i^r} \sqrt{P_i^j} \right) \right)^2}{1 + \sum_{i=1}^N \gamma_i \lambda_i P_i^r P_i^j} \quad (6.15)$$

subject to

$$0 \leq P_i^r \leq P_{\max}^r \quad (6.16)$$

and

$$\sum_{i=1}^N (w_i P_i^r + v_i P_i^j) \leq I_{\max}. \quad (6.17)$$

The objective function in (6.15) is a non-convex function of P_i^r . It is difficult to obtain a global optimal solution. The local optimal solution can be obtained by using the integer point method (IPM). The transmission power at the forwarding relaying node is not only restricted by maximum transmission power but also by the maximum interference constraint. In order to simplify the optimization problem, the maximum power constraint in (6.16) can be relaxed. After we derive a closed-form solution for the simplified problem in (6.15) using the Cauchy-Schwartz inequality, then the maximum transmission power constraint will be guaranteed.

To solve the optimal power allocation at the forwarding relaying node, the constraint given in (6.17) is used as the only constraint on the optimization problem in (6.15). The optimal solution of (6.15) is not possible if the constraint in (6.17) is not followed with strict equality. If the constraint in (6.15) is not followed by strict equality then for every solution there can exist another solution which is a linear combination of the previous solution. The new solution can be obtained by multiplying the previous solution with a constant C and which will result in higher value of the objective function in (6.15). Thus, (6.17) becomes

$$\sum_{i=1}^N (w_i P_i^r + v_i P_i^j) = I_{\max}. \quad (6.18)$$

Using (17), the objective function in (15) can be written as

$$\begin{aligned} \frac{\left(\sum_{i=1}^N \left(\sqrt{\alpha_i \gamma_i} \sqrt{P_i^r} \sqrt{P_i^j} \right) \right)^2}{1 + \sum_{i=1}^N \gamma_i \lambda_i P_i^r P_i^j} &= \frac{\left(\sum_{i=1}^N \left(\sqrt{\alpha_i \gamma_i} \sqrt{P_i^r} \sqrt{P_i^j} \right) \right)^2}{\frac{\sum_{i=1}^N (w_i P_i^r + v_i P_i^j)}{I_{\max}} + \sum_{i=1}^N \gamma_i \lambda_i P_i^r P_i^j} \\ &= \frac{\left(\sum_{i=1}^N \left(\sqrt{\alpha_i \gamma_i} \sqrt{P_i^r} \sqrt{P_i^j} \right) \right)^2}{\sum_{i=1}^N \left\{ \left(\frac{w_i + v_i}{\frac{P_i^j + P_i^r}{I_{\max}} + \gamma_i \lambda_i} \right) P_i^r P_i^j \right\}}. \end{aligned} \quad (6.19)$$

To express (19) simply, we define two new variables as

$$z_i = \sqrt{\left(\gamma_i \lambda_i + \frac{W_i + V_i}{I_{\max}} \right)} \sqrt{P_i^r P_i^j} \quad (6.20)$$

and

$$d_i = \sqrt{\frac{\alpha_i \gamma_i}{\lambda_i \gamma_i + \frac{W_i + V_i}{I_{\max}}}} \quad (6.21)$$

where $W_i = \frac{w_i}{P_i^j}$ and $V_i = \frac{v_i}{P_i^r}$. Two vectors are formed as $\mathbf{z} = [z_i]$ and $\mathbf{d} = [d_i]$ [102]. By applying these two

vectors, the objective function in (18) can be represented in vector form as

$$\mathbf{P}_r^* = \arg \max_{\mathbf{z} = f(\mathbf{p}^r)} \frac{(\mathbf{d}^T \mathbf{z})^2}{\mathbf{z}^T \mathbf{z}}. \quad (6.22)$$

The optimal solution of (22) can be found by the Cauchy-Schwartz inequality. Furthermore according to [101], the optimal solution can then be given if \mathbf{z} and \mathbf{d} are linearly dependent as

$$z_i^* = kd_i. \quad (6.23)$$

Putting value of d_i from (21), eq. (23) becomes

$$(z_i^*)^2 = k^2 \left(\frac{\alpha_i \gamma_i}{\lambda_i \gamma_i + \frac{W_i + V_i}{I_{\max}}} \right). \quad (6.24)$$

Eq. (20) can be written for z_i^* as

$$\begin{aligned} (z_i^*)^2 &= \left(\gamma_i \lambda_i + \frac{W_i + V_i}{I_{\max}} \right) P_i^r P_i^j \\ (z_i^*)^2 I_{\max} &= (I_{\max} \gamma_i \lambda_i + W_i + V_i) P_i^r P_i^j \\ P_i^r P_i^j &= \frac{(z_i^*)^2 I_{\max}}{I_{\max} \gamma_i \lambda_i + W_i + V_i} \\ (W_i + V_i) P_i^r P_i^j &= \frac{(z_i^*)^2 I_{\max}}{I_{\max} \gamma_i \lambda_i + W_i + V_i} (W_i + V_i) \\ (z_i^*)^2 &= \frac{\{(W_i + V_i) P_i^r P_i^j\} \{I_{\max} \gamma_i \lambda_i + W_i + V_i\}}{I_{\max} (W_i + V_i)}. \end{aligned} \quad (6.25)$$

Eq. (6.24) can be rewritten when the value of $(z_i^*)^2$ from (6.25) as

$$\begin{aligned} (w_i P_i^r + v_i P_i^j) &= k^2 \left(\frac{\alpha_i \gamma_i}{I_{\max} \lambda_i \gamma_i + W_i + V_i} \right) \times \frac{I_{\max}^2}{I_{\max} \gamma_i \lambda_i + W_i + V_i} (W_i + V_i) \\ 1 &= \frac{k^2 \alpha_i \gamma_i I_{\max} (W_i + V_i)}{(I_{\max} \lambda_i \gamma_i + W_i + V_i)^2}. \end{aligned} \quad (6.26)$$

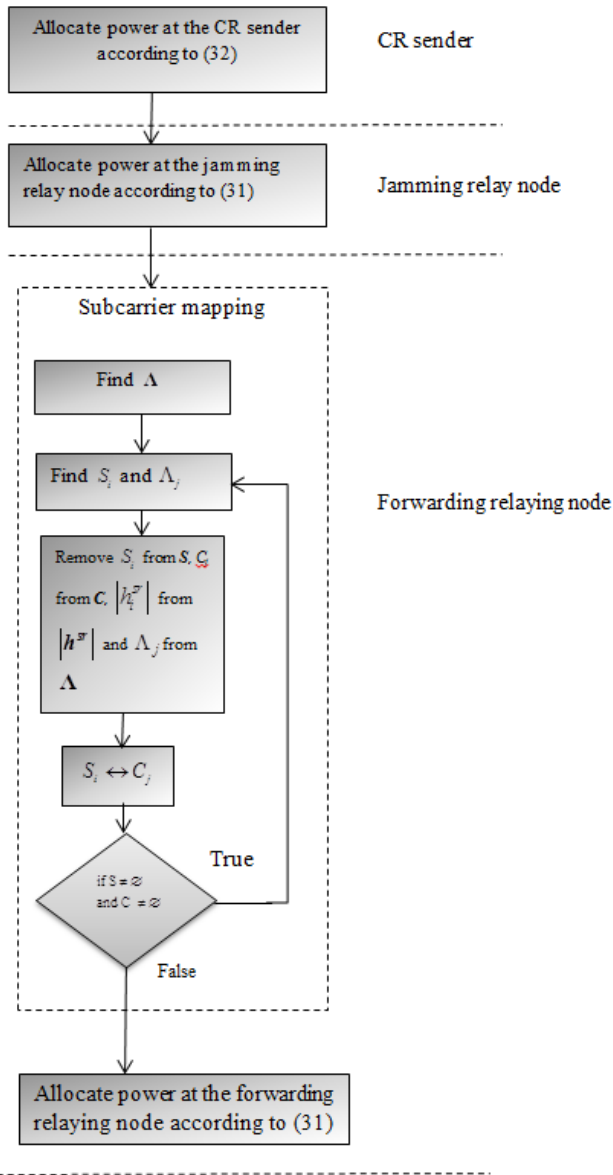


Figure 6.2 Flowchart of the proposed scheme

From (26), for the N subcarriers, k can be given as

$$k = \sqrt{\frac{1}{I_{\max} \sum_{i=1}^N \frac{(W_i + V_i) \alpha_i \gamma_i}{\{(W_i + V_i) + \gamma_i \lambda_i I_{\max}\}^2}}} . \quad (6.27)$$

If $P_{r_i}^*$ is the optimal power allocated to each subcarrier at the forwarding relaying node, then $P_{r_i}^*$ can be represented in terms according to (6.20) as

$$\begin{aligned} P_{r_i}^* &= \frac{(z_i^*)^2}{\lambda_i \gamma_i + \frac{(W_i + V_i)}{I_{\max}} P_i^j} \\ &= \frac{k^2 \frac{\alpha_i \gamma_i}{I_{\max} \lambda_i \gamma_i + (W_i + V_i)} I_{\max}^2}{I_{\max} \lambda_i \gamma_i + (W_i + V_i) P_i^j} . \end{aligned} \quad (6.28)$$

Putting value of k , $P_{r_i}^*$ becomes

$$\begin{aligned} P_{r_i}^* &= \left(\frac{1}{I_{\max} \sum_{i=1}^N \frac{(W_i + V_i) \alpha_i \gamma_i}{\{(W_i + V_i) + \gamma_i \lambda_i I_{\max}\}^2}} \right) \times \\ &\quad \left(\frac{\alpha_i \gamma_i I_{\max}^2}{\{I_{\max} \lambda_i \gamma_i + (W_i + V_i)\}^2 P_i^j} \right) . \\ &= I_{\max} \frac{\frac{\alpha_i \gamma_i}{((w_i + u_i) + \gamma_i I_{\max})^2}}{\sum_{i=1}^N \frac{(w_i + v_i) \alpha_i \gamma_i}{\{(w_i + u_i) + \gamma_i \lambda_i I_{\max}\}^2}} . \end{aligned} \quad (6.29)$$

The equation in (6.29) satisfies the maximum interference constraint only, i.e. the constraint given in (6.17). To satisfy the constraints in (6.16) (i.e. the maximum transmission

power constraint), we propose optimal power allocation at the forwarding relaying node to each subcarrier, represented by $P_{r_i}^{proposed}$, which is given as

$$P_{r_i}^{proposed} = \min(P_{max}^r, P_{r_i}^*). \quad (6.30)$$

In sub-problem 2, the power at the jamming relay node is allocated. The power to all subcarriers at the jamming relay node is allocated equally. Joint optimization of both forwarding relaying node and jamming relay node becomes intractable. The jamming signal affects the signal received by the eavesdropper more than it affects the signal received at the destination. The power allocated at the jamming relay node to each subcarrier is represented by $P_{j_i}^{proposed}$ and is given as

$$P_{j_i}^{proposed} = \eta \frac{P_j^{total}}{N} \quad (6.31)$$

where P_j^{total} is the power available at the jamming relay node, η is a factor that maintains the allocated power at the jamming relay node such that it satisfies (11), and η is selected iteratively.

In sub-problem 3, power is allocated to each subcarrier at the source, represented by $P_{s_i}^{proposed}$, as

$$P_{s_i}^{proposed} = \chi \frac{I_{max}}{g_i^{sp}} \quad (6.32)$$

where χ ensures that the allocated power satisfies the maximum transmission power constraint in (6.7). The maximum interference constraint as given in (6.10) is implicitly satisfied by (6.32).

By (6.32), more power is allocated to links with a good channel condition, and thus, CR system throughput is increased.

In the sub-problem 4, the subcarriers are matched. The channel gain from forwarding relaying node to CR receiver and the channel gain from forwarding relaying node to eavesdropper are good parameters, on the basis of which the secrecy rate can be optimized. In the algorithm presented below, \mathbf{S} is a vector that represents all the subcarriers from the CR source to the

forwarding relaying node, \mathbf{C} is a vector that represents all the subcarriers from the forwarding relaying node to the destination, \mathbf{h}^r is a vector that represents the channel gain for all subcarriers from the source to the forwarding relaying node, \mathbf{h}^{rd} is a vector that represents the channel gain for all subcarriers from the forwarding relaying node to the destination, and \mathbf{h}^e is a vector that represents the channel gain for all subcarriers from forwarding relaying node to eavesdropper. The ratio Λ_i is found out for all the subcarriers from the forwarding relaying node to the destination to calculate the ratio between the gain from the forwarding relaying node to destination and the gain from the forwarding relaying node to eavesdroppers for the subcarriers. Subcarriers having larger value of Λ_i have better gain from forwarding relaying node to destination than from forwarding relaying node to the eavesdropper and hence are better channels. This fact is exploited to map the better subcarriers from source to forwarding relaying node with subcarriers from forwarding relaying node to destination.

The complexity of the proposed algorithm in Algorithm 1 is $O(N)$ where N is the number of subcarriers. Because of the ratio vector $\mathbf{\Lambda}$ as introduced in Algorithm 1, one subcarrier from the CR sender to the forwarding relaying node is matched with a subcarrier from the forwarding relaying node to CR destination in only one iteration. The subcarrier with the maximum channel gain from the CR sender to the forwarding relaying node is matched with the subcarrier from forwarding relaying node to the CR destination which has the best ratio of channel gain from forwarding relaying node to the CR destination to the channel gain from forwarding relaying node to the eavesdropper. Thus, the mapping will be completed in N steps.

The solution to the optimization problem as presented in (6.12) is provided by the equations in (6.29), (6.30), (6.31), and Algorithm 1. Eq. (6.29) presents solution to the first sub-problem which is allocation of power at the forwarding relaying node, (6.30) provides solution to the second sub-problem which is to allocate power at the jamming relay node, (6.31) gives solution to the third sub-problem which is to allocate power at the source while Algorithm 1 presents solution to the fourth sub-problem which is subcarrier mapping at the forwarding relaying node.

Finally, Fig. 6.2 shows the flowchart of the proposed scheme. The labels on the right of the blocks in the flowchart the node at which the operation is carried out. At the forwarding relaying node both Algorithm 1 and the power allocation to subcarriers according to (31) are carried out.

Algorithm 1

$$\mathbf{S} = \{S_1, S_2, \dots, S_N\}$$

$$\mathbf{C} = \{C_1, C_2, \dots, C_N\}$$

Inputs: $|\mathbf{h}^{sr}| = \{|h_1^{sr}|, |h_2^{sr}|, \dots, |h_N^{sr}|\}$

$$|\mathbf{h}^{re}| = \{|h_1^{re}|, |h_2^{re}|, \dots, |h_N^{re}|\}$$

$$|\mathbf{h}^{rd}| = \{|h_1^{rd}|, |h_2^{rd}|, \dots, |h_N^{rd}|\}$$

1. Find $\Lambda_i = \frac{|h_i^{rd}|}{|h_i^{re}|}$ where $i = \{1, 2, \dots, N\}$. Form a vector as $\mathbf{\Lambda} = \{\Lambda_1, \Lambda_2, \dots, \Lambda_N\}$. 2. From $|\mathbf{h}^{sr}|$ find $|h_i^{sr}| = \max\{|h^{sr}|\}$. The subcarrier having the channel gain $|h_i^{sr}|$ is S_i . From $\mathbf{\Lambda}$ find $\Lambda_j = \max\{\mathbf{\Lambda}\}$. The subcarrier corresponding to Λ_j is C_j . Remove S_i from \mathbf{S} , C_j from \mathbf{C} , $|h_i^{sr}|$ from $|\mathbf{h}^{sr}|$ and Λ_j from $\mathbf{\Lambda}$.

3. Map S_i and C_j as

$$S_i \leftrightarrow C_j$$

4. if $\mathbf{S} \neq \emptyset$ and $\mathbf{C} \neq \emptyset$
Go to Step 2.

6.4 Results and Discussion

We carried out a number of simulations to verify the performance of our proposed scheme. The simulation platform used was Matlab R2017a. We assumed that the channel coefficients undergo Rayleigh fading. We also assumed that all the subcarriers face independent Rayleigh fading, both in the CR system and from the CR system to the PU system, and that the channel gains are also independent from each other. A fixed broadband wireless channel with 1 MHz bandwidth is assumed for the simulation. The noise spectrum density is set to 4.14×10^{-21} W/Hz [88]. The path loss exponent in the Rayleigh fading model is considered to be 4 which represents worst case scenarios for cellular and long-distance communications and as the value of the path loss exponent reduces, the corresponding performances can be improved [103][104]. In the simulation, the product of spectrum bandwidth and time period is assumed to be one unit. The maximum transmission power constraint is assumed to be the same at the CR source, the forwarding relaying node, and the jamming relay node, for the sake of simplicity.

We consider three types of schemes, against which we compare our proposed scheme. The first scheme is a mapping with equal power allocation scheme, which is a variant of our proposed system model, but the power is equally allocated among all subcarriers at the source, forwarding relaying node, and jamming relay node, and sub-carrier mapping is done at the forwarding relaying node, based on Algorithm 1. The interference threshold and maximum transmission power are always the same in this scheme, as in our proposed scheme. The other scheme is a baseline half-duplex scheme, as presented by Zheng et al. [72]. We call this scheme the baseline scheme where we have one relay that forwards the received information without any optimization, and the power is allocated at the relay under the maximum transmission power constraint and maximum interference constraint. The throughput rate at the destination for the baseline scheme is represented by R_d^b , and the throughput rate at the eavesdropper is represented by R_e^b , which are given as

$$R_d^b = \frac{1}{2} \log \left\{ 1 + \sum_{i=1}^N P_i^s |h_i^{sr}|^2 P_i^r |h_i^{rd}|^2 \right\} \quad (6.33)$$

and

$$R_e^b = \frac{1}{2} \log \left\{ 1 + \sum_{i=1}^N P_i^s |h_i^{sr}|^2 P_i^r |h_i^{re}|^2 \right\} \quad (6.34)$$

respectively.

The secrecy rate for the baseline scheme is represented by R_{sec}^b , and is given as

$$R_{\text{sec}}^b = R_d^b - R_e^b. \quad (6.35)$$

The third scheme is an exhaustive search scheme. In this scheme, mapping of subcarriers is carried out based on Algorithm 1, and the power in the feasible search space for power allocation is exhaustively searched for all subcarriers at the forwarding relaying node to allocate optimal transmit power to the subcarriers. This can be considered the upper bound for our proposed scheme.

For Fig. 6.3, Fig. 6.4, and Fig. 6.6, the distances between different nodes for the system model as presented in Figure 1 are as follows. The distance between the source and the relay network is 200 m; the distance between the relay network and the destination is 300 m, and the distance between the relay network and the eavesdropper is 250 m. The maximum interference constraint makes the CR system and PU system coexist, even at a closer distance.

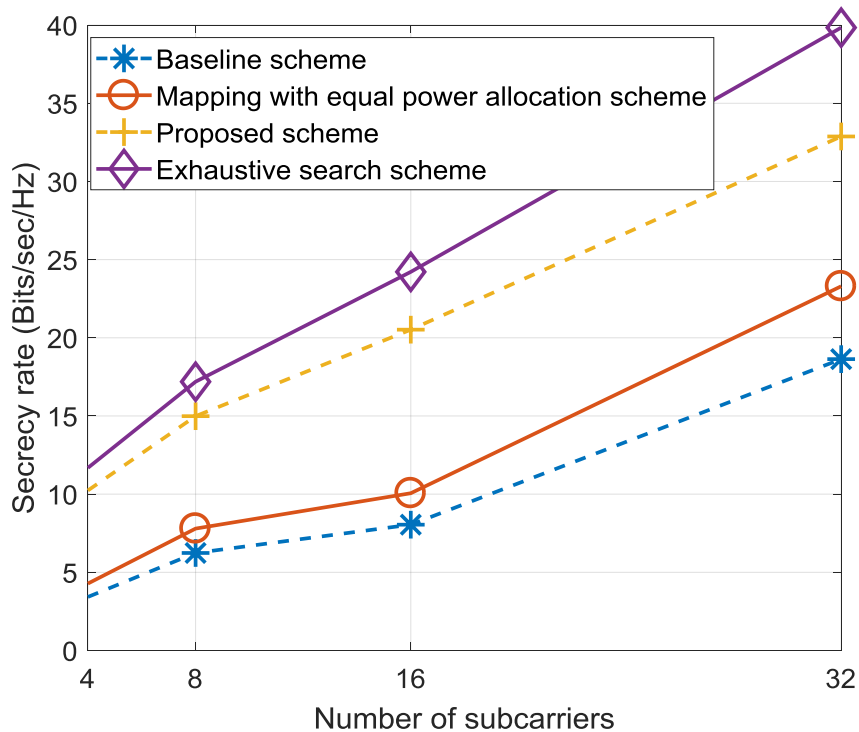


Figure 6.3 Effect of number of subcarriers on the secrecy rate

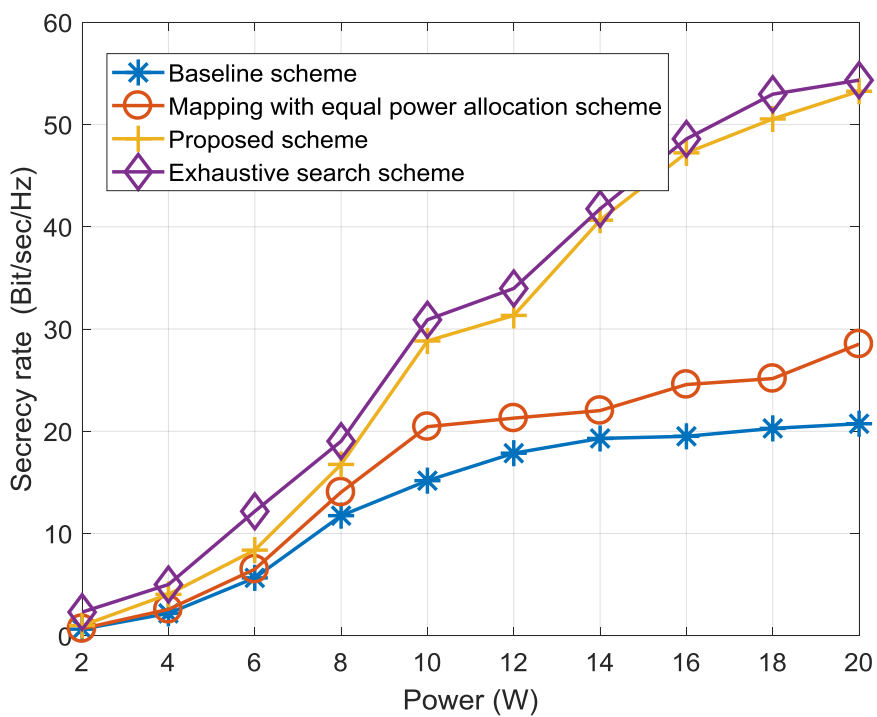


Figure 6.4 Effect of maximum transmission power on secrecy rate

Fig. 6.3 shows the effect of the number of subcarriers on the secrecy rate. The maximum transmission power is 10 W, and the maximum interference threshold is 5 dBm. The secrecy rate of our proposed scheme is higher than both of the other schemes. With an increase in the number of subcarriers, there is a steep increase in the performance of our proposed scheme. The baseline scheme does not greatly benefit from increasing the number of subcarriers because of the increased leakage to the eavesdropper. The exhaustive search scheme outperforms our proposed scheme but at the cost of computational complexity and computation time.

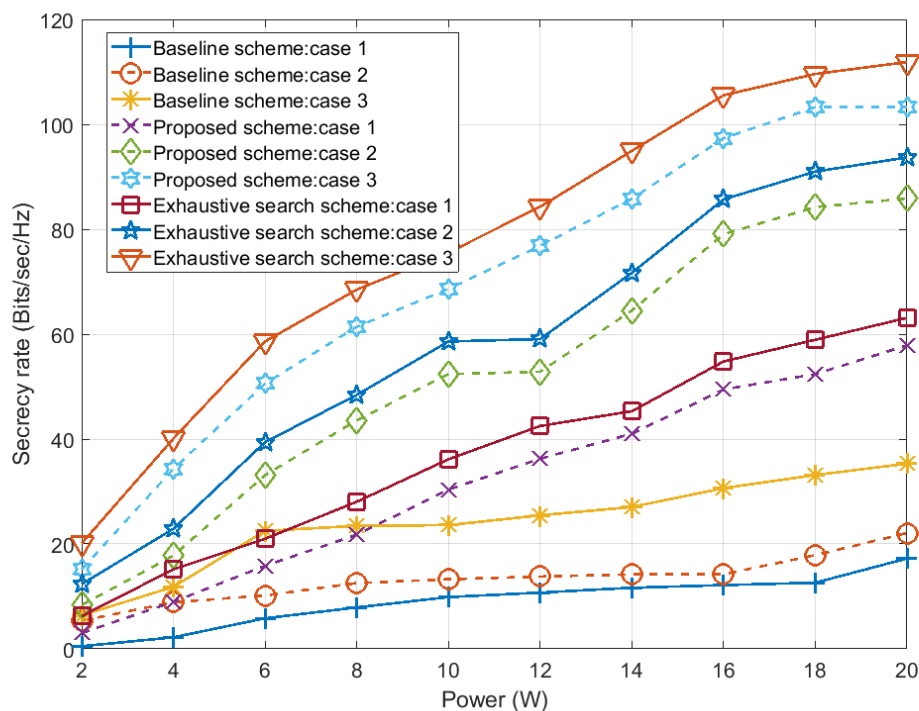


Figure 6.5 Effect of the distance between relay network and eavesdropper on the secrecy rate

Fig. 6.4 presents the effect of maximum transmission power at the source, forwarding relaying node, and jamming relay node for 32 subcarriers, and the maximum interference threshold is 3 dBm. It is clear from Fig. 6.3 that with an increase in the number of subcarriers, the secrecy rate also increases. From Fig. 6.3, it can be seen that after a certain amount of maximum transmission power, the secrecy rate becomes stable (i.e. the secrecy rate does not increase with further

increases in maximum transmission power). This is because of the interference constraint. As the maximum transmission power increases, so does the interference with the PU, and when the interference limit is reached, transmit power is not increased despite the fact that the maximum transmission power limit may not have been reached. Our proposed scheme outperforms the other schemes except for the exhaustive search scheme, but the proposed scheme converges to the upper bound and follows the exhaustive search scheme closely for the whole range of transmission power.

We have tested the proposed scheme for three distances between the relay network and the eavesdropper, as shown in Fig. 6.5. The distance between the source and the relay network is 200 m, the distance between the relay network and the destination is 300 m [103], and the maximum interference threshold is 3 dBm [12]. Only the distance between the relay network and the eavesdropper was changed. The three cases are as follows.

Case 1: The distance between the relay network and the eavesdropper is 50 m.

Case 2: The distance between the relay network and the eavesdropper is 150 m.

Case 3: The distance between the relay network and the eavesdropper is 250 m.

Our proposed scheme performs best when the eavesdropper is closer to the relay network. That is because the jamming relay node signal affects the signal received at the eavesdropper more than the interference caused at the destination. Due to the subcarrier mapping and optimal power allocation at the forwarding relaying node, the eavesdropper receives little information from the forwarding relaying node, even when it is closer. As the eavesdropper moves closer to the destination, the interference caused by the jamming relay node to both the eavesdropper and the destination reaches almost the same level. Thus, the secrecy rate drops when the eavesdropper is nearer the destination. The case for the baseline scheme is different than our proposed scheme. When the eavesdropper is near the forwarding relaying node or near the destination, the secrecy rate is almost the same. In case 1, when the eavesdropper is near the forwarding relaying node, the eavesdropper gets the same information as the CR receiver. In case 2, when the eavesdropper is near the destination, both the eavesdropper and the destination lie on the same line and distance, and hence, both receive the same information. Thus, the secrecy rate drops in this case, too.

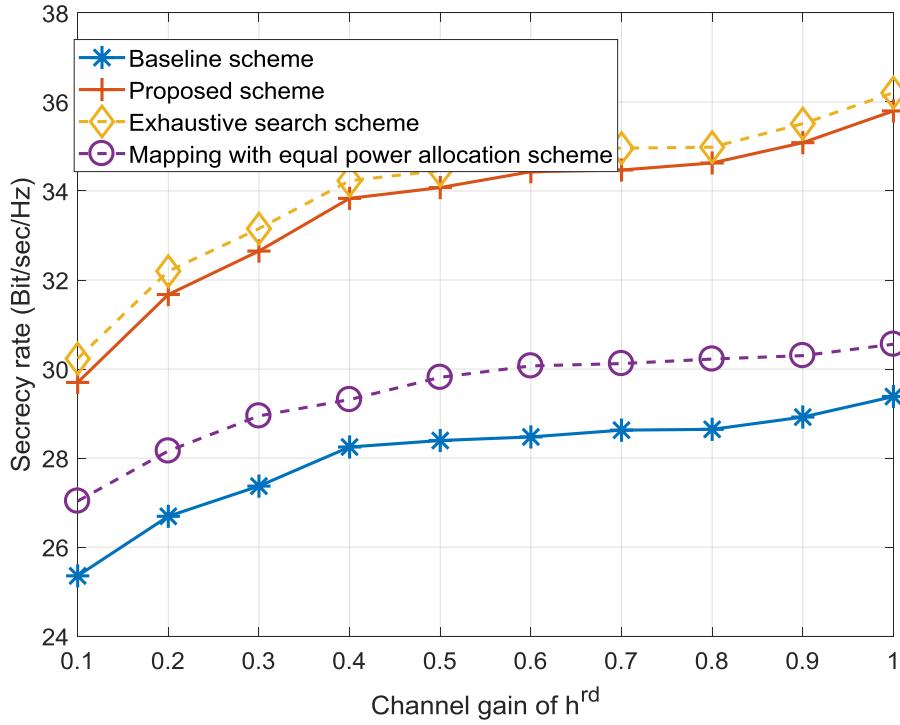


Figure 6.6 Effect of channel gain between relay and CR receiver on secrecy rate

In Fig. 6.6, the complex channel coefficient between the forwarding relaying node and the CR receiver for each subcarrier is calculated as

$$h_i^{rd} = |h_i^{rd}| \cdot e^{j\theta} \quad (6.36)$$

where $|h_i^{rd}|$ is the channel gain between the forwarding relaying node and the destination for the i -th subcarrier, and θ is uniformly distributed in $[0, 2\pi)$. The average result was obtained using Monte Carlo simulation, which consisted of 1000 trials. The simulation was run using four subcarriers, and the maximum interference threshold was 3 dBm. For simplicity, the complex channels between the other nodes are assumed to be $0.8e^{j\frac{\pi}{4}}$ [72]. In the previous simulation results the channel gains as well as the phase of the channel were kept constant and the results were obtained by changing other parameters. The proposed scheme closely follows the exhaustive search scheme as the number of iterations gets larger, and thus, the average

performance of the proposed scheme is near the optimal exhaustive search scheme, but uses less computation power and takes less computation time.

For the sake of comparing our scheme with literature, we have taken the scheme presented for secrecy capacity analysis in [105]. The scheme in [105] is similar to our scheme in terms of topology. Therefore, we consider the scheme in [105] as a reference scheme as following: The secrecy rate of the reference scheme for a transmitter-receiver pair is as [105]

$$R_{\text{sec}}^r = \max \left\{ \begin{array}{l} \log_2 \left(1 + \frac{P_T}{\|x_i - x_j\|^\alpha (B + I_p)} \right) - \\ \log_2 \left(1 + \frac{P_T}{\|x_i - e^*\|^\alpha (B + I_E)} \right), 0 \end{array} \right. \quad (6.37)$$

where P_T is the transmitted power, $\|x_i - x_j\|$ is the distance between the CR sender and CR destination, B is the noise power induced by the primary receivers to the CR destinations, I_p is the interference caused to the PU receivers by the CR transmissions, $\|x_i - e^*\|$ is the distance between the CR sender and eavesdropper, α is the path loss exponent and I_E is the leakage to the eavesdroppers. $\|x_i - x_j\|$ is 300 m, $\|x_i - e^*\|$ is 250m, α is 2, The values of B and I_E are 3 dBm while I_p is 5 dBm. The number of subcarriers is 32. For the reference scheme, the secrecy rate is calculated by summing the rates of 32 different CR sender-CR destination pairs.

Fig. 6.7 shows performance comparison between the proposed scheme and the reference [105] in terms of secrecy rate. When the transmitted power is low, the reference scheme outperforms the proposed scheme. This result is also similar to the previous figures where the proposed scheme provides low performance when total available power is low. The proposed scheme performs well under low transmission power available; however, the proposed scheme outperforms the reference and baseline schemes when enough jamming power is available within the maximum transmission power range for CRN. So, the proposed scheme is suited well for

both low power transmission regimes and high power transmission regimes. Also, it is noteworthy that the performances of the reference schemes do not improve as the transmitting power increases beyond a certain limit while the proposed scheme benefits from the increase in power.

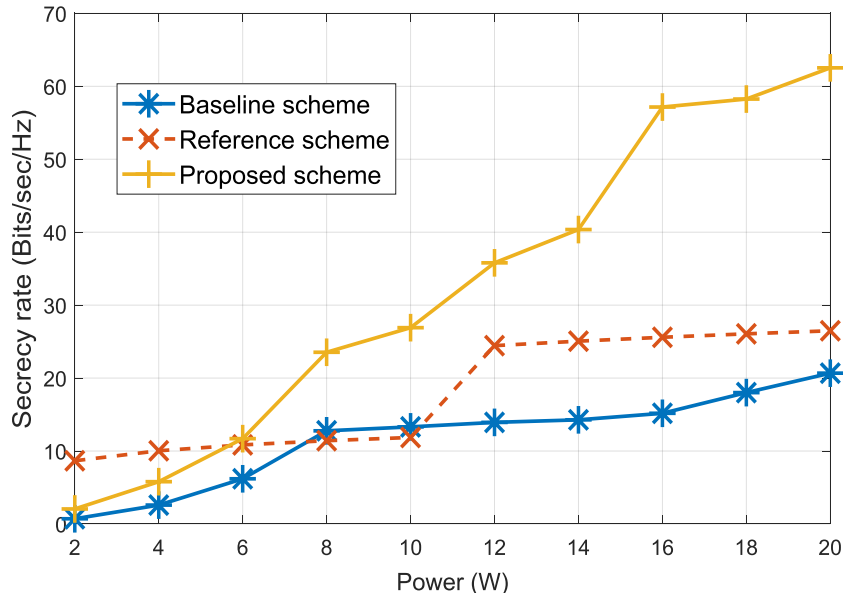


Figure 6.6 Comparison with reference scheme

6.5 Conclusion

In this paper, we studied maximizing the secrecy rate by proposing a physical layer–security scheme in an OFDM-based CRN. In order to optimize the secrecy rate, power allocation at the source, at the jamming relay node, and at the forwarding relaying node is considered, along with subcarrier mapping at the forwarding relaying node. Power to the subcarriers at the source is allocated by taking into consideration the channel gain and satisfying the maximum interference threshold. The jamming relay node sends a jamming signal against the eavesdropper, and transmission power at the jamming relay node is allocated equally to all subcarriers such that the

maximum transmission power constraint and the maximum interference threshold are satisfied. Subcarrier mapping is done at the forwarding relaying node to maximize the overall channel gain from the source to the CR destination. The power allocation problem at the forwarding relaying node is non-convex, and thus, it is difficult to obtain a global optimal solution. The optimization problem is simplified by relaxing the maximum transmission power constraint, and a local solution is obtained using IPM. The maximum power transmission constraint is satisfied after obtaining a local solution. The concept of interference alignment is incorporated implicitly into the power allocated at the source and the forwarding relaying node. The subcarrier mapping also takes into consideration that the leakage of useful information to the eavesdropper is minimal and thus the jamming signal will have the maximum effect on the received signal at the jamming relay node. The power allocated at the forwarding relaying node also aligns the interference caused to the CR receiver by the jamming signal by incorporating the power of jamming signal into the power allocation scheme at the forwarding relaying node. We have shown through simulation results that the proposed scheme can significantly enhance the secrecy rate while satisfying the interference constraints put in to safeguard the PU's communications from harmful interference. We also showed that the proposed scheme closely follows the exhaustive search scheme, which is the upper bound for our proposed scheme, while being computationally less complex.

Chapter 7

Improving physical layer security via cooperative diversity in energy-constrained cognitive radio networks with multiple eavesdroppers

7.1 Introduction

Physical layer security points to techniques incorporating digital signal processing and channel coding to achieve secure communications. For secure communications, secret keys are traditionally used, but using secret keys renders the computational costs high [71]. There exists another kind of attack other than the primary user emulation attack (PUEA) and denial of service (DoS), where communications among the legitimate users is not directly interrupted, and no harmful signals are sent by the attacker. This is called passive eavesdropping, where a legitimate communication is intercepted [106]. Because of the high cost of using secret keys and the extra cost and overhead incurred by managing the distribution of secret keys, traditional cryptographic techniques are not suitable for ad-hoc networks or for networks with other computational constraints. Instead of using cryptographic techniques, information-theoretical perspectives were first used by Shannon [107] to achieve secrecy. From the information-theoretical perspective, secrecy capacity (or secrecy rate) is the difference between the channel capacity from source to destination, referred to as the main link, and the source-to-eavesdropper link, referred to as the wiretap link. It was shown in [108] that if the channel capacity of the main link is lower than the channel capacity of the wiretap link, an intercept event occurs, and the secrecy capacity falls below zero, where the eavesdropper is able to decode communications among legitimate users. To ensure a positive secrecy rate, physical layer security techniques such as artificial noise, beamforming, and cooperative diversity are used.

Adding artificial noise to aid legitimate communication is the simplest technique for physical layer security. One or more relays work as jammers, and send jamming signals against eavesdroppers when communication among the legitimate users is taking place. Jamming to achieve physical layer security has been studied extensively in the literature [109-111]. Multiple works [112-114] have studied cooperative jamming, where external relays cooperate in jamming. Some work considered multiple antennas to create artificial noise to help secure communications [115-117]. Generating artificial noise takes extra computational resources and power. In ad-hoc networks, power is a limited resource. It was shown in [118] that in environments where gain in the main link to the wiretap link is higher than in the wiretap link, then other techniques can provide better performance. Such environments are known as high main-to-eavesdropper-ratio (MER) regimes. In high MER regimes, it becomes difficult for eavesdroppers to intercept legitimate communications, and thus, the probability that an intercept event will happen is low.

It was shown in [106] that in higher MER regimes, cooperative diversity-based schemes outperform artificial noise-based schemes in terms of secrecy rate. So, rather than wasting power resources on generating artificial noise (AN), power resources can be used for communications on the main link, and to prolong network lifetime. In such regimes, cooperative diversity can be exploited to result in a positive secrecy rate while using low transmission power. It was shown in [119] that through the use of cooperative diversity, the secrecy capacity can be significantly increased. Cooperative diversity is used when users cooperate to achieve spatial diversity by sharing their antennas [119]. The performance analysis and optimization of system parameters for cooperative diversity were carried out in [120]. Physical layer security via cooperative diversity in traditional wireless communications networks was studied, where the constraints of cognitive radio were not considered [119][121]. These works showed that through cooperative diversity, not only system reliability and throughput can be increased, but security against an eavesdropping attack can also be provided. In [122], cooperative jamming for physical layer security was studied, where multiple users cooperated to exploit spatial diversity to fend off an eavesdropping attack. Zou et al. [123] studied the use of cooperative relays for enhancing physical layer security, and showed that secrecy capacity can be increased by using cooperative relays. In a large system with multiple collaborating relay nodes, the problem of selecting only a few active relays was considered [124,125]. Other authors investigated cooperative diversity schemes for wireless networks [126-128].

The work on exploiting cooperative diversity for physical layer security in wireless networks cannot be directly applied to cognitive radio networks (CRNs). The CRN is presented as a solution to the spectrum scarcity problem, where spectrum is left unutilized by the primary user (PU). When the spectrum is underused by the PU, the cognitive radio (CR) user can access it, or the CR user can access the spectrum simultaneously with the PU provided interference with the PU is under a certain limit (underlay mode). So, CRNs have special features: the primary user (PU) always takes precedence in using the spectrum, and it is unreasonable to assume that the PU is willing to cooperate with CR users without any conditions. Along with the special features of a CRN, cooperative diversity cannot be directly exploited, as is done in traditional wireless networks, without any concern for security. In traditional cooperative diversity schemes, the channel state information (CSI) of a two-hop network (source to relay and relay to destination) is needed. While exploiting cooperative diversity for physical layer security, the CSI of the wiretap link with two-hop link CSI has to be taken into consideration.

Ad-hoc networks are energy-constrained networks where the maximum transmit energy may not always be available. For a given level of channel quality, using more transmit power will result in increased throughput, but this will also result in quick depletion of energy resources. Recently, there has been much interest in efficient use of energy resources for the sake of energy-aware network architectures and to reduce energy costs [129, 130]. To that end, energy resources have to be used according to system performance requirements. Energy harvesting from renewable energy sources (thermal, vibration, solar, acoustic, and ambient radio power) are designed to meet energy requirements, as well as contribute towards reducing harmful emissions [129]. Energy harvesting allows for theoretically perpetual lifetime operation of an ad-hoc network without any need for an external power source or battery replacement. This is an attractive model for many kinds of future wireless and cellular networks, and is most important for CRNs. Pei et al. [131] studied energy-efficient design of a spectrum-sensing scheme in cognitive radio networks. Chen et al. [132] maximized throughput given an energy budget, whereas Hoang et al. [133] designed a utility-based objective function for penalizing energy consumption. Studies have been carried in exploiting energy harvesting in ad-hoc networks [134]. For multiple relay channels, energy harvesting-based schemes were proposed [135,136]. Wang et al. [137] studied energy harvesting in heterogeneous networks, and both they and Anisi et al. [138] studied the effect of energy harvesting in sensing and body area networks.

To consider practical ad-hoc networks, taking the energy constraints into consideration is of paramount importance. When cooperative diversity-based schemes are considered, then the power used for generating AN in jamming-based schemes can be directed towards transmission on the main link. The main restraint in energy-limited wireless networks is that the power spent in a time slot should be equal to, or less than, the total energy available. The harvested energy adds to the residual energy, and thus, the network can potentially operate for eternity, provided that the rate of energy harvesting is taken into consideration. For an energy-constrained CRN, the constraints on maximum transmission power, interference with the PU, and residual energy have to be taken into consideration before transmission. To ensure long-term operation, there needs to be enough energy left in the battery for future transmissions. Thus, selecting a relay from among many in order to exploit spatial diversity is a problem to be solved in maximizing the secrecy rate, along with keeping to the PU's maximum-interference requirements and the energy budget.

In this chapter, we propose a cooperative diversity-based scheme for providing physical layer security in energy-constrained CRNs. The CRN considered is underlay, where the CR user co-exists in the spectrum with the PU. Each CR user has a rechargeable battery, and CR users harvest energy from ambient sources [129]. Main-link communications is helped by a set of relays, and multiple eavesdroppers are considered. In the proposed scheme, multiple orthogonal subchannels are considered, but we assume that each CR user is equipped with only one antenna. This assumption is taken into consideration because of the low hardware resources available in an ad-hoc network. To maximize the secrecy rate, a relay and a subchannel over that relay have to be selected to satisfy the PU interference requirements and also satisfy the long-term lifetime requirements of the system. Communications take place in two phases. In the first phase, a communication from source to relay happens, and in the second phase, the selected relay forwards the received data to the destination. An optimization problem is formulated, which aims to maximize the secrecy rate by selecting one relay and one subchannel while satisfying the energy- and interference-constraint requirements. The relay selection, along with selection of a transmission power factor, is carried out through graph theory. An algorithm based on graph theory is presented that takes into consideration the preference of each relay over each subchannel in order to have minimum leakage to the eavesdropper. Power is allocated both at the source and at the relay. In the graph theory-based cooperative-diversity scheme, where a relay and a subchannel are selected, the relays are considered one set of edges, while the subchannel

and eavesdroppers are merged to form another set of edges. The power transmission factor, which serves to satisfy the long-term energy requirements, is considered to form vertices between the edges.

The rest of this chapter is divided as follows. Section 2 presents the system model and problem formulation, while Section 3 presents the solution to the optimization problem through graph theory. Section 4 presents simulation results and analysis, and Section 5 concludes the chapter.

7.2 System Model and Problem Formulation

In this section, the system model is presented in detail, the constraints on the system are defined, and an optimization problem to maximize the secrecy rate is formulated.

7.2.1 System Model

We assume a CR system with one CR sender and one CR receiver, with a relay network having M relays, E eavesdroppers, and C orthogonal subchannels, as seen in Figure 7.1. It is assumed that the CR destination is outside the range of the CR sender, and thus, the transmission does not reach the CR destination directly. The relay network helps forward the CR source's data to the destination over one subchannel. We assume the CR source and destination do not have any energy constraints, while the relays have limited energy available. The relays harvest energy from ambient sources and store it in their batteries for future use.

Communication takes place in two phases. In the first phase, the CR sender transmits its data to the relay. In the second phase, the selected relay forwards the received data over the selected subchannel to the CR destination. The relay that forwards the received data uses amplify-and-forward protocol. The communications of the PU are not considered in this system. The only consideration is that interference with the PU must be less than the maximum interference limit so communications of the PU are protected. In the first phase of communication, interference with the PU is because of the CR sender's transmission, and in the second phase, it is because of the relay transmission. In both phases, the maximum interference limit is satisfied, such that the interference with the PU is below the threshold.

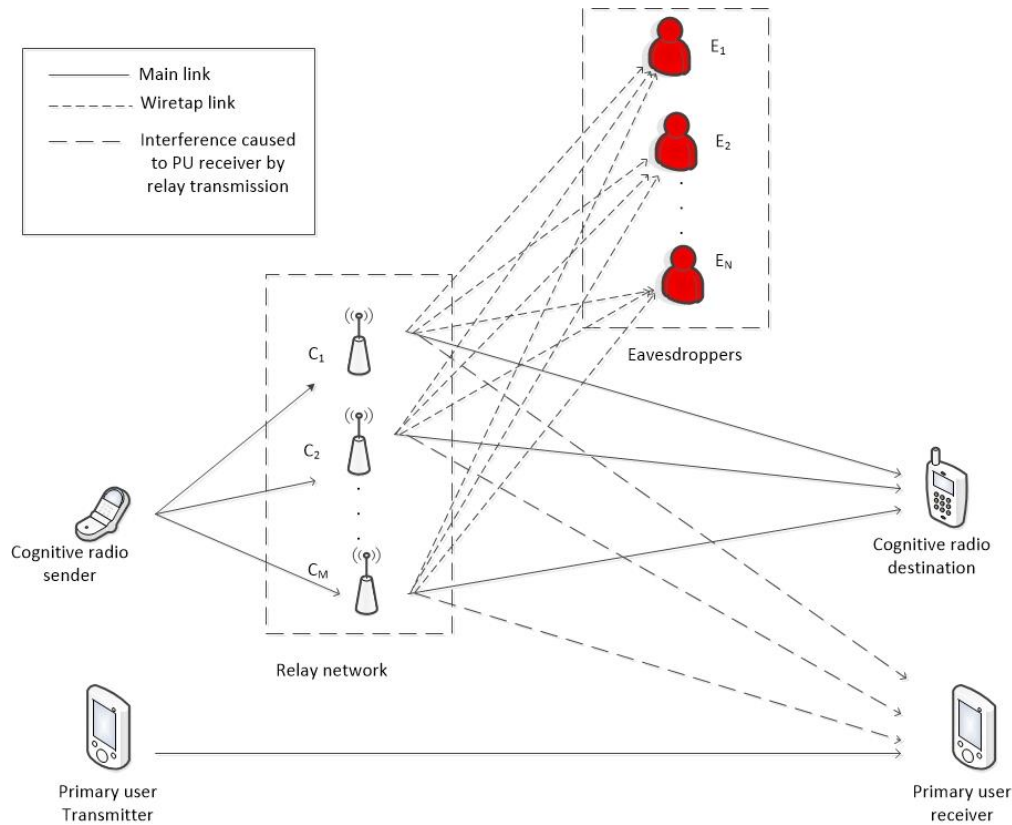


Figure 7.1 Basic system model

An underlay CR system is assumed where the CR user co-exists in the same spectrum as that of the PU, given that the interference conditions are satisfied. It is also assumed that instantaneous CSI is available, and the channel coefficients for all links are known a priori. The use of statistical channel information or erroneous channel information, and finding the gain of an eavesdropper, are practical considerations that are outside the scope of this work. A slotted time architecture is considered where, in each time slot, energy is harvested and communication is carried out. In one time frame, both phases of the communication take place. It is assumed that the relays are able to harvest energy in each time slot, and the harvested energy is available in the next time slot.

In the first phase, the source transmits to the relay network, so it is simple. In the second phase, from among M relays, one has to be selected to transmit over one subchannel from among

C orthogonal subchannels. The goal is to select a relay and a subchannel over that relay, and also to allocate power at the relay that can maximize the secrecy rate in the current time slot under the constraint of maximum energy consumption, which ensures the long-term lifetime of the CRN. Only one relay transmits over one subchannel, so the transmission rate at the destination, if the x_i -th relay forwards the received data on the c_l -th subchannel, is [106,119]:

$$R_d^{c_l}(x_i) = \frac{1}{2} \log_2 \left(1 + \frac{|h_{sx_i}^{c_l}|^2 |h_{x_i d}^{c_l}|^2 P_s \alpha_k P_r^{\max}}{(|h_{sx_i}^{c_l}|^2 + |h_{x_i d}^{c_l}|^2) \sigma_{n_{x_i d}}^2} \right) \quad (7.1)$$

where $\sigma_{n_{x_i d}}$ is the additive white Gaussian noise (AWGN) variance of the channel between the relay and eavesdropper, c_l is the subchannel allocated to the x_i -th relay, $h_{sx_i}^{c_l}$ is the channel gain between the CR source and the x_i -th relay over the c_l -th subchannel, $h_{x_i d}^{c_l}$ is the channel gain between the x_i -th relay and the CR destination over the c_l -th subchannel, P_s is the power allocated at the CR sender, P_r^{\max} is the maximum transmission power, while α_k is the transmission power factor selected to satisfy the energy consumption constraint to meet the long-term energy requirements.

If the eavesdroppers perform their interception tasks independently, then the overall rate of the wiretap links or the rate achieved at the eavesdropper network is the maximum of the individual rates achieved at E eavesdroppers [106]. The maximum achievable rate at the eavesdropper, if the x_i -th relay transmits is

$$R_e(x_i) = \max_{e_j \in \mathcal{E}} R_{e_j}(x_i) \quad (7.2)$$

where R_e is the rate received at the eavesdropper, and e_j is the j -th eavesdropper.

The transmission rate at the eavesdropper, if the x_i -th relay forwards the received data on the c_l -th subchannel is [106,119]:

$$R_e^{c_l}(x_i) = \max_{e_j \in \mathcal{E}} R_{e_j}(x_i) = \max_{e_j \in \mathcal{E}} \log_2 \left(1 + \frac{|h_{sx_i}^{c_l}|^2 |h_{x_i e_j}^{c_l}|^2 P_s \alpha_k P_r^{\max}}{(|h_{sx_i}^{c_l}|^2 + |h_{x_i e_j}^{c_l}|^2) \sigma_{n_{x_i e_j}}^2} \right) \quad (7.3)$$

where $h_{x_i e_j}^{c_l}$ is the channel gain between the x_i -th relay and the e_j -th eavesdropper over the c_l -th subchannel, and $\sigma_{n_{x_i e_j}}$ is the variance of AWGN between the relay and the eavesdropper. The secrecy rate, according to the above equations, is then given as

$$R_s^{c_l}(x_i) = \left[R_d(x_i) - \max_{E_j \in \mathcal{E}} R_{e_j}(x_i) \right]^+ \\ = \left[\log_2 \left(\frac{|h_{sx_i}^{c_l}|^2 |h_{x_i d}^{c_l}|^2 P_s \alpha_k P_r^{\max}}{(|h_{sx_i}^{c_l}|^2 + |h_{x_i d}^{c_l}|^2) \sigma_{n_{x_i d}}^2} \right) - \log_2 \left(1 + \max_{e_j \in \mathcal{E}} \frac{|h_{sx_i}^{c_l}|^2 |h_{x_i e_j}^{c_l}|^2 P_s \alpha_k P_r^{\max}}{(|h_{sx_i}^{c_l}|^2 + |h_{x_i e_j}^{c_l}|^2) \sigma_{n_{x_i e_j}}^2} \right) \right]^+ \quad (7.4)$$

where $[\cdot]^+$ indicates that the secrecy rate cannot be negative, i.e.

$$R_s^{c_l}(x_i) = \max[R_d(x_i) - \max_{E_j \in \mathcal{E}} R_{e_j}(x_i), 0].$$

The main objective is to maximize the secrecy system as given in (4). In the next section, the constraints on the maximization problem are defined.

7.2 System Constraints Definitions

Because of Eq. (7.2), an eavesdropper that has the maximum gain over a subchannel from a relay is considered (simply to take into consideration the worst case scenario). This results in combining the eavesdroppers and subchannels and treating them as a pair. Given that the instantaneous CSI is known, the gain from a relay over a subchannel to an eavesdropper can be considered a pair, and this has to be taken into consideration in the relay selection. The aim of the proposed scheme is to select a relay and a subchannel for that relay to transmit over, such that the leakage to the eavesdropper having the maximum gain over that subchannel is minimal. Let us denote the l -th subchannel–eavesdropper pair as ce_l .

Three selections have to be made: (1) the relay over which to transmit, (2) the subchannel–eavesdropper pair for that relay, and (3) the transmission power factor that will select transmission power such that the maximum transmission energy constraint is satisfied. We are assuming that, at one time only, one relay will transmit over one subchannel, because we are considering single-antenna nodes. To meet this constraint, let us define a binary variable:

$$\ell(x_i, ce_l) = \begin{cases} 1, & \text{if } x_i\text{-th relay transmits over } ce_l\text{-th subcarrier-eavesdropper pair} \\ 0, & \text{otherwise.} \end{cases} \quad (7.5)$$

It can also be written as

$$\sum_{i=1}^M \ell(x_i, ce_l) = 1 \quad \forall ce_l \quad \sum_{l=1}^{CE} \ell(x_i, ce_l) = 1 \quad \forall x_i. \quad (7.6)$$

The above equation restricts one relay to transmitting over one subchannel only, and at one time, the subchannel can be assigned to one relay only. To meet the maximum transmission energy constraint to fulfill the long-term battery performance of the system, another variable is introduced that indicates the transmission factor at relay x_i :

$$v(x_i, \alpha_k) = \begin{cases} 1, & \text{if the transmission power factor for } x_i \text{ is } \alpha_k \\ 0, & \text{otherwise.} \end{cases} \quad (7.7)$$

This can also be written as

$$\sum_{\alpha_k = \alpha_{\min}}^{\alpha_{\max}} v(x_i, \alpha_k) = 1. \quad (7.8)$$

The transmission factor is utilized in transmission energy at relay x_i in time slot t , represented by e_t , as

$$e_t = \alpha_k P_r^{\max} \quad \alpha_k \in [\alpha_{\min}, \alpha_{\min}] \quad (7.9)$$

It is assumed that each relay node is equipped with a battery of finite capacity, and it has an energy harvester that converts ambient energy into electricity. The harvested energy is represented by a set of non-negative real numbers. If the energy arrival process, $e_h^t \subset R^+$, is assumed to be independent and identically distributed (i.i.d.) sequences of variables, then $\mathbf{E}\{e_h^t\} = e_h$ [129]. It is also assumed that the energy harvested in time slot t is immediately available in slot $t+1$.

The total energy consumed in the transmission by the relay at time t is

$$E_r = \tau(e_t + e_c) \quad (7.10)$$

where τ is the duration of the slot, and e_c is the energy consumed by the circuitry. One of the ways to ensure long-term performance of a wireless system is to keep the energy spent in one particular time slot under a constraint. Energy harvesting provides for a constraint where, in any given time slot, the energy spent should be less than or equal to the harvested energy. In this paper, we are proposing that the residual energy after the transmission in the current time slot should be enough for N future time slots. This is done to keep under consideration the random nature of the energy harvesting process. In some future slots, the energy harvested may not equal the transmission energy. Thus, the residual energy should be

$$E_t \geq N(E_r - e_h) \quad (7.11)$$

Keeping τ and e_c fixed, e_t has to be optimized in order for (7.11) to hold.

The power available at the source has to satisfy both the maximum transmission power and the maximum interference constraint. The maximum transmission power constraint at the source is assumed to maintain the same allowed power level as that of the transmission relay nodes. As the communication happens in two phases, the interference with the PU in the first phase is because of the transmission of the CR source. The constraints are given as

$$P_s \leq P_s^{\max} \quad (7.12)$$

where P_s^{\max} is the maximum transmission power at the source, and

$$|g_{sp}|^2 P_s \leq I_{\max} \quad (7.13)$$

where g_{sp} is the channel gain between the CR source and the PU, and I_{\max} is the maximum interference threshold.

The constraint on maximum transmission energy at the relay node, which is meant to ensure long-term performance, was given in (7.11). As the relay transmission happens in the second phase, the interference with the PU is only because of the relay's transmission. So the transmission power at the relay should be

$$|g_{x_i p}^{c_i}| P_r \leq I_{\max} \quad (7.14)$$

where $g_{x_i p}^{c_i}$ is the channel gain between relay x_i and the PU over subchannel c_i .

7.2.3 Problem Formulation

The source power in the system has to satisfy only the maximum transmission power constraint and the maximum interference constraint, because we assume that the CR source is not energy-constrained, and only the relays are energy-constrained (but they harvest energy). This is a non-trivial problem but is easily solved. The aim of this paper is to optimize selection of the relay that will forward the CR source's transmission, choose the subchannel on which to transmit, and set the power transmission factor with which to transmit in order to meet the energy restraints. In CR systems with no security issues, the power allocation problem can be simple, even in the underlay CR network model. The transmission power is selected under the constraint that the maximum interference threshold is satisfied. An increase in power in a CR system with eavesdroppers present can also result in more leakage to the eavesdropper, and hence, a decrease in the secrecy rate. An increase in power to increase the secrecy rate may also cause an increase in interference with the PU, as well to the underlay CR system.

The optimization parameters are given for the second phase of communication, and optimization happens in that second phase. The selection of the relay to transmit over is optimized, and the subcarrier for the selected relay is optimized along with the transmission power factor. With these optimization variables the optimization problem (OP) is given as

OP:

$$\arg \max_{\ell, v, \alpha_k} \sum_{i=1}^M \sum_{l=1}^{CE} \sum_{k=\alpha_{\min}}^{\alpha_{\max}} \ell(x_i, ce_l) v(x_i, \alpha_k) \left[\log_2 \left(\frac{|h_{sx_i}^{c_l}|^2 |h_{x_i d}^{c_l}|^2 P_s \alpha_k P_r^{\max}}{(|h_{sx_i}^{c_l}|^2 + |h_{x_i d}^{c_l}|^2) \sigma_{n_{x_i d}}^2} \right) - \log_2 \left(1 + \max_{e_j \in \mathcal{E}} \frac{|h_{sx_i}^{c_l}|^2 |h_{x_i e_j}^{c_l}|^2 P_s \alpha_k P_r^{\max}}{(|h_{sx_i}^{c_l}|^2 + |h_{x_i e_j}^{c_l}|^2) \sigma_{n_{x_i e_j}}^2} \right) \right] \quad (7.15)$$

s.t. (6), (7), (11) and (14).

7.3 Relay and subchannel selection under energy constraints and a power allocation scheme

Power allocation at the source is relatively easy, as it can be found through a unified equation. The solution to power allocation at the source is in the subsection about final power allocations at the end of this section. The solution to the OP given in (7.15) is solved through graph theory. Due to the $\log_2(\cdot)$ functions and the interference constraints, the OP in (7.15) is a

non-linear optimization problem, and thus, it is non-trivial to convert it to a convex optimization problem. It was shown in [139] that such optimization problems are NP-hard, and the optimal solution cannot be found in polynomial time. We convert the OP to a matching graph and solve it through a graph theory-based algorithm that gives the solution to the graph problem. Graph theory helps in visualization of the complex problem. When the complex OP is converted into a graph, the solution can be found through simple and repetitive steps. The graph theory-based algorithm that we present arranges the problem linearly, and thus, the search space can be reduced. In the linear arrangement of the complex OP, the search ends at the step where the next possible solution gives less-optimal values. The space of possible solutions, which in our case is maximum secrecy rate under the constraints given in (15), is arranged in decreasing order. So, if the next possible solution is less optimal than the current one, the search stops.

Di et al. used matching theory to solve the optimization problem of resource allocation in a multi-node and multi-subchannel scenario [140]. The concept of a preference list, as used there, is employed in the matching graph here, and thus, a node retains a list of its historical preferences. Bipartite graphs were used for analysis and optimization in [141]. The process of optimizing neighbor discovery is represented through a bipartite graph, and the cardinality of the graphs represents the number of elements in a set of nodes. In the next subsection, we will translate the OP to a graph problem by showing it through a simple example.

7.3.1 Representing the OP through a graph

Let there be two sets of nodes, one set representing the relays and the other the subchannel-eavesdropper pairs. The nodes representing relays are denoted by x_i , whereas the other nodes, for the sake of simplicity, are denoted by c_l . Let us say there are two relays, three subchannels, and two eavesdroppers. Let Table 7.1 represent $\max\{e_j\}$ for each x_i over each c_l , as given in (7.2). The edges represent the values of the power transmission factor as given in (7.9). Suppose there are three values for the power transmission factor.

Table 7.1 Maximum gain of an eavesdropper over subchannels for relays

Relay \ SC	c_1	c_2	c_3
x_1	e_1	e_2	e_1
x_2	e_2	e_1	e_2

First, for each relay, all values of α are checked for all subchannel–eavesdropper pairs. In Figure 2, the H values are represented by $h_{x_i e_j}^{\alpha}$. When the comparisons are made in Step 1, as shown in Fig. 7.2, the values of α are found in Step 2. In Fig. 7.3, Step 2 is shown, and it is assumed that the value of α representing the edge satisfies (7.9). Let us now suppose that c_2 with α_1 as the transmission power factor gives the highest secrecy rate; then, for x_1 , the matching is (α_1, c_2) . After the value of α is known for one relay over a subchannel pair, the process is repeated for the other relay in Step 3, as shown in Fig. 7.4. The steps given for x_1 are repeated for x_2 . Let us suppose that x_2 with α_2 gives the highest secrecy rate over c_3 . Then the matchings are presented in Fig. 5.

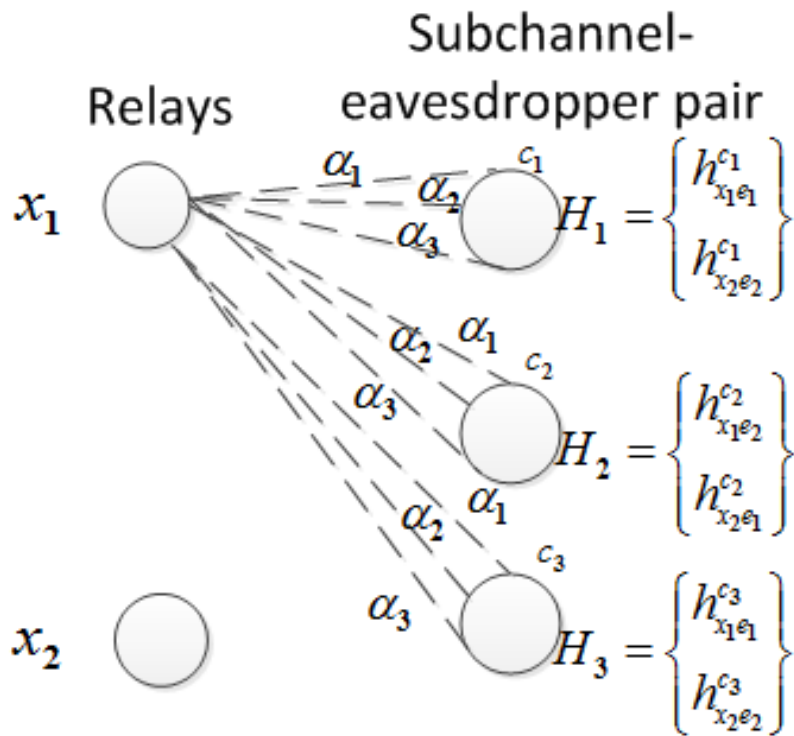


Figure 7.2 Step 1 in graph matching

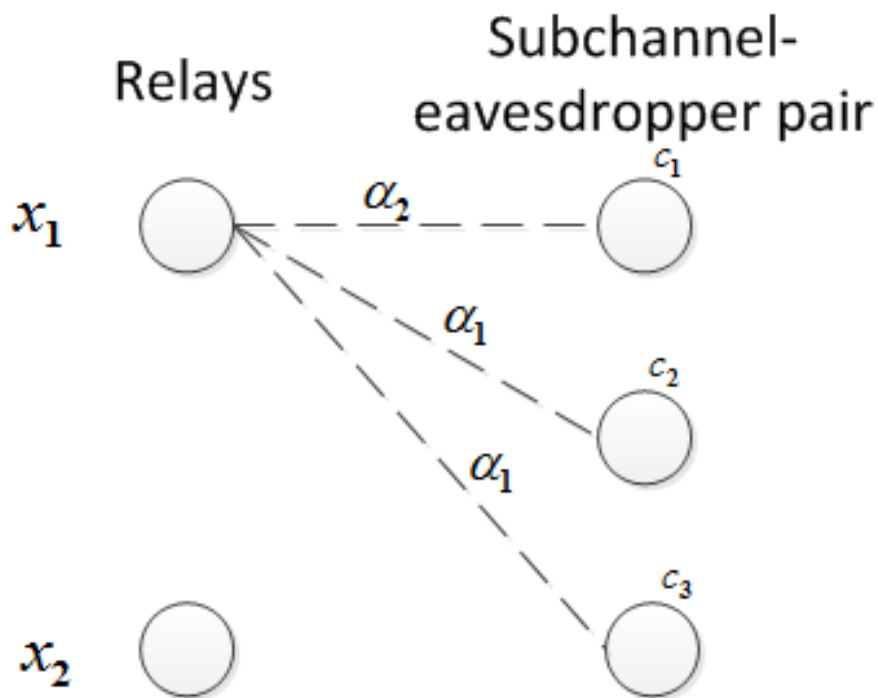


Figure 7.3 Step 2 in graph matching

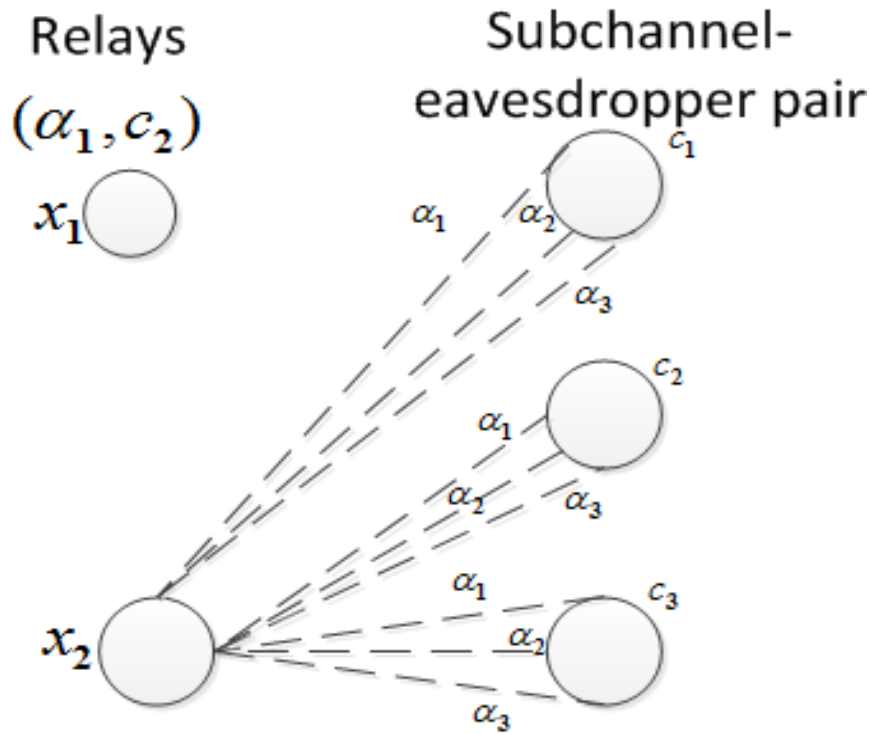


Figure 7.4 Step 3 in graph matching

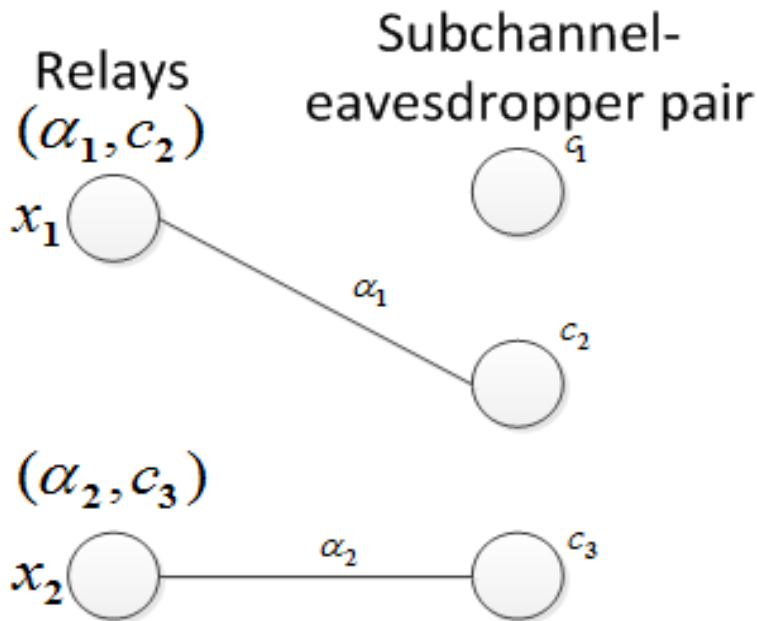


Figure 7.5 Step 4 in graph matching

Let $R_s^{(c_2, \alpha_1)}(x_1)$ be the secrecy rate for x_1 by using subchannel c_2 , and let power transmission power factor α_1 and $R_s^{(c_3, \alpha_2)}(x_2)$ be the secrecy rate for x_2 by using subchannel c_3

with power transmission power factor α_2 . If $R_s^{(c_2, \alpha_1)}(x_1) > R_s^{(c_3, \alpha_2)}(x_2)$, then the matching graph algorithm will return relay x_1 over c_2 with power transmission power factor α_1 ; otherwise, it will return relay x_2 over c_2 with power transmission power factor α_2 .

7.3.2 Relay and subchannel selection algorithm

In this section, the graph representation presented in the previous subsection will be generalized to M relays, to CE subchannel–eavesdropper pairs, and to a discrete number of values for α in the range $[\alpha_{\min}, \alpha_{\max}]$. In the first stage, a priority list for each relay is determined over ce while using maximum transmission power at the relay in (7.4). The priority list is important, so each relay has a preference over the subchannel–eavesdropper pairs. Through the priority list and the modification in each iteration in the priority list, the changes in the environment can also be reflected. The priority list ensures that the number of comparisons for any given relay can be less than the maximum possible number of comparisons. The priority list is arranged in descending order, which shows that the first entry means that the ce pair for the relay gives a higher secrecy rate than the second, and the second, higher than the third, and so on.

In the second stage, the value of α_k is changed in each iteration over the same ce unless (7.9) is satisfied. For each relay, a pair for ce is obtained that has the maximum secrecy rate under the constraint in (7.19). Then, the maximum of these relay– ce pairs is found in the third stage and used as the best relay and subchannel on which to transmit. The priority list for relay–over- ce pairs is computed by finding the secrecy rate using the maximum transmission power. The priority list is arranged in descending order, so if the secrecy rate for a relay over a ce pair is β -times higher than the next entry, then they are not checked further. This reduces computational complexity. The change in channel conditions over time are also taken into consideration through updating the priority list, and thus, the relay selection takes into account the dynamic nature of wireless channels.

In Step 2, first the current ce pair is assigned. In Step 2.1, the entry next to the current ce pair is taken from the priority list. In Step 2.4, if the second pair gives a higher secrecy rate, then update the priority list; otherwise, return the current pair. In Step 2.5, check to see if the second pair gives a β -times higher secrecy rate than the third pair; if so, the second pair becomes the

current pair, and the algorithm moves to the next pair. In Step 2.7, the loop exits if the condition is satisfied; otherwise, the priority list and current pair are updated, and the next ce pair is checked. In Step 2.8, if the last pair in the priority list is checked, and the optimal pair that satisfies the criteria is not found, then NULL for the current relay is returned; otherwise, the ce pair for the optimal value of α was found. The process is repeated for all relays. In Step 3, the pairs of relays with optimal subchannels and transmission power factors are arranged into a vector, θ . The maximum of the vectors is found, and $q(x_b)$ is the solution to the OP. The best-relay/subchannel–selection algorithm under the maximum energy transmission constraint is given in Algorithm 1.

Algorithm 1

1. Priority list initialization

(i) calculate secrecy rate for each x_i over all subcarrier–eavesdropper pairs as $R_s^{ce}(x_i)$ where $ce = \{ce_1, ce_2, \dots, ce_C\}$ according to (4) where $P_r = P_{\max}$

(ii) Find $R_s^{ce_n} = \max\{R_s^{ce}(x_i)\}$. The subchannel–eavesdropper pair corresponding to $R_s^{ce_n}(x_i)$ is ce_n

(iii) The entry into the priority list of x_i is

$$PL^k(x_i) \leftarrow (ce_n)$$

(iv) Remove ce_n from ce

(v) if $ce \neq \emptyset$

$$k = k + 1$$

Go to step (ii)

(vi) Repeat (i)-(v) for $\forall x_i$; the priority for x_i is

$PL(x_i) = \{PL^1(x_i), PL^2(x_i), \dots, PL^C(x_i)\}$ where
 $PL^1(x_i) > PL^2(x_i), \dots, > PL^C(x_i)$

2. Matching and priority list update phase

$x_{matchlist} = \{x_1, x_2, \dots, x_M\}$

while $x_i \in x_{matchlist}$ do

$Q(t_i) = PL^1(x_i)$

$k = 1$

$LP = 0$

while (LP=0)

(i) $k = k + 1$

(ii) Find $R_s^{Q(t_i), \alpha^1}(x_i) \quad \forall \alpha$

Such that (19) satisfies

$\alpha_1 = \alpha$

(iii) Find $R_s^{PL^k(t_i), \alpha^1}(x_i) \quad \forall \alpha$

such that (19) satisfies

$\alpha_2 = \alpha$

(iv) If $R_s^{PL^k(t_i), \alpha^1}(x_i) > R_s^{Q(t_i), \alpha^1}(x_i)$
 $PL^{k-1}(x_i) \leftarrow PL^k(x_i)$

else

$LP = 1, \alpha^* = \alpha_1$

end if

(v) if $R_s^{PL^k(x_i), \alpha^1}(x_i) > \beta R_s^{Q(t_i), \alpha^1}(x_i)$
 $Q(x_i) \leftarrow PL^k(x_i)$

end if

(vi) Find α such that the value of α satisfies (19)

(vii) if $R_s^{\{PL^k(x_i), \alpha\}}(x_i) > \beta R_s^{\{PL^{k+1}(x_i), \alpha\}}(x_i)$

$$LP = 1, \alpha^* = \alpha_2$$

else if $R_s^{\{PL^{k+1}(x_i), \alpha\}}(x_i) > R_s^{\{PL^k(x_i), \alpha\}}(x_i)$

$$Q(x_i) \leftarrow PL^{k+1}(x_i); \alpha_1 = \alpha$$

$$PL^k(x_i) \leftarrow PL^{k+1}(x_i)$$

end if

(viii) if $Q(x_i) = PL^C(x_i)$ and α^* is not found

$$Q(x_i) = \emptyset, \alpha^* = \emptyset$$

$$LP = 1$$

end if

end while

$$q(x_i) \leftarrow \{Q(x_i), \alpha^*\}$$

Remove X_i from $X_{matchlist}$

end while

3. Best relay selection

$$\theta = \{q(x_1), q(x_2), \dots, q(x_M)\}$$

$$\text{Find } \mathbf{R}_s^\theta = \{R_s^{q(x_1)}, R_s^{q(x_2)}, \dots, R_s^{q(x_M)}\}$$

$$\text{Find } R_s^{q(x_b)} = \max\{\mathbf{R}_s^\theta\}$$

7.3.3 Power Allocation

The power allocation at the source needs to satisfy the maximum transmission power constraint and the maximum interference power constraint. We assume that the CR sender is not energy-constrained. The power allocated at the source is given as

$$P_s = \min \left\{ P_s^{\max}, \frac{I_{\max}}{|g_{x_i,p}^{c_l}|} \right\} \quad (7.16)$$

where $g_{x_i,p}^{c_l}$ is the channel gain between the CR sender and the PU, if the transmission is to relay x_i over subchannel c_l .

Algorithm 1 gives α^* , which is the optimal value of α for the optimal x_i over the optimal c_l . To satisfy the maximum interference constraint, the power at the optimal relay over the optimal subchannel is given as

$$P_r^{\text{proposed}} = \min \left\{ \alpha^* P_r^{\max}, \frac{I_{\max}}{|g_{x_i,p}^{c_l}|} \right\} \quad (7.17)$$

7.4 Results and Analysis

In this section, we present the results from the simulation carried out to verify the performance of the proposed scheme. The simulation platform was Matlab R2017a. For the simulation, we assumed the channels undergo Rayleigh fading. The subchannels were assumed to face independent Rayleigh fading. It was also assumed that each channel gain is independent of the others. The bandwidth was assumed to be 6 MHz, while the time frame was considered 100 ms. The distance between the CR sender and the CR destination was fixed at 200 m, while the relays (which varied for the simulation) were distributed between the CR sender and CR destination. The number of subchannels is specified for each simulation result. The range of the CR sender did not cover the CR destination, and hence, one of the relays was used to carry the CR sender's transmission forward. The circuit power consumption was kept fixed at 210 [129,131]. The transmit power varied for the different simulation results, and is given for each.

The maximum transmission power was considered the same for the CR sender and for the relay. The noise spectrum density was taken to be 4.4×10^{-21} W/Hz [142]. For the Raleigh fading channels, the path loss exponent was 4, which according to some is the worst case scenario for cellular and long-distance communications [143,144]. As the path loss exponent is reduced, the corresponding performance improved. The number of subchannels was fixed at eight.

We consider an infinite battery scheme to be the upper bound for the proposed scheme. In the infinite battery scheme, the priority list is made according to the maximum transmission power, as explained in the first stage of the proposed algorithm. A relay and a subchannel to transmit over at that relay were selected according to the initial priority list, and then maximum transmission power was used, provided that the interference constraint for the PU is satisfied. Each time, the relay and the subchannel with the maximum secrecy rate were selected from among all the relays and all the subchannels. The infinite battery capacity scheme assumes that the maximum transmission power is available in every time frame, and thus, there is no need to satisfy the maximum energy constraint.

We also considered two versions of the proposed scheme in some simulations. The proposed scheme performance is affected by the energy available, and (because we considered energy harvesting) the rate at which energy is harvested affects the performance of our proposed scheme. We considered two different rates for the energy arrival process. The mean of the energy arrival process is determined as

$$e_h = \chi(e_c + e_t) \tag{7.18}$$

For one version, we considered χ to be 0.3, and for the other, to be 0.6. The initial energy was assumed to be $0.6(e_c + e_t)$.

Figure 7.6 presents the effect of the energy harvesting rate. At one level, the result shown is intuitive, in that, with the increase in the energy harvesting rate (and thus, the energy available for transmission), the secrecy rate improves. Because the selected relay transmits over a subchannel that has the least leakage to the eavesdropper with the maximum channel gain from the relay over that subchannel, an increase in transmission power increases the secrecy rate. For Figure 6, the number of future slots is assumed to be three, i.e. $N = 3$ in (7.11). The result shows that, given less energy available for transmission under the constraint to satisfy the long-term

energy requirements, the proposed scheme closely follows the infinite battery scheme, especially when the power is in the mid-to-high range. For the proposed scheme with $\chi=0.3$, a lot less energy is available, because it also has to satisfy the constraint in (7.11) with $N = 3$, so the gap in performance between this version and the upper bound is large.

Figure 7.7 represents how the main-to-eavesdropper ratio can affect the performance of the system. It also shows the effect of the constraint to fulfil the energy requirements for future time slots. The MER gives the difference between the average gain of the eavesdroppers' link to that of the link from the relay to the CR destination. So when the MER is 2, the main link's average is 2 dB higher than the average gain of the eavesdropper's link. The maximum transmission power is 110 mW, and $\chi=0.6$ in (7.18) for Figure 7.7. From the figure, we can see that, as the number of future slots (i.e. N) is reduced, the secrecy rate improves. When MER increases, the secrecy rate of the scheme with $N = 2$ outperforms the other. From the figure, we can see that, even at a higher long-term energy constraint of $N = 5$, the proposed scheme achieves a positive secrecy rate above 3 bits/sec/Hz. As the long-term energy constraint is relaxed, so the secrecy rate of the proposed scheme also improves.

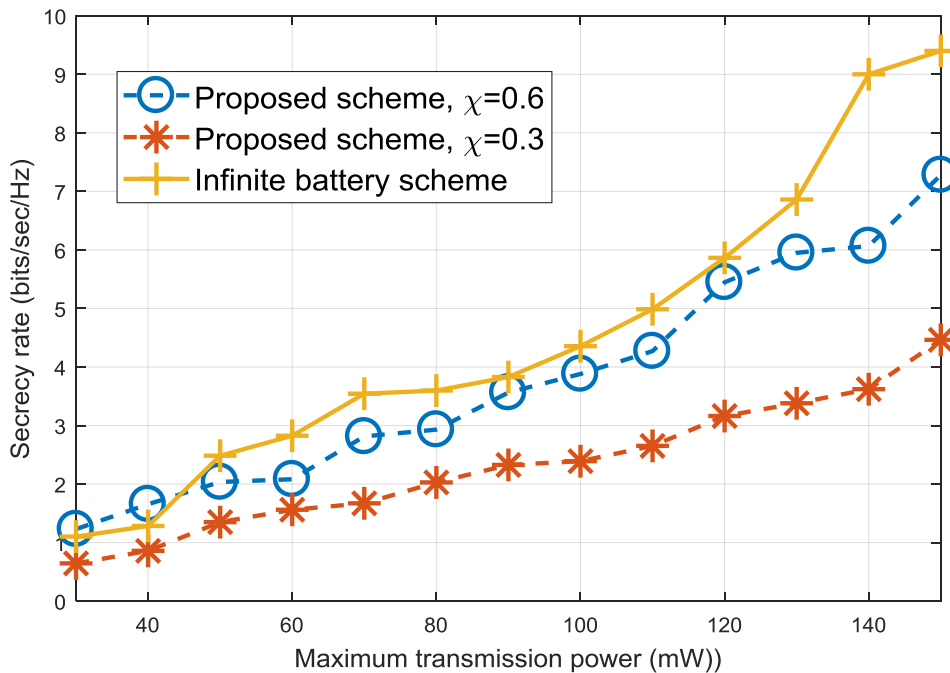


Figure 7.6 Effect of the energy harvesting rate

Figure 7.8 shows the effect of varying the number of relays for a fixed number of eavesdroppers at six. When the number of eavesdroppers equals the number of relays (as can be seen from the graph when $M=6$), the secrecy rate is the lowest. As the number of relays increases, so does the secrecy rate. It can also be seen that a certain number of relays gives almost the same performance (e.g. when $M=12$ and $M=20$). That is because the cooperative diversity gained from the small increase in the number of relays is not significant. When the number of relays increases to 32, the area covered by the relay (and hence, the spatial diversity achieved) increases. The infinite battery scheme also benefits from increases in the number of relays, but as the transmission power increases to 120 mW, the infinite battery schemes with 32 relays and 20 relays converge. We can also see from the figure that the proposed schemes converge at a transmission power of 120 mW when $M=6$, $M=12$, and $M=20$.

Figure 7.9 presents the effect of varying the number of eavesdroppers. The number of relays is fixed at four. As can be seen from the figure, when transmission power is 70 mW, the proposed scheme converges. This is because, as the number of eavesdroppers increases, so the range in the available channel gain also incorporates the eavesdroppers, which can have somewhat better channel conditions. As we increase the power beyond 70 mW, eavesdroppers with better channel conditions benefit more than the main link. A high number of eavesdroppers affects the secrecy rate, but as can be seen, although the number of eavesdroppers is double the number of relays, our proposed scheme achieves a positive secrecy rate.

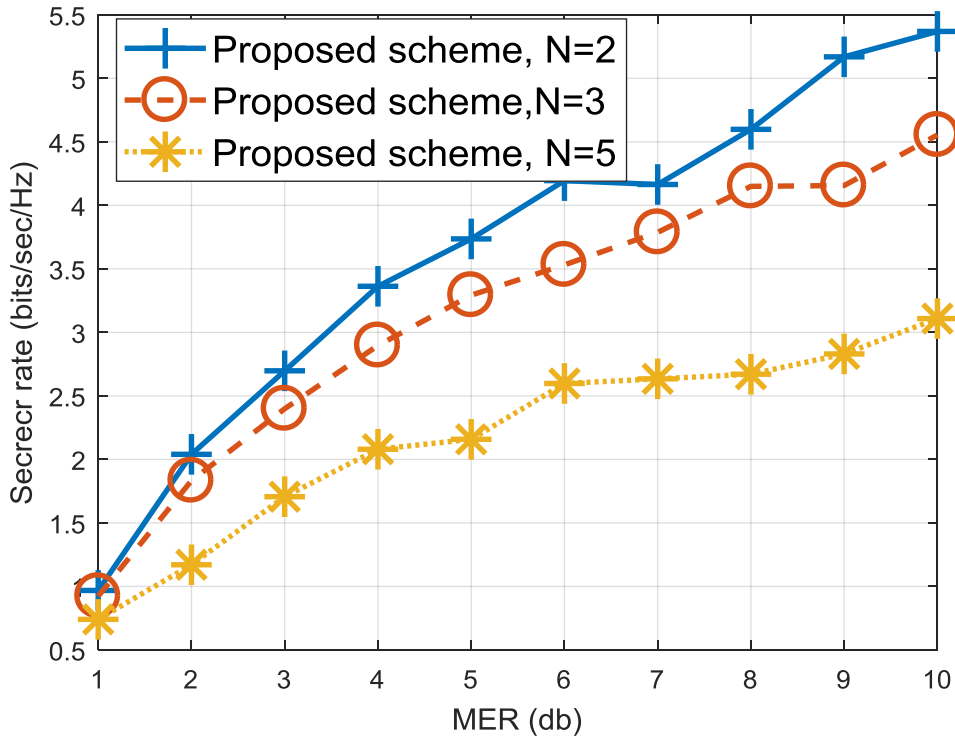


Figure 7.7 Effect of the long-term energy constraint

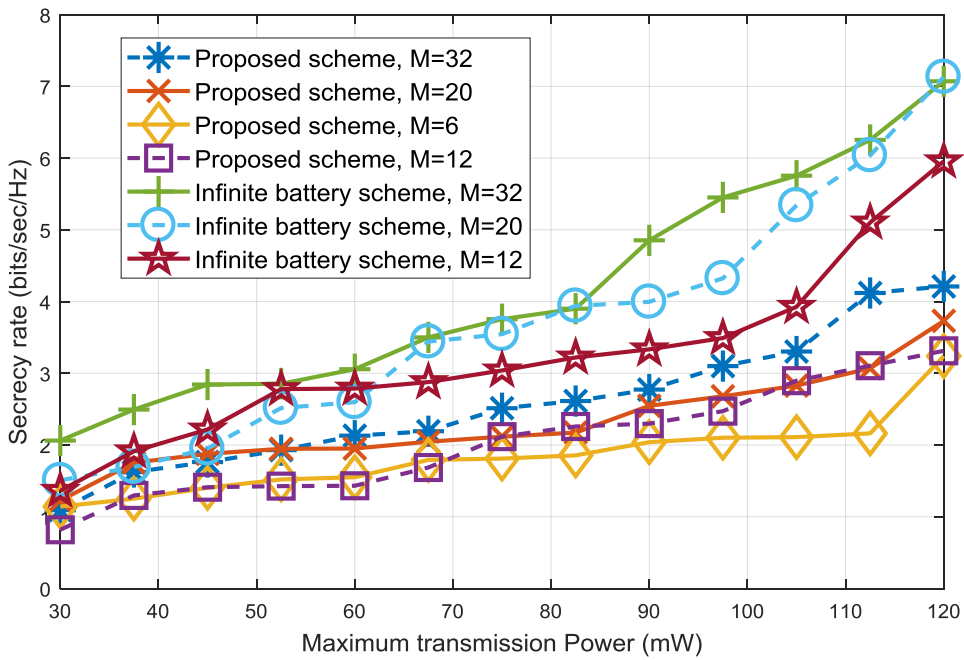


Figure 7.8 Effect of the number of relays on the secrecy rate

We compared our proposed scheme and the infinite battery scheme with our previous scheme given in reference [145] in Fig. 7.10. This is denoted as the *reference scheme*. The reference scheme employs an orthogonal frequency-division multiplexing (OFDM) technique, and solves the power allocation problem at the relay. Thus, the power allocated to the subchannels at the relay ensures that the leakage to the eavesdropper is at a minimum. The reference scheme also takes help from a jammer. Subcarrier mapping is carried at the relay, and the power allocation problem is also solved at the jammer. For the sake of comparison, we assumed the number of subchannels to be 32. In the reference scheme, the transmission is carried on all the subcarriers, while in our proposed scheme and the infinite battery scheme, there are four relays, and transmission takes place on only one subchannel. We assume there is only one eavesdropper for all three schemes, and that transmission power is 120 mW. The reference scheme outperforms our proposed scheme, but that is because the proposed scheme has little transmission power available because of the long-term energy requirements. The infinite battery scheme, which exploits cooperative diversity but has the maximum transmission power available, outperforms the reference scheme. This result confirms that cooperative diversity-based schemes outperform the AN-based scheme when the MER improves. As the MER improves, the cooperative diversity-based scheme outperforms the AN-based scheme until both converge. The proposed scheme where the long-term energy requirements are met closely follows the reference scheme in certain MER regions. After a certain MER value, the proposed scheme converges, but we can see that the proposed scheme (even under the constraint of long-term energy requirements) provides good performance in terms of secrecy rate.

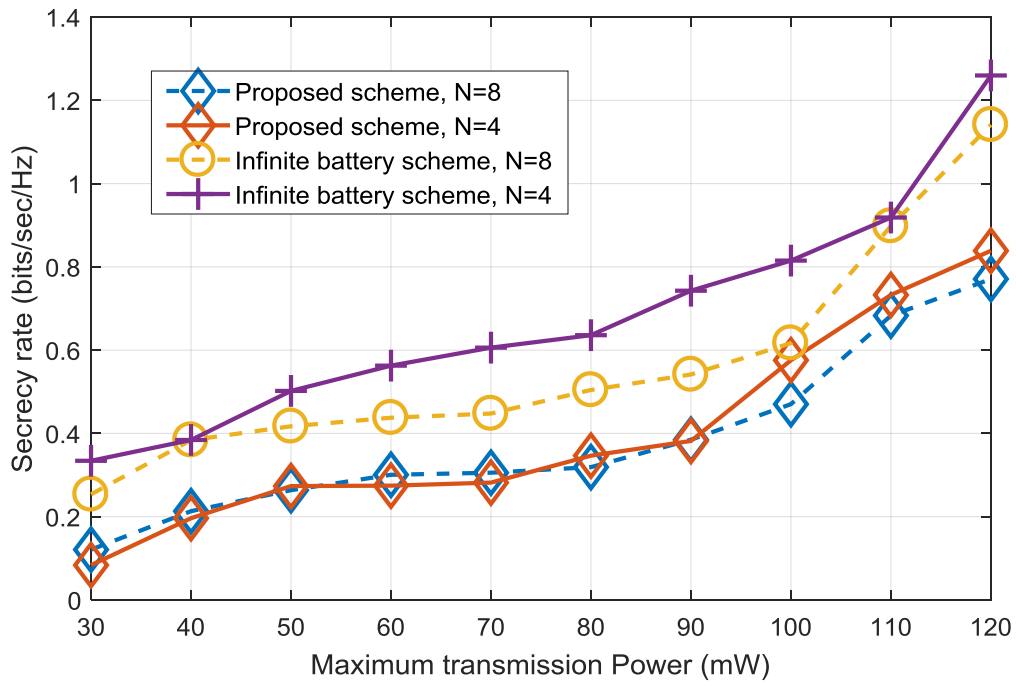


Figure 7.9 Effect of the number of eavesdroppers on secrecy rate

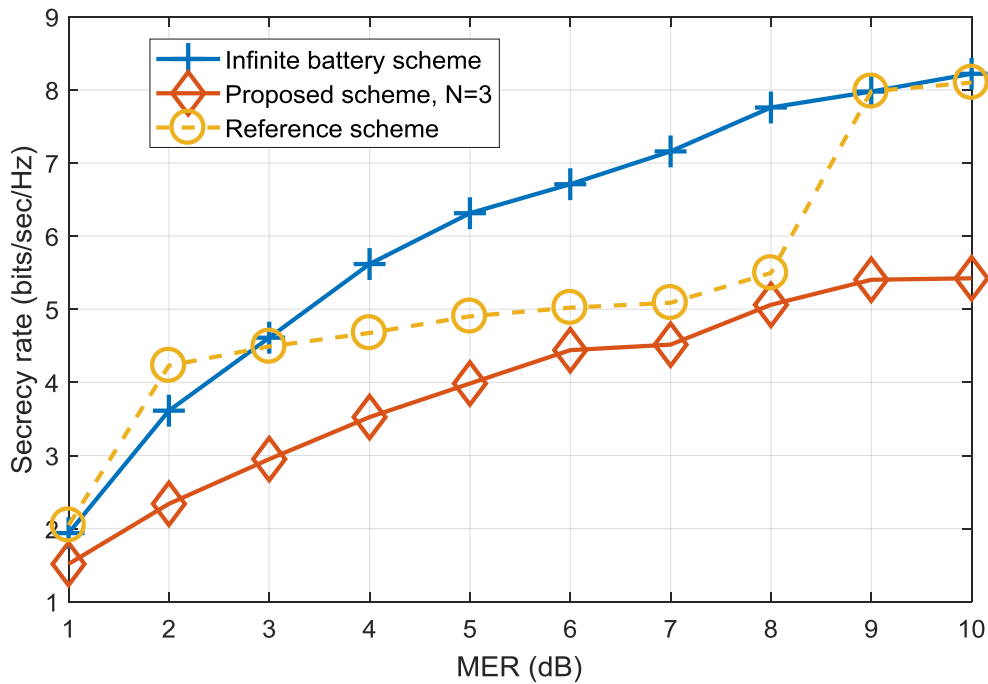


Figure 7.10 Comparison with the reference scheme

7.5 Conclusions

When the MER of the system improves, then creating AN to fend off the secrecy issues results in a needless waste of resources. Exploiting cooperative diversity to keep leakage to eavesdroppers at a minimum was studied in this paper. Multiple eavesdroppers were considered along with multiple relays, but we had to select one subchannel from multiple subchannels to transmit over. Energy-constrained relays also had the capacity to harvest energy, and relay selection was carried out under a maximum-energy constraint. The maximum energy constraint was considered to ensure long-term operation of the system. A relay with a subchannel and a transmission power factor was selected using a relay-selection/subchannel-selection algorithm that employs graph theory. The relay/subchannel selection algorithm uses priority lists, and thus, the changing conditions of wireless channels are reflected in the relay-and-subchannel selection. The algorithm also includes a power transmission factor, which is then used in the final power allocation in the selected relay to satisfy the maximum-interference constraint for the PU. The proposed algorithm reduces the computational complexity of the relay-selection and power transmission-factor selection problem. Power allocation at the source is also carried out while satisfying the PU maximum-interference constraint.

Chapter 8

Summary of Contributions and Future Work

8.1 Introduction

The main contributions of this dissertation have been presented in this chapter. Chapter 2 to chapter 7 presented the schemes and research carried out. Section 8.2 will present the main contributions of those works while section 8.3 will discuss the future research directions.

8.2 Summary of Contributions

The dissertation has focused on two aspects of cognitive radio networks. The first one is reliable spectrum sensing in a CRN and the second one contributes to the research on physical layer security. Chapter 2 to 4 are schemes and investigations into spectrum sensing while chapter 5 focuses on a joint spectrum sensing and transmission framework. Chapter 6 and 7 are contributions to research on physical layer security. The contributions of this dissertation to reliable spectrum sensing are given below:

- A Bioinformatics inspired quantization based spectrum sensing scheme for CRN has been proposed. The scheme outperformed conventional decision combination schemes. In the spectrum sensing process malicious users were assumed and the spectrum sensing process took into consideration the skewedness in the data that was introduced by the result of the malicious users. On the basis of robust statistics and an algorithm widely used in bioinformatics called Smith Waterman algorithm the score for each user was calculated and the malicious user detected. Moreover a global combination scheme was

also proposed which took into consideration the weight which is calculated from history into the final decision combination.

- Accurate quantization thresholds for spectrum sensing data were found out. The energy distribution under the hypothesis that the PU is absent and the hypothesis that the PU is present were analyzed through an iterative algorithm to find out the optimal quantization thresholds. The working of optimal quantization scheme was also analyzed theoretically. An iterative algorithm for finding the optimal quantization thresholds was proposed. The fact that the optimal thresholds also took into consideration the global decisions and the status of the optimal value of thresholds at other CR users made the optimal quantization thresholds globally applicable.
- A machine learning based spectrum sensing has been proposed. The environment in which a CRN operates is susceptible to learning and the CR users contributing to spectrum sensing can know the accuracy of the spectrum sensing process and then can make adjustments to their own sensing behaviors. The CR users assign each sensing report to a class on the basis of global decision and ACK signal. KNN is a machine learning algorithm which is resilient to errors and thus it is used for this purpose in the proposed scheme. When the training phase is complete the CR users have enough data to reflect accurately the environment and its own behavior to the changing environment. A posterior probability of the current sensing report is calculated with all the classes and on the basis of combined score a sensing decision is taken. The local and global probabilities of detection and of false alarm were also analyzed and found out theoretically.
- A joint sensing and transmission framework was considered for a CRN. Actor critic algorithm was used to decide the action taken at the CR user after the sensing decision is taken. The space of available actions also takes into consideration the future energy requirement of the user. On the basis of transition probabilities and the reward brought each state is associated with a value. In the training phase the optimal value function and optimal policy function are obtained. Moreover the sensing scheme is based on quantized values and there are multiple actions available on the basis of the residual energy so the

both the reliability of the sensing-transmission framework and its long term performance is guaranteed.

The second part of the thesis contributes to the literature on physical layer security in CRN as below:

- A physical layer security scheme for OFDM based CRN is considered. In the proposed subcarrier mapping is also considered at the forwarding relay node which ensures that the leakage to the eavesdropper is at the minimum. The power allocation is optimized at the relay and the power allocation scheme also takes into consideration the interference introduced by the jammer and the leakage to the eavesdropper. The power allocation at the forwarding relay node is a non-convex problem which is first reduced into a convex problem by relaxing the maximum transmission power constraint.
- A cooperative diversity scheme with multiple eavesdroppers has been proposed. The cooperative diversity schemes exploits the diversity brought by multiple relays and subchannel. For the sake of practical purposes the CR users are assumed to be energy-constrained and they harvest energy from ambient sources. To the literature on cooperative diversity an investigation on the multi-tier selection of relay, subchannel and a transmission power factor is contributed. The problem of relay and subchannel and transmission power factor is translated to a graph. To solve the graph problem an algorithm is proposed which calculates priority lists for each relay and each subchannel and then finds the best matching. Moreover the proposed algorithm also takes into consideration the historical preference of each relay and subchannel and thus reflects accurately the wireless channel environment.

8.3 Future Work

As is explained in the previous section the primary focus of this dissertation is reliable spectrum sensing and physical layer security in cognitive radios. Chapter 2 to 7 elaborated on the contributions and the investigations carried out on the topics. Though the research on these areas

was a detailed one there are other topics and techniques which are needed to be investigated for exhaustive details. Some of these future topics are presented below;

- The ability to sense multiple channels with multiple malicious users present is an interesting and possible extension of the work proposed in this dissertation. Sensing multiple channels and then combining the sensing decision while taking into consideration the malicious users become a hard problem as detecting which malicious activity belong to which channel is complex. Detecting malicious users in a multi-channel scenario is also a practical consideration as a CR user is interested in multiple channels at the same time.
- Other than the conventional machine learning techniques like SVM other new machine learning techniques can be applied to investigate complex scenarios like learning the behavior of multiple PUs active in the same coverage area. Layered machine learning algorithms such as deep learning and deep HMM are suitable candidates for this scenario as each layer can be dedicated to one particular PU or coverage area and all the results can be merged to have a unified perspective of the wireless environment in one region.
- Spectrum sensing is not limited to CRN. It is needed in other emerging future wireless communication technologies and applications. For instance smart grids and Internet of Things (IoT) need the techniques of spectrum sensing as they rely for most part on the presence or absence of an activity. CRN can be merged into both smart grids and IoT to efficiently use the spectrum and save the cost of dedicated leased spectrum. The amount of data generated by spectrum sensing activity of IoT and smart grids is on the scale of big data and thus machine learning algorithms like deep learning can be applied to make accurate decisions.
- The spectrum sensing techniques discussed in this dissertation wait till the end of the sensing slot to make a spectrum decision. Fast detection techniques can be incorporated in the spectrum sensing process to make an earlier detection possible. The statistical analysis of the received energy samples can be used to know the number of energy

samples required for taking an earlier decision. The earlier detection decision is beneficial both to the CRN and to the PU as it will increase the spectrum efficiency and will also ensure protection of the PU data if the PU appears during the CR user transmission.

- In future work, a joint solution to the optimization problem, where power allocation at the source, at the jamming relay node, and at the forwarding relaying node, and subcarrier mapping is done jointly to find an optimal solution to the optimization problem formulated in this OFDM based relaying network. The current system model in the respective chapter in this dissertation for the optimization problem and hence the solution do not take into consideration the effect of multiple eavesdroppers, relays and PUs. Therefore it can also be planned to extend the system model to take into consideration multiple eavesdroppers, relays and PUs.
- In future work the energy-constrained CR sender can be assumed, which in the work on cooperative diversity is assumed to have the maximum transmission power available in each time slot. The relay selection and the power transmission-factor selection (at both the CR sender and the relay) can be carried out under a unified framework. The current system model and the optimization problem focus on the relay network, and only power selection at the CR sender (while keeping it under the maximum interference constraint) is considered.

Publications

SCI (E)

1. Hurmat Ali Shah, Muhammad Usman, and Insoo Koo, "Bioinformatics-inspired quantized hard combination-based abnormality detection for cooperative spectrum sensing in cognitive radio networks," *IEEE Sensors Journal*, 15.4 (2015): 2324-2334.
2. Hurmat Ali Shah, and Insoo Koo, "A Novel Physical Layer Security Scheme in OFDM-based Cognitive Radio Networks," *IEEE Access*, 6 (2018): 29486 – 29498.
3. Hurmat Ali Shah, and Insoo Koo, "Optimal multi-threshold quantization scheme for bioinformatics inspired cooperative spectrum sensing in cognitive radio networks," *International Journal of Electronics* (2018): 1-17.
4. Hurmat Ali Shah, and Insoo Koo, "Reliable Machine Learning Based Spectrum Sensing in Cognitive Radio Networks," *Wireless Communications and Mobile Computing* (2018), <https://doi.org/10.1155/2018/5906097>.

Under-review

1. Hurmat Ali Shah, and Insoo Koo, "Improving physical layer security via cooperative diversity in energy-constrained cognitive radio networks with multiple eavesdroppers," (International Journal of Communication Systems).

Current study

1. Designing an actor-critic algorithm based combined sensing-transmission framework for energy-constrained cognitive radio networks

Others

1. Hurmat Ali Shah, Laiq Hasan, and Nasir Ahmad, "An optimized and low-cost FPGA-based DNA sequence alignment—A step towards personal genomics, " *Proc. 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Osaka, Japan, 2013*.

-
2. Hurmat Ali Shah, and Insoo Koo, "Optimal Quantization and Efficient cooperative spectrum sensing in cognitive radio networks," *Proc. 2015 International Conference on Emerging Technologies (ICET), Peshawar*, 2015.
 3. Hurmat Ali Shah, Laiq Hasan, and Insoo Koo, "Optimized and Portable FPGA-Based Systolic Cell Architecture for Smith–Waterman-Based DNA Sequence Alignment," *Journal of information and communication convergence engineering*, 14.1 (2016): 26-34.
 4. Hurmat Ali Shah et al., "On Experimental Comparison of Color and Supervised Face Detection", *Sindh Univ. Res. Jour. (Sci. Ser.)*, 44 (4) (2012): 561-564.
 5. Hurmat Ali Shah et al., "Understanding Gene Prediction: A Descriptive Analysis", *Sindh Univ. Res. Jour. (Sci. Ser.)*, 45 (1) (2013).

References

- [1] J. Mitola, "Cognitive Radio---An Integrated Agent Architecture for Software Defined Radio," Ph.D. Thesis, KTH, Stockholm, Sweden, 2000.
- [2] P. Kolodzy, "Spectrum policy task force," Federal Commun. Comm., Washington, DC, Rep. ET Docket 02-135, 2002.
- [3] F. Rongfei and H. Jiang, "Optimal multi-channel cooperative sensing in cognitive radio networks," IEEE Trans. Wireless Commun., vol. 9, no. 3, pp. 1128-1138, Mar. 2010.
- [4] J. Ma, G. Zhao and Y. Li, "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks," IEEE Trans. on Wireless Commun., vol. 7, no.11, pp. 4502-4507, 2008.
- [5] S. Kyperountas, N. Correal and Q. Shi, "A comparison of fusion rules for cooperative spectrum sensing in fading channels," EMS Research, Motorola, 2010.
- [6] H. Guo, W. Jiang and W. Luo, "Linear Soft Combination for Cooperative Spectrum Sensing in Cognitive Radio Networks," IEEE Communications Letters, vol. 21, no. 7, pp. 1573-1576,
- [7] Ghasemi, Amir, and Elvino S. Sousa. "Collaborative spectrum sensing for opportunistic access in fading environments.", IEEE Int. Symp. on New Frontiers in Dynamic Spectrum Access Networks DYSPAN 2005, pp.131-136.
- [8] Fan, Rongfei, and Hai Jiang. "Channel sensing-order setting in cognitive radio networks: A two-user case.", IEEE Trans. Veh. Technol., vol. 58, no. 9, pp. 4997-5008, Nov. 2009.
- [9] Liang, Ying-Chang, et al. "Sensing-throughput tradeoff for cognitive radio networks", IEEE Trans. Wireless Commun., vol. 7, no. 4: pp.1326-1337, Apr. 2008.
- [10] Zeng, Kun, and Youxi Tang. "Impact of Misbehaviors in Cooperative Spectrum Sensing for Cognitive Radio Networks", Proc. IEEE Int. Conf. Wireless Communications, Networking and Mobile Computing (WiCOM 2011), pp.1-4.

-
- [11] Sakran, Hefdhallah, and Mona Shokair. "Hard and softened combination for cooperative spectrum sensing over imperfect channels in cognitive radio networks", *Telecommun. Syst.*, vol. 52, no.1, pp. 61-71, Jan. 2013.
- [12] G. A. S. Sidhu, F. Gao, W. Wang, and W. Chen, "Resource allocation in relay-aided OFDM cognitive radio networks," *IEEE Trans. Vehicular Technology*, vol. 62, no. 8, pp. 3700-3710, 2013.
- [13] N. Zhing, N. Lu, N. Cheng, J. W. Mark, and X. S. Shen, "Cooperative spectrum access towards secure information transfer for CRNs," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 11 pp. 2453-2464, 2013.
- [14] Li, Husheng, and Zhu Han. "Catch me if you can: an abnormality detection approach for collaborative spectrum sensing in cognitive radio networks", *IEEE Trans. Wireless Commun.*, vol.9, no.11, pp.3554-3565, Nov. 2010.
- [15] Wang, W., Li, H., Sun, Y. L., and Han, Z. "Attack-proof collaborative spectrum sensing in cognitive radio networks", *IEEE Conf. Information Sciences and Systems (CISS 2009)*, pp. 130-134.
- [16] Zheng, Yi, Xianzhong Xie, and Lili Yang. "Cooperative spectrum sensing based on SNR comparison in fusion center for cognitive radio.", *IEEE Conf. Advanced Computer Control(ICACC 2009)*, pp.212-216
- [17] Chen, Ruiliang, Jung-Min Park, Y. Thomas Hou, and Jeffrey H. Reed. "Toward secure distributed spectrum sensing in cognitive radio networks", *IEEE Commun. Mag.*, vol. 46, no. 4 , pp.50-55, Apr. 2008.
- [18] Noon, Evan, and Husheng Li. "Defending against hit-and-run attackers in collaborative spectrum sensing of cognitive radio networks: A point system", *IEEE Vehic. Tech. Conf. (VTC 2010-Spring)*, pp.1-5
- [19] M. Usman and I. Koo, "Secure cooperative spectrum sensing for the cognitive radio network using non-uniform reliability", *The Scientific World Journal*, vol. 2014, p. 10, Aug. 2014
- [20] Rawat, Ankit Singh, et al. "Countering byzantine attacks in cognitive radio networks", *IEEE Int. Conf. Acoustics Speech and Signal Processing (ICASSP 2010)*, pp.3098-3101.
- [21] Birkan Yilmaz, H., Tuna Tugcu, and Fatih Alagoz. "Novel quantization- based spectrum sensing scheme under imperfect reporting channel and false reports", *Int. J. Commun. Sys.*, vol. 27, no.10, pp. 1459-1475, Oct. 2014.
- [22] Chen, Ruiliang, Jung-Min Park, and Kaigui Bian. "Robust distributed spectrum sensing in cognitive radio networks", *IEEE Conf. Computer Communications (INFOCOM 2008)*.
- [23] Kaligineedi, Praveen, and Vijay K. Bhargava. "Sensor allocation and quantization schemes for multi-band cognitive radio cooperative sensing system", *IEEE Trans. Wireless Commun.*, vol. 10, no.11, pp.284-293, Jan. 2011.

-
- [24] S. Eryigit, S. Bayhan, and T. Tugcu, "Energy-efficient multi-channel cooperative sensing scheduling with heterogeneous channel conditions for cognitive radio networks," *IEEE Trans. on Vehic. Tech.*, vol. 62, no. 6, Feb. 2013.
- [25] Needleman, Saul B., and Christian D. Wunsch. "A general method applicable to the search for similarities in the amino acid sequence of two proteins", *J. Mol. Bio.*, vol. 48, no. 3, pp. 443-453, Mar. 1970.
- [26] Smith, Temple F., and Michael S. Waterman. "Comparison of biosequences", *Adv. Appl. Math.*, vol. 2, no.4, pp. 482-489, Dec. 1981.
- [27] Huber, Peter J. *Robust statistics*, Springer Berlin Heidelberg, 2011.
- [28] X. Zhang, Q. Wu, and J. Wang, "Optimization of sensing time in multichannel sequential sensing for cognitive radio," *International Journal of Communication Systems*, vol. 26, no. 2, pp. 222-235, Feb. 2013.
- [29] Y. Chen, "Analytical performance of collaborative spectrum sensing using censored energy detection," *IEEE Trans. Wireless Commun.*, vol .9, no. 12 ,pp. 3856-3865, Dec. 2010.
- [30] M. B. Ghorbel, H. Nam, and M. S. Alouini,, "Exact Performance of Cooperative Spectrum Sensing for Cognitive Radios with Quantized Information under Imperfect Reporting Channels," *IEEE 78th Vehicular Technology Conference (VTC Fall)*, pp. 1-5, Sept. 2013.
- [31] Y. Liu et al., "Adaptive double threshold energy detection based on Markov model for cognitive radio," *PloS one*, vol. 12, no. 5, e0177625.
- [32] S. Ghosh et al., "Performance of weighted fusion based spectrum sensing under double threshold in cognitive radio network," in *proc. IEEE International conference on Microelectronics, Computing and Communications (MicroCom)*, Durgapur, 2016, pp. 1-4.
- [33] D. Das, and S. Das, "A novel approach for energy- efficient resource allocation in double threshold based cognitive radio network," *International journal of Communication Systems*, vol. 30, no. 9, June 2017, DOI: 10.1002/dac.3198.
- [34] S. Zhu, C. Guo, C. Feng, and X. Liu, "User correlation and double threshold based cooperative spectrum sensing in dense cognitive vehicular networks," in *proc. IEEE International Symposium on Wireless Communication Systems (ISWCS)*, Poznan, 2016, pp. 281-285.
- [35] A. Bagwari, and G. S. Tomar, "Adaptive double-threshold based energy detector for spectrum sensing in cognitive radio networks," *International journal of Electronics Letter*, vol. 1, no. 1, pp. 24-32, 2013.

-
- [36] A. Bagwari, and G. S. Tomar, "Cooperative spectrum sensing with adaptive double-threshold based energy detector in cognitive radio networks," *Wireless Personal Communications*, vol. 73, No.3, pp 1005-1019, 2013.
- [37] A. Singh, M. R. Bhatnagar, and R. K. Mallik, "Cooperative spectrum sensing in multiple antenna based cognitive radio network using an improved energy detector," *IEEE Communications Letters*, vol. 16, no. 1, pp. 64-67, 2012.
- [38] A. Singh, M. R. Bhatnagar, and R. K. Mallik, "Threshold optimization of a finite sample-based cognitive radio network using energy detector," *EURASIP Journal on Wireless Communications and Networking*, vol. 1, pp. 1-17, 2013.
- [39] A. Singh, M. R. Bhatnagar, and R. K. Mallik, "Optimization of cooperative spectrum sensing with an improved energy detector over imperfect reporting channels," in *proc. IEEE Vehicular Technology Conference (VTC Fall)*, San Francis, pp. 1-5, 2011.
- [40] Z. Han, R. Zheng and H. V. Poor, "Repeated auctions with Bayesian nonparametric learning for spectrum access in cognitive radio networks," *IEEE Trans. on Wireless Comm.*, vol. 10, no. 3, pp. 890-900, 2011.
- [41] J. Lundén et al., "Reinforcement learning based distributed multiagent sensing policy for cognitive radio networks," in *proc. IEE symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, Aachen, 2011.
- [42] M. Bkassiny, K. J. Sudharman and K. A. Avery, "Distributed Reinforcement Learning based MAC protocols for autonomous cognitive secondary users," in *proc. 20th Annu. IEE Conf. Wireless and Optical Communications Conference (WOCC)*, Taiwan, 2011.
- [43] A. Galindo-Serrano and L. Giupponi, "Distributed Q-learning for aggregated interference control in cognitive radio networks," *IEEE Trans. Veh. Techn.*, vol. 59, no. 4, pp. 823-1834, 2010.
- [44] B. Y. Reddy, "Detecting primary signals for efficient utilization of spectrum using Q-learning," in *proc. IEEE 5th Annu. Conf. Information Technology: New Generations*, Nevada, 2008.
- [45] Q. Zhu, Z. Han and T. Başar, "No-regret learning in collaborative spectrum sensing with malicious nodes," in *proc. IEE International Conf. Communications*, Cape Town, 2010.
- [46] T. K. Madushan et al., "Machine learning techniques for cooperative spectrum sensing in cognitive radio networks," *IEEE Journal on Selected Areas in Comm.*, vol. 31, no. 11, pp. 2209-2221, 2013
- [47] M.Y. Kiang, "A comparative assessment of classification methods," *Decision Support Systems*, vol. 35, no.4, pp. 441-454, 2003.

-
- [48] K. M. Thilina, K. W. Choi, N. Saquib and E. Hossain, "Pattern classification techniques for cooperative spectrum sensing in cognitive radio networks: SVM and W-KNN approaches," IEEE Global Communications Conference , Anaheim, CA,, pp. 1260-1265, 2012.
- [49] Mengyun Tang, Ze Zheng, G. Ding and Zhen Xue, "Efficient TV white space database construction via spectrum sensing and spatial inference," IEEE 34th International Performance Computing and Communications Conference , Nanjing, pp. 1-5, 2015
- [50] A. M. Mikaeil, B. Guo and Z. Wang, "Machine Learning to Data Fusion Approach for Cooperative Spectrum Sensing," International Conf., on Cyber-Enabled Distributed Computing and Knowledge Discovery, Shanghai, pp. 429-434, 2014.
- [51] J. Kanti, G.S. Tomar and A. Bagwari, "A Novel Multiple Antennas Based Centralized Spectrum Sensing Technique," Lecture Notes in Computer Science, vol. 10220, 2017.
- [52] A. Bagwari, G. S. Tomar, "Cooperative Spectrum Sensing Based on Two-Stage Detectors With Multiple Energy Detectors and Adaptive Double Threshold in Cognitive Radio Networks," Canadian Journal of Electrical and Computer Engineering, vol., 36, no, 4, pp. 172-180, 2013.
- [53] J. Kanti, G.S. Tomar and A. Bagwari, "An improved-two stage detection technique for IEEE 802.22 WRAN," Optik-International Journal for Light and Electron Optics, vol. 140, pp. 695-708, 2017.
- [54] J. Kanti and G. S. Tomar, "Improved sensing detector for wireless regional area networks," Cogent Engineering, doi: <https://doi.org/10.1080/23311916.2017.1286729>, 9 Feb, 2017.
- [55] A. Samarah et al., "Double Stage Energy Detectors for Sensing Spectrum in Cognitive Radio Networks," Fifth International Con. On Communication Systems and Network Technologies, Gwalior, India, 2015, doi: 10.1109/CSNT.2015.259.
- [56] [A. Bagwari and G.S. Tomar, "Cooperative Spectrum Sensing with Multiple Antennas Using Adaptive Double-Threshold Based Energy Detector in Cognitive Radio Networks," Journal of the Institution of Engineers (India): Series B, vol. 95, no. 2, pp. 107-112, 2014.
- [57] A. Bagwari and G. S. Tomar,"Comparison between Adaptive Double-Threshold Based Energy Detection and Cyclostationary Detection Technique for Cognitive Radio Network," Fifth International Conference on Computer Intelligence and Communication Networks, Mathura, India, doi: 10.1109/CICN.2013.47, Sept, 2013.
- [58] K. M. Thilina, K. W. Choi, N. Saquib and E. Hossain, "Pattern classification techniques for cooperative spectrum sensing in cognitive radio networks: SVM and W-KNN approaches," 2012 IEEE Global

- Communications Conference (GLOBECOM), Anaheim, CA, 2012, pp. 1260-1265. doi: 10.1109/GLOCOM.2012.6503286.
- [59] Mengyun Tang, Ze Zheng, G. Ding and Zhen Xue, "Efficient TV white space database construction via spectrum sensing and spatial inference," 2015 IEEE 34th International Performance Computing and Communications Conf. (IPCCC), Nanjing, 2015, pp. 1-5. doi: 10.1109/PCCC.2015.7410268,
- [60] A. M. Mikaeil, B. Guo and Z. Wang, "Machine Learning to data fusion approach for cooperative spectrum sensing," 2014 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Shanghai, 2014, pp. 429-434. doi: 10.1109/CyberC.2014.80.
- [61] Y. C. Liang et al., "Sensing-throughput tradeoff for cognitive radio networks," IEEE Trans. Wireless Commun., vol. 7, no. 4, pp.1326-1337, 2008.
- [62] Y. C. Liang et al., "Sensing-throughput tradeoff for cognitive radio networks," IEEE Trans. Wireless Commun., vol. 7, no. 4, pp.1326-1337, 2008.
- [63] T. Kenichi et al., "IEEE 802.21: Media independent handover: Features, applicability, and realization," IEEE Communications Magazine, vol. 47, no. 1, pp. 112-120, 2009.
- [64] M. Usman and I. Koo, "Secure cooperative spectrum sensing via a novel user-classification scheme in cognitive radios for future communication technologies," Symmetry, vol. 7, no. 2, pp. 675-688, 2015.
- [65] H. B. Yilmaz, T. Tugcu and F. Alagoz, "Novel quantization-based spectrum sensing, scheme under imperfect reporting channel and false reports," International Journal of Communication Systems, vol. 27, no. 10, pp. 1459-1475, 2014.
- [66] H. V. V-Van and I. Koo, "A cluster-based sequential cooperative spectrum sensing scheme utilizing reporting framework for cognitive radios," IEEJ Trans. Electrical and Electronic Engineering, doi: 10.1002/tee.21968, 21 April, 2014.
- [67] H. Sakran et al., "Three bits softened decision scheme in cooperative spectrum sensing among cognitive radios," 28th National Radio Science Conference, Cairo, Egypt, doi : 10.1109/NRSC.2011.5873630, April 2011.
- [68] F. Gabry et al., "Energy efficiency analysis of cooperative jamming in cognitive radio networks with secrecy constraints," IEEE Wireless Communications Letters, vol. 4, no. 4, pp. 437-470, 2015.
- [69] V. R. Konda, and J. N. Tsitsiklis, "Actor-critic algorithms." Advances in neural information processing systems. 2000.

-
- [70] R.S. Sutton, and A.G. Barto, "Reinforcement Learning: An Introduction", MIT Press, 1998.
- [71] L. Ozarow and A. Wyner, "Wiretap channel II," in *Advances in Cryptology*, Springer, pp-33-50, 1985.
- [72] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Processing*, vol. 61, no. 20, pp. 4962-4974, 2013.
- [73] A. K. Sadek, W. Su, and K.J.R. Liu, "Multinode cooperative communications in wireless networks," *IEEE Trans. Signal Processing*, vol. 55, no.1, pp. 341-355, 2007.
- [74] K.G. Seddik, A.K. Sadek, W. Su, and K.J. R. Liu, "Outage analysis and optimal power allocation for multinode relay networks," *IEEE Signal Processing Letters*, vol. 14, no.6, pp. 377-380, 2007.
- [75] L. Hu, B. Wu, J. Tang et al., "Outage constrained secrecy rate maximization using artificial-noise aided beamforming and cooperative jamming," in *Proc. IEEE-ICC*, Kuala Lumpur, Malaysia, 2016.
- [76] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," In *proc. IEEE-ICASP*, Taipei, Taiwan, 2009, pp-2437-2440.
- [77] S. Sarma and J. Kuri, "SNR based secure communication via untrusted amplify-and-forward relay nodes using artificial noise," *Wireless Networks* , pp. 1-12, 2016.
- [78] J. Zhang, G. Pan, and H.M. Wang, "On physical-layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system," *IEEE Access*, vol.4, pp.3887-3893, 2016.
- [79] T. Zhang, Y. Chai, Y. Huang et al., "Secure full-duplex spectrum-sharing wiretap networks with different antenna reception schemes," *IEEE Trans. Communications*, vol.65, no.1, pp. 335-346, 2017.
- [80] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Processing Letters*, vol.22, no.8, pp. 1147-1151, 2015.
- [81] N. Zhao, F. R. Yu, M. Li et al. , "Physical layer security issues in interference-alignment-based wireless networks," *IEEE Communications Magazine*, vol.54, no.8,pp. 162-168, 2016.
- [82] K. Cumanan, h. Xing, P. Xu et al., "Physical layer security jamming: Theoretical limits and practical designs in wireless networks," *IEEE Access*, vol.5, pp. 3603-3611, 2017.
- [83] G. Zheng, L.C. Choo, and K. K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Processing*, vol. 59, no. 3, pp. 1317-1322, 2011.
- [84] I. Krikidis, J.S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Communications*, vol. 8, no.10, pp. 5003-5011, 2009.

-
- [85] Z. Ding, M. Peng, and H. H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Trans. Communications*, vol. 60, no. 11, pp-3461-3471, 2012.
- [86] H. M. Wang, Q. Yin, and X. G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Processing*, vol.60, no.7, pp. 3532-3545, 2012.
- [87] K. Lee, C. B. Chae, and J. Kang, "Spectrum leasing via cooperation for enhanced physical-layer secrecy," *IEEE Trans. Vehicular Technology*, vol. 62, no.9, pp-4672-4678, 2013.
- [88] H. Mu, M. Tao, W. Dang, and Y. Xiao, "Joint subcarrier-relay assignment and power allocation for decode-and-forward multi-relay OFDM systems," In *proc. IEEE Fourth International Conference on Communications and Networking in China*, pp. 1-6, 2009.
- [89] C. K. Ho, R. Zhang, and Y.C. Liang, "Two-way relaying over OFDM: optimized tone permutation and power allocation," In *proc. IEEE-ICC, Beijing, China*, pp. 3908-3912, 2008.
- [90] K. Jitvanichphaibool, Y.C. Liang, and R. Zhang, "Beamforming and power control for multi-antenna cognitive two-way relaying," In *proc. IEEE Conference on Wireless Communications and Networking, Budapest, Hungary*, pp.1-6, 2009.
- [91] G. Bansal, M. J. Hossain, and V. K. Bhargava, "Adaptive power loading for OFDM-based cognitive radio systems," *IEEE Trans. Wireless Communications*, vol.10, no.9, pp.2786-2791, 2011.
- [92] S. Yan and X. Wang, "Power allocation for cognitive radio systems based on nonregenerative OFDM relay transmission," In *proc. IEEE 5th International Conference on Wireless Communications, Networking and Mobile Computing, Beijing, China*, pp.1-4, 2009.
- [93] J. Jia, J. Zhang, and Q. Zhang, "Cooperative relay for cognitive radio networks," In *proc. of IEEE-INFOCOM, Rio de Janeiro, Brazil*, pp. 2304-2312, 2009.
- [94] M. Herdin, "A chunk based OFDM amplify-and-forward relaying scheme for 4G mobile radio systems," In *proc. IEEE-ICC, Istanbul, Turkey*, vol. 10, pp. 4507-4512, 2006.
- [95] I. Hammerstrom and A. Wittneben, "Power allocation schemes for amplify-and-forward MIMO-OFDM relay links," *IEEE Trans. Wireless Communications*, vol. 6, no.8, 2007.
- [96] Y. Li, W. Wang, J. Kang, and M. Peng, "Subcarrier pairing for amplify-and-forward and decode-and-forward OFDM relay links," *IEEE Communications Letters*, vol. 13, no.4, pp. 209-211, 2009.
- [97] C. M. Yetis, T. Gao, S. A. Jafar, and A. H. Kayran, "On feasibility of interference alignment in MIMO interference networks," *IEEE Trans. Signal Processing*, vol. 58, no.9, pp. 4771-4782, 2010.

-
- [98] J. Xie and S. Ulukus, "Secure degrees of freedom of K-user Gaussian interference channels: A unified view," *IEEE Trans. Info. Theory*, vol. 61, no. 5, pp. 2647-2661, 2015.
- [99] A. Khisti and D. Zhang, "Artificial-noise alignment for secure multicast using multiple antennas," *IEEE Communications Letters*, vol. 17, no. 8, pp. 1568–1571, 2013.
- [100] A. Khisti, "Interference alignment for the multiantenna compound wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2976–2993, 2011.
- [101] Z. Zhou and Q. Zhu, "Joint optimization scheme for power allocation and subcarrier pairing in OFDM-based multi-relay networks," *IEEE Communications Letters*, vol. 18, no. 6, pp.1039-1042, 2014.
- [102] M. Choi, J. Park, and S. Choi, "Simplified power allocation scheme for cognitive multi-node relay networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 6, pp. 2008–2012, Jun. 2012
- [103] J. Dorleus, R. Holweck, Z. Ren et al., "Modeling and simulation of fading and pathloss in opnet for range communications," In *proc. IEEE Radio and Wireless Symposium*, Long Beach, CA, USA, 2007, DOI: 10.1109/RWS.2007.351854.
- [104] F. Gabry, A. Zappone, R. Thobaben et al., "Energy efficiency analysis of cooperative jamming in cognitive radio networks with secrecy constraints." *IEEE Wireless Communications Letters*, vol. 4, no.4, 437-440, 2015.
- [105] Z. Shu, Yi Qian, and Song Ci, "On physical layer security for cognitive radio networks," *IEEE Network*, vol.27, no., pp. 28-33, 2013.
- [106] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 5103-5113, 2013.
- [107] C.E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656-715, 1949.
- [108] S. K. Leung-Yan-Cheong, and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE transactions on information theory*, vol 24, no. 4, 451-456, 1978.
- [109] G. Zheng, I. Krikidis, J. Li, A.P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Processing*, vol. 61, no. 20, pp. 4962-4974, 2013.
- [110] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Proces.*, vol. 58, no. 3, pp. 1875–1888, 2010.

-
- [111] J. Li, A. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Processing*, no. 99, pp. 1–1, 2011
- [112] 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.
- [113] G. Zheng, L. Choo, and K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Proces.*, vol. 59, no. 3, pp. 1317–1322, 2011.
- [114] J. Li, A. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Processing*, no. 99, pp. 1–1, 2011
- [115] S. Goel, and R. Negi. "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no.6, pp. 2180-2189,2008.
- [116] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," In *proc. Of IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 2437-2440, 2009
- [117] Li, Qiang, Wing-Kin Ma, and Anthony Man-Cho So, "Safe convex approximation to outage-based MISO secrecy rate optimization under imperfect CSI and with artificial noise," In *proc. of IEEE Forty Fifth Conference on Signals, Systems and Computers*, pp. 207-211, 2011.
- [118] J. N. Laneman, G.W. Wornell, "Distributed space-time-coded protocols for exploiting cooperative diversity in wireless networks," *IEEE Transactions on Information theory*, vol. 49, no.10, pp. 2415-2425, 2003
- [119] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099-2111 , 2013.
- [120] M. Safar, M. Uysal, and K. Zhang, "Cooperative Diversity over Log-Normal Fading Channels," In *Information Theory, IEEE 10th Canadian Workshop on*, pp. 13-16. 2007.
- [121] F. Oggier, and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," In *Information Theory, 2008. IEEE International Symposium on*, pp. 524-528, 2008.
- [122] E. Tekin, and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp.2735-2751, 2008.
- [123] Y. Zou, X. Wang, and W. Shen, "Eavesdropping attack in collaborative wireless networks: Security protocols and intercept behavior," In *IEEE 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pp. 704-709, 2013.

-
- [124] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE transactions on wireless communications*, vol. 12, no. 12, pp. 6076-6085, 2013.
- [125] S. Luo, H. Godrich, A. Petropulu, and H. Vincent Poor, "A knapsack problem formulation for relay selection in secure cooperative wireless communication," In *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 2512-2515, 2011.
- [126] Heidarpour, A. Reza, G. K. Kurt, and M. Uysal. "Finite-SNR diversity-multiplexing tradeoff for network coded cooperative OFDMA systems." *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1385-1396, 2017.
- [127] R. Waseem, H. Nasir, N. Javaid et al., "Buffer size and link quality based cooperative relay selection in wireless networks," In *13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 1489-1494, 2017.
- [128] Swamy, V. Narasimha, S. Suri et al., "Real-time cooperative communication for automation over wireless," *IEEE Transactions on Wireless Communications*, vol. 16, no. 11, pp. 7168-7183, 2017.
- [129] S. Park, H. Kim, and D. Hong, "Cognitive radio networks with energy harvesting." *IEEE Transactions on Wireless communications*, vol. 12, no. 3, pp. 1386-1397, 2013.
- [130] L. Cai., H. Poor, Y. Liu, T. Luan, X. Shen, and J. Mar, "Dimensioning network deployment and resource management in green mesh networks," *IEEE Wireless Communications*, vol. 18, no. 5, pp. 58-65, 2011.
- [131] Y. Pei, Y. Liang, K. Teh, and K. Li, "Energy-efficient design of sequential channel sensing in cognitive radio networks: optimal sensing strategy, power allocation, and sensing order," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 8, pp. 1648-1659, 2011.
- [132] Y. Chen, Q. Zhao, and A. Swami, "Distributed spectrum sensing and access in cognitive radio networks with energy constraint," *IEEE transactions on signal processing*, vol. 57, no. 2, pp. 783-797, 2009.
- [133] A. T. Hoang, Y.-C. Liang, D. C. Wong, Y. Zeng, and R. Zhang, "Opportunistic spectrum access for energy-constrained cognitive radios," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1206-1211, 2009.
- [134] J. Yang, O. Ozel, and S. Ulukus, "Broadcasting with an energy harvesting rechargeable transmitter," *IEEE Transactions on Wireless Communications*, vol. 11, no. 2, pp. 571-583, 2012.
- [135] H. Li, N. Jaggi, and B. Sikdar, "Relay scheduling for cooperative communications in sensor networks with energy harvesting," *IEEE Transactions on Wireless Communications*, vol. 10, no. 9, pp. 2918-2928, 2011.

-
- [136] I. Krikidis, T. Charalambous, and J. Thompson, "Stability analysis and power optimization for energy harvesting cooperative networks," *IEEE Signal Processing Letters*, vol. 19, no. 1, pp. 20-23, 2012.
- [137] L. Wang, K. Wong, S. Jin et al., "A new look at physical layer security, caching, and wireless energy harvesting for heterogeneous ultra-dense networks," *IEEE Communications Magazine*, vol. 56, no. 6, pp. 49-55, 2018.
- [138] M. Anisi, G. Abdul-Salaam, M. Idris et al., "Energy harvesting and battery power based routing in wireless sensor networks," *Wireless Networks*, vol. 23, no. 1, pp. 249-266, 2017.
- [139] F. Akhtar, and M. Rehmani, "Energy harvesting for self-sustainable wireless body area networks," *IT Professional*, vol. 19, no. 2, pp. 32-40, 2017.
- [140] B. Di, S. Bayat, L. Song, Y. Li, and Z. Han, "Joint user pairing, subchannel, and power allocation in full-duplex multi-user ofdma networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 260-8272, 2016.
- [141] A. Stajkic, F. Clazzer, and G. Liva, "Neighbor discovery in wireless networks: A graph-based analysis and optimization." In *IEEE International Conference on Communications Workshops (ICC)*, pp. 511-516, 2016.
- [142] H. Mu, M. Tao, W. Dang, Y. Xiao, "Joint subcarrier-relay assignment and power allocation for decode-and-forward multi-relay OFDM systems," In *proc. of IEEE Fourth International Conference on Communications and Networking in China*, pp. 1-6, 2009.
- [143] J. Dorleus, R. Holweck, Z. Ren et al., "Modeling and simulation of fading and pathloss in opnet for range communications," In *IEEE Radio and Wireless Symposium, Long Beach, CA, USA*, pp. 407-410, 2007.
- [144] F. Gabry, A. Zappone, R. Thobaben et al., "Energy efficiency analysis of cooperative jamming in cognitive radio networks with secrecy constraints," *IEEE Wireless Communications Letters*, vol. 4, no. 4 pp. 437-440, 2015.
- [145] H. A. Shah, and I. Koo, "A Novel Physical Layer Security Scheme in OFDM-based Cognitive Radio Networks," *IEEE Access*, 2018, doi: 10.1109/ACCESS.2018.2842826.