

Electronic Theses and Dissertations, 2004-2019

2015

Opportunistic Spectrum Utilization by Cognitive Radio Networks: Challenges and Solutions

Muhammad Faisal Amjad
University of Central Florida

 Part of the [Computer Sciences Commons](#), and the [Engineering Commons](#)
Find similar works at: <https://stars.library.ucf.edu/etd>
University of Central Florida Libraries <http://library.ucf.edu>

This Doctoral Dissertation (Open Access) is brought to you for free and open access by STARS. It has been accepted for inclusion in Electronic Theses and Dissertations, 2004-2019 by an authorized administrator of STARS. For more information, please contact STARS@ucf.edu.

STARS Citation

Amjad, Muhammad Faisal, "Opportunistic Spectrum Utilization by Cognitive Radio Networks: Challenges and Solutions" (2015). *Electronic Theses and Dissertations, 2004-2019*. 49.
<https://stars.library.ucf.edu/etd/49>

OPPORTUNISTIC SPECTRUM UTILIZATION BY COGNITIVE RADIO NETWORKS:
CHALLENGES AND SOLUTIONS

by

MUHAMMAD FAISAL AMJAD
M.S. National University of Sciences and Technology Pakistan, 2005

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in the Department of Electrical Engineering and Computer Science
in the College of Engineering and Computer Science
at the University of Central Florida
Orlando, Florida

Spring Term
2015

Major Professor: Cliff C. Zou

© 2015 Muhammad Faisal Amjad

ABSTRACT

Cognitive Radio Network (CRN) is an emerging paradigm that makes use of Dynamic Spectrum Access (DSA) to communicate opportunistically, in the un-licensed Industrial, Scientific and Medical bands or frequency bands otherwise licensed to incumbent users such as TV broadcast. Interest in the development of CRNs is because of severe under-utilization of spectrum bands by the incumbent Primary Users (PUs) that have the license to use them coupled with an ever-increasing demand for unlicensed spectrum for a variety of new mobile and wireless applications. The essence of Cognitive Radio (CR) operation is the cooperative and opportunistic utilization of licensed spectrum bands by the Secondary Users (SUs) that collectively form the CRN without causing any interference to PUs' communications.

CRN operation is characterized by factors such as network-wide quiet periods for cooperative spectrum sensing, opportunistic/dynamic spectrum access and non-deterministic operation of PUs. These factors can have a devastating impact on the overall throughput and can significantly increase the control overheads. Therefore, to support the same level of QoS as traditional wireless access technologies, very closer interaction is required between layers of the protocol stack.

Opportunistic spectrum utilization without causing interference to the PUs is only possible if the SUs periodically sense the spectrum for the presence of PUs' signal. To minimize the effects of hardware capabilities, terrain features and PUs' transmission ranges, DSA is undertaken in a collaborative manner where SUs periodically carry out spectrum sensing in their respective geographical locations. Collaborative spectrum sensing has numerous security loopholes and can

be favorable to malicious nodes in the network that may exploit vulnerabilities associated with DSA such as launching a spectrum sensing data falsification (SSDF) attack. Some CRN standards such as the IEEE 802.22 wireless regional area network employ a two-stage quiet period mechanism based on a mandatory Fast Sensing and an optional Fine Sensing stage for DSA. This arrangement is meant to strike a balance between the conflicting goals of proper protection of incumbent PUs' signals and optimum QoS for SUs so that only as much time is spent for spectrum sensing as needed. Malicious nodes in the CRN however, can take advantage of the two-stage spectrum sensing mechanism to launch smart denial of service (DoS) jamming attacks on CRNs during the fast sensing stage.

Coexistence protocols enable collocated CRNs to contend for and share the available spectrum. However, most coexistence protocols do not take into consideration the fact that channels of the available spectrum can be heterogeneous in the sense that they can vary in their characteristics and quality such as SNR or bandwidth. Without any mechanism to enforce fairness in accessing varying quality channels, ensuring coexistence with minimal contention and efficient spectrum utilization for CRNs is likely to become a very difficult task.

The cooperative and opportunistic nature of communication has many challenges associated with CRNs' operation. In view of the challenges described above, this dissertation presents solutions including cross-layer approaches, reputation system, optimization and game theoretic approaches to handle (1) degradation in TCP's throughput resulting from packet losses and disruptions in spectrum availability due non-deterministic use of spectrum by the PUs (2) presence of malicious SUs in the CRN that may launch various attacks on CRNs' including

SSDF and jamming and (3) sharing of heterogeneous spectrum resources among collocated CRNs without a centralized mechanism to enforce cooperation among otherwise non-cooperative CRNs.

I dedicate this dissertation to my wife, Faiza, for her love and support and to our sons,
Faayed and Faizaan, who are our pride and joy.

ACKNOWLEDGMENTS

I would like to thank my advisor, Dr. Cliff C. Zou for his guidance, support and encouragement throughout my PhD program at University of Central Florida.

I would also like to thank members of my dissertation committee: Dr. Mostafa Bassiouni, Dr. Damla Turgut and Dr. Morgan Wang for their valuable guidance and suggestions on my dissertation.

I would especially like to thank Dr. Mainak Chatterjee for his help and guidance on numerous occasions during my PhD.

I would also like to thank the Fulbright Program of the Institute of International Education USA, the US Educational Foundation in Pakistan and the Higher Education Commission Government of Pakistan, for providing me with an opportunity and all the funding to pursue my PhD degree.

TABLE OF CONTENTS

LIST OF FIGURES	xiv
LIST OF TABLES.....	xix
CHAPTER 1: INTRODUCTION.....	1
1.1 Overview: Cognitive Radio Networks.....	1
1.2 Motivation.....	5
1.3 Proposed Work and Contributions.....	6
1.4 Organization of Dissertation.....	7
1.5 References.....	7
CHAPTER 2: TRANSPARENT CROSS-LAYER SOLUTIONS FOR TCP THROUGHPUT BOOST	9
2.1 Related Work	10
2.2 Motivation.....	13
2.2.1 Quiet Period for Spectrum Sensing	13
2.2.2 Primary Users' Activity.....	16
2.2.3 Primary User Detection Accuracy.....	18
2.3 Proposed Solutions.....	18
2.3.1 Local Loss Recovery at Base Station	19
2.3.2 Split TCP Connections	22

2.4	Discussion on proposed approaches	23
2.5	Performance Evaluation	24
2.6	Conclusion	28
2.7	References	29
CHAPTER 3: REPUTATION AWARE SPECTRUM SENSING AGAINST SPECTRUM SENSING DATA FALSIFICATION ATTACKS		32
3.1	Motivation	33
3.2	Proposed Work and Contribution	34
3.3	Related Work	35
3.4	System Model and Assumptions	37
3.5	Reputation Aware Spectrum Sensing Framework	40
3.5.1	Semi-Supervised Spatio-Spectral Anomaly Detection	41
3.5.2	Spectrum Sensing Data Aggregation	46
3.5.3	Spectrum Map Construction	48
3.5.4	Reputation Management	52
3.6	Performance Evaluation	55
3.6.1	Variants of SSDF Attacks	55
3.6.2	Simulation Setup	58
3.6.3	Simulation Results	60

3.7	Conclusion	64
3.8	References.....	64
CHAPTER 4: ADAPTIVE SPECTRUM SENSING UNDER NOISE AND SMART JAMMING		
ATTACK		67
4.1	Motivation and Contributions.....	69
4.2	Related Work	70
4.3	System Model, Attack Model and Assumptions.....	72
4.3.1	System Model	72
4.3.2	Assumptions	74
4.3.3	Attack Model	75
4.4	DS3: An Adaptive Spectrum Sensing Framework	76
4.4.1	The Core idea for Adaptive Spectrum Sensing	76
4.4.2	Markov ON/OFF Model for Prediction of PU Activity	77
4.4.3	DS3 Framework.....	79
4.4.4	Discussion on DS3's handling of various network conditions	85
4.5	Performance Evaluation.....	93
4.5.1	Simulation Setup.....	93
4.5.2	Simulation Results.....	93
4.6	Conclusion	97

4.7	References.....	97
CHAPTER 5: AN EVOLUTIONARY GAME THEORETIC APPROACH TOWARDS LONG-TERM SELF COEXISTENCE.....		
		100
5.1	Motivation and Contribution.....	101
5.2	Related Work	103
5.3	System Model and Assumptions.....	106
5.3.1	System Model	106
5.3.2	Assumptions	107
5.4	Evolutionary Anti-Coordination Spectrum Sharing Game.....	110
5.4.1	Evolutionary Game Theory: Basics.....	110
5.4.2	Game Formulation.....	111
5.4.3	Pure and Mixed Strategy Nash Equilibria	113
5.4.4	Evolutionary Stability of the Game's Equilibria.....	116
5.4.5	Replicator Dynamics and K-Channel Scenario	118
5.5	Fairness Analysis of Derived Equilibria	121
5.6	Simulations and Results.....	122
5.6.1	Preliminaries	122
5.6.2	Results	123
5.7	Conclusion	128

5.8	References.....	129
CHAPTER 6: COEXISTENCE IN HETEROGENEOUS SPECTRUM THROUGH		
DISTRIBUTED CORRELATED EQUILIBRIUM 132		
6.1	Motivation and Contribution.....	133
6.2	Related Work	135
6.3	System Model and Assumptions.....	137
6.3.1	System Model	137
6.3.2	Assumptions	139
6.4	Equilibrium Solutions for Heterogeneous Spectrum Sharing Game	140
6.4.1	Game Formulation.....	141
6.4.2	Pure and Mixed Strategy Nash Equilibria	142
6.4.3	Centralized Correlated Equilibrium for 2-Player Game.....	145
6.4.4	Distributed Correlated Equilibrium for N-Player Game	149
6.5	Fairness and Efficiency of Derived Equilibria.....	151
6.6	Simulations and Results.....	156
6.6.1	Simulation Setup.....	156
6.6.2	Simulation Results.....	157
6.7	Conclusions.....	162
6.8	References.....	162

CHAPTER 7: CONCLUSION 165

LIST OF FIGURES

Figure 1.1: Typical Cognitive Radio Cycle	2
Figure 1.2: Dynamic Spectrum Access by Cognitive Radio Networks	3
Figure 1.3: Infrastructured and Ad hoc CRN architecture.....	4
Figure 2.1: Two Stage Spectrum Sensing in IEEE 802.22 WRAN.....	14
Figure 2.2: Impact of Quiet Periods on TCP's Throughput	15
Figure 2.3: Impact of PU Activity and Packet Loss Rate on TCP's Throughput	16
Figure 2.4: Impact of Fine Sensing Duration on TCP's Throughput	17
Figure 2.5: Performance of Proposed Solutions at various Loss Rates	25
Figure 2.6: Performance of Local Loss Recovery at various Loss Rates	26
Figure 2.7: Performance of Split TCP (Pre-ACK) at various Loss Rates.	26
Figure 2.8: Performance comparison at Fine Sensing Duration 5% of TCP RTO.....	27
Figure 2.9: Performance comparison at Fine Sensing Duration 15% of TCP RTO.....	27
Figure 3.1: Ad hoc CRN with malicious nodes. Only the spectrum sensing reports sent by SU nodes in PU's coverage area should be considered for making final spectrum decisions and reputation updates.	34
Figure 3.2: Anomaly detection in reported RSS (a) SUs that reported PU's presence including a malicious node. (b) Distances from an honest node to all other reporting SUs. Distance to malicious node is abnormal, other distances are normal. (c) Distances from a malicious node to all other reporting SUs. Since majority of its distances are abnormal, the node in the middle is classified as outlier.....	44

Figure 3.3: Error in spectrum map construction using circular regression with a single RSS level. Final PU localization is done with weighted average of localizations with all of the M RSS levels.	49
Figure 3.4: Two-tiered sliding window Reputation Table.....	52
Figure 3.5: Average number of SUs in PU's range in dense and sparse networks.	58
Figure 3.6: Spectrum Decision Accuracy under Denial of Service Attack.	59
Figure 3.7: Spectrum Decision Accuracy under Spectrum Report Reversal Attack.	60
Figure 3.8: Spectrum Decision Accuracy under (a) Induction attack (b) All attacks combined. .	61
Figure 3.9: Malicious node detection accuracy under various SSDF attacks.....	62
Figure 3.10: Incorrect labeling of honest SUs as malicious under various SSDF attacks.....	63
Figure 4.1: Markov ON/OFF model for PUs Spectrum Usage.	74
Figure 4.2: Effect of state transition probability α on P_k	78
Figure 4.3: Relationship between α and β and the amount of PU's spectrum usage π_1	78
Figure 4.4: Effect of Sensitivity c on the cost γkt of interfering	84
Figure 4.5: DS3's handling of Low PU activity on the channel as compared with IEEE 802.22's spectrum sensing actions.....	86
Figure 4.6: DS3's handling of High PU activity on the channel as compared with IEEE 802.22's spectrum sensing actions.....	88
Figure 4.7: DS3's handling of smart jamming attack on the channel as compared with IEEE 802.22's spectrum sensing actions.....	90
Figure 4.8: DS3's performance with various parameters (a) Spectrum opportunity utilization (b) PU detection delay at varying degrees of jamming attack severity.	94

Figure 4.9: DS3's performance with various parameters (a) Spectrum opportunity utilization (b) PU detection delay with varying sensitivity towards PU detection delay.	95
Figure 4.10: DS3's performance with various parameters (a) Spectrum opportunity utilization (b) PU detection delay with varying degree of PU's spectrum usage (%).	96
Figure 5.1: (a) Collocated CRNs competing for (b) Heterogeneous channels. The channels of the spectrum band may vary in quality with respect to availability, bandwidth or SNR, etc..	106
Figure 5.2: Channel access probabilities and average payoffs when the number of channels available for contention is $k = 2$. (a) Channel access probability and (b) average payoffs when the initial probabilities are unequal, figures (c) and (d) show the results when initial probabilities are equal, (e) and (f) results under changing network conditions i.e., quality of channel 1 becomes worse than channel 2 at time $t = 50$	123
Figure 5.3: (a) Total payoff for both channels becomes equal when initial probability of selecting channel 1 equals $p_1 = 0.5625$ i.e., the ESS probability. (b) Channel access probability and (c) average payoffs when the initial probabilities are equal for a 3-channel scenario.	126
Figure 5.4: (a), (c) and (e) Channel access probabilities and (b), (d) and (f) average payoffs. For (a) and (b) the number of channels available for contention is 3 i.e., $k = 3$ and initial probabilities are <i>un-equal</i> . For (c) and (d) the number of channels available for contention is 4 i.e., $k = 4$ and initial probabilities are <i>equal</i> whereas for (e) and (f) $k = 4$ and initial probabilities are <i>un-equal</i>	127
Figure 5.5: (a) and (c) Channel access probabilities and (b) and (d) average payoffs when the number of channels available for contention is 5 i.e., $k = 5$. For (a) and (b) initial probabilities are <i>equal</i> . For (c) and (d) the initial probabilities are <i>un-equal</i>	128

Figure 6.1: Collocated CRNs competing for Heterogeneous channels. 137

Figure 6.2: Expected utilities per CRN for $n = 2$ and $k = 2$, and utilities from the two channels are: $u_1 = 9$ and $u_2 = 7$ with varying inertia parameter μ . (a) $\mu = 20$, (b) $\mu = 100$, (c) $\mu = 200$ and (d) $\mu = 300$. Different values of μ achieve the same convergence value of expected utility however as inertia increases, it causes a decrease in convergence rate. .. 157

Figure 6.3: Comparison of CE at different values of the number of networks (n) and channels (k). Y-axes represent expected utility per CRN. For this simulation $n = k$ where (a) $n = k = 2$, (b) $n = k = 3$ and (c) $n = k = 4$ such that $u_1 = 9, u_2 = 7, u_3 = 6$ and $u_4 = 5$ 158

Figure 6.4: Comparison of CE when $k \geq n$ and number of networks is kept fixed. Y-axes represent expected utility per CRN. (a) $k = n = 4$, (b) $k = 5, n = 4$, (c) $k = 6, n = 4$. CRNs always select the best out of the available pool of channels therefore the convergence value of expected utilities are equal however convergence rate increase as $n \rightarrow k$ 159

Figure 6.5: (a), (b) and (c) $n \leq k$ and number of networks is kept fixed. Y-axes represent expected utility per CRN. (a) $k = n = 4$, (b) $k = 3, n = 4$, (c) $k = 2, n = 4$. Decrease in number of networks results in an increase in expected utilities and convergence rate decreases as the number of channels increases. (d), (e) and (f) $n \geq k$ and number of channels is kept fixed. Y-axes represent expected utility per CRN. (a) $k = n = 2$, (b) $k = 2, n = 3$, (c) $k = 2, n = 4$. Increase in number of networks results in a corresponding decrease in expected utility per CRN however the convergence rate decreases as the number of channels increases. 160

Figure 6.6: Channel access pattern of CRNs. (a) Selfish behavior from CRNs for best quality channel (channel 1) will always result in a collision. (b) Fair distribution of spectrum resource when CRNs mix their choice of channels according to MSNE. However, MSNE is inefficient because of collisions and wasted opportunities. (c) Fair and efficient resource distribution with Correlated Equilibrium..... 161

LIST OF TABLES

Table 2.1: Local Loss Recovery Algorithm implemented at the CRN base station.	21
Table 3.1: List of Notations and acronyms – Chapter 3	38
Table 3.2: Spatio-Spectral Anomaly Detection Algorithm.....	45
Table 3.3: Reputation Management Algorithm	55
Table 4.1: Notations and acronyms – Chapter 4.....	73
Table 4.2: Algorithm for DS3 Framework	92
Table 5.1: Notations and acronyms – Chapter 5.....	109
Table 5.2: Strategic form representation of a 2-channel evolutionary game	112
Table 5.3: MSNE of a 2-channel evolutionary spectrum sharing game	115
Table 5.4: Replicator Dynamics Algorithm.....	120
Table 6.1: Notations and acronyms – Chapter 6.....	138
Table 6.2: Strategic form representation of a 2-player anti-coordination game	143
Table 6.3: Joint probability distribution over strategies a_1 and a_2	146
Table 6.4: Channel Selection Learning Algorithm	151

CHAPTER 1: INTRODUCTION

1.1 Overview: Cognitive Radio Networks

Studies on spectrum utilization have shown that static allocation of the spectrum has resulted in severe under-utilization of this scarce resource, even as low as 14% [1]. With the proliferation of devices that rely on wireless access to the internet, the demand for wireless spectrum bands is ever-increasing. This wide gap in the demand and supply of wireless spectrum resource forced regulatory bodies such as the FCC to allow un-licensed access to spectrum bands, also referred to as the TV white spaces, otherwise licensed to the Primary Users (PUs) in an opportunistic and non-interfering basis [2]. This has given rise to a challenging as well as an exciting type of networks consisting of devices called the Cognitive Radio (CR) which is defined by FCC [3] as “A radio that can change its transmitter parameters based on interaction with the environment in which it operates”. A cognitive radio network (CRN) comprises devices that are capable of sensing their radio environment and adjusting operational parameters to communicate in an efficient manner while avoiding any interference with the PUs. The idea of Cognitive Radio (CR) was first presented in [4] which envisioned a CR as a fully cognitive device capable of observing and adjusting to all possible radio parameters.

CRNs operate in the licensed as well as un-Licensed spectrum bands, by opportunistically utilizing bands that are not used by the incumbent user at a given time. CR paradigm is gaining widespread recognition as a solution to the problem of spectrum scarcity however the opportunistic manner of communication in CRNs has opened up numerous challenges to the research community resulting in research initiatives such as the DoD’s Joint Tactical Radio

System, DARPA's Next Generation (XG) program, IEEE 802.11af [5] also known as White-Fi or super Wi-Fi and IEEE 802.22 Wireless Regional Area network (WRAN) [6]. Research in this area is aimed towards both civilian applications, such as provisioning broadband Internet access in rural areas using TV white spaces under the IEEE 802.22 WRAN working group, as well as military applications such as DARPA's XG communications program.

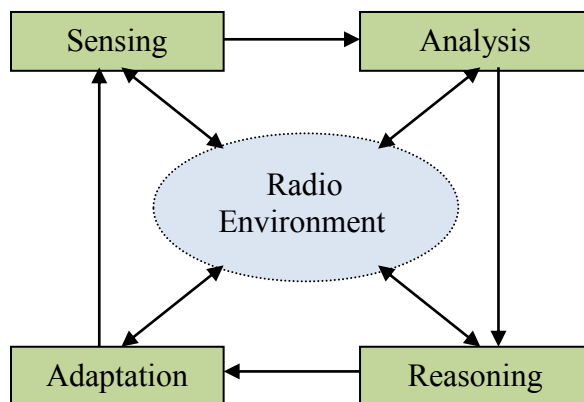


Figure 1.1: Typical Cognitive Radio Cycle

In order to detect and use a vacant spectrum band, a CRN relies on cooperative sensing feedback from CR devices that periodically sense the spectrum for the presence of PUs' signals and report the spectrum's occupancy status to a fusion center (FC). A typical CR cycle [7] is shown in figure 1.1 wherein devices that form part of a CRN, also called the secondary users (SUs), cooperatively perform spectrum sensing, exchange their sensed data which is then aggregated at the FC which then decides whether to continue communicating using the current channels or to switch to some other channels and/or communication parameters. This method of dynamically adjusting to changing radio environment is also known as dynamic spectrum access

(DSA) and is shown in figure 1.2 which shows how a CRN would make use of spectrum opportunities i.e., switch to channels that may become available with the passage of time. In addition to switching channels based on PU activity, DSA also includes varying communication parameters according to user needs as well as other radio environments.

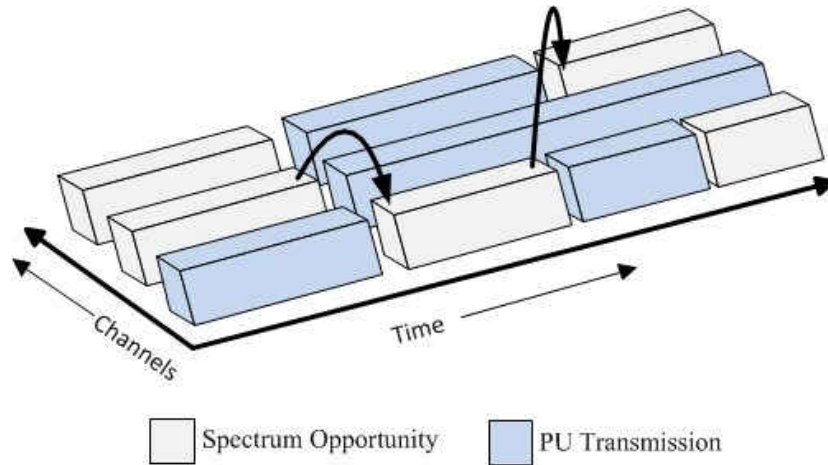


Figure 1.2: Dynamic Spectrum Access by Cognitive Radio Networks

CRNs may be operated as infrastructured or ad hoc networks. Intuitively, the infrastructured CRN has a base station (BS) that controls every aspect of the network including aggregation of spectrum sensing reports from its SUs and the decision of selecting vacant channels for communication. On the other hand, since there is no central entity to control network operations in an ad hoc CRN, the task of spectrum sensing reports' aggregation and channel selection decision may be assigned to any SU based on some algorithm for selecting cluster heads.

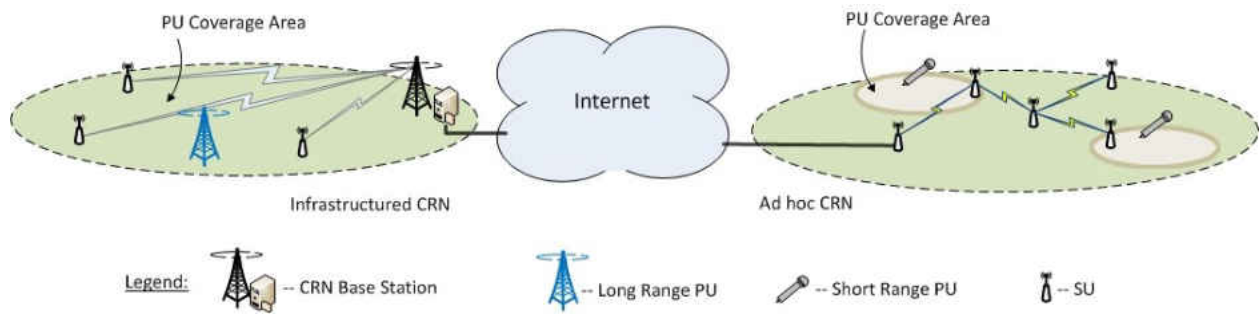


Figure 1.3: Infrastructure-based and Ad hoc CRN architecture

IEEE 802.22 WRAN [6] is a technology which is being developed as an infrastructure-based CRN and is expected to see deployment especially in the rural areas or areas lacking communications infrastructure. It is designed to operate in TV bands from 54-862 MHz with a total of 47 channels. These frequency bands allow long range communication typically from 17 – 30 km with a maximum range of 100 km. The network is organized in a Point-to-Multipoint configuration called a Cell, has a fixed Base Station (BS) and up to 512 simultaneously associated SUs per Cell.

IEEE 802.11af [5] is a standard developed for opportunistic communication utilizing the TVWS portion of the spectrum that can be used in ad hoc configuration. It is designed to operate in TV bands from 54 – 790 MHz giving a total of 39 channels with the option of channel bonding/aggregation of up to 4 channels. The standard has a maximum transmission range of 5 km. Layout of a typical CRN in infrastructure-based and ad hoc mode is shown in figure 1.3.

1.2 Motivation

Opportunistic spectrum access is the fundamental property of a CRN. The defining characteristics of opportunistic spectrum access are non-deterministic nature of PUs' spectrum usage and the network wide quiet periods that are used to determine whether or not PU(s) signals are present on the spectrum. These characteristics give rise to numerous challenges that form the motivation for this dissertation and are highlighted subsequently.

Majority of the research efforts in DSA have been directed towards the Physical (PHY) and Medium Access (MAC) layers of the protocol stack while the upper layers, especially the transport layer, have not received that much attention. Unlike traditional radio technologies and protocols, much closer interaction among transport layer and the MAC/PHY layers is required in cognitive radio network, mainly because of network-wide quiet periods, opportunistic / dynamic spectrum access, and non-deterministic operation of PUs. These factors can increase retransmission overheads significantly and have a devastating impact on the overall throughput QoS.

Opportunistic spectrum utilization without causing interference to the PUs is only possible if the SUs periodically 'sense' the spectrum for the presence of PUs' signal. To minimize the effects of errors in spectrum sensing, DSA is undertaken in a collaborative manner, where SUs periodically carry out spectrum sensing in their respective geographical locations and report their measurements to the FC which then decides whether to continue using a specific spectrum band or to vacate it. However, DSA can also be favorable to malicious nodes in the network that may provide false spectrum sensing reports or jam spectrum opportunities for the CRN. Such attacks

may adversely affect spectrum sensing decisions causing harmful interference to the PUs or deny the use of the vacant spectrum bands to the CRN. Measures to guard against such attacks are vital for the success of CRNs.

There may be many CRNs collocated in a given region all of whom compete for access to the available channels, a situation called self co-existence in the context of CRNs. Most coexistence protocols do not take into consideration the fact that these channels can be heterogeneous in the sense that they can vary in their characteristics and quality. Without any mechanism that can enforce fairness in accessing varying quality channels with optimum utilization of spectrum opportunities, coexistence for CRNs is likely to become a very difficult task.

1.3 Proposed Work and Contributions

The proposed work is to overcome challenges associated with the opportunistic spectrum access by the CRNs. The contributions of this dissertation are summarized below.

- Design of two cross-layer schemes to boost TCP's throughput that is degraded because of additional delays in packet delivery as well as packet losses due to network wide quiet periods for spectrum sensing and non-deterministic nature of PUs' communications.
- Design of a framework for integrating a reputation system with a spatio-spectral anomaly/outlier detection system to defend against spectrum sensing data falsification (SSDF) attacks.
- Design of an adaptive defense framework which enables the CRN to thwart *smart* jamming attacks and improve spectrum utilization under noise.

- Formulation of an evolutionary game theoretic framework through which contending collocated CRNs evolve their strategies to select a channel from a set of disparate channels and converge to an evolutionarily stable state.
- Formulation of an anti-coordination game with a set of disparate channels for collocated CRNs to approach Correlated Equilibrium which is both fair as well as optimum in both the centralized as well as decentralized settings.

1.4 Organization of Dissertation

Remainder of this dissertation is organized as follows: Chapter 2 presents transparent cross-layer solutions for throughput boost in CRNs. Chapter 3 gives the design of a framework that integrates a reputation system with an outlier detection scheme to defend against SSDF attacks. Chapter 4 discusses the design of the proposed adaptive spectrum sensing framework that guards against smart jamming attacks and improves spectrum opportunity utilization under noisy channel conditions. Chapter 5 presents an evolutionary game theoretic framework for long-term coexistence in CRNs when the channels available for unlicensed access are of varying quality. Chapter 6 presents an anti-coordination game for collocated CRNs to approach Correlated Equilibrium which is both fair as well as optimum with regards to disparate channels. Chapter 7 gives the conclusion.

1.5 References

[1] T.M. Taher, R.B. Bacchus, K.J. Zdunek, D.A. Roberson, "Long-term spectral occupancy findings in Chicago," New Frontiers in Dynamic Spectrum Access Networks (DySPAN) 2011.

- [2] U.S. FCC ET Docket 04-186, "Notice of Proposed Rule Making, in the matter of Unlicensed Operation in the TV Broadcast Bands," May 25, 2004.
- [3] B. Fette, "Introduction to Cognitive Radio," SDR Forum Technical Conference 2005.
- [4] J. Mitola III, "Cognitive Radio An Integrated Agent Architecture for Software Defined Radio," PhD Dissertation KTH Royal Institute of Technology, May 8, 2000.
- [5] IEEE STANDARD 802.11af-2013 - IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Television White Spaces (TVWS) Operation.
- [6] IEEE STANDARD 802.22-2011 - IEEE Standard for Information technology-- Local and metropolitan area networks- Specific requirements- Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Policies and procedures for operation in the TV Bands.
- [7] Online: University of Maryland, Signals & Information Group, <http://www.cspl.umd.edu/sig/research/> - accessed May 2014.

CHAPTER 2: TRANSPARENT CROSS-LAYER SOLUTIONS FOR TCP THROUGHPUT BOOST

Unlike traditional wireless communication technologies and protocols, much closer interaction among transport layer and the MAC/PHY layers is required in CRNs because of its communication characteristics such as network-wide quiet periods, opportunistic / dynamic spectrum access, and non-deterministic nature of PUs' communication patterns. These factors can have a devastating impact on the networks' throughput and can cause significant retransmission overheads. TCP being the predominant transport protocol of the Internet needs to be capable of handling additional constraints imposed by peculiar communication characteristics of CRNs.

There has been a lot of research to tackle the problems associated with TCP's handling of DSA [1, 2, 4 – 7] when dealing with communications between devices in the CRN and the Internet. However transparency, a key property for any solution to be economical and scalable, has largely been ignored in the aforementioned context. Existing solutions require either the presence of special purpose devices in the CRN or modification in TCP implementations of devices taking part in communications across CRNs and the internet. Our solutions to transparently boost TCP's throughput is specifically designed for infrastructured CRNs such as the IEEE 802.22 WRAN and take advantage of the presence of a BS through which all traffic to and from the Internet has to pass.

The main contribution of our proposed solutions is that they provide throughput boost transparently i.e. without any need for special purpose devices in the network or requiring any

changes in the end systems making them ideal for initial deployment of a WRAN. The two solutions presented are proposed to be implemented only at the CRN BS and provide alternatives in situations where end to end semantics of TCP connections may or may not be important for communication across the CRN and the Internet.

This chapter is organized as follows: In section 2.1 an overview of the works related to our proposed TCP throughput boost is presented. Section 2.2 gives the detailed design of our proposed solutions. Section 2.3 presents performance evaluation of the proposed solutions through simulations and section 2.4 gives a discussion on the solutions' design and performance. Section 2.5 concludes this chapter.

2.1 Related Work

TP-CRAHN [1] is a protocol designed for use within ad hoc CRNs. It incorporates a cross-layer design with explicit feedback from every node between the source and destination nodes, regarding their sensing schedules and the length of quiet periods intended for detecting PUs through spectrum sensing. Its transport protocol interacts with physical layer's channel information, link layer's buffer management as well as a mobility prediction framework to cater for varying parameters and network dynamics. This protocol however does not cater for the situations when either source or the destination of a TCP connection is outside the CRN and the impact DSA in the CRN will have on TCP's timeout intervals and congestion control mechanism for such connections. This is especially the case when the sender is at the Internet side of the connection and is unaware of additional delays caused due to CRN's DSA.

TCPE [2] protocol is designed for heterogeneous networks involving CRNs and the wired Internet. It aims to achieve better throughput through available bandwidth estimation and round-trip-time (RTT) difference between successive TCP segments. It assumes packet delays to have been caused by spectrum sensing if the difference between successive RTTs is more than 90% of *spectrum sensing duration* (SSD). The study does not consider the situation when the source is in the Internet and destination node is located in a CRN, in which case the source node in the Internet would have to know the SSD for destination node's network, which can vary by technology [3].

An approach based on local loss recovery has been employed in [4] which is somewhat similar to our proposed solutions however this scheme is designed for Cellular networks to mitigate the effects of losses due to high bit-errors and handoffs. It requires the use of either Explicit Congestion Notifications (ECN) or Negative Acknowledgements (NACK). Due to non-deterministic nature of PUs' spectrum usage, ECN and NACK can be expected to cause significant throttling of TCP's traffic as well as increased control overhead. Our proposed solutions on the other hand are designed to cater for packet losses and delays that occur due to DSA in a transparent manner in *addition* to the typical delays and losses of a wireless network.

To alleviate TCP poor performance in wireless networks, I-TCP [5] has been proposed to split a TCP connection at the BS into two separate connections. It however requires special devices called *Mobility Support Routers* in the wireless network and also requires modification to the TCP code in mobile hosts thus making it unsuitable for a scalable deployment. It also does not take into account the need for maintaining TCP semantics violated due to split connections.

In [6], another split TCP connection approach is proposed for *ad hoc* cognitive networks to mitigate the effects of TCP un-fairness towards nodes that are relatively farther away from the source node. It works by forming a chain of suitably selected nodes to act as TCP proxies between the source and destination of a TCP connection, both of which must lie within the ad hoc network.

A Semi-Split TCP has been proposed in [7], in which a CRN's BS buffers the ACKs received from the receiver in cognitive network and controls the amount of ACKs relayed back to the sender in order to throttle the sender and to prevent the BS's buffers from starvation. The proposed semi-split TCP solution is basically meant to achieve a slower yet smooth flow of packets from a source in the Internet and a destination in the CRN.

Our research differs from the work presented above in many ways. The most important difference in our work is that the proposed solutions are transparent to both the source as well as the destination machines of a TCP connection. Our proposed solutions can be implemented only at the CRN BS in order to achieve the boost in TCP's throughput. These solutions also do not require any additional special purpose devices to be placed in a CRN in order to mitigate the effects of DSA on TCP's performance. Our proposed solutions are intended for TCP flows that span across the CRN and the Internet as opposed to some of the above solutions that cater for TCP flows only inside the CRN. Since TCP flow semantics are lost due to splitting up of TCP connections, our proposed solutions provide two alternatives for situations when TCP flow semantics may or may not be important for hosts.

2.2 Motivation

In this section, we discuss how TCP congestion control algorithm and hence network's throughput may suffer in the context of IEEE 802.22 WRAN based CRN. The features of a CRN that could impact TCP performance are: (i) quiet period duration i.e., time that is used for spectrum sensing (ii) the amount of PU activity in the region of a CRN and (iii) CRN's accuracy in detecting PU's presence on the spectrum. We use the terms CRN and WRAN interchangeably unless there is a specific need to distinguish between the two. In the subsequent subsections, we present the motivation behind this work by describing the impact of the aforementioned CRN features on TCP's performance.

2.2.1 Quiet Period for Spectrum Sensing

In order to protect the incumbent PUs from harmful interference, a CRN has to enforce quiet periods in the network to effectively sense the spectrum for its availability. The length of these quiet periods and spectrum sensing can vary depending on the algorithm used [3] that may have significant impact on QoS. Users in a CRN would expect the same level of QoS (e.g. max delay of 20 msec in case of voice traffic) as in any other network.

To strike a balance in the conflicting goals of protecting PUs' communication and achieving a desired level of QoS, IEEE 802.22 WRAN standard employs a two-stage quiet period management scheme, where the stages are fast sensing ($\sim 9 - 20 \mu\text{sec}$) and fine sensing ($\sim 0.3 - 160 \text{ msec}$) [8]. The network is synchronized and every time slot (160 msec) is called a Channel Detection Time (CDT). Every CDT can have one or more fast sensing periods and at most one

fine sensing period. However, the BS decides to carry out fine sensing and determines the required duration based on the outcome of fast sensing periods. The fine sensing period may occupy a whole time slot. The two stage quiet period mechanism for spectrum sensing in IEEE 802.22 WRANs is shown in figure 2.1.

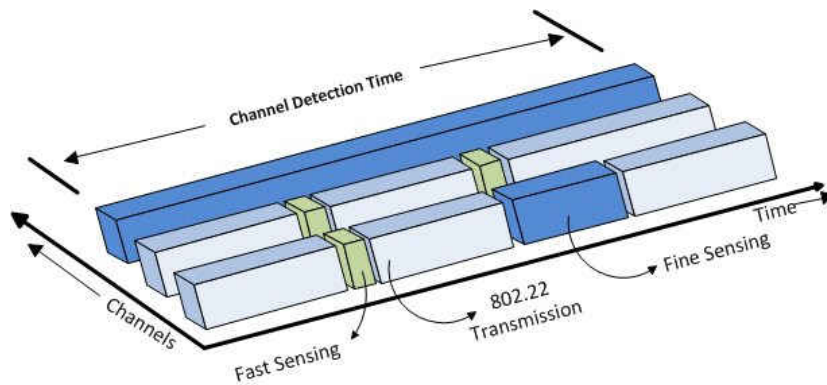


Figure 2.1: Two Stage Spectrum Sensing in IEEE 802.22 WRAN

TCP uses RTT measurements for estimating available bandwidth and calculating a suitable Retransmission Timeout (RTO) interval for a particular connection, which is further used in its congestion control algorithm [9]. As per standard TCP Timer management [10], RTO values should be at least 1 sec and implementations must never be more aggressive by selecting smaller values. However, if smaller values of RTO are used e.g. 500 msec in [11] or 200 msec as in [12] as well as Linux, the RTO values will become comparable to WRAN's fine sensing times. In that case, whenever a packet is delayed in WRAN because of fine sensing duration, the source TCP will have a good chance to have premature timeout, erroneously attributing it to congestion and

will resort to un-necessary retransmissions, resulting in increased overheads and decreased throughput.

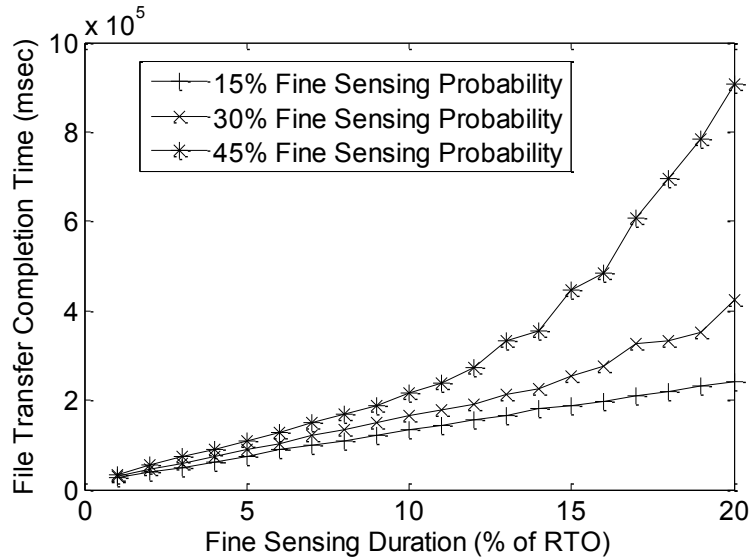


Figure 2.2: Impact of Quiet Periods on TCP's Throughput

Figure 2.2 shows the significant impact of CRN's fine sensing on the performance of TCP communication. For the purpose of this work, we call the probability for BS to decide to conduct fine sensing in a CDT slot as Fine sensing Probability. The results shown in Figure 2.2 show the file transfer completion time (Y-axis) for a file size of 4 MB, in an FTP application at three different fine sensing probabilities and for fine sensing durations kept from 0 to 20% of TCP RTO interval (X-axis).

As concluded in [12], spectrum sensing quiet periods are most debilitating for TCP performance in a DSA network. We believe that a transparent mechanism is therefore needed to

monitor the interaction of TCP RTO interval and spectrum sensing quiet periods in the WRAN and take appropriate measures for DSA not to affect TCP congestion control. This would result in boosting TCP throughput while minimizing retransmission overheads and if possible, maintaining the end-to-end semantics of TCP connections.

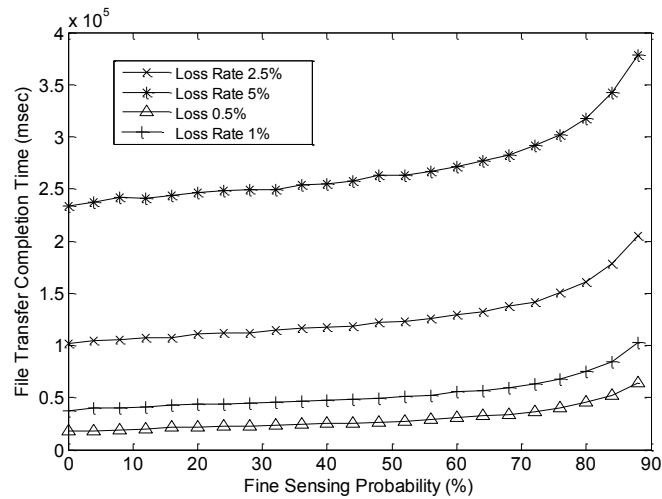


Figure 2.3: Impact of PU Activity and Packet Loss Rate on TCP's Throughput

2.2.2 Primary Users' Activity

The two-stage quiet period and spectrum sensing mechanism of IEEE 802.22 WRAN as shown in figure 2.1 is intended to strike a balance in ensuring that the PUs are protected from harmful interference from the un-licensed use of spectrum and its efficient utilization in the absence of PUs. During every CDT every SU in the WRAN carries out fast sensing across a specified number of channels and reports its measurements to the BS. Based on these measurements, the BS may decide not to resort to fine sensing if it concludes that PU's presence

on a specific channel is not detected, or it may ask the SUs to go into fine sensing period, if it suspects presence of a PU and needs further confirmation.

Clearly, the two stage sensing mechanism is intended to carry out fine sensing of the spectrum in each CDT slot only if it is necessary as it would result in the waste of a large chunk of spectrum resource if the PU was not utilizing the spectrum. Figure 2.3 shows the performance of TCP under various fine sensing probabilities and packet loss rates. It is worth noting that fine sensing probability is directly proportional to the amount of PUs' activity on the spectrum. Similarly, as the duration of fine sensing increases with respect to TCP's RTO interval, it has greater impact on TCP's throughput as can be seen in figure 2.4. For these reasons, a mechanism is needed that would monitor the level of PU activity in the WRAN and not let it affect TCP congestion control mechanism.

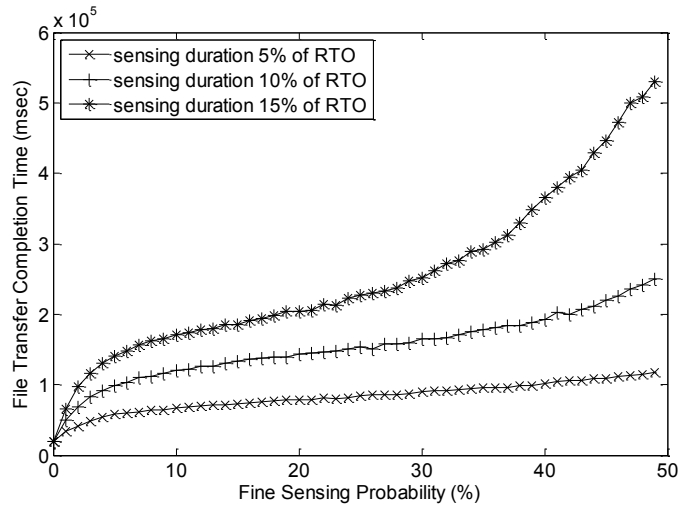


Figure 2.4: Impact of Fine Sensing Duration on TCP's Throughput

2.2.3 Primary User Detection Accuracy

Another factor that will have adverse effects on TCP performance in a CRN is the accuracy of PU detection scheme(s). On one hand, false alarms in detection of PU's signal will result in wasted spectrum opportunities. On the other hand, if a PU is transmitting in a spectrum band and the CRN is unable to detect its activity, then it will result in harmful interference to the PU as well as packet losses for the CRN. If the probability of not detecting PU's presence is high then there will be significant amount of packet losses in the CRN due to this false spectrum sensing.

In a recent study, probability of PU detection in an IEEE 802.22 WRAN was found out to be 0.9 while the probability of a false alarm as 0.1 for all signal types [13]. Increase in packet loss probability will further deteriorate the already error prone nature of wireless communications. Therefore, a CRN must have a robust mechanism to recover from packet losses due to spectrum sensing errors.

2.3 Proposed Solutions

In this section, we present the details of our proposed solutions for throughput boost in an IEEE 802.22 WRAN. These solutions are *transparent* because all the proposed enhancements are implemented at the WRAN BS and no changes are required at source or the destination of a TCP connection. The reasons for this choice are: (i) On one hand, BS is the controller of all WRAN operations and therefore responsible for scheduling spectrum sensing and usage by SUs while on the other hand, it also is the gateway to Internet, as shown in figure 1.3. It therefore has the capability to transparently improve TCP throughput. (ii) Implementing enhancements at the

BS only and not at the sender or receiver, resolves the issue of scalability in the context of Internet, and facilitates smooth transition in upgrading BS incrementally. The two solutions are: local loss recovery at the BS and split TCP connection both of which are explained subsequently.

2.3.1 Local Loss Recovery at Base Station

The first of our proposed solutions to mitigate the effects of increased packet losses and delays due to DSA is local loss recovery by the WRAN BS. Specifically, the BS continuously monitors all TCP traffic to and from the host(s) in the Internet. It does so by implementing a Loss Recovery Module (LRM). The LRM records information regarding all TCP traffic traversing through it in both directions and their associated TCP state which includes sequence numbers and advertised window sizes as well as timers.

The LRM restricts the number of un-acknowledged packets sent to the SU to a parameter *ADV_WIN* which represents the *current* size of the receiver's advertised window. It however does not implement TCP congestion control mechanism because it has little significance within the context of the *one-hop* WRAN. For the lifetime of TCP connections, the BS maintains separate duplicate buffers used to maintain copies of *all* un-acknowledged packets of a particular TCP connection. Packet loss is detected if an acknowledgement (ACK) is not received before expiration of the local timer or 3 duplicate ACKs of a TCP packet are received. Duplicate copy of a lost packet is retransmitted for local recovery of the loss and this is repeated for a maximum of *MAX_RETRY* times.

Algorithm for the algorithm implemented in LRM is shown in table 2.1. While any packet loss is recovered locally, any duplicate ACKs from the receiver are dropped at the BS. Values for the retransmission timers at the BS are kept at values selected to ensure that these are large enough so that un-necessary retransmissions are avoided if the ACKs are delayed due to spectrum sensing, but small enough to ensure that packet losses within the WRAN are recovered locally and the sender's RTO interval does not expire. The main advantage of this approach is that the sender's congestion control mechanism does not oscillate un-necessarily, due to losses that occur in the WRAN. The LRM maintains duplicate copies of all TCP packets forwarded to receivers in the WRAN and removes the copies for which ACKs have been received and relayed to the sender in the Internet (lines 8 and 9 of *Process ACK packets* in table 2.1). It however keeps track of duplicate ACKs and if 3 duplicate ACKs are received or its local timer expires, it is treated as an indication of a lost packet resulting in appropriate packets being retransmitted out of duplicate buffer. Sending of new or duplicate packets is kept within the limit of advertised window size of the receiver (line 7 of *Process data packets* in table 2.1). The *Fast Retransmit* option enables the BS to recover from a packet loss without the expiry of its local timer.

Table 2.1: Local Loss Recovery Algorithm implemented at the CRN base station.

Data: Duplicate_ACK_count, Lost_pkt_number, flight_size

Result: Local Loss Recovery at CRN Base Station.

Initialization: Duplicate_ACK_count \leftarrow 0, Lost_pkt_number \leftarrow 0, flight_size \leftarrow 0

Process ACK Packets

for every packet in ACK buffer do

1. **if** ACK number is equal to Largest ACK number received **do**
 2. increment Duplicate_ACK_count
 3. **if** Duplicate_ACK_count > 3 (i.e., case for fast retransmit option) **do**
 4. Packet is lost
 5. Retrieve lost packet number from ACK
 6. Retransmit lost packet from local buffer
 7. **else**
 8. Relay ACK back to sender
 9. Remove copy of data packet from duplicate buffer
 10. **end if**
 11. **end if**
- end for**
-

Process Data Packets

while sessions are established between sender and receiver do

1. **if** flight_size = 0 **do**
 2. **if** no ACK is pending **do**
 3. send new data packets from data packet buffer
 4. **end if**
 5. **else**
 6. **if** largest ACK number received = ACK number expected **do**
 7. send new packets from local data packet buffer equal to advertised window
 8. **else**
 9. **if** retransmission timer has expired OR 3 duplicate ACKs received **do**
 10. send duplicate packets from local duplicate buffer for pending ACKs
 11. **end if**
 12. **end if**
 13. **end if**
- end while**
-

2.3.2 Split TCP Connections

Our second approach to boost TCP throughput for data transfers across a WRAN is to implement what we call a split TCP. Differences between existing split TCP mechanisms [19], [20], [21] and our approach are:

- Our approach does not require modifications in either the source or the destination;
- It is specifically designed for IEEE 802.22 WRANs;
- It pre-acknowledges TCP packets to shield the sender from unusually large spectrum sensing delays.

The BS implements this scheme with a module similar to LRM, which Pre-Acknowledges TCP packets received at the BS, on behalf of the receiver in WRAN, effectively sending spoofed ACKs to the sender. This module is called the Pre-Acknowledgement Module (PAM). PAM maintains the state of all TCP connections traversing the BS, and just as the LRM, maintains a duplicate buffer for every TCP connection to ensure delivery of all of its packets. PAM also does not implement the complete TCP and its congestion control mechanism; however it restricts the number of packets transmitted to the receiver's advertised window size along with local timers for reliable delivery. Unlike LRM, values for PAM's retransmission timers are not associated with the sender's RTO interval because in this case the sender's transmissions are independent of losses or delays in the WRAN. Therefore, PAM's local timers can be configured to suit the requirements of WRAN.

Algorithm of PAM is similar to LRM as shown in figure-6, with following exceptions: (i) whenever new packets are received at the BS from a sender in the Internet, an Acknowledgement is immediately sent to sender, and (ii) when an ACK is received from the receiver in WRAN, it is dropped and corresponding duplicate packets are dropped from duplicate buffer. Packet retransmissions out of duplicate buffer are triggered when the BS's local timer expires or with the receipt of 3 duplicate acknowledgements to trigger Fast Retransmission.

2.4 Discussion on proposed approaches

The split TCP connection approach for boosting TCP performance uses spoofed acknowledgements by the BS which essentially breaks the end-to-end semantics of a TCP connection since a packet is acknowledged to its sender whereas it might not have been received by its intended receiver. This situation may not be acceptable to certain applications that work on the guarantees from TCP regarding actual delivery of a packet that is acknowledged. However, in situations where TCP RTO interval is comparable to fine sensing duration of the WRAN, pre-acknowledgement might be the only option for preventing the TCP congestion control algorithm to timeout repeatedly and incorrectly attributing it to congestion. On the other hand, local recovery of lost packets by the BS preserves end-to-end semantics of TCP connections and provides a throughput boost as well. Therefore, the solution with pre-acknowledgements by BS may be selected for applications such as file transfer that may not be concerned with preserving end-to-end semantics while local loss recovery may be selected for the rest.

The main advantage of our schemes is that they provide throughput boost transparently i.e. without any need for changes in the end systems making them ideal for initial deployment of a WRAN.

2.5 Performance Evaluation

We consider a file transfer application in which a node in an IEEE 802.22 WRAN communicates with an FTP server in the Internet. We have developed a simulator to model a WRAN in which the BS and its associated CPEs resort to DSA to communicate with each other while the BS acts as gateway to Internet for the WRAN. Every node (CPE) in the network is equipped with a single radio transceiver that can be tuned to one channel at a time, however all nodes in the network are tuned to the same channel and the use or switching to/from a specific channel is controlled by the BS. The TCP module of our simulator implements slow start, congestion avoidance and fast retransmission schemes. However, since there have been various values for RTO interval for TCP implementations, we have also studied the impact of varying its values in our simulations. The downlink bandwidth from BS to CPEs is 1.5 Mbps downlink and uplink bandwidth per CPE is 384 kbps [13], [17]. The receiver of a TCP packet never delays an outgoing ACK for piggybacking i.e. it sends one ACK for every packet received. Bandwidth between the WRAN BS and FTP server is assumed to be 10 Mbps and file size for FTP transfer is 4 MB. Measurements for every data point were recorded by averaging the results of 1000 simulation runs.

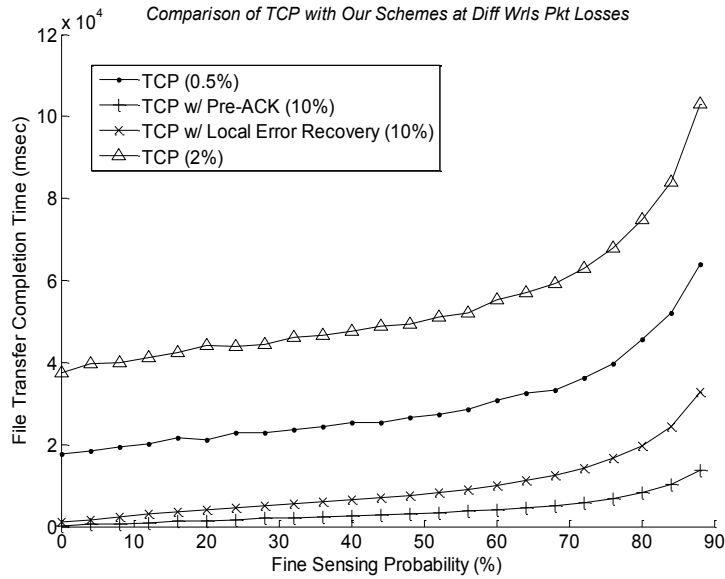


Figure 2.5: Performance of Proposed Solutions at various Loss Rates

Figure 2.5 shows the performance of our proposed solutions in comparison with TCP where the figure shows TCP performance at packet loss rates of 0.5% and 2% for the WRAN link whereas our proposed schemes were run with 10% packet loss rate in the WRAN. As it is evident, our proposed schemes increase the throughput by 20 times.

Figures 2.6 and 2.7 show the performance of our proposed schemes individually where the simulations were run for packet loss rates from 0.5% to 10% and the overall file transfer times (y-axis) were recorded against varying fine sensing probabilities (x-axis) from 0 to 90%. The difference in performance of local loss recovery and pre-acknowledgement schemes can be observed because in case of local recovery, the sender does not send new packets unless the losses in WRAN have been recovered by the BS, whereas for pre-acknowledgement, the sender

can send new packets at the full capacity of the Internet link and is not restricted due to losses and delays in the WRAN. In this way, losses in the WRAN have some impact on the overall throughput of local loss recovery mechanism but none for pre-acknowledgement scheme.

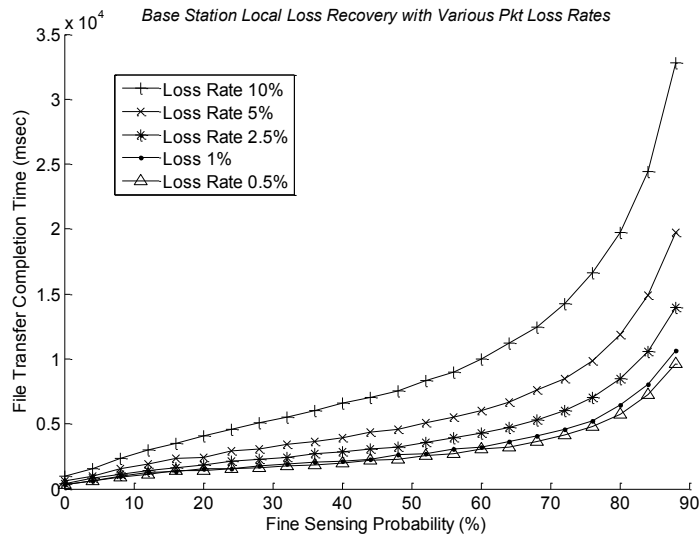


Figure 2.6: Performance of Local Loss Recovery at various Loss Rates

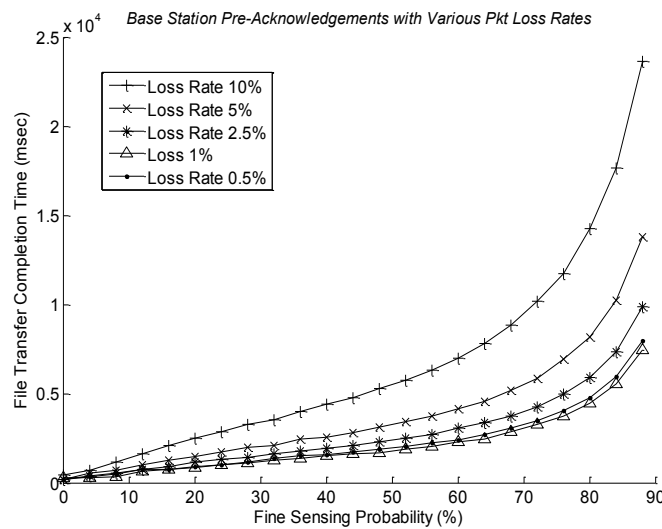


Figure 2.7: Performance of Split TCP (Pre-ACK) at various Loss Rates.

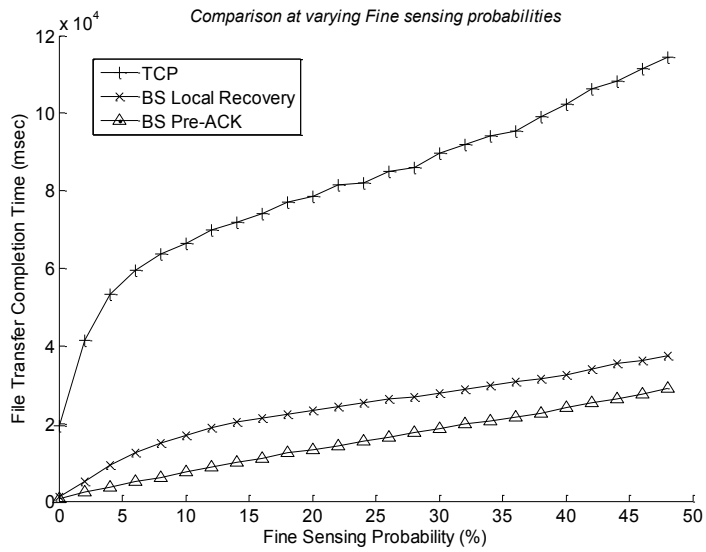


Figure 2.8: Performance comparison at Fine Sensing Duration 5% of TCP RTO.

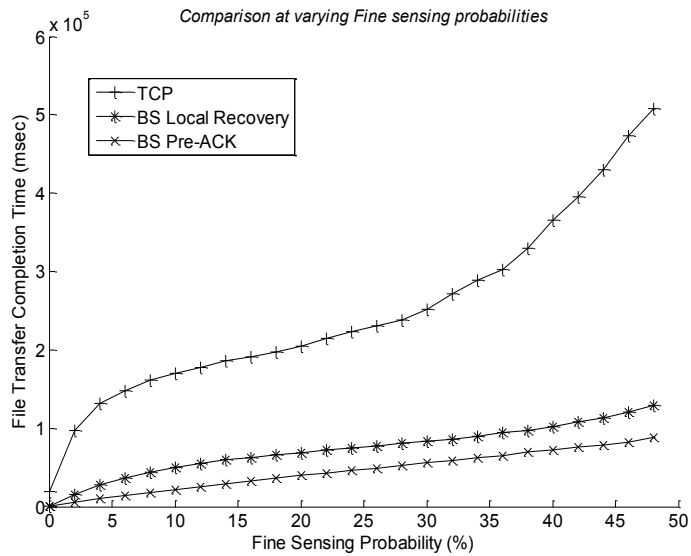


Figure 2.9: Performance comparison at Fine Sensing Duration 15% of TCP RTO.

Figures 2.8 and 2.9 show a comparison of TCP's performance with our proposed solutions, at fine sensing durations 5% and 15% of TCP RTO intervals respectively, where the packet loss rate is kept constant at 0.2% for WRAN and 0.01% for Internet. In addition to preventing the fine sensing periods to interfere with TCP RTO interval, our schemes provide better throughput even when there are no fine sensing periods, because they are also able to recover from packet losses without having the sender TCP being affected by them.

Our proposed solutions perform better than TCP in scenarios where TCP flows suffer heavy packet losses and the sender has to invoke its congestion control mechanism very frequently. On the other hand, our solutions shield the sender from adverse effects of losses in the WRAN. When compared with each other, the two proposed solutions exhibit different performance as well. Split TCP connection with Pre-Acknowledgements has better performance than the local loss recovery by BS, but may be a less favorable option when it comes to preserving the end-to-end semantics of a TCP connection. However, we propose that the choice of selecting a transfer mechanism other than TCP, be negotiated by CPEs with the BS at the time of joining the WRAN or for specific TCP flows.

2.6 Conclusion

In this work we have shown that TCP performance is affected adversely due to PU activity in a WRAN, DSA by the un-licensed users and associated quiet periods that can be comparable with RTO interval of the sender's TCP, a scenario which can trigger TCP's congestion control mechanism un-necessarily and fruitlessly. We have shown that our solutions transparently remedy this situation by coping well with packet losses that are inherent to the wireless medium

as well as resulting from inaccuracies in detection of PUs and network-wide quiet periods for spectrum sensing. To the best of our knowledge, there is however, no work that analyses TCP performance in the context of an IEEE 802.22 WRAN, or proposes solutions that would result in throughput boost for these networks. Currently we are investigating the impact of DSA in a multi-hop cognitive radio network such as IEEE 802.11af.

2.7 References

- [1] Mitola, J. III, Maguire, G.Q Jr, "Cognitive radio: making software radios more personal," IEEE Personal Communications, vol.6, no.4, pp.13-18, Aug 1999.
- [2] Taher, T.M, Bacchus, R.B, Zdunek, K.J.; Roberson, D.A, "Long-term spectral occupancy findings in Chicago," New Frontiers in Dynamic Spectrum Access Networks (DySPAN) 2011.
- [3] U.S. FCC, ET Docket 04-186, "Notice of Proposed Rule Making, in the matter of Unlicensed Operation in the TV Broadcast Bands," May 25, 2004.
- [4] Mishra, S.M. Cabric, D. Chang, C. Willkomm, D. van Schewick, B. Wolisz, S. Brodersen, B.W. , "A real time cognitive radio testbed for physical and link layer experiments," New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2005
- [5] IEEE 802.22-2011 - IEEE Standard for Local and metropolitan area networks - Specific requirements - Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Policies and procedures for operation in the TV Bands. <http://www.ieee.org/22>
- [6] Nekovee, M. , "A survey of cognitive radio access to TV White Spaces," ICUMT 2009.
- [7] Ian F. Akyildiz, Won-Yeol Lee, and Kaushik R. Chowdhury. "CRAHNs: Cognitive radio ad hoc networks". Ad Hoc Networks, 2009.
- [8] Minden, G.J, Evans, J.B, Searl, L, DePardo, D, Petty, V.R, Rajbanshi, R, Newman, T, Chen, Q, Weidling, F, Guffey, J, Datla, D, Barker, B, Peck, M, Cordill, B, Wyglinski, A.M,

Agah, A, "KUAR: A Flexible Software-Defined Radio Development Platform," New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2007.

[9] Chowdhury, K.R, Di Felice, M, Akyildiz, I.F, "TP-CRAHN: a Transport Protocol for Cognitive Radio Ad-Hoc Networks," INFOCOM IEEE Conference on Computer Communications, 2009.

[10] Sarkar, D, Narayan, H, "Transport Layer Protocols for Cognitive Networks," INFOCOM IEEE Conference on Computer Communications, 2010.

[11] Yucek, T, Arslan, H, "A survey of spectrum sensing algorithms for cognitive radio applications," Communications Surveys & Tutorials, IEEE , vol.11, pp.116-130, 2009.

[12] Slingerland, A.M.R, et. Al. "Performance of Transport Control Protocol Over Dynamic Spectrum Access Links," New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2007.

[13] Stevenson, C, et.al, W, "IEEE 802.22: The first cognitive radio wireless regional area network standard," IEEE Communications Magazine, vol.47, pp.130-138, 2009.

[14] Cordeiro, C, Challapali, K, Birru, D, Sai Shankar, N, "IEEE 802.22: the first worldwide wireless standard based on cognitive radios," New Frontiers in Dynamic Spectrum Access Networks,. DySPAN 2005.

[15] Allman, M, Paxson, V, "Computing TCP Retransmission Timer", RFC 2988, November 2000.

[16] Allman, M, Paxson, V, Blanton, E, "TCP Congestion Control", RFC 5681, September 2009.

[17] IEEE 802.22 Draftv3.0 –Members only Documents of the IEEE 802.22 Working Group.

[18] Balakrishnan, H, Seshan, S, Katz,R.H, "Improving reliable transport and handoff performance in cellular wireless networks", Wireless Networks Journal 1995.

[19] Bakre, A. Badrinath, B.R., "I-TCP: indirect TCP for mobile hosts," 15th International Conference on Distributed Computing Systems, 1995.

[20] Kopparty, S. Krishnamurthy, S.V. Faloutsos, M. Tripathi, S.K., "Split TCP for mobile ad hoc networks," IEEE Globecom 2002.

[21] Xie, F, Jiang N, Hua, Y. H, Hua, K.A., "Semi-Split TCP: Maintaining End-to-End Semantics for Split TCP," IEEE LCN 2007.

CHAPTER 3: REPUTATION AWARE SPECTRUM SENSING AGAINST SPECTRUM SENSING DATA FALSIFICATION ATTACKS

Low Power Auxiliary Devices (LPAD) that operate in the analog TV bands can be registered with the FCC [1] in order to protect themselves from interference from other White Space Devices (WSD) that operate opportunistically in the same spectrum bands. By registering specific spectrum bands, the LPADs become PUs of the allocated spectrum bands. These LPADs include wireless microphones, intercom/talk back systems, in-ear monitors, audio instrument links and cueing equipment and have a typical transmission range between 100 and 200 meters [1]. A CRN [2] on the other hand may be much bigger in size as compared with the transmission range of the PUs. Collaborative spectrum sensing becomes essential in such situations since PU's signal may only be received by a small subset of the SU nodes. Therefore, the FC has to rely on spectrum sensing reports from SUs spread across the CRN.

Collaborative spectrum sensing can also be favorable to malicious nodes in the network that may provide false spectrum sensing reports, a byzantine attack called Spectrum Sensing Data Falsification (SSDF) attack [3-7, 12]. Such an attack may adversely affect spectrum sensing decisions, which in turn may cause harmful interference to the PUs or deny the use of the vacant spectrum bands to the CRN. An SSDF attack may be aimed at gaining spectrum opportunities for the malicious nodes' own advantage or to disrupt CRN operation. As shown in the next section, efforts have been made to defend against SSDF attacks in CRNs, but there is a lack of research to deal with the situation where PUs are mobile and their transmission range is small as compared with the overall CRN size.

Reputation systems have been used frequently in computer networks to guard against malicious behavior from its entities. Reputation score typically represents an entity's long term contribution in a network's operation. The reputation scores are usually derived from some form of a voting mechanism and are used as weights in the system's decision making process. Reputation systems are therefore a means to keep selfish or malicious entities from having an adverse influence on a network's functioning. A CRN is vulnerable to selfish or malicious behavior because if left unchecked, the SSDF attacks may result in disruption of its operation to an extent that may even jeopardize its existence.

3.1 Motivation

Some reputation systems have been proposed for CRNs [6, 7] where final spectrum sensing decision at a given time is based on votes gathered from all SUs in the entire CRN. A node's vote is calculated as a function of its spectrum sensing report and its reputation score. However, any reputation system based on voting from all of network's nodes will not work in situations where a PU's transmission can be received by only a small subset of nodes in the CRN. Therefore, a reputation system is needed for collaborative spectrum sensing which can cater for the short range PUs and will update the reputation scores of SUs that are within the range of a PU at a given time and not the entire CRN based on the validity of spectrum sensing reports.

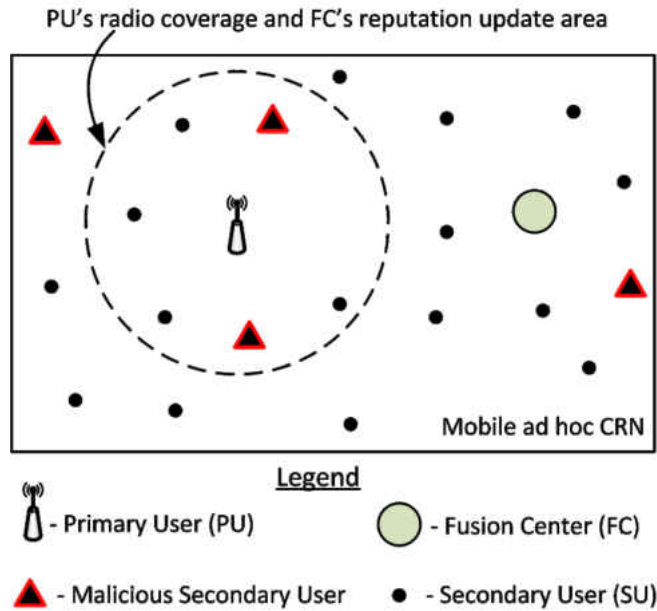


Figure 3.1: Ad hoc CRN with malicious nodes. Only the spectrum sensing reports sent by SU nodes in PU's coverage area should be considered for making final spectrum decisions and reputation updates.

3.2 Proposed Work and Contribution

In this chapter, we present a novel framework for collaborative spectrum sensing for ad hoc cognitive radio networks under byzantine SSDF attacks. This framework incorporates a spatio-spectral anomaly detection¹ system that functions in conjunction with a reputation system to detect malicious nodes in the CRN. Under typical network conditions and attack scenarios, our proposed framework is capable of reliably detecting malicious SUs and making the correct spectrum sensing decisions under SSDF attacks. This framework is especially suited for

¹ We use the terms outlier detection and anomaly detection interchangeably.

situations where PUs have smaller transmission ranges compared to the coverage area of the CRN as shown in figure 3.1.

Specifically, we have made following contributions:

- Identified limitations of existing CRN spectrum sensing and reputation systems in dealing with short-range PUs.
- Developed a spectrum map construction system and formulated spatio-spectral anomaly detection for CRNs with short-range PUs.
- Proposed a novel framework for integrating reputation with a spatio-spectral anomaly detection system to defend against SSDF attacks.
- Presented an evaluation of our proposed framework under three variants of byzantine SSDF attacks.

3.3 Related Work

A comprehensive study of trust and reputation management systems proposed for CRNs is provided in [6]. Authors have given a taxonomy of reputation management systems and discuss various attack models and associated challenges pertaining to collaborative spectrum sensing in CRNs. A collaborative spectrum sensing scheme is presented in [7] which introduces Location Reliability and Malicious intent as trust parameters. The authors employ the Dempster-Shafer theory of evidence to evaluate trustworthiness of reporting secondary user nodes. The proposed scheme assigns trust values to different cells in the network which may receive abnormal levels of PU's signal due to the effects of multi-path, signal fading and other factors in the radio

environment. Equal emphasis is given to the spectrum sensing reports from SUs using Equal Gain Combining while using trust values of the cells from where these reports were received as weights for data aggregation. This approach also assumes that the PU's communication range is large enough to be received by the entire CRN and uses the spectrum sensing reports of all CRN nodes to reach the final spectrum decision.

Authors in [8] propose a verification framework utilizing primary user emulation signals in order to confirm the correctness of spectrum sensing reports provided by SUs. An anti-jamming scheme is presented in [9] which uses a game theoretic approach to select a subset of channels that are not being used by a PU. The authors model the channel hopping, jamming and anti-jamming process as a Markov decision process. To reduce the computational complexity of a policy iteration scheme, they propose a Q-Function approach. The transmission ranges of the SUs, PUs and the jammers are assumed to be large enough to cover the entire CRN.

An anti-jamming spectrum access protocol is presented in [10]. The authors contend that existing solutions to model PU spectrum access and communications assume a priori knowledge of states and traffic statistics. In order to assume a realistic scenario, the authors formulate the problem of anti-jamming multichannel access in CRNs and solve it as a non-stochastic multi-armed bandit problem where the SUs adaptively choose their channel hopping sequence. As with other solutions, this approach also assumes that the transmission ranges of both the PUs and the SUs are large enough to be received in the entire CRN coverage area. Authors in [11] tackle the problem of PU emulation, an attack aimed at denying the use of vacant spectrum bands to the CRN. In order to evade the pursuing jammer, the SUs employ a game theoretic channel hopping

strategy where they have to employ a strategy that would ensure the utilization of the best among the set of vacant channels. The game is analyzed by finding the optimal strategy of the jammer using the framework of partially observable Markov decision process (POMDP).

Another collaborative spectrum sensing scheme is presented in [12] which uses pre-filtering to remove extreme spectrum sensing reports and a simple average combining scheme to calculate spectrum sensing decisions while considering all reports that pass the pre-filtering phase. This approach also assumes PU's transmission range to be large enough to cover entire CRN and their attack model is limited only to 'Always-ON' or 'Always-OFF' attacks. A secure and distributed spectrum sensing technique is presented in [13] which assumes that the PU's transmission range is large enough to be received in the entire CRN. It characterizes the spectrum sensing problem as an M-ary hypotheses testing problem and considers a cluster-based CRN where cluster heads receive and process raw spectrum sensing data before forwarding to the FC. Because the authors assume that the PU's transmission range is large enough to be received by every node in the network with varying signal strength, this approach cannot be adopted for a CRN in which a PU has much smaller transmission range.

3.4 System Model and Assumptions

We model the Ad hoc CRN (figure 3.1) as a region in which the PUs and SUs are mobile under general mobility model. There can be one or more PUs operating within the CRN at any given time. To guard against PU emulation attacks, there is a need to uniquely identify all transmitters. With techniques such as Radio Frequency Fingerprinting (RFF) [14] all devices in the CRN as well as the PU can be uniquely identified. Therefore, in this chapter, we treat

uniquely identifying a transmitter as a black box and assume that nodes in the CRN as well as the FC are capable of uniquely identifying every other device in the CRN area and malicious nodes in the CRN cannot provide spectrum sensing reports on behalf of other nodes. Table 3.1 lists the notations and acronyms used in this chapter.

Table 3.1: List of Notations and acronyms – Chapter 3

Notation	Definition
$P_{r,i,k}$	Received power (RSS) at node i at time k
γ_m	Max width of annular region of RSS level m
$l_{i,k}$	Location of SU i at time k
$r_{i,k}$	Reported RSS level of SU i at time k
$\delta_{j,k}$	Distance between node j and k
τ	PU detection threshold (RSS level above which PU is considered detected)
$\varphi_{i,j}$	Minimum distance between RSS levels i and j
$\psi_{i,j}$	Maximum distance between RSS levels i and j
$\theta_{j,k}$	Classification of node j being outlier or normal at time k
R_j	Outlier / normal entry for node j in lower tier of reputation table
M_j	Malicious / honest entry for node j in upper tier of reputation table
$D_{j,k}$	Spectrum decision with soft combining for node j at time k
D_k^F	Final spectrum decision for CRN at time k
PU	Primary User
SU	Secondary User
FC	Fusion Center
RSS	Received Signal Strength
CDT	Channel Detection Time
SSDF	Spectrum Sensing Data Falsification

A spectrum band is considered to be vacant when it is not being used by any PU, and occupied otherwise. Reputation update cycle is termed as the Channel Detection Time (CDT) slot during which SUs report their sensed Received Signal Strength (RSS) to the FC, a special SU node in the CRN selected to aggregate spectrum sensing data from SUs and make spectrum sensing decisions. Selection of FC may be carried out in a similar manner as cluster heads are selected in various kinds of networks e.g. [15]. However, selection of FC is out of the scope of this work and assumed to be achieved by other protocols. It is also assumed that SUs have an on-board GPS device, know their location at all time and include this information in every spectrum sensing report.

After every CDT slot k , each SU i sends its spectrum sensing report to the FC including the RSS value $P_{r,i,k}$ and its location $l_{r,i,k}$. This is essential for the FC to construct a spatio-spectral map of the entire CRN which is then utilized to calculate spectrum occupancy decision. We also define a Detection Threshold τ which corresponds to the RSS level below which a PU's signal is not considered to have been detected. Because of the limited transmission range of a PU, it is possible that the FC does not receive PU's signal directly when the PU is far away. For a robust system design, we assume that the FC always relies on the reports from the SUs to construct the spatio-spectral map of the CRN.

Attack Model: With the presence of malicious nodes in the CRN which may provide false spectrum sensing information to the FC, the accuracy of the spectrum sensing decisions could be severely degraded thereby jeopardizing the operation of the CRN. Malicious nodes may provide false spectrum sensing report or misreport their current location in order to affect the outcome of

spectrum report aggregation. Although it is possible for malicious nodes in a CRN to launch various kinds of attacks such as the PU emulation (PUE) attack or jamming attacks that target different channels including the common control channel, but SSDF attack is the only focus of this chapter. Presence of malfunctioning nodes, i.e., Byzantine Failure is treated in the same manner as a SSDF attack.

3.5 Reputation Aware Spectrum Sensing Framework

Spectrum sensing reports from SUs in detecting a PU can vary significantly because of small communication range of the PU relative to the size of CRN and mobility of both SUs and PUs. In addition, this situation is very suitable for malicious nodes to launch SSDF attacks and cause errors in spectrum decisions. It is therefore vital for the FC to identify malicious nodes and prevent them from inducing spectrum decision errors. To detect malicious nodes and guard against SSDF attacks, our proposed reputation aware spectrum sensing framework has four components:

- Semi-supervised spatio-spectral anomaly detection.
- Spectrum sensing data aggregation.
- Spectrum map construction.
- Reputation management.

We describe each of these components in detail in this section. Description of notations is given in table 3.1.

3.5.1 Semi-Supervised Spatio-Spectral Anomaly Detection

Collection of spectrum reports is assumed to be carried out with existing routing protocols and is not the focus of this work. Here we briefly present the process through which RSS is calculated by the SUs and when reported through spectrum sensing reports, converted into discrete levels by the FC. Next we demonstrate how the FC uses the RSS levels to detect anomalous behavior by SUs.

3.5.1.1 RSS Calculation

RSS is a powerful tool that has been extensively used in wireless networks for various purposes such as transmitter localization [16], ranging [17] and construction of radio environment maps [18] (also called spectrum maps). Since FCC has mandated presence of online databases of licensed users of spectrum in a given geographical area, it is reasonable to assume that PUs' communication parameters are known to the CRN. For the purpose of detecting anomalies in spectrum reports as well as localizing PU and construction of its radio environment map, we leverage the known characteristics of PUs' communications for calculating RSS values in different parts of the CRN.

Let $P_{r,i,k}$ denote the RSS of PU's signal at secondary user i at time k , which can be calculated according to [19] as follows:

$$P_{r,i,k} = G_{r,i} P_t G_t \frac{\lambda}{\{4\pi S_{i,k}\}^2} \quad (1)$$

where $G_{r,i}$ is the antenna gain of node i , P_t is the transmitted power of the PU and G_t is antenna gain of the PU, λ is PU's signal wavelength and $S_{i,k}$ is distance between the PU and receiving SU i at time k . From equation 1 we define RSS level m at a given distance $S_{i,k}$ from PU as a discrete region defined by γ_m as the width of a ring-shaped annular region. A node i , whose reported RSS satisfies the inequality

$$m - 1 < P_{r,i,k} < m + 1, \forall m \in \{0,1,2, \dots M\} \quad (2)$$

belongs to RSS level m , where M is the number of discrete RSS levels a PU's transmission is divided into. RSS level < 1 means that a SU is not within PU's transmission range and cannot detect its signals.

3.5.1.2 Spatio-Spectral Anomaly Detection

A spectrum sensing report from a SU contains the RSS as well as the node's current location, both of which can be falsely reported by malicious nodes. We employ a semi-supervised anomaly detection system to detect whether a spectrum sensing report falls within the expected normal values for reported RSS level. We define the normal behavior for reporting SUs in the form of upper and lower bounds on the distance between a given pair of RSS levels reported by two SU nodes. These lower and upper bounds on normal behavior are formulated as matrices φ and ψ respectively, elements of these behavior matrices are derived as follows:

$$\varphi_{i,j} = \begin{cases} \sum_{m=i+1}^{j-1} \gamma_m & \text{if } |j - i| \geq 1 \\ 0 & \text{if } j = i \\ \sum_{m=j+1}^{i-1} \gamma_m & \text{if } |j - i| \leq -1 \end{cases} \quad (3)$$

$$\psi_{i,j} = \sum_{m=1}^i \gamma_m + \sum_{m=1}^j \gamma_m \quad (4)$$

where the element $\varphi_{i,j}$ is the *minimum* distance and the element $\psi_{i,j}$ is the *maximum* distance between two SU nodes that reported RSS levels i and j , respectively and γ_m is width of the annular region of the RSS level m .

After gathering all reports from the SUs, the FC performs a pairwise comparison of every reported RSS level and classifies the distance between the nodes under consideration as either a normal or abnormal distance. This classification is performed by comparing the distance with both the minimum as well as maximum distance matrices. Consider the set of spectrum sensing reports S in a given CDT slot, to be:

$$S = \{s_1(l_1, r_1), s_2(l_2, r_2), \dots, s_n(l_n, r_n)\}, \forall n \in \{1, 2, \dots, N\} \quad (5)$$

where N is the number of SUs in the CRN, l_n is the location and r_n is the reported RSS level of node n . Distance between nodes i and j is given by $\delta_{i,j}$ which can be calculated from their reported location information. Classification of a distance between a pair of nodes i and j , denoted by $C_{i,j}$ is given as:

$$C_{i,j} = \begin{cases} 1 & \text{if } \varphi_{r_i, r_j} \leq \delta_{i,j} \leq \psi_{r_i, r_j} \\ -1 & \text{otherwise} \end{cases} \quad (6)$$

where $C_{i,j} = 1$ represents that the distance is within normal range and -1 means that the distance is classified as abnormal. At the end of distance classification, the number of normal and abnormal distances of a given node from all other reporting nodes is compared. As shown in figure 3.2, if majority of a node's distances are normal then the node is considered honest in the

current CDT slot, otherwise it is treated as an outlier node and its reputation score is decremented by the reputation management system.

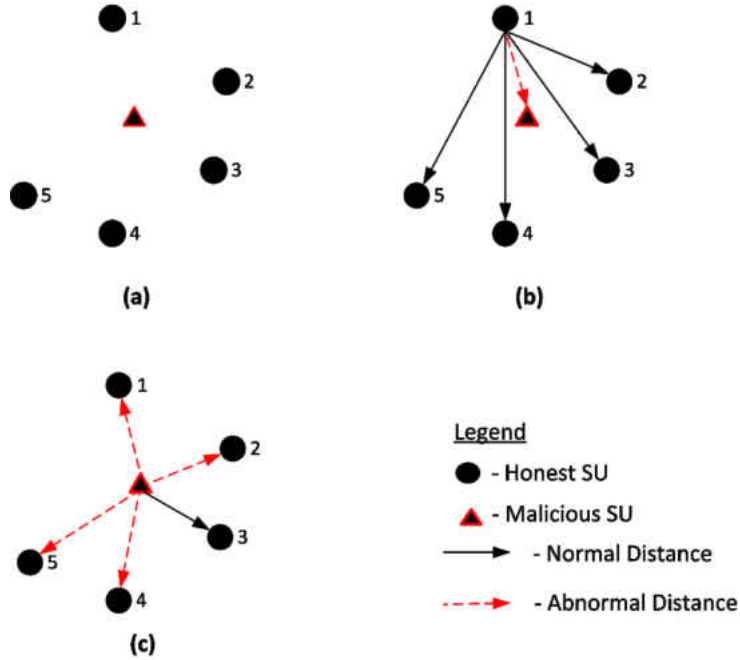


Figure 3.2: Anomaly detection in reported RSS (a) SUs that reported PU's presence including a malicious node. (b) Distances from an honest node to all other reporting SUs. Distance to malicious node is abnormal, other distances are normal. (c) Distances from a malicious node to all other reporting SUs. Since majority of its distances are abnormal, the node in the middle is classified as outlier.

The final classification of a node as an outlier, denoted by $\theta_{j,k}$ is given as per algorithm 1 as follows:

$$\theta_{j,k} = \begin{cases} 0 & \text{if } \sum_{j=1}^m C_{j,k} \geq 0 \\ 1 & \text{otherwise} \end{cases} \quad (7)$$

where $\theta_{j,k} = 0$ represents that node j is a normal node at time slot k , and 1 represents an outlier/abnormal node at CDT slot k . All the nodes that reported the presence of PU on the spectrum and classified as normal nodes in equation 7 are next used in the spectrum report aggregation process to reach a spectrum decision explained in next subsection. The algorithm for anomaly detection in spectrum sensing reports is given in Table 3.2.

Table 3.2: Spatio-Spectral Anomaly Detection Algorithm

Data: $S_{i,j}, r_i, r_j, \varphi_{r_i r_j}, \psi_{r_i r_j}, x$
Result: Outlier Classification of (x) of SU node

begin

1. **for** $i = 1 \rightarrow N$
2. **for** $j = 1 \rightarrow N$
3. **if** $S_{i,j} < \varphi_{r_i r_j} \vee S_{i,j} > \psi_{r_i r_j}$
4. $x \leftarrow x + 1$
5. **else**
6. $x \leftarrow x - 1$
7. **end if**
8. **end**
9. **end**
10. **if** $x > 1$
11. mark node i as outlier in reputation table
12. **end**

end

3.5.2 Spectrum Sensing Data Aggregation

Typically, spectrum sensing reports are aggregated using voting mechanisms based on either the majority rule, the AND rule or the OR rule [20]. As evident from figure 3.1, these aggregation rules cannot be applied in situations where PU's transmission range is much smaller as compared with the overall size of the CRN. This is because even in the absence of malicious nodes, the number of nodes receiving PU's signal is expected to be much less than the total number of nodes in the CRN. Therefore, our proposed spectrum data aggregation technique determines the presence or absence of PU within an area of CRN that is equal to the PU's transmission range. When all spectrum reports are collected at FC, each node is classified as behaving normally or abnormally in every CDT slot. This node classification at each CDT slot can be viewed as a node's instantaneous reputation; however, the reputation score of every node used in our proposed system is accumulated with the passage of time and can be viewed as its long-term reputation. As discussed in subsequent sections, our proposed reputation scheme is composed of three-phases.

3.5.2.1 Report Aggregation with Soft Combining

For the purpose of data aggregation we use soft-combining technique where, instead of its spectrum sensing decision, a CRN node reports its RSS level to the FC which then aggregates these reports to calculate its final spectrum sensing decision. Nodes whose spectrum sensing reports are considered anomalous in current CDT slot are classified as outliers and their reputation scores are decremented. Spectrum sensing reports that pass the anomaly detection phase are next processed in data aggregation. In our reputation-aware spectrum sensing

framework a node has to have a minimum reputation score to be considered honest at the current CDT slot for its report to be included in calculation of spectrum decision. Calculation of reputation score and classification of a node as either honest or malicious is explained in the next section. The three phase approach for behavior classification explained in the following subsection is used because a malicious node may report correct spectrum sensing results in some of the CDT slots to hide its SSDF attacks with a few correct reports as well as to improve its reputation score.

3.5.2.2 Spectrum State Decision

In a CDT slot k , if no honest SU reported presence of a PU's signal then the spectrum decision D_k is *vacant*. If there were some reports from honest nodes that indicated presence of PU's signal on the spectrum then a majority vote is conducted based on a Detection Threshold τ to determine the spectrum sensing decision:

$$D_{j,k} = \begin{cases} 1 & \text{if } r_{j,k} > \tau \\ -1 & \text{if } 0 < r_{j,k} \leq \tau \end{cases} \quad (8)$$

$$D_k^F = \begin{cases} 1 & \text{if } \sum_{j=1}^m D_{j,k} \geq 0 \\ 0 & \text{otherwise} \end{cases} \quad (9)$$

where $D_{j,k}$ is the spectrum sensing decision (occupied = 1, vacant = -1) from report $r_{j,k}$ of node j and D_k^F is the final spectrum sensing decision (occupied = 1, vacant = 0) of the CRN for CDT slot k . A node once labeled as malicious may regain an honest status by providing correct spectrum sensing reports however, the rate of reputation improvement is much slower than its

decline. This difference in the rate of reputation change ensures that the malicious nodes do not manipulate their reputation scores to their advantage.

3.5.3 Spectrum Map Construction

If the spectrum report aggregation results in a decision that the spectrum is occupied then spectrum map has to be constructed and the PU has to be localized. The accuracy of PU localization however depends on the number of SUs in PU's range as well as the RSS levels received by those SUs. This phenomenon is represented by the errors in detecting malicious nodes as well as incorrectly labeling honest nodes as malicious as shown in the performance evaluation (section 3.6).

For localization of PU with the help of RSS values calculated above, we need a technique to fit a circle to the locations of SUs that report same RSS levels in a given time slot. A number of methods exist to fit a circle to a collection of data points such as full least squares, average of intersections etc.

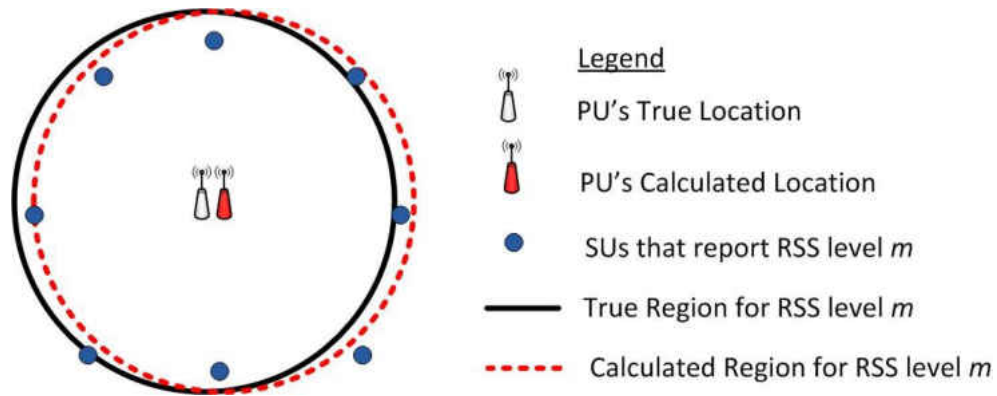


Figure 3.3: Error in spectrum map construction using circular regression with a single RSS level. Final PU localization is done with weighted average of localizations with all of the M RSS levels.

3.5.3.1 Circular Regression with SU locations

We employ the *Kåsa* method of circular regression [21] shown in figure 3.3 which is summarized as follows: On a two-dimensional plane we want to find a circle that best fits the given set of points that represent reporting SUs locations in a sense of least squares approximation. Suppose the fitted circle has the center point (a, b) i.e. the PU's calculated location and a radius of R that represents PU's transmission range. The observed set of points that represent N reporting SUs' locations is given by:

$$L = \{(x_1, y_1), (x_2, y_2), \dots, (x_i, y_i)\}, \forall i \in \{1, 2, \dots, N\} \quad (10)$$

If all of the points (x_i, y_i) fall exactly on the circle, then equation $(x_i - a)^2 + (y_i - b)^2 = R^2$ is satisfied. If the SUs' locations under consideration are not on the circle then there exists a fitting

error $f_i = (x_i - a)^2 + (y_i - b)^2 - R^2$ whose magnitude will be directly proportional to the distance of points (x_i, y_i) from the true circle.

The objective function \mathcal{F} for the Kåsa method is to minimize the summation of the above fitting errors of all observed points i.e., SUs' reported locations:

$$\mathcal{F}(a, b, R) = \sum_{i=1}^n [(x_i - a)^2 + (y_i - b)^2 - R^2]^2 \quad (11)$$

By using the transform $B = -2a, C = -2b, D = a^2 + b^2 - R^2$, the above objective function becomes:

$$\mathcal{F}(a, b, R) = \sum_{i=1}^n [x_i^2 + y_i^2 + Bx_i + Cy_i + D]^2 \quad (12)$$

The derivative of \mathcal{F} in equation (12) with respect to B, C and D yields a system of linear equations:

$$\sum x_i^2 B + \sum x_i y_i C + \sum x_i D = -\sum x_i (x_i^2 + y_i^2) \quad (13)$$

$$\sum x_i y_i B + \sum y_i^2 C + \sum x_i D = -\sum y_i (x_i^2 + y_i^2) \quad (14)$$

$$\sum x_i B + \sum y_i C + D = -\sum (x_i^2 + y_i^2) \quad (15)$$

3.5.3.2 PU Localization

Solving the system of linear equations (13 - 15) gives B, C and D and thus the center of the circle, i.e., the location of PU (a, b) and is given by:

$$a = -B/2, b = -C/2 \quad (16)$$

It is to be noted that the center of the annular region calculated in equation (16) is the result of n SUs reporting the same RSS level. Greater value of n will in turn, increase the accuracy of PU localization. We carry out the same process of circular regression with each of the M RSS levels for which the number of reporting SUs is at least 3 because a smaller number greatly increases the fitting error. PU's localization with M RSS levels is done as follows: Let (a_m, b_m) be the center of the annular region calculated for RSS level $m \in \{1, 2, \dots, M\}$. If $P \subset N$ is the total number of SUs that reported PU's presence and n_m is the number of SUs that reported RSS level m , then the final location (a^F, b^F) of the PU is calculated as a weighted average of P points as:

$$a^F = a_m \cdot n_m / P, \quad b^F = b_m \cdot n_m / P \quad (17)$$

If spectrum report aggregation concludes that the PU is on air then it is localized as shown above. Thereafter, the next step is to detect any malicious nodes that were within PU's coverage area but did not report the presence of PU, an SSDF attack we refer to as the Induction attack which needs some additional processing at the FC. Detection of induction attack is carried out as follows: Let node n represent an honest node that reported RSS level r_m in current CDT slot and whose surrounding areas are being scanned next for the presence of *non-reporting* malicious node(s). Let φ_{r_m, r_0} be the minimum distance between RSS levels m and RSS level 0 from equation (17), then any SU node at a distance *less* than φ_{r_m, r_0} from node n that did not report the presence of PU is considered to be malicious because it lies within PU's transmission range and should have reported some RSS value.

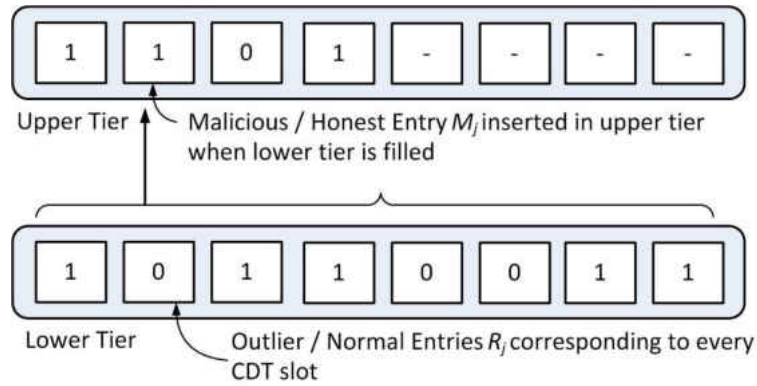


Figure 3.4: Two-tiered sliding window Reputation Table.

3.5.4 Reputation Management

During every CDT slot, reputation score for a SU may be *decremented* in any of the three subsections above because of anomalous behavior and *incremented* only if its contribution is positive in *all* of these steps. A reputation table is implemented as a two-tiered sliding window for every node in the CRN, as shown in figure 3.4.

3.5.4.1 Reputation Update Phase-1

After the anomaly detection phase when a node has been classified as behaving either normally or abnormally according to equation 7 a corresponding entry R_j is added in the lower tier of the reputation table, where an outlier entry corresponds to $R_j = 1$ and a normal entry corresponds to $R_j = 0$.

3.5.4.2 Reputation Update Phase-2

After spectrum reports are aggregated and the final spectrum decision D_k^F reached, SUs whose spectrum sensing reports contributed positively towards reaching the final decision are rewarded and the SUs whose reports contributed negatively towards reaching the final spectrum sensing reports are punished by the reputation system by adding relevant malicious / honest entries R_j in the lower tier of the reputation table.

3.5.4.3 Reputation Update Phase-3

The reputation system takes different courses of action for the two spectrum decisions: If the spectrum decision was ‘vacant’, then all nodes that reported presence of PU’s signal are punished by adding a malicious entry $R_j = 1$ in the lower tier of the reputation table. However, if the spectrum decision was ‘occupied’ then the FC has to first determine the location of the PU in order to reward or punish the nodes in its coverage area only, as shown in figure 3.1. Based on the spectrum reports of honest nodes, the FC then constructs a spectrum map of the PU and calculates the *expected* spectrum sensing reports of SUs within PU's transmission range. For a given CRN node, if reported and expected spectrum sensing reports do not match, then a malicious entry $R_j = 1$ is added in the lower tier of the node’s reputation table. Otherwise, an ‘honest’ entry $R_j = 0$ is added in the reputation table:

$$R_j = \begin{cases} 0 & \text{if } \textit{normal behavior} \\ 1 & \text{if } \textit{outlier} \end{cases} \quad (18)$$

Classification of a CRN node j to be malicious or otherwise at any given time is represented by an entry M_j in the upper tier of the reputation table as:

$$M_j = \begin{cases} 0 & \text{if } \sum R_{j,l} \leq T \\ 1 & \text{otherwise} \end{cases} \quad (19)$$

where l is the size of the reputation table and T is the threshold for a node j to be considered honest. A summary of reputation update process is shown in Algorithm 2.

The two-tiered implementation of reputation table as shown in figure 3.4 is used to normalize the difference between the speed of a node's mobility and the frequency of its spectrum sensing reports. Consider an SU moving at 3 m/sec and a CDT slot equal to 100 msec. If it took the SU 7 seconds to move from its current RSS level to an adjacent one, it would generate 70 spectrum sensing reports during this time period all of which would be highly correlated in a single-tier implementation of reputation table. In our two-tiered implementation once the lower tier of the reputation table is filled, a corresponding entry M_j is added in the upper tier of the table and the lower tier is reset. The decision for adding an honest or a malicious entry in the upper tier of the reputation table is reached based on majority rule applied on the lower tier. The algorithm for reputation management is given in Table 3.3. Implementation of the reputation table as a sliding window serves two purposes: first, it represents the latest behavior of a node and prevents malicious nodes from taking advantage of their reputation score from distant past and second, it gives a chance to nodes incorrectly labeled as malicious to improve their reputation in the CRN through the forgetting characteristic of the sliding window.

Table 3.3: Reputation Management Algorithm

Data: D_k^F, r_n
Result: malicious/honest Classification of SU nodes

begin

1. **for** every CDT slot k **do**
2. detect and remove anomalous reports r_n (phase-1)
3. calculate final spectrum decision D_k^F
4. punish/reward SUs by comparing reports r_n and final spectrum decision D_k^F
5. **if** $D_k^F = 1$ **then**
6. localize PU
7. calculate expected spectrum reports of SUs
8. punish non-reporting SUs (phase-3)
9. **else if** $D_k^F = 0$ **then**
10. punish SUs that reported PU's presence
11. **end if**
12. **end for**

end

3.6 Performance Evaluation

In this section we present an evaluation of our proposed reputation aware collaborative spectrum sensing framework to defend against three different variants of SSDF attacks. These variants include Induction attack, Denial of Service attack and the Spectrum Sensing Report Reversal attack. For the purpose of our simulations, we define these three attacks in the following subsection.

3.6.1 Variants of SSDF Attacks

3.6.1.1 Induction Attack

A CRN is expected to utilize vacant spectrum bands in an opportunistic manner i.e., to vacate it whenever a PU is sensed to be communicating. As per FCC regulations SUs must vacate the

spectrum upon arrival of the PU within a specified time called Maximum Detection Time or MDT [22]. The Induction attack refers to malicious nodes reporting absence of PUs from the spectrum band which in fact, might currently be using the spectrum. The purpose of this attack is to trick the CRN into believing that the spectrum is vacant and “induce” transmission by SUs thereby causing interference to the PUs. This attack can have devastating and far reaching effect on the CRN, as it can cause harmful interference to PU's signal and can jeopardize the existence of the CRN.

3.6.1.2 Denial of Service Attack

The Denial of Service (DoS) attack is intended by a malicious node in the CRN to deny the use of vacant spectrum bands to SUs. Because of short transmission range of the PUs, FC relies on spectrum sensing reports from the SUs to determine if the spectrum is vacant or occupied in order for it to be utilized by the CRN. However, malicious nodes launching a DoS attack can provide false spectrum sensing report always indicating that the spectrum is currently being used by the PUs thereby preventing the CRN from utilizing spectrum opportunities. The malicious nodes in the CRN may launch a DoS attack in order to gain unfair advantage over other SUs, utilizing the spectrum for their own communications or simply to deny the same to the rest of the CRN. Although such an attack would not cause interference to the PUs, it will severely degrade CRN's system performance by denying the spectrum opportunities to the honest nodes.

3.6.1.3 Report Reversal Attack

The spectrum sensing Report Reversal attack is essentially a combination of the two attacks described above i.e. the Denial of Service attack and the Induction attack. A malicious node will

launch a DoS attack only when the spectrum is sensed to be idle and an Induction attack will be launched only when the spectrum is being used by one or more PUs. On the other hand, a malicious node launching a Report Reversal attack will always provide a spectrum sensing report for spectrum's state that is the reverse of the actual PU's spectrum utilization state. For the previous two attack types, a malicious node will have to wait for the correct PU's spectrum state to launch an SSDF attack however, when a malicious node intends to launch a report reversal attack it will always be able to do so whether the PU is idle or active on the spectrum.

As we will demonstrate in the next sub-sections, the Report Reversal attack is intuitively much more detrimental to the collaborative spectrum sensing and the overall CRN operation as compared with DoS attack or the Induction attack. Another highlight of our simulations' results is that the DoS and Report reversal attacks need much fewer number of malicious nodes to achieve the same degree of success as opposed to Induction attack.

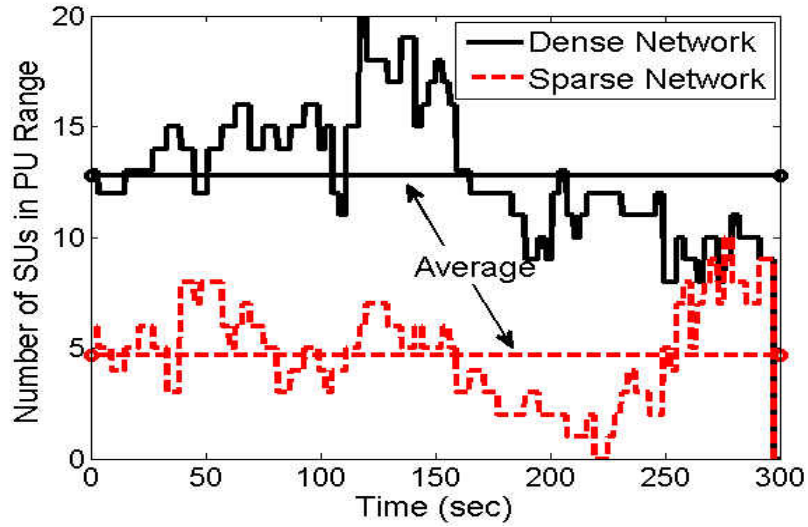


Figure 3.5: Average number of SUs in PU's range in dense and sparse networks.

3.6.2 Simulation Setup

For the purpose of evaluating our proposed framework for defending against aforementioned SSDF attacks, we have considered an ad hoc CRN of size 1000m x 1000m and the PU and the SUs whether honest or malicious, are mobile with their speed varying between 0 and 4m/s which represents a CRN user moving around on foot. The maximum transmission ranges for both the PU and the SUs is 200 meters. We have carried out simulations for both dense (100 nodes) and sparse (50 nodes) network configurations. The impact of collusion among malicious nodes in an ad hoc CRN is beyond the scope of this work.

Figure 3.5 shows the number of SUs within PU's transmission range at any given time during a simulation run with the mean 4.7 and variance 5.1 for a sparse network and a mean 12.7 and variance 9.2 for a dense network. The threshold T for a node to be considered as malicious is

kept at 3 malicious entries in the reputation window with the total reputation window size $l = 20$. Spectrum sensing reports are generated by the SUs in every CDT slot which equals 100 msec. At every CDT slot the sensing reports are then aggregated by the FC to reach the final spectrum sensing decision D_k^F as per equation (9) for the current CDT slot. All the graphs represent results that are averaged over 100 simulation runs. Every simulation run is 300 seconds in length unless specified otherwise.

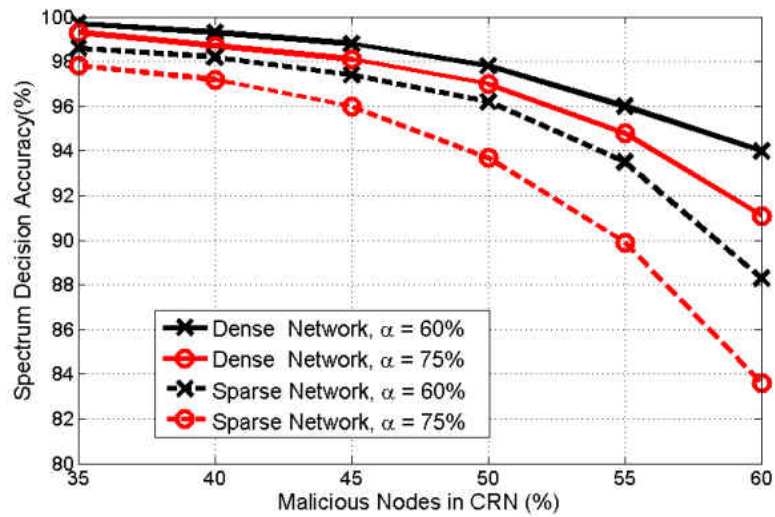


Figure 3.6: Spectrum Decision Accuracy under Denial of Service Attack.

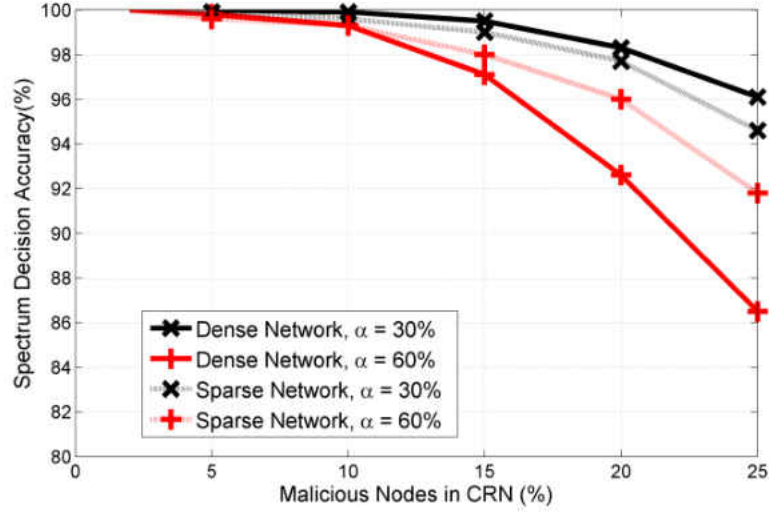


Figure 3.7: Spectrum Decision Accuracy under Spectrum Report Reversal Attack.

3.6.3 Simulation Results

Spectrum sensing accuracy is the most important metric with regards to the collaborative spectrum sensing because the existence of the CRN depends on accurate spectrum sensing decisions. Performance of our proposed reputation aware collaborative spectrum sensing framework with respect to spectrum sensing accuracy is shown in figures 3.6, 3.7 and 3.8 for the three variants of SSDF byzantine attack, where α represents PU's spectrum usage probability. As the number of malicious users in the CRN grows, it will have a negative impact on the overall spectrum sensing decision accuracy. Our proposed framework successfully detects malicious behavior and reaches correct spectrum sensing decisions up to 99.3% of the time when malicious nodes are 10% of the entire SUs which is a fairly large number of malicious nodes. Spectrum decision accuracy of our proposed framework drops to

94% when the number of malicious nodes increases to 25% of the CRN, a number that can be considered a highly unlikely number of malicious nodes in a network.

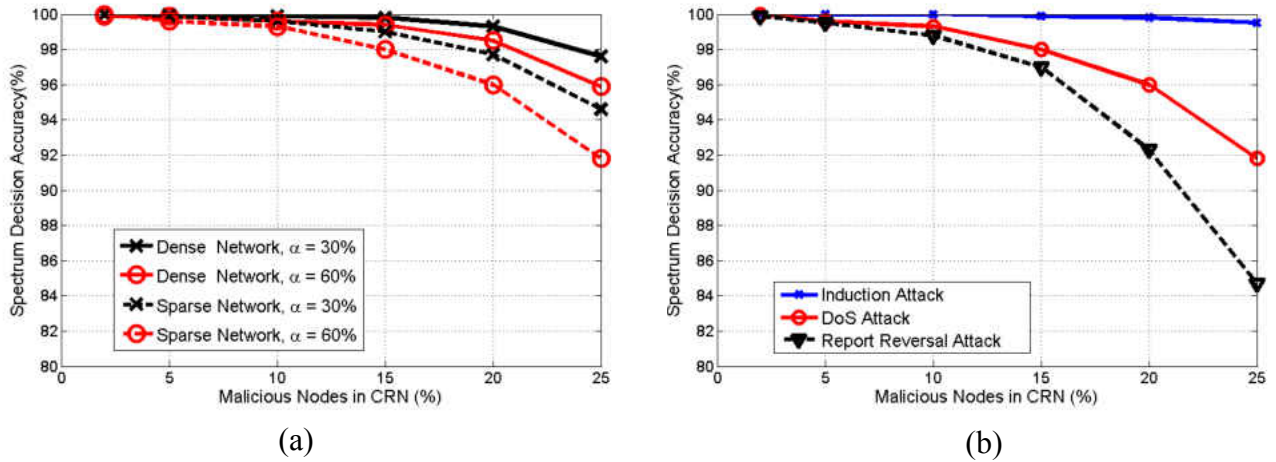


Figure 3.8: Spectrum Decision Accuracy under (a) Induction attack (b) All attacks combined.

Among the three variants of SSDF attacks, it can be seen from figure 3.8(b) that Report Reversal attack has the most severe impact on the spectrum sensing accuracy while the Induction attack has the least. To elaborate consider this: In order to launch an Induction attack in a CRN a malicious node has to report the absence of the PU in the spectrum band when it is actually been used by a PU. The honest nodes in the vicinity of a malicious node will however report the presence of the PU and the attempted attack on the CRN will fail. This makes the Induction attack comparatively difficult to launch as well as difficult to detect by the FC. In order to find out exactly how difficult it is for a malicious node to launch an Induction attack without collusion with other malicious nodes, we increased the malicious node population to a highly unlikely number of 60% of the total nodes in the CRN as shown in figure 3.7(a). Still the attack's

success rate was around 6% for a sparse network and our reputation framework was able to achieve a spectrum decision accuracy of 94%. Therefore, our proposed framework achieves spectrum decision accuracy of around 99.3% within a reasonable malicious node probability of 10% for all the three types of SSDF attacks.

Error! Reference source not found. shows the speed and accuracy of our proposed framework to detect malicious nodes in dense as well as sparse networks under the three variants of SSDF attack. The figures demonstrate that the majority of malicious nodes are detected within 60 seconds however intuitively the detection rate is comparatively slower for sparse networks.

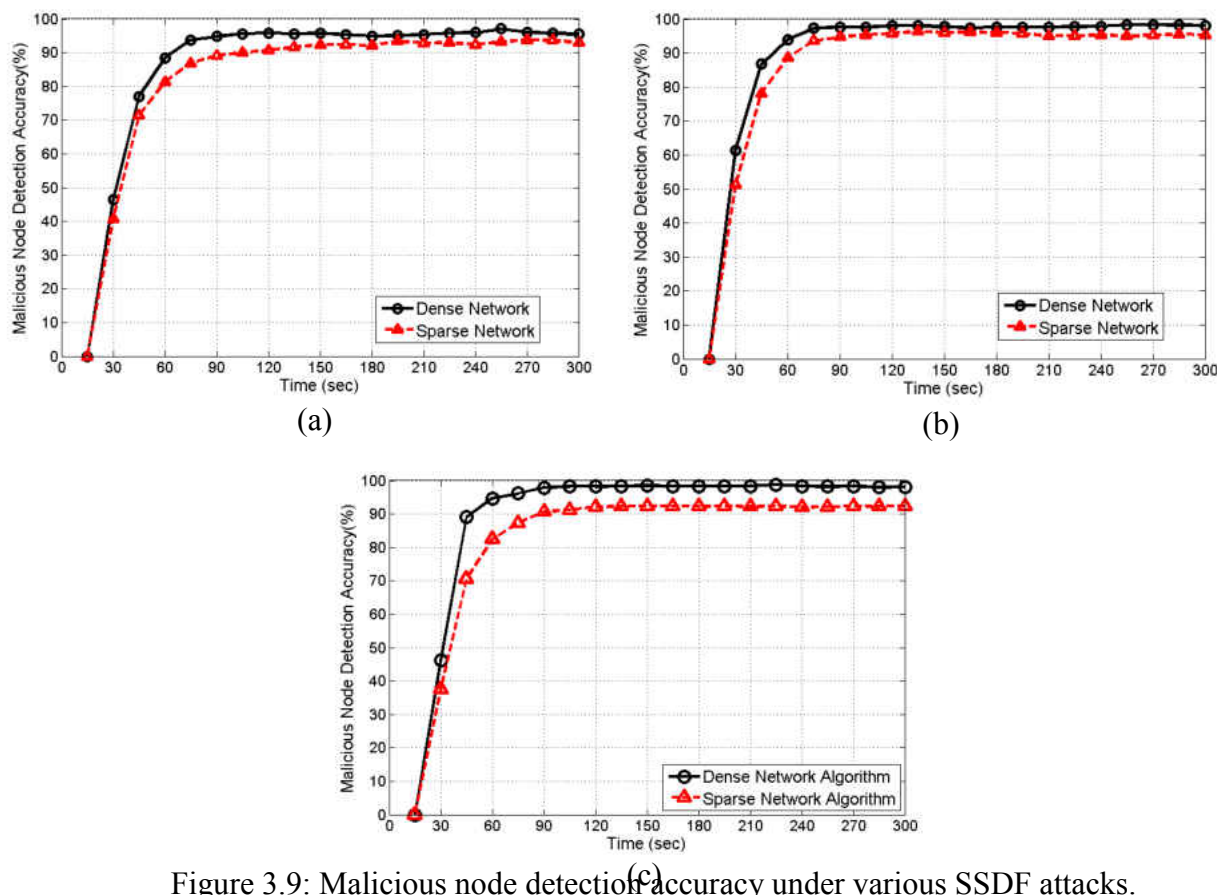
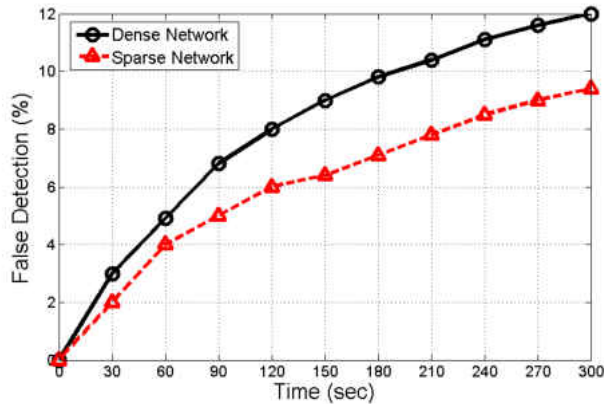
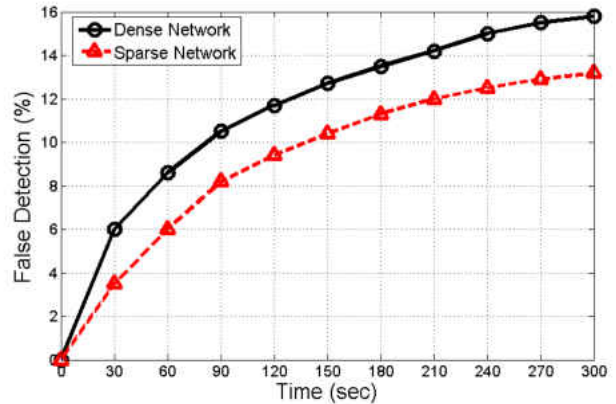


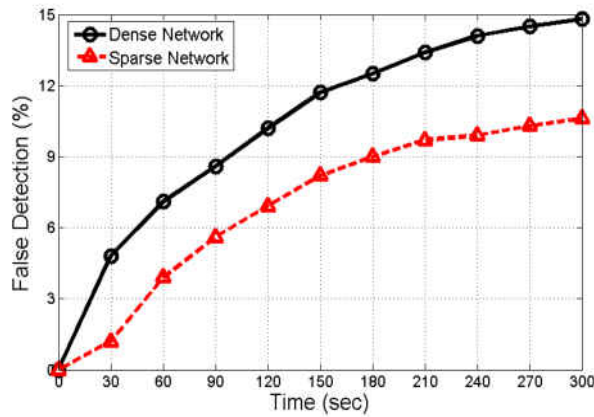
Figure 3.9: Malicious node detection accuracy under various SSDF attacks.



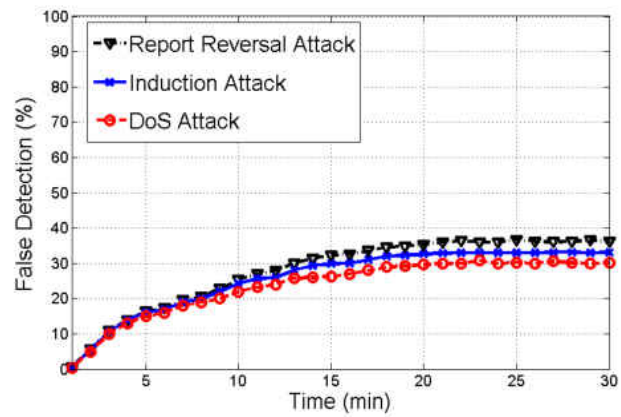
(a)



(b)



(c)



(d)

Figure 3.10: Incorrect labeling of honest SUs as malicious under various SSDF attacks.

Figures 3.10(a), (b) and (c) show the error rate of categorizing an honest node as a malicious node (labeled as ‘False Detection %’) by our proposed reputation framework under the three variants of SSDF attack. Figure 3.10(d) shows the long term dynamic for false detection percentage under the three SSDF attacks which is close to 30%. It is however pointed out that for the simulation of figure 3.10(d) the malicious SU population was kept significantly higher (60%)

for simulating induction attack as opposed to the other two attacks for which the malicious node population in CRN was kept at 30%.

3.7 Conclusion

Malicious nodes may provide false spectrum sensing reports in order to disrupt the operation of a CRN or to maximize spectrum opportunities for themselves. This can affect CRN's operation to an extent that may even jeopardize its existence. In this work we have proposed a novel reputation aware collaborative spectrum sensing framework based on spatio-spectral anomaly detection. Our proposed system is well suited for situations where the PU's communication range is limited within a sub-region of the CRN. Simulations of our system show that it is robust against SSDF attacks and can detect malicious behavior up to 99.3% of the time when malicious node density is within a reasonable range and is still very effective when the number of malicious nodes is even greater. Our proposed system is also flexible enough to be used where PU's communication range spans the entire CRN.

3.8 References

[1] FCC's Overview of LPAD registration procedure, <http://www.fcc.gov/help/overview-unlicensed-wireless-microphone-registrations>.

[2] IEEE STANDARD 802.11af-2013 - IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Television White Spaces (TVWS) Operation.

- [3] R. Chen, J.-M. Park, Y Ilou, and J. Reed ,“Toward secure distributed spectrum sensing in cognitive radio networks,” IEEE Comm. Mag., vol. 46, pp. 50-55, Apr. 2008.
- [4] Wang. W., Li. H., Sun. Y., Han. Z., “CatchIt: Detect Malicious Nodes in Collaborative Spectrum Sensing,” IEEE Global Telecommunications Conference, GLOBECOM 2009.
- [5] Wang. W., Li. H., Sun. Y., Han. Z., “Attack-proof collaborative spectrum sensing in cognitive radio networks,” 43rd Annual Conference on Information Sciences and Systems, ACISS 2009.
- [6] Ling, M. H., Yau, K.-L. A. and Poh, G. S., “Trust and reputation management in cognitive radio networks: a survey”. Wiley J. of Security & Comm. Networks (2013). doi: 10.1002/sec.899.
- [7] Jana, S., et al., “Trusted collaborative spectrum sensing for mobile cognitive radio networks,” 32nd IEEE International Conference on Computer Communications, INFOCOM 2012.
- [8] Kim, M., Chung, M. Y. and Choo, H., “VeriEST: verification via primary user emulation signal-based test for secure distributed spectrum sensing in cognitive radio networks”. Wiley J. of Security & Comm. Networks (2012), 5: 776788. doi: 10.1002/sec.372.
- [9] Chen. C., Song. M., Xin. C., Backens, J., “A game-theoretical antijamming scheme for cognitive radio networks,” IEEE Network, vol.27, no.3, May-June 2013.
- [10] Wang. Q., Ren. K., Ning. P., “Anti-jamming communication in cognitive radio networks with unknown channel statistics,” 19th IEEE International Conference on Network Protocols (ICNP), Oct. 2011.
- [11] Li. H., Han. Z., “Dogfight in Spectrum: Jamming and Anti-Jamming in Multichannel Cognitive Radio Systems,” IEEE Global Telecommunications Conference, GLOBECOM 2009.
- [12] P. Kaligineedi., et al., “Secure Cooperative Sensing Techniques for Cognitive Radio Systems”, International Conference on Communications, ICC 2008.
- [13] Jin Wei., et al., “Two-Tier Optimal-Cooperation Based Secure Distributed Spectrum Sensing for Wireless Cognitive Radio Networks,” IEEE INFOCOM 2010.

- [14] C. C. Loh et al., "Identifying unique devices through wireless fingerprinting," in Proc. of the first ACM conference on Wireless network security, Mar. 2008, pp. 4655.
- [15] Xia. D., Vljajic. N., "Near-optimal node clustering in wireless sensor networks for environment monitoring," in IEEE 21st International Conference on Advanced Networking and Applications, AINA May 2007.
- [16] Zhu, X., Wu, X., Chen, G., "Relative localization for wireless sensor networks with linear topology". Elsevier Computer Communications Sep. 2013.
- [17] Zhang, D., Liu, Y., Guo, X., Gao, M., Ni, L.M., "On distinguishing the multiple radio paths in RSS-based ranging," IEEE INFOCOM, 2012.
- [18] Yilmaz, H.B., Tugcu, T., Alagoz, F., Bayhan, S., "Radio environment map as enabler for practical cognitive radio networks," IEEE Communications Magazine, vol.51, no.12, pp.162,169, December 2013.
- [19] Stutzman, W. L., Thiele, G. A., "Antenna Theory and Design," 3rd Edition, John Wiley and Sons, Inc. 2012.
- [20] Xu, S., et al. "Double thresholds based cooperative spectrum sensing against untrusted secondary users in cognitive radio networks." IEEE VTC 2009.
- [21] N. Chernov., "Circular and linear regression: Fitting circles and lines by least squares", Chapman & Hall/CRC June 2010.
- [22] Stevenson, C, et al., "'IEEE 802.22: The first cognitive radio wireless regional area network standard," IEEE Communications Magazine, vol.47, pp.130-138, 2009.

CHAPTER 4: ADAPTIVE SPECTRUM SENSING UNDER NOISE AND SMART JAMMING ATTACK

Wireless Regional Area Network (WRAN) based on IEEE 802.22 standard [1, 2] referred to as CRN from here on, employs Cognitive Radio [3-6] techniques to provide broadband Internet access using the analog TV bands in an opportunistic, unlicensed and non-interfering basis. The TV bands made available by FCC for unlicensed use [4] by CRNs fall in the 54-698 MHz frequency range. To operate in a non-interfering manner, devices in a CRN are required to sense the spectrum periodically and vacate the spectrum band if they detect the presence of incumbent PU. In order to strike a balance between the conflicting goals of proper protection of incumbent PU's communication and optimum QoS for SUs, CRNs employ a two-stage spectrum sensing approach: these stages are called fast sensing and fine sensing [1]. Fast sensing as the name suggests, usually takes 9~20 microseconds depending on the technique used [7] such as energy detection, and therefore can only report the presence or absence of a signal on the spectrum band and cannot determine the type of the received signal. On the other hand fine sensing employs sophisticated techniques for identification of signals present on the spectrum and may take up to 160 msec [8] i.e. the entire duration of a super frame also called the Channel Detection Time (CDT) [1, 2].

Due to large transmission range of 35~100 km, IEEE 802.22 standard employs collaborative spectrum sensing i.e. the CRN base station (BS) not only carries out its own spectrum sensing but also relies on spectrum sensing reports from SUs in order to determine the spectrum state. As part of the collaborative spectrum sensing, devices in a CRN are synchronized and carry out the mandatory fast sensing during every CDT slot. The result of fast sensing is reported by all SUs to

the BS which then decides if fine sensing needs to be carried out. To ensure that everyone in the CRN senses PU's signals and not their own, quiet period for spectrum sensing are also synchronized. IEEE 802.22 standard mandates the CRN to always carry out fine sensing when the fast sensing stage reports presence of any signal on the spectrum [1]. As discussed subsequently, it is this static nature of spectrum sensing that can be exploited by malicious nodes in the CRN to launch smart jamming attacks and the adaptive spectrum sensing framework presented in this chapter is primarily aimed at modifying this specific static behavior of the IEEE 802.22 standard.

At the time when PU is not using the spectrum, a state referred to as spectrum opportunity for DSA, malicious users in the CRN can launch a Denial of Service (DoS) attack by jamming the frequency band currently being used by CRN, for the whole duration of every CDT. However, such an attack has the disadvantage of rendering the jammed frequency band unusable by the attacker as well and it requires a lot of transmission power. On the other hand an attacker can take advantage of the fixed nature of the two stage spectrum sensing mechanism by transmitting a short jamming signal during the fast sensing stage only. We call this kind of an attack as a smart jamming/denial of service attack. Since fast sensing stage is significantly shorter than the CDT, a smart jamming attack would consume far less energy than jamming the entire CDT slot and will force the rest of the CRN to carry out fine sensing denying them the spectrum opportunity with the additional benefit of the possibility of utilizing it for their own communications. In order to mitigate the effects of smart jamming attacks on spectrum opportunity utilization, an adaptive spectrum sensing technique is needed.

4.1 Motivation and Contributions

The IEEE 802.22 standard imposes an upper bound on the maximum delay allowed for the detection of incumbent PU's signal and for the CRN to vacate current channel. This time limit is called the Maximum Detection Time (MDT) [1, 5, 9] and is equal to 2 seconds. We leverage the MDT constraint to propose a framework for adaptive defense against smart jamming attack in IEEE 802.22 CRNs. We call this framework DS3: Dynamic and Smart Spectrum Sensing. The main difference between the spectrum sensing decision of existing IEEE 802.22 standard and our proposed DS3 framework is that whenever fast sensing stage reports presence of some signal on spectrum, the former always carries out fine sensing while DS3 dynamically adjusts the threshold for conducting fine sensing in response to an alert from fast sensing. As explained in section IV, the dynamic threshold depends on a cost minimization function in conjunction with the latest estimate of jamming attack severity.

Specifically, following contributions are made:

- Carried out an analysis of the impact of smart jamming/DoS attack on CRN's dynamic spectrum access.
- Proposed a novel adaptive defense framework called DS3 which enables the CRN to thwart smart jamming attacks as well as improve spectrum utilization by SUs under noisy channel conditions.
- Carried out simulation study of the proposed DS3 framework and demonstrated its improved performance as compared with the IEEE 802.22 standard under smart jamming attacks.

4.2 Related Work

Opportunistic spectrum access in CRNs makes them an easy target for attackers that may jeopardize its operation for their individual gains or merely because of malicious intent. Therefore, security of DSA in CRNs has been the focus of attention for many research efforts lately. This section provides an overview of related work and provides an insight as to how these studies differ from the work presented in this chapter.

Byzantine failure and spectrum sensing data falsification attacks are considered in [10] and a defense mechanism based on filtering out suspicious spectrum reports with weighted sequential probability ratio test (WSPRT) is proposed. Measures to prevent jamming of Common Control Channel (CCC) in an ad hoc CRN are presented in [11]. It assumes that the jammers are aware of the protocol specifics as well as cryptographic quantities used to secure network operations. The authors propose two techniques to identify malicious nodes that act independently and those that collude to jam the CCC. They also propose generation and secure dissemination of hopping sequences for the CRN to elude jammers. This however is primarily aimed at defending against jamming the CCC through which spectrum sensing and other control data are shared. On the other hand, our work addresses defense against jamming of spectrum sensing itself.

A collaborative spectrum sensing scheme is presented in [12] which introduces Location Reliability and Malicious intent as trust parameters. The authors employ the Dempster-Shafer theory of evidence to evaluate trustworthiness of reporting secondary user nodes. The proposed scheme assigns trust values to different cells in the network which may receive abnormal levels of PU's signal due to the effects of multi-path, signal fading and other factors in the radio

environment. The approach adopted by the authors does not cater for a two-stage spectrum sensing and the possibility of a smart jamming attack by malicious nodes.

Authors in [13 - 17] present various game theoretic approaches to defend against various jamming attacks in the collaborative spectrum sensing of CRNs. The common theme in all of these defense strategies against jamming is to hop to a channel that might not be jammed by the jammer. Our proposed adaptive spectrum sensing framework on the other hand, does not resort to channel hopping and evades jamming while staying in the same channel.

A collaborative defense technique is presented in [18] where the SUs in a CRN defend against a collaborative DoS attack launched by sweeping and jamming the channels in the entire spectrum. The SUs make use of spatial and temporal diversity to form proxies in order to continue communicating. This work however does not consider that the jammer may seek to minimize its jamming power budget by jamming only the fast sensing stage. Also, the main defense against jamming attack is for the CRN to hop to another channel.

Authors in [19] present a game theoretic approach to defend against jamming attacks in CRNs. They derive an optimal strategy for the SUs to decide whether to remain in the current band or to hop to another band by employing a Markov Decision Process approach. In addition to formulating a channel hopping strategy, the authors also propose a learning process through which SUs estimate current network conditions based on past observations using the maximum likelihood estimation technique and further incorporate this information in their defense strategy for optimization. This work also does not consider the two-stage spectrum sensing that is employed in the current IEEE 802.22 WRAN standard, and the defense against jamming is for

CRN to hop to another channel. Techniques to optimize the channel sensing duration under different SNR conditions are proposed in [20]. However, the work does not consider intentional jamming attacks.

To the best of our knowledge this is the first attempt to 1) address a smart jamming attack in IEEE 802.22 CRNs by malicious SUs and 2) maximize utilization of spectrum opportunities while staying in the spectrum band that is being jammed and not hopping away from it.

4.3 System Model, Attack Model and Assumptions

4.3.1 System Model

We consider an IEEE 802.22 Cognitive Radio Network spread across a wide area in which collaborative spectrum sensing is undertaken for detection of licensed PU in the region. All of the CRN's devices are synchronized for network-wide quiet periods during which they carry out the mandatory fast sensing in every super frame. Fast sensing reports from all SUs are aggregated at the CRN BS which then decides if some signals are present on the spectrum that must be further investigated. If so, the entire CRN carries out fine sensing which may take all of the remaining time in current CDT slot. A list of notations and acronyms used in this chapter is given in table 4.1.

Maximum delay allowed for the detection of incumbent PU's signal and for the CRN to vacate current channel is called maximum detection time (MDT). A CDT slot spans 160 msec [1] whereas the MDT duration is 2 seconds [5, 9] giving the CRN a maximum of:

$$\tau = \lfloor MDT / CDT \rfloor \quad (1)$$

discrete time slots to detect the presence of a PU and vacate the spectrum band. IEEE 802.22 standard mandates conduct of fine sensing in a CDT slot if the result of fast sensing suggests presence of some signals that might be from the PU. However under our proposed DS3 framework, even if the fast sensing stage reports presence of a signal on spectrum, the BS may or may not decide to conduct fine sensing in a CDT slot. This adaptive decision is based on a cost minimization function and is explained in subsequent section.

Table 4.1: Notations and acronyms – Chapter 4

Notation	Definition
k	time since PU was last detected as active
P_k	Probability PU is ON after it stays in OFF state for k consecutive CDT slots
p_t	Probability of CRN carrying out fine sensing
τ	Num. of CDT slots in MDT (12 CDT slots as per IEEE 802.22 standard)
t	running time
π_1	PU's spectrum usage (%)
α	Prob. of PU to transition from state 0 to state 1
β	Prob. of PU to transition from state 1 to state 0
γ_{kt}	Cost of missing PU detection
φ_t	Cost of wasting a spectrum opportunity
p_t^*	Optimal spectrum sensing decision
J_t	DS3's cost minimization function
c	Sensitivity towards PU detection delay
N	Size of the attack history window
n_i	History window entries
v_t	Estimate of current attack severity
CDT	Channel Detection Time / 1 superframe (160 msec)
MDT	Maximum (PU) Detection Time (2 seconds)

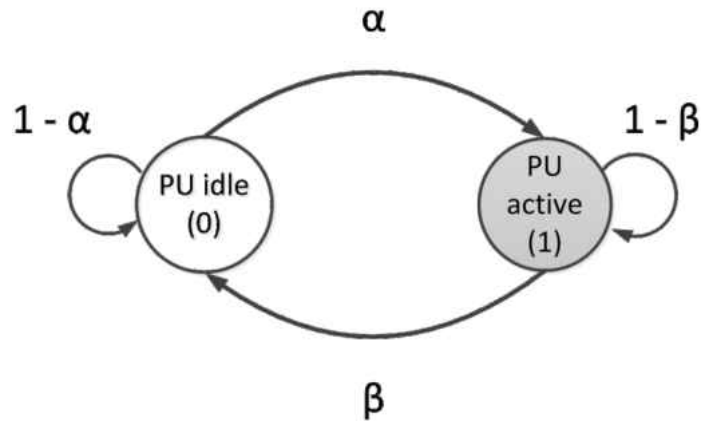


Figure 4.1: Markov ON/OFF model for PUs Spectrum Usage.

4.3.2 Assumptions

DS3 framework is meant to be implemented *only* at the BS which makes it highly scalable and is aimed to replace the existing static fine sensing decision criterion of the IEEE 802.22 standard with a dynamic one. The PU's use of spectrum is modeled as a Markov ON/OFF process [21, 23] as shown in figure 4.1 where α is the probability that the PU will transition from state 0 to 1 and β is the transition probability from state 1 to 0. State 0 represents OFF/idle and 1 represents ON/active state of the PU. Fast sensing is assumed to have high false positive under large noise or smart jamming attack but has no false negative to miss the detection of any signal on the spectrum. Fine sensing may consume a whole CDT slot i.e. 160 msec whereas fast sensing lasts only for 9 to 20 micro seconds depending on the technique used [7, 8]. Since fine sensing employs sophisticated spectrum sensing techniques and in doing so takes much longer

time than fast sensing, it has no false negative i.e., it does not miss the detection of PU if it is present on the spectrum.

Experimental data recorded in the Chicago city area [22] shows that the TV spectrum is severely under-utilized and the long term average spectrum occupancy of the TV spectrum is 30% while the short term spectrum occupancy is close to 14%. Based on these figures, we can conclude the following:

- Because of low spectrum utilization, the PU can reasonably be assumed to remain idle for majority of the time, and
- Since the spectrum being used opportunistically by CRN belongs to PUs which are basically TV broadcast stations, it is reasonable to assume that whether in the OFF or the ON state, a PU is expected to remain in that state for a much longer time than 160 msec, i.e., one super frame time.

4.3.3 Attack Model

Malicious users in the CRN do not attack PU's communications and are interested in denying spectrum use only to the CRN. They do so by launching a smart jamming attack i.e., transmitting a short jamming signal during the fast sensing stage in order to force the CRN to conduct fine sensing which in turn means that the CRN cannot avail the spectrum opportunity that arises because of PU's absence. This is a smart jamming attack since it denies the use of spectrum to the CRN while consuming very little energy as compared with jamming the whole superframe.

In addition, the smart jamming attack allows the malicious nodes to utilize rest of the CDT slot for their own communications while the CRN is busy conducting fine sensing.

4.4 DS3: An Adaptive Spectrum Sensing Framework

In this section we first present the core idea behind our proposed DS3 framework in section 4.4.1 and the Markov ON/OFF model upon which DS3 is based in section 4.4.2. The details of DS3 framework are laid out in section 4.4.3 followed by a discussion on DS3's adaptive property and its handling of various network conditions in section 4.4.4.

4.4.1 The Core idea for Adaptive Spectrum Sensing

As explained in the assumptions, the duration of PU being in ON state or OFF state is much larger than one superframe duration. Therefore when PU becomes idle, the CRN BS can safely assume that it will remain idle for a few more CDT slots and has the option to dynamically decide whether or not the CRN needs to conduct fine sensing during subsequent superframes in which the fast sensing reports from SUs suggest presence of some signal on the spectrum. The original IEEE 802.22 CRN protocol mandates that fine sensing be carried out every time fast sensing report aggregation concludes presence of some signal on the spectrum including signals of the PU. Such a static method of conducting fine sensing which can consume one or more CDT slots would result in wastage of spectrum resources when it is very unlikely that the PU becomes active in the very next CDT slot right after becoming idle. Probability of PU becoming active at a given CDT slot is one of the components of DS3 framework and is derived in next subsection. Therefore the core idea of DS3 is to dynamically determine when to conduct fine sensing in

order to save spectrum resource for SUs' usage and at the same time not to delay detection of PU's presence on the spectrum for more than the time limit of MDT mandated by the IEEE 802.22 standard [1, 5, 9].

4.4.2 Markov ON/OFF Model for Prediction of PU Activity

PU's activity on its licensed spectrum bands has often been modeled as Markov ON/OFF process [23] and we have also assumed the same model for predicting PU's activity. We are only concerned with adaptive spectrum sensing during PU's idle/OFF period i.e., in state 0 since an attacker is not assumed to attack PU's communications and wants to deny the use of vacant spectrum to SUs in the CRN only. After transitioning to OFF state, let X denote the number of CDT slots the PU stays in that state until it jumps back to the ON state, where $X \in \{1,2,3, \dots\}$. This r.v. X follows a geometric distribution with parameter α which is the probability of PU to transition from OFF to ON state. Let P_k denote our prediction of PU's activity which is the probability that given the PU is in the OFF state at time 0, the PU transitions to ON state by time interval k , i.e., $P_k \equiv P(X \leq k)$. Thus P_k is given by the cumulative distribution function of the geometric distribution represented as:

$$P_k \equiv P(X \leq k) = 1 - (1 - \alpha)^k \quad (2)$$

Physically, it means that as time goes on, the PU initially in the OFF state at time $k = 0$ has more and more chance to become active again and transition to ON state. Thus equation 2 represents our prediction of PU's activity in the future and is incorporated in our dynamic fine sensing framework's cost minimization function.

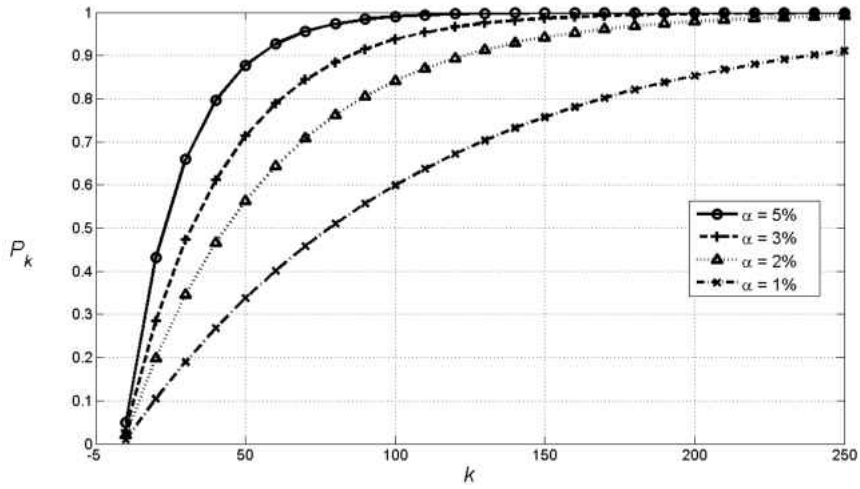


Figure 4.2: Effect of state transition probability α on P_k .

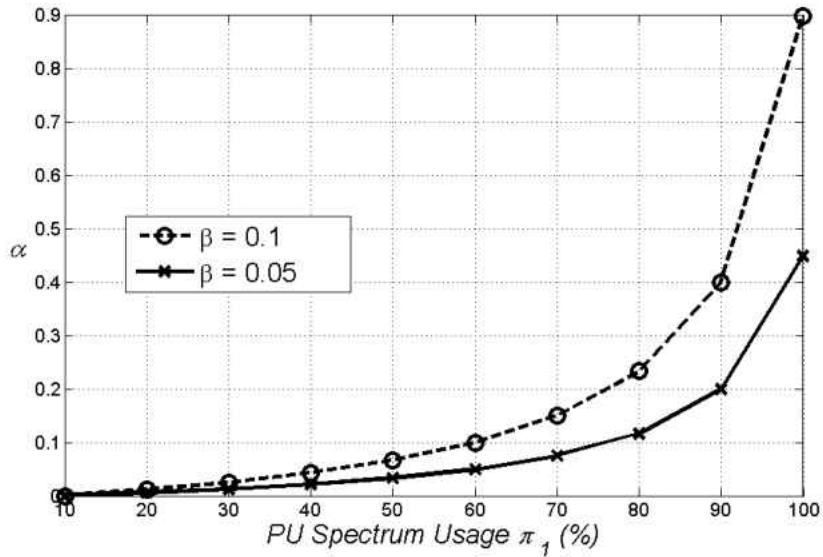


Figure 4.3: Relationship between α and β and the amount of PU's spectrum usage π_1 .

In the Markov ON/OFF model, the staying time at each state before transitioning to the other state has the memory less characteristic. That is to say, given that at the discrete CDT slot s we

know that the PU is in OFF state, the probability that the PU will transition back to ON state at interval $s + k$ will still be equal to P_k . Based on our assumption a fine sensing carried out at a time slot s will tell us whether or not the PU is in OFF state at that time slot. Thus the variable k in the notation P_k represents how many discrete time units have passed since the last fine sensing which concluded that the PU is OFF. On the other hand, if the last fine sensing concluded that the PU is ON, then DS3 will carry out fine sensing statically and continuously for subsequent CDT slots according to the original IEEE 802.22 standard.

From the Markov ON/OFF model, the probability of PU being in state 0 or 1 is represented as the steady state probability π_0 and π_1 respectively, where $\pi_0 + \pi_1 = 1$. It is clear that if we define PU spectrum usage as the fraction of time PU utilizes the spectrum under consideration, then PU spectrum usage is equal to π_1 . Figure 4.2 shows the impact of α on P_k . Based on past observation data of PU spectrum usage, we can calculate the average amount of time PU stays in OFF state, i.e., we know the value of $E[X]$. Since the geometrically distributed r.v. X is given by $E[X] = 1/\alpha$, therefore we can calculate the value of α from observed data as:

$$\alpha = 1/E[X] \quad (3)$$

Figure 4.3 shows the relationship between the state transition probabilities α and β and the amount of PU's spectrum usage π_1 .

4.4.3 DS3 Framework

DS3 is based on a cost minimization function that includes cost of interfering with PU's communications when PU is active and cost of wasting spectrum opportunities when the PU is

idle. However, before discussing details of the cost minimization function we first present how the CRN BS estimates attack severity at any given time. We also discuss a parameter called sensitivity which represents the BS's aversion towards delaying PU detection. By selecting appropriate values for sensitivity, the DS3 framework can be made to behave as the original IEEE 802.22 standard.

4.4.3.1 Estimation of Attack Severity

Estimation of attack severity at CDT slot t is based on a sliding window that contains a record of past N CDT slots' fast sensing reports. The sliding window is meant to ensure that the information contained in it represents the recent past only. For every CDT slot, attack severity v_t is calculated as:

$$v_t = \frac{\sum_{i=1}^N n_i}{N}, \forall n_i \in \{0, 1\}, \forall i \in N \text{ and } N \neq 0 \quad (4)$$

where n_i represents the history window entries, $n_i = 0$ represents the spectrum was reported to be vacant and $n_i = 1$ represents the spectrum was reported to be occupied during fast sensing report aggregation at CDT slot i . A fast sensing alert recorded as $n_i = 1$ in the history window could mean the presence of a PU on the spectrum, a jamming attack or noise on the spectrum. Whenever fine sensing is carried out after MDT and the PU is not detected as active, then all $n_i = 1$ entries in the hind sight are considered as smart jamming attacks and utilized in subsequent CDT slots as estimate of current attack severity v_t .

4.4.3.2 Cost Minimization Function

DS3 algorithm is based on a cost minimization function with the goal of minimizing the overall “costs” associated with dynamic spectrum sensing. There are two possible costs that we consider related to our fine sensing decision:

- The cost of delaying PU’s detection when the PU is actually using the spectrum while we choose to skip fine sensing i.e., causing interference to the PU's communications.
- The cost of wasting spectrum opportunity when PU is in the idle state but DS3 chooses to carry out fine sensing in response to a fast sensing alert.

Both of the above scenarios along with smart jamming attack are depicted in figure 5. In the first scenario as depicted in figure – 5(b), the cost represents interference caused to the PU when the CRN misses detecting PU's activity in the current CDT time slot. In the current IEEE 802.22 CRN standard, short-term interference is acceptable as long as it is less than the Maximum Detection Time (MDT), which is 2 seconds [5, 9]. Meanwhile, the second scenario shown in figure – 5(a) and (c), happens when the CRN wastes the CDT slot by conducting fine sensing as the fast sensing produces alert, i.e., it encounters either a smart jamming attack or noise on the spectrum band, both treated as the same in this chapter.

Intuitively, an increase in the number of fast sensing alerts due to noise or smart jamming attack will result in a corresponding increase in attack severity estimation. This in turn means that in response to fast sensing alerts, it is more likely that the CRN will resort to fine sensing and spectrum opportunities will be wasted. Therefore, we need a relative increase in the cost of spectrum opportunity wastage and to achieve that we incorporate attack severity estimate v_t in

the cost (scenario 2 above). Let the probability of the BS choosing to carry out fine sensing at the CDT slot t be represented as p_t . Equation 5 represents the two costs discussed above respectively where $P_k(1 - p_t)$ is the probability of causing interference to the PU and $p_t(1 - P_k)$ is the probability of wasting spectrum opportunity. Both of the cost factors include DS3's prediction PU's activity which is estimated in equation 2 as well as the current estimate of jamming attack severity v_t given by equation 4. The total cost J_t associated with dynamically deciding whether or not to conduct fine sensing after receiving an alert from fast sensing at time t is weighted sum of the two costs given by:

$$J_t = \gamma_{kt}P_k(1 - p_t) + v_t\varphi_t p_t(1 - P_k) \quad (5)$$

The derivative of equation 5 will represent how the total cost of adaptive spectrum sensing changes with the BS's decisions for conducting or skipping fine sensing after receiving fast sensing alerts from SUs. It is given as follows:

$$\frac{dJ_t}{dp_t} = v_t\varphi_t(1 - P_k) - \gamma_{kt}P_k \quad (6)$$

where γ_{kt} represents the cost factor for missing the detection and causing interference to the PU, φ_t represents the cost for carrying out fine sensing under smart jamming attack and thereby wasting the current CDT slot, k is the number of CDT slots passed since the last fine sensing which concluded that PU is in OFF state and v_t is the current attack severity estimate.

The cost of wasting spectrum resource for the CRN should increase linearly with time therefore the second cost factor φ_t of equation 5 can be treated as a constant value. However this

is not true for the first cost factor γ_{kt} . It is because potential interference caused to PU's spectrum usage should increase significantly when the PU detection delay becomes larger. In addition, we should never allow a PU detection time to be longer than the maximum detection time (MDT) specified in the standard. For this reason, the cost factor γ_{kt} cannot be a constant value. In our proposed DS3 framework we use the following relationship to determine current cost factor which forms part of the dynamic fine sensing threshold:

$$\gamma_{kt} = \begin{cases} c/\tau - k & \text{when } k < \tau \\ \infty & \text{when } k \geq \tau \end{cases} \quad (7)$$

where c is a parameter representing the ‘‘sensitivity’’ of the BS towards PU detection. The larger the value of c , the more sensitive (or aggressive) the BS will be towards fast sensing stage's alert reports. Sensitivity is further discussed in next subsection.

Based on Equations 6 and 7 the optimum value for probability of the BS choosing to carry out fine sensing as a result of fast sensing alert from SUs at the CDT slot t is represented as p_t^* and is given by:

$$p_t^* = \begin{cases} 0 & \text{if } dJ_t/dp_t > 0 \\ 1/2 & \text{if } dJ_t/dp_t = 0 \\ 1 & \text{if } dJ_t/dp_t < 0 \end{cases} \quad (8)$$

4.4.3.3 Dynamic Fine Sensing Threshold

The first term on the right hand side of equation 6 i.e., $v_t \varphi_t (1 - P_k)$ represents DS3's dynamic fine sensing threshold. It is dynamic because it contains estimates of both the current attack severity as well as PU's activity on the spectrum. If the current estimate of attack severity v_t is high then the dynamic fine sensing threshold will have a higher value. This means that under higher jamming attacks, DS3 will be biased towards ignoring the fast sensing alerts. On the other hand, if the probability of PU being active on the spectrum P_k is higher then the dynamic fine sensing threshold will have a smaller value. This means that DS3 will be more likely to carry out fine sensing as a result of fast sensing alert. The cost factor $\gamma_{kt} P_k$ is shown in figure 5 as the red solid curve while the dynamic fine sensing threshold is shown as the blue dotted line. The interaction between DS3 and various channel conditions are shown in figure 4.5.

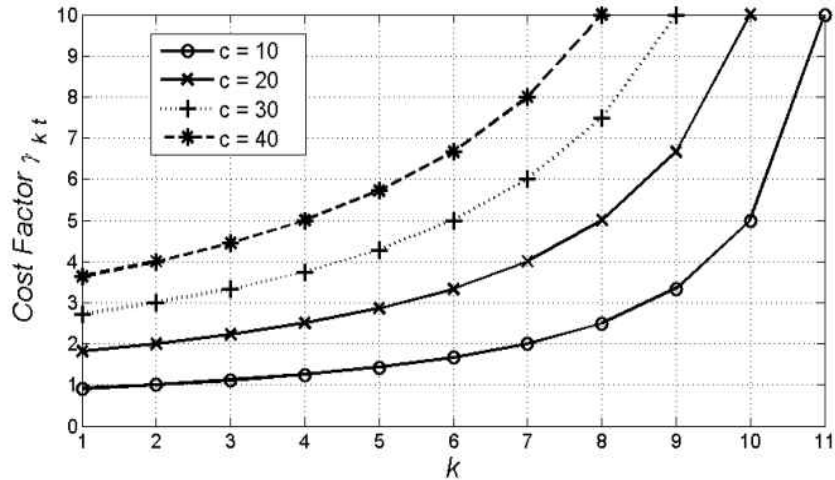


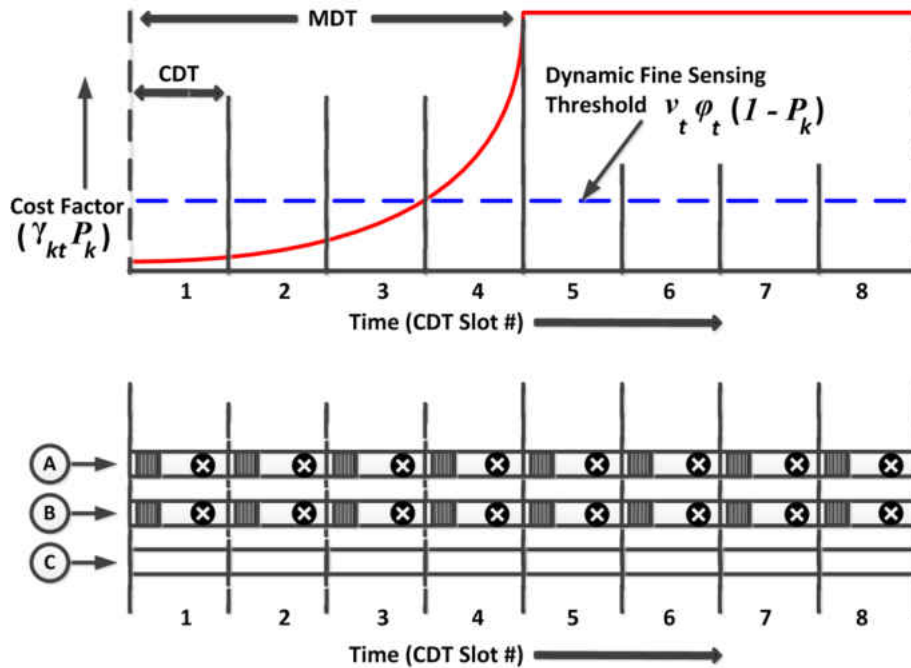
Figure 4.4: Effect of Sensitivity c on the cost γ_{kt} of interfering

4.4.3.4 Sensitivity towards PU Detection Delay

Figure 4.4 shows how the sensitivity c from equation 7 affects the cost factor $\gamma_{kt}P_k$. As the sensitivity increases, the cost for not carrying out fine sensing after k consecutive CDT slots reaches infinity much faster. In figure 4.4 with $c = 10$ the cost factor reaches infinity for not carrying out fine sensing at CDT slot 11 while for $c = 40$ it reaches infinity for not carrying out fine sensing at CDT slot 8. Therefore, by increasing the value of sensitivity to a sufficiently large value we can make DS3 to function as the original static fine sensing decision algorithm of IEEE 802.22 standard. Algorithm 1 lists the pseudo-code of the proposed DS3 framework.

4.4.4 Discussion on DS3's handling of various network conditions

Our proposed adaptive spectrum sensing framework DS3 has the dual advantage of providing security against smart jamming attacks and at the same time making the spectrum utilization more efficient than the static algorithm employed by the IEEE 802.22 standard under noisy channel conditions. A strong feature of DS3 framework is its adaptability for varying network conditions due to its intrinsic optimization approach. By incorporating an estimate of current attack severity as well as noise in its objective function, the DS3 framework becomes more aware of the spectrum environment. As will be shown in the next section, attack severity estimation enables the DS3 framework to significantly reduce the latency in PU detection and improved spectrum opportunity utilization. Various network conditions are depicted in figure 4.5, 4.6 and 4.7 however due to space considerations, MDT is set at 4 CDT slots instead of the standard specified 12 CDT slots.



Legend

- (A) DS3's Spectrum Sensing Actions
- (B) IEEE 802.22 standard's Spectrum Sensing Actions
- (C) Channel State

Spectrum Sensing Actions

- Mandatory Fast Sensing
- ⊗ Fine Sensing NOT carried out
- ☑ Fine Sensing carried out

Channel States

- PU Inactive (spectrum vacant)
- ▨ PU Active (spectrum occupied)
- Smart Jamming Attack when PU is inactive

Figure 4.5: DS3's handling of Low PU activity on the channel as compared with IEEE 802.22's spectrum sensing actions.

4.4.4.1 Low PU Activity

Figure 4.5 depicts the scenario when the PU is inactive on the spectrum. The upper half of the figure shows how the cost factor $\gamma_{kt} P_k$ grows relative to the amount of time since last fine

sensing was carried out. As the time limit of MDT approaches without carrying out fine sensing, cost factor $\gamma_{kt}P_k$ will approach infinity and will remain at that value. In this case whenever fast sensing stage's spectrum report aggregation alerts for the presence of some signal on the spectrum, fine sensing will be carried out just like the IEEE 802.22 standard. The details of DS3's approach towards dynamic spectrum sensing under low PU activity are explained as follows:

In the optimization objective function of equation 5, the cost factor γ_{kt} is a parameter that changes based on the value of k as calculated in Equation 7. k represents the number of discrete CDT slots that have passed since the last fine sensing concluded that the PU is OFF. Therefore, if the network is not under smart jamming attack as shown in figure 5a, then fast sensing in each CDT time slot will rarely raise an alert when PU is in OFF state. Under such network conditions if fast sensing raises an alert, it is very likely that $k > \tau$ since it is the number of time slots from the current time slot to the previous CDT time slot when fine sensing was conducted. Equation 7 shows that in this case $\gamma_{kt} = \infty$ and therefore the cost factor $\gamma_{kt}P_k$ will also become infinity which will force DS3's cost minimization function to take the optimal fine sensing decision $p_t^* = 1$ according to Equation 8. This means that on average under normal network conditions fine sensing will immediately be carried out as soon as the fast sensing report aggregation at the BS suggests presence of some signal on the spectrum. Therefore DS3 framework will not introduce extra delay in the detection of PU under normal network conditions and will behave just as the IEEE 802.22 standard.

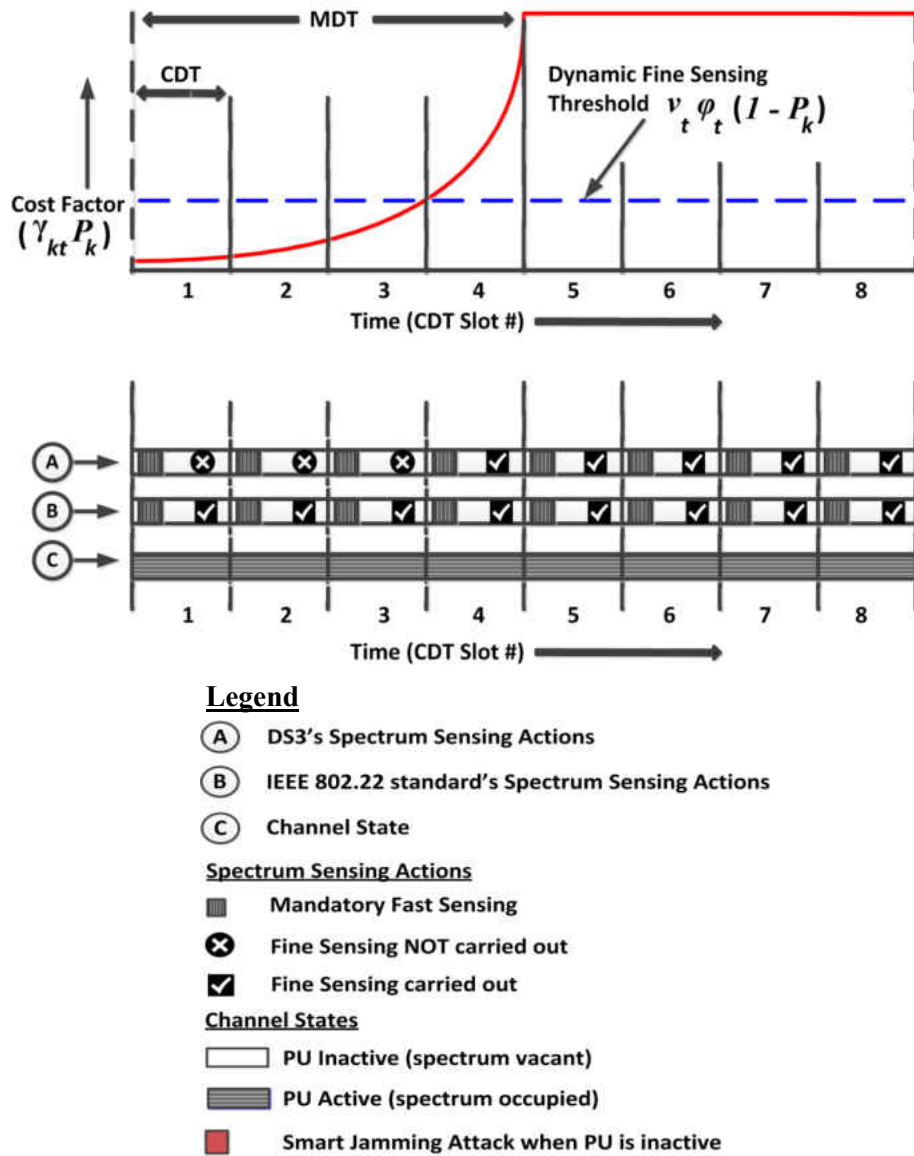


Figure 4.6: DS3's handling of High PU activity on the channel as compared with IEEE 802.22's spectrum sensing actions.

4.4.4.2 High PU Activity

The scenario when there is high PU activity on the spectrum is shown in figure 4.6. The figure shows that although the PU is active and the fast sensing stage gives an alert for presence of some signal on the spectrum, DS3 does not carry out fine sensing because the cost factor

$\gamma_{kt}P_k$ is below the fine sensing threshold during the first 3 time slots. Notice that the IEEE 802.22 standard carries out fine sensing during every time slot that the fast sensing stage raises an alert.

This scenario represents the interference caused by DS3 to PU's communications but that interference lies within the constraints of MDT set by FCC and DS3 is able to detect PU's presence on the spectrum within that time limit. DS3 delays the detection of PU until the cost for delaying becomes greater than the fine sensing threshold at which point fine sensing is carried out. The cost for delaying PU's detection remains above threshold for PU's communications during subsequent time slots which causes the CRN to continue performing fine sensing as a result of fast sensing alerts until the PU becomes idle again. The total interference caused to PU's communication due to delaying fine sensing can be controlled by selecting appropriate value for sensitivity in equation 7.

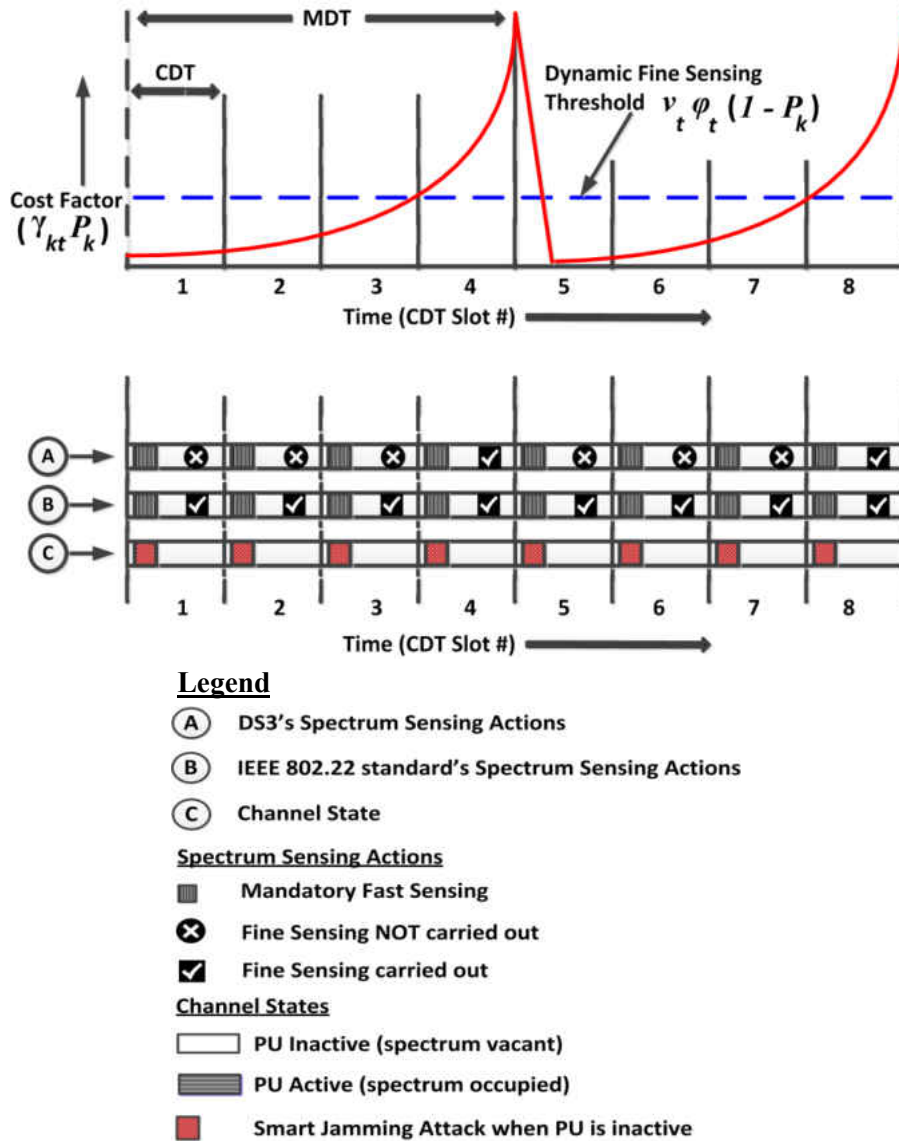


Figure 4.7: DS3's handling of smart jamming attack on the channel as compared with IEEE 802.22's spectrum sensing actions.

4.4.4.3 Smart Jamming attack and/or Noisy channel

The scenario when malicious nodes in the CRN launch smart jamming attacks due to inactivity from the PU is shown in figure 4.7. Fast sensing stage in every time slot reports presence of some signal on the spectrum and IEEE 802.22 standard's response under such

conditions would be to carry out fine sensing in every CDT slot. On the other hand, DS3 framework will make the CRN to conduct fine sensing only when the cost factor $\gamma_{kt}P_k$ for ignoring fast sensing reports rises above the dynamic fine sensing threshold while adhering to the MDT constraint. This will happen once after observing a number of fast sensing alerts.

In figure 4.7, fast sensing alerts during every time slot cause the IEEE 802.22 standard to carry out fine sensing and results in wastage of all spectrum opportunities due to static fine sensing decisions. On the other hand, DS3 ignores alerts from fast sensing during time slots 1 through 3 because the cost factor $\gamma_{kt}P_k$ is below the dynamic fine sensing threshold. At time slot 4, the cost function becomes greater than the threshold and DS3 carries out fine sensing only to detect that the alert was not due to PU's signals. This makes DS3's cost function to decrease back to its minimum value for subsequent time slots. Although the malicious nodes have launched smart jamming attack during every spectrum opportunity, DS3 is able to utilize 75% of them whereas the IEEE 802.22 wasted all of them. Simulation results with actual parameters of MDT and CDT of section 4.5 show even higher values of spectrum opportunity utilization. Dynamic spectrum sensing ensures that the CRN utilizes spectrum opportunities as much as possible and will not be frequently interrupted because of noise or smart jamming attacks. Algorithm for DS3 framework is listed in table 4.2.

Table 4.2: Algorithm for DS3 Framework

Initialization: $c, \tau \leftarrow \lfloor MDT / CDT \rfloor, k \leftarrow 0, v_t, t \leftarrow$ running time
Result: Dynamic spectrum sensing decision

begin

1. $s \leftarrow$ time when PU became idle
2. **for** every CDT slot t
3. **if** PU state was *idle* at time $t - 1$
4. **if** fast sensing result is positive **then**
5. $k \leftarrow t - s$
6. $P_k \equiv P(X \leq k) \leftarrow 1 - (1 - \alpha)^k$
7. **if** $k < \tau$ **then**
8. $\gamma_{kt} \leftarrow c / \tau - k$
9. **else**
10. $\gamma_{kt} \leftarrow \infty$
11. **end if**
12. $J_t \leftarrow \gamma_{kt} P_k (1 - p_t) + (v_t \varphi_t p_t (1 - P_k))$
13. $dJ_t / dp_t \leftarrow v_t \varphi_t (1 - P_k) - \gamma_{kt} (P_k)$
14. **if** $dJ_t / dp_t < 0$ **then**
15. $p_t^* \leftarrow 1, k \leftarrow 0$
16. **else if** $dJ_t / dp_t = 0$ **then**
17. $p_t^* \leftarrow 1/2$
18. **else**
19. $p_t^* \leftarrow 0$
20. **end if**
21. **end if**
22. **else**
23. Do not perform fine sensing
24. **end**
25. **else**
26. perform fine sensing statically as per IEEE 802.22 standard
27. $s \leftarrow t$
28. **end if**
29. **end for**
30. **end**

4.5 Performance Evaluation

4.5.1 Simulation Setup

One time slot in simulations which is the same as the protocol's superframe equals 160 milliseconds and the maximum time available to the CRN for detection of a PU's signal is 2 seconds or 12 time slots, [1] also called the *Maximum Detection Time* or MDT, therefore based on the current cost function of DS3, the BS may defer fine sensing even when fast sensing reports presence of some signal on the spectrum. However with the 802.22 standard, the CRN always conducts fine sensing whenever fast sensing gives an alert, and fine sensing always consumes the whole CDT slot. The overall fraction of time that the PU is active on the spectrum is called PU's Spectrum Usage (%). The absence of PU on the spectrum is called Spectrum Opportunity for CRN. A malicious user in the CRN launches a smart DoS attack in spectrum opportunity by transmitting a jamming signal during the fast sensing stage of the CDT slot with some probability. Every data point shown in figures of this section corresponds to the average of 100 simulation runs.

4.5.2 Simulation Results

Figure 4.8(a) shows a comparison of spectrum opportunity utilization by the IEEE 802.22 standard and the DS3 framework. Without the adaptive sensing framework DS3, spectrum opportunity utilization decreases proportional to the increase in jamming attacks whereas with the DS3 framework, the decrease is at a much slower rate and remains close to 90% even when the malicious users jam every possible spectrum opportunity. By keeping the delay in PU

detection within the limits set by the FCC as well as the 802.22 standard, DS3 enables the CRN to achieve one of the fundamental requirements for its operation i.e. non-interference with the licensed PU. The results shown in figure 6 were recorded while keeping the sensitivity to its minimum value of 10 and PU Spectrum Usage at 30%. Subsequent simulations show how varying these parameter affects DS3's performance.

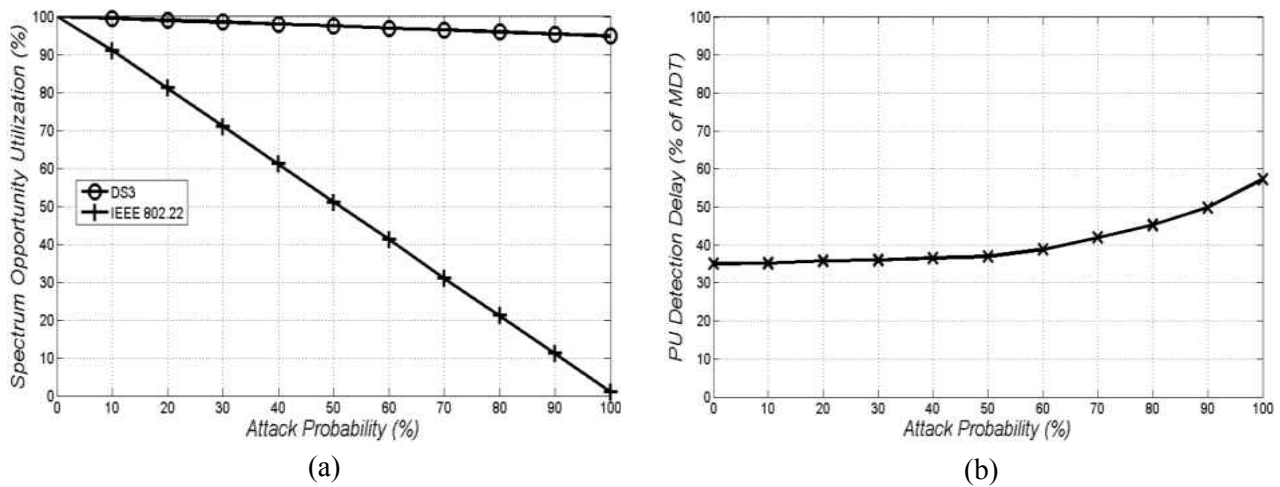


Figure 4.8: DS3's performance with various parameters (a) Spectrum opportunity utilization (b) PU detection delay at varying degrees of jamming attack severity.

Figure 4.8(b) shows how the delay in detection of PU on the spectrum is affected with increasing jamming attacks. The delay remains constant at 35% up to a jamming attack severity of 50% and increases to approximately 57% which is still within the MDT constraint even when every possible spectrum opportunity is jammed. Notice that spectrum opportunity utilization by DS3 is more than 90% compared to a total shutdown of IEEE 802.22 at 100% jamming attack rate.

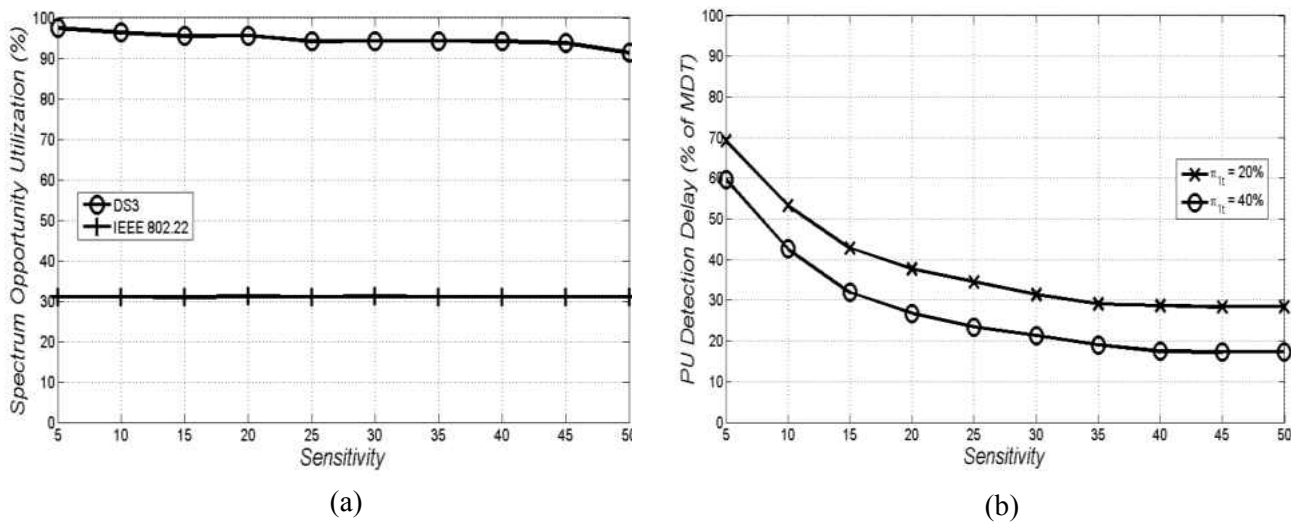


Figure 4.9: DS3's performance with various parameters (a) Spectrum opportunity utilization (b) PU detection delay with varying sensitivity towards PU detection delay.

Figures 4.9(a) and 4.9(b) show the spectrum opportunity utilization and PU detection delay of DS3 framework as compared with the IEEE 802.22 standard by varying the sensitivity at a fixed jamming attack rate of 70%. Without the benefit of adaptive spectrum sensing, the IEEE 802.22 standard achieves spectrum opportunity utilization close to 30% whereas it ranges between 97% and 91% with the DS3 framework. A lower sensitivity to detect PU's signal means that the cost factor has a lower value and the BS is inclined more towards deferring fine sensing to a later CDT slot. It is worth mentioning here that by increasing the CRN's sensitivity towards the detection of PU's signal, we can achieve comparable PU detection performance with the IEEE 802.22 standard as evident from 4.9(b) while at the same time achieving far greater spectrum opportunity utilization under smart jamming attacks.

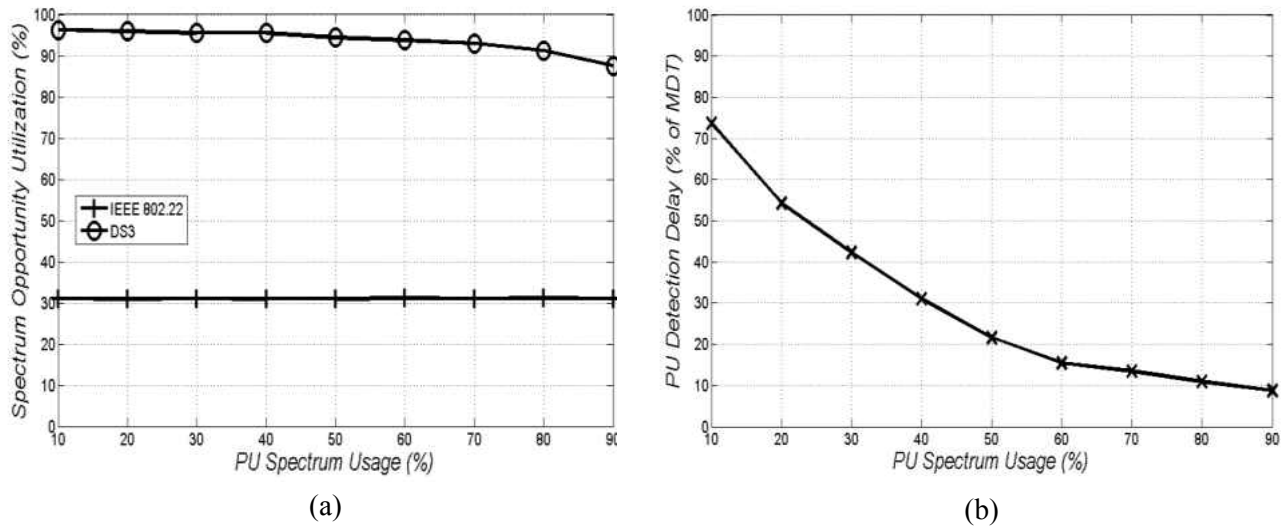


Figure 4.10: DS3's performance with various parameters (a) Spectrum opportunity utilization (b) PU detection delay with varying degree of PU's spectrum usage (%).

A comparison of spectrum opportunity utilization is shown between the IEEE 802.22 standard and DS3 in figure 4.10(a) with respect to varying PU spectrum usage. It shows that PU's spectrum usage has very little impact on spectrum opportunity utilization of the adaptive sensing framework. On the other hand the IEEE 802.22 standard is able to utilize only 30% of the spectrum opportunities when the attacker jams 70% of the spectrum opportunities. It is emphasized here that spectrum opportunity as well as a smart jamming attack is relevant only when the PU is idle i.e., during the time slots left over from PU's spectrum usage. Figure 4.10(b) demonstrates the effects of PU's spectrum usage on the delay in DS3's detection of its signals. As the PU becomes more active on the spectrum, the relative attack severity v_t on the spectrum decreases which in turn makes DS3 to increase the cost of missing PU's detection. Therefore PU's signals are detected much faster when it is more active on the spectrum.

4.6 Conclusion

In this chapter we presented a novel adaptive spectrum sensing framework called DS3 which minimizes the effects of smart jamming as well as noise on the fast sensing phase of DSA and improves spectrum utilization through dynamic fine sensing decision. DS3 utilizes the constraint of maximum delay in detection of incumbent signal imposed by FCC in its dynamic fine sensing decision algorithm and achieves up to 90% improvement in spectrum utilization under smart jamming attack while keeping the PU detection delay to within the maximum allowed delay for detecting the PU.

4.7 References

- [1] IEEE 802.22-2011 - IEEE Standard for Local and metropolitan area networks - Specific requirements - Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Policies and procedures for operation in the TV Bands.
- [2] C. Cordeiro, K. Challapali, D. Birru, S. Shankar, "*IEEE 802.22: the first worldwide wireless standard based on cognitive radios*," New Frontiers in Dynamic Spectrum Access Networks, (DySPAN) 2005.
- [3] J. Mitola, G.Q Jr. Maguire, "*Cognitive radio: making software radios more personal*," IEEE Personal Communications, vol.6, no.4, pp.13-18, Aug 1999.
- [4] U S. FCC, ET Docket 04-186, "*Notice of Proposed Rule Making, in the matter of Unlicensed Operation in the TV Broadcast Bands*," May 25, 2004.
- [5] C. Stevenson, G. Chouinard, Z. Lei, W. Hu, S. Shellhammer, W. Caldwell, "*IEEE 802.22: The first cognitive radio wireless regional area network standard*," IEEE Communications Magazine, vol.47, pp.130-138, 2009.
- [6] I. F. Akyildiz, W. Lee, K. Chowdhury, "*CRAHNs: Cognitive radio ad hoc networks*". Ad Hoc Networks, 2009.

- [7] T. Yucek, H. Arslan, "A *survey of spectrum sensing algorithms for cognitive radio applications*," IEEE Communications Surveys & Tutorials, vol.11, pp.116-130, 2009.
- [8] K. Kim, I. A. Akbar, K. K. Bae, U. Jung-Sun, C. M. Spooner, J. H. Reed, "Cyclostationary Approaches to Signal Detection and Classification in Cognitive Radio," IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN) 2007.
- [9] S. Shellhammer, "Spectrum Sensing in IEEE 802.22," IAPR Workshop on Cognitive Information Processing (CIP), 2008.
- [10] R. Chen, J. Park, K. Bian, "Robustness against Byzantine Failures in Distributed Spectrum Sensing," Elsevier Computer Communications 2012.
- [11] S. Liu, L. Lazos, M. Krunz, "Thwarting Control-Channel Jamming Attacks from Inside Jammers," IEEE Transactions on Mobile Computing, vol.11, no.9, pp.1545,1558, Sept. 2012.
- [12] S. Jana, et al., "Trusted collaborative spectrum sensing for mobile cognitive radio networks," 32nd IEEE International Conference on Computer Communications, INFOCOM 2012.
- [13] Q. Wang, K. Ren, P. Ning, "Anti-jamming communication in cognitive radio networks with unknown channel statistics," 19th IEEE International Conference on Network Protocols (ICNP) 2011.
- [14] B. Wang, Y. Wu, K. J. R. Liu, T. C. Clancy, "An anti-jamming stochastic game for cognitive radio networks," IEEE Journal on Selected Areas in Communications (JSAC), vol.29, no.4, pp.877,889, April 2011.
- [15] H. Li, Z. Han, "Dogfight in Spectrum: Jamming and Anti-Jamming in Multichannel Cognitive Radio Systems," IEEE Global Telecommunications Conference (GLOBECOM) 2009.
- [16] S. Sodagari, T. C. Clancy, "An anti-jamming strategy for channel access in cognitive radio networks," 2nd international conference on Decision and Game Theory for Security (GameSec), 2011.
- [17] C. Chen, M. Song, C. Xin, J. Backens, "A game-theoretical anti-jamming scheme for cognitive radio networks," IEEE Network, vol.27, June 2013.

- [18] W. Wenjing, M. Chatterjee, K. Kwiat, “*Collaborative jamming and collaborative defense in Cognitive Radio Networks*,” IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011.
- [19] Y. Wu, B. Wang, K. Liu, “*Optimal Defense against Jamming Attacks in Cognitive Radio Networks Using the Markov Decision Process Approach*,” IEEE Global Telecommunications Conference (GLOBECOM) 2010.
- [20] X. Zhang, Q. Wu, J. Wang, “*Optimization of sensing time in multichannel sequential sensing for cognitive radio*,” International Journal of Comm. Systems 2013. doi: 10.1002/dac.1341.
- [21] C. Ghosh, C. Cordeiro, D. Agrawal, M. Rao, “*Markov chain existence and Hidden Markov models in spectrum sensing*,” IEEE International Conference on Pervasive Computing and Communications, (PerCom) 2009.
- [22] T. Taher et al., “*Long-term spectral occupancy findings in Chicago*”, New Frontiers in Dynamic Spectrum Access Networks (IEEE DySPAN) 2011.
- [23] L. Xiaoyuan, W. Dexiang, M. Xiang, J. McNair, “*On the Accuracy of Maximum Likelihood Estimation for Primary User Behavior in Cognitive Radio Networks*,” IEEE Communications Letters, vol.17, no.5, pp.888,891, May 2013.

CHAPTER 5: AN EVOLUTIONARY GAME THEORETIC APPROACH TOWARDS LONG-TERM SELF COEXISTENCE

The Federal Communications Commission (FCC) made TV white space (TVWS) channels in the 54-698 MHz frequency range available [1] for secondary unlicensed access after the TV broadcast was switched from analog to digital signal in 2009. Opening up of the TVWS for unlicensed use was the result of a realization that the gap between the demand and supply of wireless spectrum resource is ever increasing and fixed spectrum allocation is causing its severe under-utilization [2]. Strict requirements are however placed on the Secondary Users (SU) of the spectrum which is otherwise allocated to licensees called primary users (PU), to continuously sense the spectrum and vacate it when the presence of the PU is detected and not to cause them any interference. This type of spectrum access is intuitively called Dynamic Spectrum Access (DSA). Cognitive Radio Network (CRN) is a paradigm that meets precisely these communication requirements and utilizes DSA to enable secondary, unlicensed access to TVWS spectrum bands in an opportunistic and non-interfering basis [1].

DSA allows CRNs to ensure that their use of spectrum does not cause interference to PUs while at the same time all spectrum opportunities are utilized to the maximum. Within a CRN, the decision to select a specific channel for DSA is usually made by a central entity such as its base station or in case of an ad hoc CRN, an algorithm that enables all SUs to reach a consensus for choosing specific channel in a distributed manner. IEEE 802.22 wireless regional area network (WRAN) [3] is an example of CRNs in which the base station controls all the operation of the CRN including the choice of spectrum bands for communication. Regardless of how a decision to select a specific channel is made, every entity within the CRN is bound to abide by

that decision. On the other hand, there may be multiple collocated CRNs within a geographical region all of which compete for access to the same set of available channels. Sharing of spectrum by collocated CRNs is called self coexistence in the context of CRNs which employ coexistence protocols such as the IEEE 802.22 standard's Coexistence Beacon Protocol (CBP). However without any controlling entity, fair distribution of *heterogeneous* spectrum resources is non-trivial in the case of multiple collocated CRNs as they may be independently owned and operated by different service providers. This brings us to the definition of the problem statement for long term coexistence with heterogeneous spectrum, in the following subsection.

5.1 **Motivation and Contribution**

Coexistence protocols employed by collocated CRNs work under the assumption that all spectrum bands afford the same level of QoS and do not take into consideration the fact that these channels can be heterogeneous. The heterogeneity of channels can be in the sense that they may vary in their characteristics such as SNR or bandwidth. Similarly, a channel whose PU remains idle for most of the time may be more attractive for a CRN as compared with a channel whose PU remains mostly active. This would entail that some channels can be considered better than others and therefore can have an associated *quality* parameter. As a result, CRNs are expected to have a preference over the set of available channels for secondary access. Without any incentive for altruism, all CRNs would want to gain access to the highest quality channels resulting in a conflict among rational entities. Therefore, in the absence of any centralized enforcement mechanism, *evolution of a strategy that would ensure long term coexistence with*

fair distribution of heterogeneous spectrum resources among collocated CRNs is a challenge and is the focus of this chapter.

Game theory provides an elegant means to model strategic interaction between agents which may or may not be cooperative in nature. It has been applied to numerous areas of research involving conflict, competition and cooperation in multi-agent systems which also encompass wireless communications. Therefore, by leveraging the mechanisms of game theory, we model the long term sharing of heterogeneous spectrum by CRNs as an evolutionary anti-coordination spectrum sharing game in which collocated CRNs in a given region are its players. The payoff for every player in the game is determined by the quality of the spectrum band to which it is able to gain access. We present a detailed analysis on the evolutionary stability as well as fairness of the solution. For any system with non-cooperative entities, it is likely that there will be some associated inefficiency. However, it is worth pointing out that *fairness* is the primary objective of our proposed evolutionary heterogeneous spectrum sharing game. We also confirm our findings through detailed simulations.

We formulate an evolutionary spectrum sharing anti-coordination game and propose its solution that is stable even with the presence of greedy strategy, robust under changing network conditions and at the same time results in fair distribution of the spectrum resources. Specifically, we have made the following contributions:

- As potential solutions for the heterogeneous spectrum sharing game, we have derived the game's pure and mixed strategy Nash Equilibria (PSNE and MSNE respectively).

- To show that the game's strategy in MSNE is evolutionarily stable strategy (ESS), we prove that it cannot be invaded by a greedy strategy and is robust under changing network conditions.
- We have derived replicator dynamics of the proposed evolutionary game, a mechanism with which players can learn from their payoff outcomes of strategic interactions and modify their strategies at every stage of the game and subsequently converge to ESS.
- Finally, we have presented a fairness analysis of the proposed evolutionary game using Jain's fairness index.

5.2 Related Work

In this section we provide an overview of some of the works carried out in the domain of self coexistence in CRNs as well as application of some of the game theoretic solution concepts in the context of communication networks.

Authors of [5] have applied the evolutionary game theoretic concepts in order to make secondary users (SU) of a CRN to participate in collaborative spectrum sensing in a decentralized manner. SUs learn through strategic interactions at every stage of the game and the learning behavior is modeled with the help of replicator dynamics. A game theoretic approach based on correlated equilibrium has been proposed in [6] for multi-tier decentralized interference mitigation in two-tier cellular systems. Authors of [7] propose a multi-cell resource allocation game for efficient allocation of resources in orthogonal frequency division multiple access

(OFDMA) systems based on throughput, inter-cell interference and complexity. The subcarriers are considered as players of the game while the base station acts as the provider of external recommendation signal needed for achieving correlation of strategies of players.

Authors of [8] model the competition among multiple femtocell base stations for spectrum resource allocation in an OFDMA LTE downlink system as a static non-cooperative game. The correlated equilibrium of the game is derived through a distributed resource block access algorithm which is a variant of the No-Regret learning algorithm. CRNs with SUs having variable traffic characteristics are considered in [9] to tackle the problem of distributed spectrum sensing by modeling it as a cooperative spectrum sensing game for utility maximization. The authors have proposed another variant of the no-regret learning algorithm called neighborhood learning (NBL) which achieves correlated equilibrium for the spectrum sensing game. In contrast to the no-regret learning algorithm, NBL is not completely distributed and requires some coordination among players to achieve better performance.

Correlated equilibrium has been employed in [10] for a P2P file sharing non-cooperative game to jointly optimize players' expected delays in downloading files. Not uploading files for others causes an increase in file download time for all players which in turn, forces even the non-cooperative players to cooperate. The authors of [11] tackle the self-coexistence problem of finding a mechanism that achieves a minimum number of wasted time slots for every collocated CRN to find an empty spectrum band for communications. To do so, they employ a distributed modified minority game under incomplete information assumption.

Different punishment strategies have been employed in [12] that form part of a Gaussian interference game in a one-shot game as well as an infinite horizon repeated game to enforce cooperation. Spectrum sharing is however considered within the context of a single CRN. Evolutionary game theory is applied in [13] to solve the problem in a joint context of spectrum sensing and sharing within a single CRN. Multiple SUs are assumed to be competing for unlicensed access to a single channel. SUs are considered to have half-duplex devices so they cannot sense and access a channel simultaneously. Correlated equilibrium has been proposed in [14] as a solution for efficient coexistence by colocated CRNs with heterogeneous channels.

Utility graph coloring is used to address the problem of self-coexistence in CRNs in [15]. Allocation of spectrum for multiple overlapping CRNs is done using graph coloring in order to minimize interference and maximize spectrum utilization using a combination of aggregation, fragmentation of channel carriers, broadcast messages and contention resolution. The authors of [16] achieve correlated equilibrium with the help of No-regret learning algorithm to address the problem of network congestion when a number of SUs within a single CRN contend for access to channels using a CSMA type MAC protocol. They model interactions of SUs within the CRN as a prisoner's dilemma game in which payoffs for the players are based on aggressive or non-aggressive transmission strategies after gaining access to idle channels.

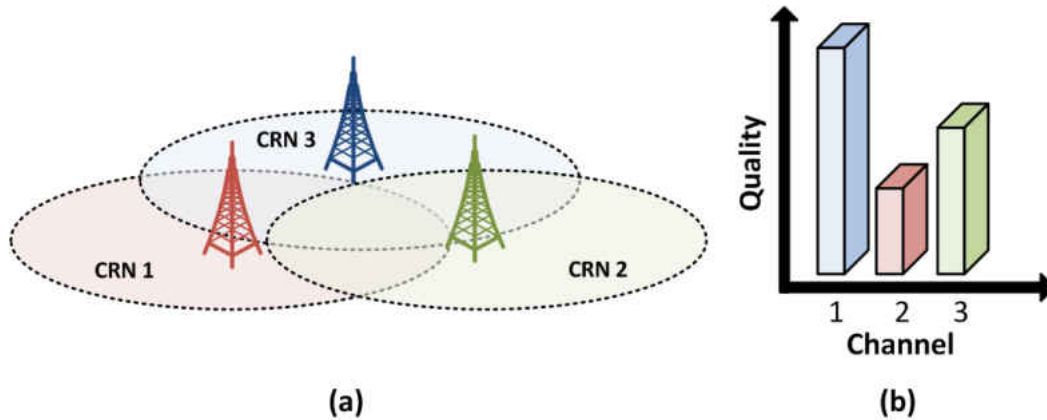


Figure 5.1: (a) Collocated CRNs competing for (b) Heterogeneous channels. The channels of the spectrum band may vary in quality with respect to availability, bandwidth or SNR, etc.

5.3 System Model and Assumptions

5.3.1 System Model

As shown in figure 5.1, we consider a region where overlapping CRNs co-exist and compete with each other for secondary access to the licensed spectrum bands. We model the entire TVWS spectrum band that is available for unlicensed use by CRNs as a set of $K = \{1, 2, \dots, k\}$ channels. The spectrum band is heterogeneous by virtue of the ‘quality’ of a channel which is determined by the probability P_k with which PUs access their licensed channels. Since knowledge of PU’s spectrum allocation/activity is mandated by the FCC for CRNs [1][3], is publically available through online databases [17][18] and also sensed by CRNs at regular intervals, players can calculate current values of P_k based on past observations. Higher P_k for a given channel k means it is of a lower quality and vice versa and CRNs compete to access the best quality channels.

Gaining access to higher quality channel results in higher payoff u_k while lower quality channel yields lower payoff for CRNs where payoff $u_k = 1 - P_k$ from gaining access to channel k .

CRNs need to gain access to a channel in every time slot also called a Channel Detection Time (CDT) slot [3]. Players are assumed to be rational and non-cooperative i.e., they do not share a common goal and therefore do not cooperate with each other. It is in every CRN's interest to gain access to the channels with minimum PU activity i.e., minimum value of P_k . When two or more CRNs select the same channel for access in a given time slot, a contention/collision situation arises and that particular time slot's spectrum opportunity is wasted. Having payoffs for selecting a specific channel derived from common knowledge such as P_k is an intuitive choice and makes distributed implementation of our proposed framework possible. It is worth mentioning that any positive value for payoff derived from any other parameter e.g., QoS or bandwidth can be used instead of P_k without affecting our analysis and the outcomes. As demonstrated subsequently, the number of collocated CRNs does not play any part in the game model because an evolutionary game is concerned with the *evolution of strategies*, associated payoffs and their stability.

5.3.2 Assumptions

Following are the underlying assumptions for the work presented in this chapter:

- **Time:** A single MAC superframe constitutes one time slot. Every CRN needs to gain access to a channel for which it contends with all other collocated CRNs in every time slot.

- ***Spectrum opportunity and wastage***: A given time slot's spectrum opportunity arises due to the absence of its PU may result in a collision and therefore be wasted if two or more CRNs select the same channel for access.
- ***Knowledge about PU activity***: In addition to the FCC mandated continuous spectrum sensing to detect PUs' activity, CRNs are also required to periodically access online databases such as [17][18] in order to gain up-to-date information about licensed PUs operating in a given region.
- ***Channel quality***: The amount of PU activity, bandwidth and SNR which collectively determine a channel's quality can be learnt from online databases and measured through spectrum sensing over a period of time. Due to the fact that all contending CRNs are collocated in a given region, it is reasonable to assume that a given channel's quality is common knowledge.
- ***Non-cooperative behavior***: All CRNs are independent as they do not share a common goal and therefore do not cooperate with each other. Being rational about their choices, every player has a clear preference of selecting the best available channel before the start of every time slot. Consequently, if every player tries to access the best channel, it will result in a collision and the spectrum opportunity being wasted.
- ***Payoffs***²: Players³ that eventually gain access to higher quality channels will gain higher payoffs as compared to the players that end up with lower quality channels. In subsequent section, we show that our proposed spectrum sharing game can be implemented solely on the basis of a CRN's common knowledge payoff observations.

² We use the terms utility and payoff interchangeably.

³ Similarly, we use the terms CRNs and players interchangeably.

Table 5.1: Notations and acronyms – Chapter 5

Notation	Definition
K	set of available channels
A	set of available actions (of selecting specific channels)
a_k	CRN's action of selecting channel k
U	set of channels' utilities
u_k	CRN's utility for gaining access to channel k
a_{-i}^*	best actions/strategies played by players other than player i
a_i^*	action/strategy of player i which is the best response (PSNE) to a_{-i}^*
\hat{p}	prob. distribution over set of channels in MSNE – The incumbent strategy
p'	prob. distribution greedier than MSNE – The mutant strategy
EU_k	Expected Utility from accessing channel k
u_0	Initial fitness of every CRN
\bar{u}	Total average payoff of the entire CRN population
p'_k	probability of selecting a channel for next time slot
ESS	Evolutionarily Stable Strategy
PU	Primary User
SU	Secondary User
NE	Nash Equilibrium
PSNE	Pure Strategy Nash Equilibrium
MSNE	Mixed Strategy Nash Equilibrium
CDT	Channel Detection Time (equal to one superframe)

5.4 Evolutionary Anti-Coordination Spectrum Sharing Game

In this section, we first present the basics of evolutionary game theory followed by formulation of our proposed evolutionary spectrum sharing game. Next, we derive solutions for the game for a 2-channel scenario and extend it for a K -channel scenario with replicator dynamics.

5.4.1 Evolutionary Game Theory: Basics

Evolutionary game theory formalizes the way in which various strategies of a population mix interact while competing against each other. As a result of such competitions, relative *fitness* of strategies can be determined based upon the payoffs that the strategies bring. An incumbent strategy of a population may be invaded by a mutant strategy if, on average, the mutant strategy can bring higher payoffs than the incumbent strategy. A strategy that cannot be invaded by a mutant strategy is said to be an evolutionarily stable strategy or ESS. We consider the action of selecting a specific channel as a CRN's strategy and need to determine which strategies are fair and stable for the long term. To that end, we derive the PSNE and MSNE as the game's solutions and prove that MSNE is ESS i.e., MSNE cannot be invaded by a mutant strategy that is greedier than MSNE. In addition to being evolutionarily stable, MSNE of the game is also fair because of its definition, which is presented subsequently.

5.4.2 Game Formulation

The heterogeneous spectrum sharing anti-coordination game presented here is a non-cooperative repeated game with perfect information because:

- Being rational players, CRNs compete for the best channels available in the spectrum band and are interested only in maximizing their own utility. Therefore, CRNs are not bound to cooperate with each other.
- Utilities are common knowledge since the quality of various network parameters can be measured by every CRN. Also, every CRN can tell which channels other CRNs were able to gain access to in the past hence they know other CRNs' payoffs.

The evolutionary heterogeneous spectrum sharing game is represented as $\mathcal{G} = \langle (K), (A), (U) \rangle$ where $K = \{1, 2, \dots, k\}$ denotes the set of available channels. Every player in the game has the same action space represented by $A = \{a_1, a_2, \dots, a_k\}$ and there is a bijection between the sets A and K . The set of utilities of the channels is represented as $U = \{u_1, u_2, \dots, u_k\}$. Strategy a_k means selecting channel k for communication and a player gets a payoff of u_k if it selected channel k and no other player selected the same channel for a given time slot. The payoff for players playing strategies a_k and a_j when competing against each other is denoted by the ordered pair $u(a_k, a_j) \in U$ and is a function of an individual channel's quality given by:

$$u(a_k, a_j) = \begin{cases} (u_k, u_j), & \text{when } k \neq j \\ (0, 0), & \text{otherwise} \end{cases} \quad (1)$$

Table 5.2: Strategic form representation of a 2-channel evolutionary game

	\mathbf{a}_k	\mathbf{a}_j
\mathbf{a}_k	$(0, 0)$	$(\mathbf{u}_k, \mathbf{u}_j)$
\mathbf{a}_j	$(\mathbf{u}_j, \mathbf{u}_k)$	$(0, 0)$

where the first element of the ordered pair $u(a_k, a_j)$ represents the payoff for player that selected channel k and the second element for player that selected channel j . For the sake of clarity and ease in analysis and without any loss of generality, we assume that $u_k > u_j, \forall u \in \mathbb{R}_{\geq 0}^k$. Also, we initially consider a 2-channel game i.e., a game with 2 heterogeneous channels and derive its PSNE and MSNE as potential solutions. Later, we consider the k -channel scenario where $k = |K|$, in section 5.4.5 and derive the *Replicator Dynamics* of the proposed evolutionary game. Replicator dynamic is a mechanism with which players can learn from their payoff outcomes of strategic interactions and modify their strategies at every stage of the game to converge to ESS.

The game represented by equation (1) can also be represented in strategic form as table 5.2 which shows the payoffs for two players selecting channels k or j . Since $u_k > u_j$, it is in every CRN's interest to choose channel k instead of channel j for a larger payoff. However, when the players select the same channel it results in a collision, the spectrum opportunity being wasted and both player end up with a payoff of 0. On the other hand, if both players select different channels then their payoffs reflect the quality of the channel to which they are able to gain access, hence the name *anti-coordination* game. As shown in table 5.2, this game is the reverse

of the classic *Battle of the Sexes* game and is classified as an anti-coordination game where it is in both players' interest not to end up selecting the same strategy.

5.4.3 Pure and Mixed Strategy Nash Equilibria

In this subsection we first derive the PSNE followed by MSNE, which are the two potential solutions that are considered for our evolutionary spectrum sharing anti-coordination game.

Definition 1: The *Pure Strategy Nash Equilibrium* [19][22] of the spectrum sharing game is an action profile $a^* \in A$ of actions, such that:

$$u(a_i^*, a_{-i}^*) \succeq u(a_i, a_{-i}^*), \quad \forall i \in K \quad (2)$$

where \succeq is a preference relation over payoffs of strategies a_i^* and a_i . The above definition means that for a_i^* to be a pure strategy NE, it must satisfy the condition that no player i has another strategy that yields a higher payoff than the one for playing a_i^* given that every other player plays their equilibrium strategy a_{-i}^* .

Lemma 1: Strategy pairs (a_k, a_j) and (a_j, a_k) are pure strategy NE of the anti-coordination game.

Proof: Assume player 1 to be the row player and player 2 to be the column player in table 6.2. From equation 1 it follows that both u_k and u_j are positive values and therefore the payoffs for strategy pairs (a_j, a_k) and (a_k, a_j) are greater than the payoffs for strategy pairs (a_k, a_k) and (a_j, a_j) . Consider the payoff for strategy pair (a_j, a_k) from table 6.2. Given that the player playing strategy a_j continues to play this strategy, then from definition 1 for NE, it follows that

the player playing strategy a_k does not have any incentive to change his choice to a_j i.e., it will receive a smaller payoff of 0 if it switched to a_j . Therefore, (a_j, a_k) is a PSNE. The same argument can be applied to prove that the strategy pair (a_j, a_k) is the second PSNE of this game. ■

Definition 2: The *Mixed Strategy Nash Equilibrium* [19][22] of the spectrum sharing game is a probability distribution \hat{p} over the set of actions A for any player such that:

$$\hat{p} = \{p_1, p_2, \dots, p_k\} \in \mathbb{R}_{\geq 0}^k, \text{ and } \sum_{j=1}^k p_j = 1 \quad (3)$$

which makes the opponents indifferent about the choice of their strategies by making the payoffs from all of their strategies equal. Let α be the probability with which player 1 plays strategy a_k and $\beta = (1 - \alpha)$ be the probability of playing strategy a_j , then from the payoffs of table 6.2, the expected utility of player 2 for playing strategy a_k is given by:

$$EU_2(a_k) = \alpha u(a_k, a_k) + \beta u(a_j, a_k) = \alpha(0) + \beta(u_k) \quad (4)$$

Similarly, the expected utility of player 2 for playing strategy a_j is given by:

$$EU_2(a_j) = \alpha u(a_k, a_j) + \beta u(a_j, a_j) = \alpha(u_j) + \beta(0) \quad (5)$$

According to definition 2, player 2 will be indifferent about the choice of strategies when the expected utilities from playing strategies a_k and a_j are equal, i.e.,

$$EU_2(a_k) = EU_2(a_j) \quad (6)$$

Substituting equations 4 and 5 in equation 6, we have $\beta u_k = \alpha u_j$. Therefore:

$$\alpha = \frac{u_k}{u_k + u_j} \quad (7)$$

$$\beta = 1 - \alpha = \frac{u_j}{u_k + u_j} \quad (8)$$

The mixed strategy NE for the heterogeneous spectrum sharing game is given by the distribution $\hat{p} = \{\alpha, \beta\}$ of equations 7 and 8 and shown in table 5.3 which means that when both players select strategies a_k and a_j with probabilities α and β respectively, then their opponents will be indifferent about the outcomes of the play. This means that all CRNs in a given region form a polymorphic population in which every CRN mixes for its choice of available channels according to the probability distribution \hat{p} which is the MSNE for our evolutionary channel sharing game. The probability distribution \hat{p} also represents the proportions of the population adopting different strategies at any given stage of the game. To generalize, expected utility for every player in a k -channel heterogeneous spectrum sharing game is given as follows:

$$EU_m = \sum_{m=1}^k u_m p_m, \forall m \in K \quad (9)$$

where p_m represents the probability of a CRN selecting channel m all other CRNs not selecting channel m .

Table 5.3: MSNE of a 2-channel evolutionary spectrum sharing game

\hat{p}	<i>Prob.</i> ($a_k = \alpha$)	<i>Prob.</i> ($a_j = \beta$)
<i>Prob.</i> ($a_k = \alpha$)	(0,0)	(u_k, u_j)
<i>Prob.</i> ($a_j = \beta$)	(u_j, u_k)	(0,0)

5.4.4 Evolutionary Stability of the Game's Equilibria

To determine if the game's solutions derived in preceding subsection can be invaded by a mutant strategy that is greedier; we analyze its evolutionary stability with the help of definition 3 as follows:

Definition 3: For a strategy \hat{p} to be ESS, it must satisfy the following conditions [20]:

1. $u(\hat{p}, \hat{p}) \geq u(p', \hat{p})$ and
2. if $u(\hat{p}, \hat{p}) = u(p', \hat{p})$ then $u(\hat{p}, p') > u(p', p')$

where \hat{p} is the strategy played by the population and can therefore be termed as the population's incumbent strategy while p' is a mutant strategy that competes with the incumbent strategy. According to the first condition of definition 3, an incumbent strategy (1) must be a symmetric NE and (2) must perform at least as good against itself as it does against a mutant strategy. According to the second condition of definition 3, if an incumbent strategy is not a strict NE then the incumbent strategy must do strictly better against a mutant than a mutant strategy does against itself. Now we analyze both PSNE and MSNE derived in preceding subsection according to definition 3 to see if they are evolutionarily stable.

5.4.4.1 Evolutionary Stability of PSNE

Earlier we proved that the strategies (a_k, a_j) and (a_j, a_k) are the PSNE of our evolutionary game. If two players play the same strategy i.e., play (\hat{p}, \hat{p}) and are in equilibrium, then it is said to be a symmetric NE. Clearly, the PSNE of our game are not symmetric NE and by condition

(1) of definition 3, $u(\hat{p}, \hat{p}) < u(p', \hat{p})$. Therefore, pure strategy NE is not evolutionarily stable according to definition 3. Another aspect of the PSNE is that it is always unfair for the player that selected the lower quality channel therefore making it impractical as a long term strategy for CRNs' channel selection.

5.4.4.2 Evolutionary Stability of MSNE

With no pure strategy NE for our evolutionary game as ESS, we now determine if the MSNE that we derived in equations (7) and (8) is an ESS according to definition 3. To do so, we first calculate $u(\hat{p}, \hat{p})$ i.e., see how the incumbent strategy \hat{p} fares against itself and then determine the payoff of a mutant strategy p' against the incumbent strategy. Consider the payoff matrix of table 5.3 where the players select strategies a_k and a_j with the probability distribution of the incumbent strategy $\hat{p} = \{\alpha, \beta\}$ then:

$$u(\hat{p}, \hat{p}) = \alpha\beta(u_k + u_j) \quad (10)$$

In equation (10) above, we have determined the payoff of incumbent strategy \hat{p} when it competes against itself i.e., $u(\hat{p}, \hat{p})$. Now consider a mutant strategy $p' = \{\alpha + \delta, \beta - \delta\}$ which is greedier than the incumbent strategy \hat{p} and assume that it selects the higher quality channel k with a higher probability i.e., $\alpha + \delta$ and selects the lower quality channel j with lower probability i.e., $\beta - \delta$, where δ is a small positive number that represents the increase in greediness/probability of a mutant strategy to select a higher quality channel. Because of the existence of two competing strategies, we now calculate $u(p', \hat{p})$ i.e., the utility of the mutant strategy against the incumbent strategy:

$$u(p', \hat{p}) = \alpha\beta(u_k + u_j) - \delta(\alpha u_k - \beta u_j) \quad (11)$$

Since $u_k > u_j$ as assumed in section 5.3, we know that αu_k is greater than βu_j and therefore the second term of equation (11) is positive. From equations (10) and (11) we have $u(\hat{p}, \hat{p}) > u(p', \hat{p})$. Since $u(\hat{p}, \hat{p})$ is strictly greater than $u(p', \hat{p})$, we do not need to check for the second condition of definition 3 and we conclude that the incumbent strategy \hat{p} does strictly better than the mutation p' , which will die out in the evolutionary game. Hence our MSNE cannot be invaded by the greedier mutation p' and is therefore an ESS.

It is pointed out that derivation of MSNE becomes intractable when the number of channels is greater than 2. To expand our analysis for a k -channel scenario, we now introduce the concept of replicator dynamics in the following subsection.

5.4.5 Replicator Dynamics and K-Channel Scenario

In the above section, we have shown that the mixed strategy NE of our proposed evolutionary game framework is evolutionarily stable. Evolutionary stability has provided us with a means to evaluate how the channel selection strategies perform in the long run when the CRNs do not cooperate with each other. This concept is somewhat static in nature because it does not demonstrate the dynamics with which the strategies evolve and converge to an equilibrium state. Replicator Dynamics explain how players evolve their behaviors by learning through strategic interactions at every stage/generation of the game to reach the equilibrium state which is also evolutionarily stable. In order to show the dynamics and to extend our analysis to

the k -channel scenario, we now derive the Replicator Dynamics of our evolutionary heterogeneous spectrum sharing game.

Following our analysis from the previous section, let $\hat{p} = \{p_1, p_2, \dots, p_k\}$ and $\sum_{j=1}^k p_j = 1$ where \hat{p} represents the strategy of selecting channel k with probability p_k . Alternatively, we can also think of p_k as the proportion of population that select channel k at any given time. Furthermore, let u_0 be the initial fitness of every CRN and the average payoff of CRNs selecting channel k at a given stage of the game be represented by the set $U = \{u_1, u_2, \dots, u_k\}$. Then payoff for a CRN selecting channel k can be calculated as:

$$u_k = u_0 + \sum_{m=1}^k p_m \cdot u(a_k, a_j) \quad (12)$$

where $u(a_k, a_j)$ is the fitness of a CRN that selects channel k in a pairwise competition against a CRN that selects channel j . Let \bar{u} be the total average payoff of the entire CRN population at any given time. Then \bar{u} is given by:

$$\bar{u} = \sum_{n=1}^k p_n \cdot u_n, \forall n \in K \quad (13)$$

and the probability p'_k of a CRN selecting channel k for the next stage/time slot of the game is given by:

$$p'_k = p_k + \frac{p_k \cdot (u_k - \bar{u})}{\bar{u}} \quad (14)$$

Equations (12) to (14) are the replicator dynamics of our evolutionary spectrum sharing game. The idea behind the replicator dynamics is that if selecting channel k in the current time slot results in a higher average fitness for the CRNs that selected it than the overall fitness of the entire CRN population, then the proportion of CRNs selecting channel k in the next time slot

will increase. CRNs are able to calculate the total average payoff for the entire CRN population \bar{u} of equation (13) because it is based on common knowledge parameters: p_n is the proportion of population that selected channel n while channel quality represented by u_n is also known to every CRN. In general, if selecting a particular channel in a given time slot results in a higher than total average payoff then that channel will be selected more frequently in subsequent time slots, ultimately converging to ESS.

Table 5.4: Replicator Dynamics Algorithm

Data: u_0 , set of available channels K and their utilities U
Result: Channel selection strategies converge to ESS.
Initialization: initial fitness of CRNs u_0 , population distribution p_k , channel utilities u_k

for every stage/time step of the game do

1. With current channel utilities, compute average payoff u_k for the proportion of CRN population that selected channel k at current time – equation (12);
2. Compute total average payoff \bar{u} for the entire CRN population at current time – equation (13);
3. Calculate new Channel selection strategies of CRNs – equation (14)

end for

5.5 Fairness Analysis of Derived Equilibria

We now provide an analysis on the fairness of the Nash equilibria derived in preceding section. For the sake of clarity and ease of understanding, we consider the case of a 2-channel heterogeneous spectrum sharing game while the same arguments can be applied for analyzing a k -channel scenario. The Nash equilibria being considered as solutions for the spectrum sharing heterogeneous game are:

- Two pure-strategy NE for the anti-coordination game are (a_k, a_j) and (a_j, a_k) .
- A mixed strategy NE defined by the probability distribution $\hat{p} = \{\alpha, \beta\}$ given by equations (7) and (8).

One of the ways to determine if entities receive a fair share of the system's resources is with Jain's fairness index [21]. If there are N CRNs and every CRN's utility is given as u_i then fairness of the derived Nash equilibria can be measured by Jain's equation as:

$$J(u_1, u_2, \dots, u_N) = \frac{(\sum_{i=1}^N u_i)^2}{N \cdot \sum_{i=1}^N u_i^2} \quad (15)$$

As assumed previously in section 5.3.1 for a 2-channel scenario, channel k is of higher quality than channel j therefore $u_k > u_j$. Then from the payoff matrix of table 5.2, gaining access to channel k brings a larger payoff to a CRN whereas being of comparatively lower quality, channel j brings a smaller payoff. There are two pure-strategy Nash equilibria (a_k, a_j) and (a_j, a_k) , however intuitively, both of them are unfair because $u_k \neq u_j$ and one player always gets a smaller payoff than the other. This can be confirmed with equation (15) as

follows: whenever all u_i are equal then the ratio $\frac{(\sum_{i=1}^N u_i)^2}{N \cdot \sum_{i=1}^N u_i^2}$ in equation (15) yields a value equal to N and Jain's index would be equal to 1 i.e., the maximum, while for an unequal distribution of payoffs it would be smaller than 1. Since PSNE does not result in equal payoff for all CRNs, it is not a fair solution.

Let us now consider fairness of MSNE. According to definition 2, MSNE is a probability distribution over the set of strategies which makes the players indifferent about their choice of strategies by making the payoffs equal even though the channels are of different quality. When all the payoffs u_i become equal then from the same argument of the preceding paragraph, equation (15) yields an index equal to 1 resulting in the MSNE's resource distribution to be fair.

5.6 Simulations and Results

5.6.1 Preliminaries

We have conducted simulations to study the effects of applying evolutionary game theoretic model for self-coexistence with heterogeneous channels and to study how the channel selection strategies in mixed strategy Nash Equilibria are also the evolutionarily stable states. We first show the results of simulations in which the collocated CRNs have only two available channels for which they contend and converge to an evolutionary stable state. Later, we show that our evolutionary game converges to ESS when there are more than 2 channels available for contention. To that end, we have implemented the Replicator dynamics and provide results of our experiments with 3, 4 and 5 heterogeneous channels as well. We also show that the evolutionary game can converge to new ESS when the network conditions may be changing

requiring that the CRNs adjust to the new environments. As described in section 5.3, a_k means the action of selecting channel k .

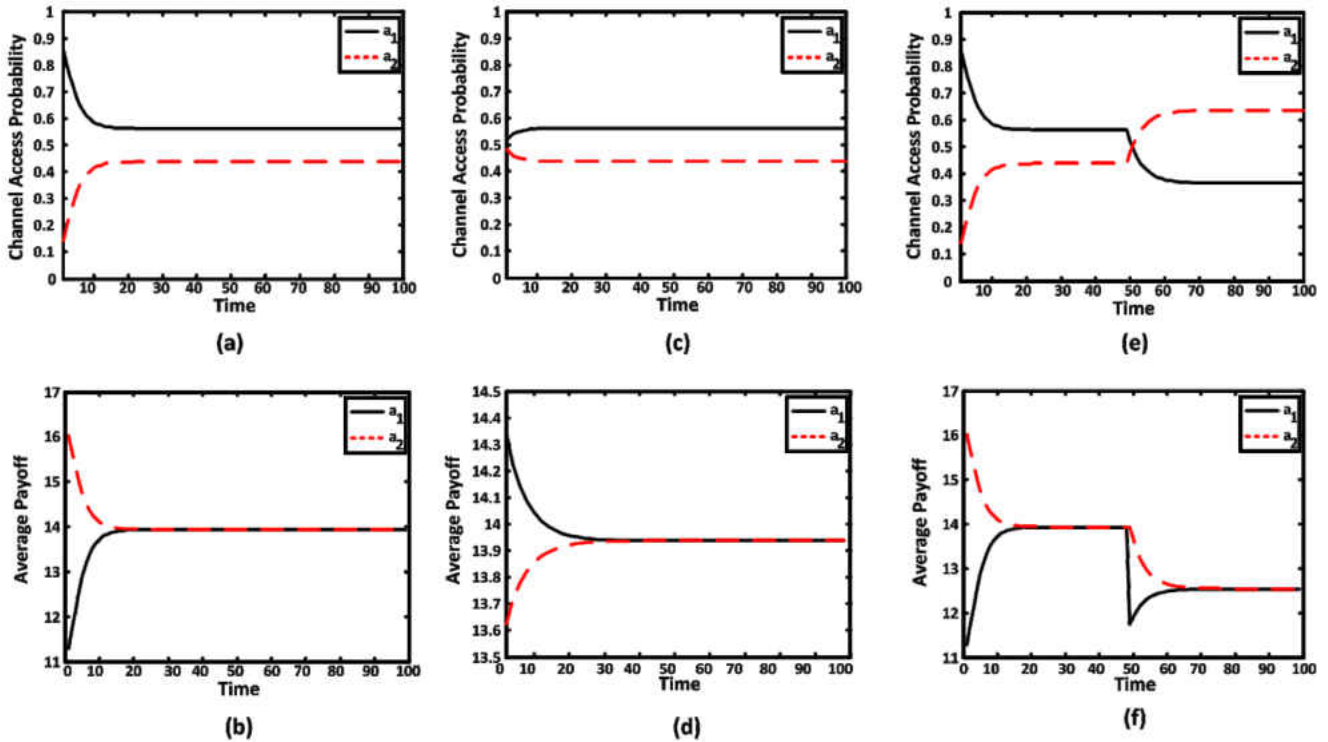


Figure 5.2: Channel access probabilities and average payoffs when the number of channels available for contention is $k = 2$. (a) Channel access probability and (b) average payoffs when the initial probabilities are unequal, figures (c) and (d) show the results when initial probabilities are equal, (e) and (f) results under changing network conditions i.e., quality of channel 1 becomes worse than channel 2 at time $t = 50$.

5.6.2 Results

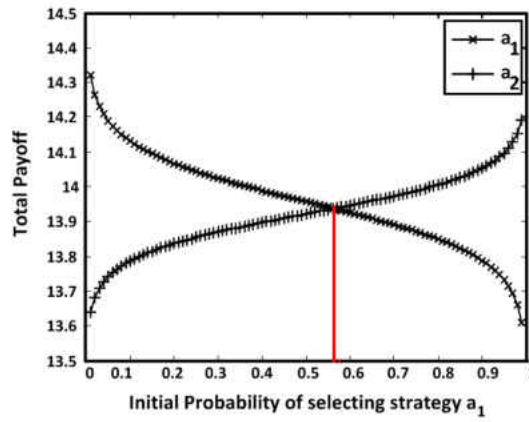
Figure 5.2 represents the scenario in which CRNs contend for 2 channels for secondary access. Figure 5.2(a) shows how CRNs select one out of two available channels with some probability where channel 1 is of better quality than channel 2. Any positive values for channel

utilities would work however in case of simulations of figure 5.2 are assumed to be $u_1 = 9$ and $u_2 = 7$ for channels 1 and 2 respectively and its MSNE is $p_1 = 0.5625, p_2 = 0.4375$. Payoff from such strategic interactions is shown in figure 5.2(b) based on which, CRNs modify the probabilities of selecting the same channels in subsequent time slots/stages.

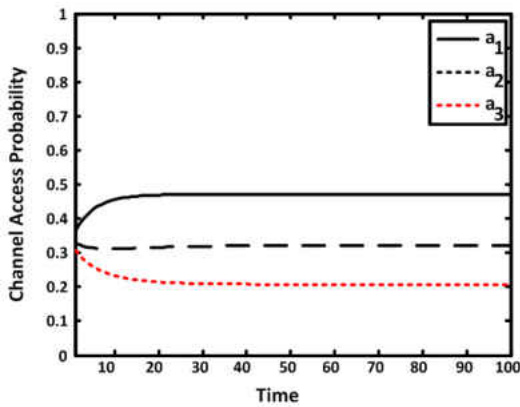
Let us first consider payoffs of CRNs that select channels with smaller payoffs. As shown in figure 5.2(b), CRNs that select the lower quality channel receive a larger average payoff at $t = 1$ than CRNs that select higher quality channel. This happens because more CRNs would want to gain access to higher quality channel resulting in collisions and a zero payoff. Receiving higher payoff makes the CRNs that selected smaller payoff channels to further increase the probability of selecting the lower quality channel at $t = 2$ (figure 5.2(a)). This however, results in lower average payoff for them at $t = 2$ than at $t = 1$. This happens because the higher quality channels are accessed with a relatively smaller probability at $t = 2$ because in previous time slot, it had resulted in smaller payoff. A relatively smaller payoff at $t = 2$ compared with higher payoff at $t = 1$ from accessing channel 2 is still greater than the total average payoff of the entire CRN which results in an even greater probability of selecting lower quality channel in subsequent stages. A similar yet opposite pattern can be seen for CRNs that select higher quality channels with higher probabilities. Stated in another way, the proportion of CRNs selecting a particular channel increases if its payoff is bigger than total average payoff of the entire population and vice versa.

CRNs keep modifying their channel selection probabilities in the same manner until their payoffs converge and they reach the ESS, which in the case of figure 5.2(a) is $p_1 = 0.5625, p_2 =$

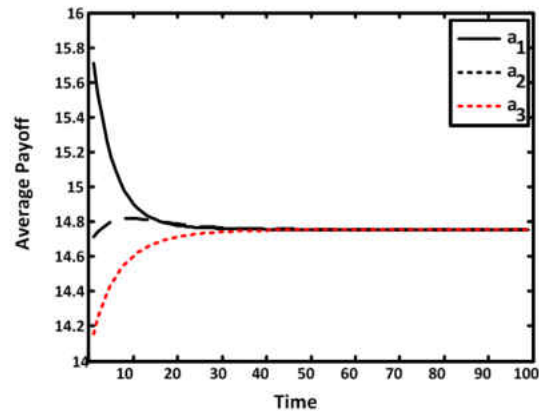
0.4375 at around $t = 25$. The amount of time taken to converge to ESS is important as it would determine spectrum wastage because of collisions and is demonstrated in subsequent simulations. The average payoff u_k of selecting a given channel k is calculated by having the initial payoff u_0 of equation (12) equal to 1. Figures 5.2(c) and 5.2(d) represent the case when initial channel selection probabilities are equal yet they still converge to ESS. Figures 5.2(e) and 5.2(f) represent changing network conditions i.e., quality of channel 1 becomes worse than channel 2 at $t = 50$ yet the channel selection strategies still converge to a new ESS.



(a)



(b)



(c)

Figure 5.3: (a) Total payoff for both channels becomes equal when initial probability of selecting channel 1 equals $p_1 = 0.5625$ i.e., the ESS probability. (b) Channel access probability and (c) average payoffs when the initial probabilities are equal for a 3-channel scenario.

Figure 5.3(a) shows that the total payoff for both channels becomes equal when initial probability of selecting channel 1 equals $p_1 = 0.5625$ and the probability of selecting channel 2 equals $p_2 = 0.4375$ which is the game's ESS. It also shows that ESS is the only point where CRNs can have a fair distribution of spectrum resources. Figures 5.3(b), 5.3(c), 5.4 and 5.5 show the convergence of channel selection probabilities to ESS along with their respective average payoffs in cases where the number of channels is increased to 3, 4 and 5 respectively and channel

utilities are varied between values such as 9 and 4. It is however pointed out that any values of channel utilities can be used without affecting our analyses. The initial channel selection probabilities may be equal or unequal, yet in any case the game always converges to the ESS for any given set of channel utilities. Another important observation is that the convergence rate to ESS decreases with the increase in number of channels and how accurate the initial probabilities are as compared to the ESS.

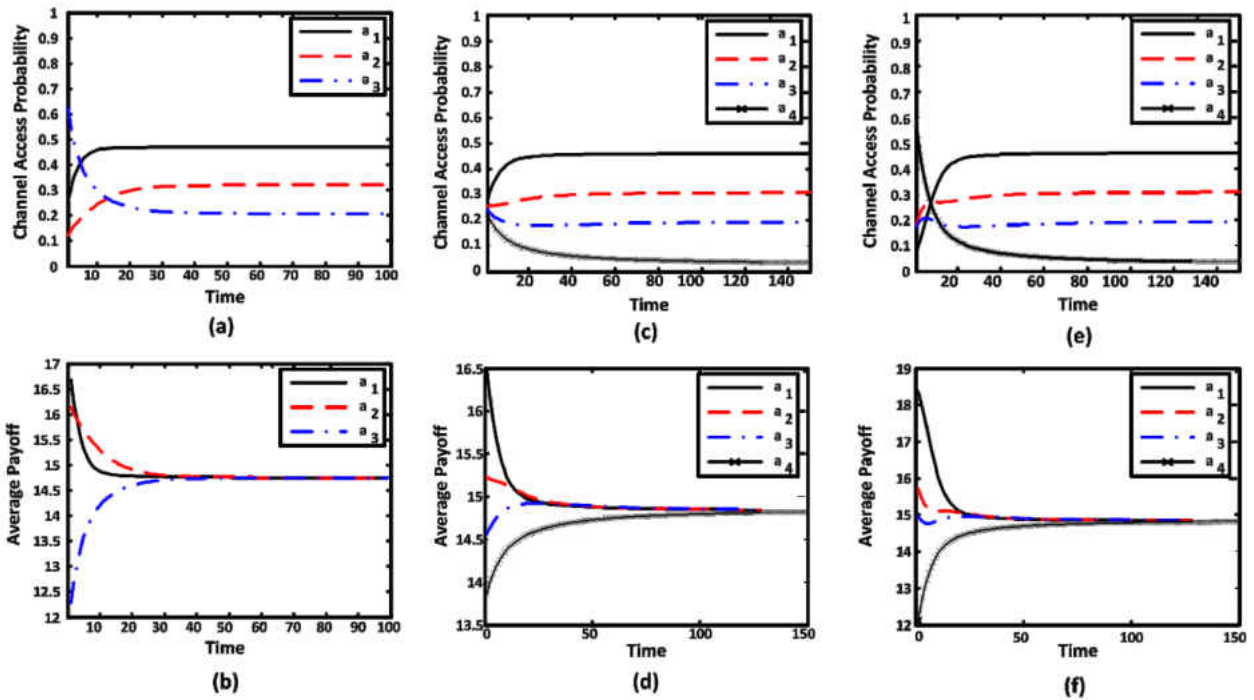


Figure 5.4: (a), (c) and (e) Channel access probabilities and (b), (d) and (f) average payoffs. For (a) and (b) the number of channels available for contention is 3 i.e., $k = 3$ and initial probabilities are *un-equal*. For (c) and (d) the number of channels available for contention is 4 i.e., $k = 4$ and initial probabilities are *equal* whereas for (e) and (f) $k = 4$ and initial probabilities are *un-equal*.

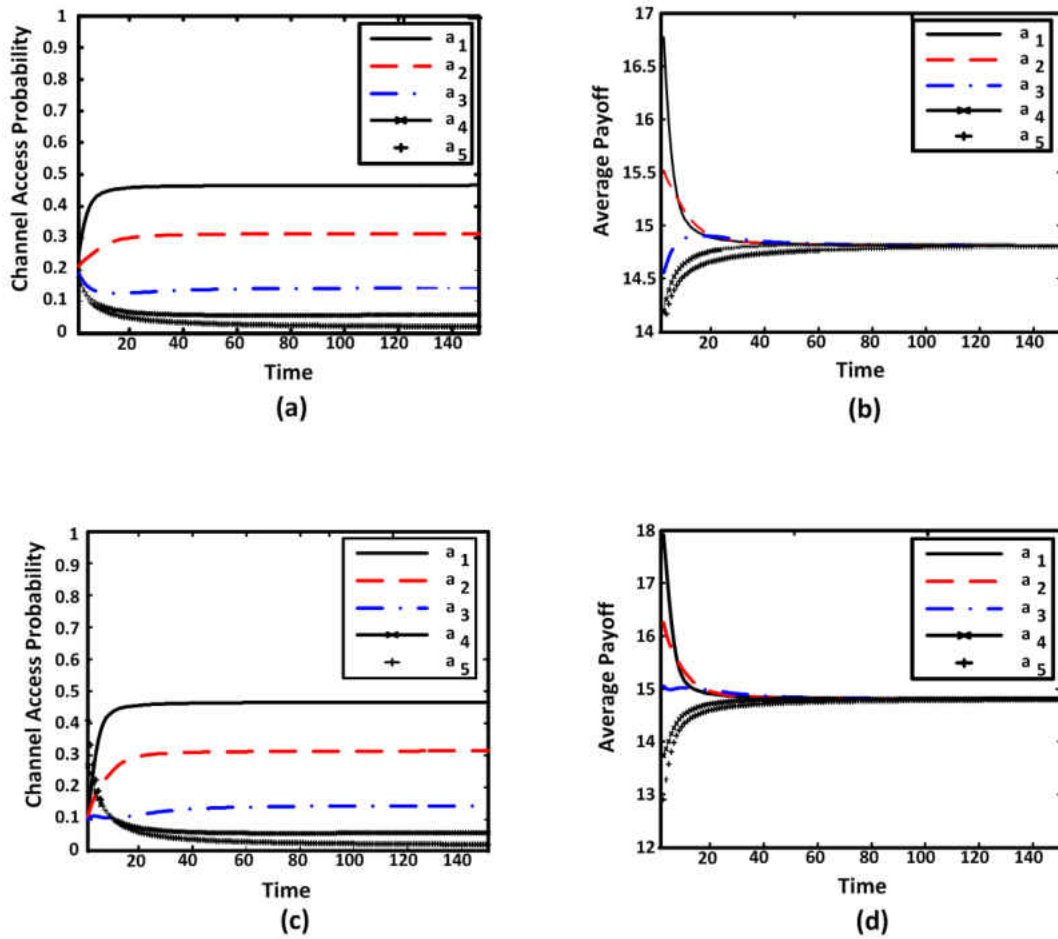


Figure 5.5: (a) and (c) Channel access probabilities and (b) and (d) average payoffs when the number of channels available for contention is 5 i.e., $k = 5$. For (a) and (b) initial probabilities are *equal*. For (c) and (d) the initial probabilities are *un-equal*.

5.7 Conclusion

Coexistence protocols employed by CRNs do not take into consideration the fact that spectrum bands vary significantly with regards to channel *quality* thereby making some channels

of the spectrum bands more attractive to CRNs than others. This work aimed at answering the fundamental question of how CRNs should share heterogeneous spectrum bands in a distributed yet *fair* manner and proposed an evolutionary game theoretic framework to achieve that. We derived equilibrium strategies for CRNs' spectrum sharing game for selecting particular spectrum bands and proved that the mixed strategy Nash Equilibria derived in the process are evolutionarily stable strategies (ESS) while also being fair. We also derived the mechanism of Replicator Dynamics with which players learn from payoff outcomes of their strategic interactions and modify their strategies at every stage of the evolutionary game. Since all players approach the ESS based solely upon the common knowledge payoff observations, our proposed evolutionary framework can be implemented in a distributed manner.

5.8 References

- [1] U.S. FCC, ET Docket 04-186, "*Notice of proposed rule making, in the matter of unlicensed operation in the TV broadcast bands*", May 25, 2004.
- [2] T. M. Taher, R. B. Bacchus, K. J. Zdunek, D. A. Roberson, "*Long-term spectral occupancy findings in Chicago*", IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2011.
- [3] IEEE 802.22TM 2011 Standard for Wireless Regional Area Networks in TV Whitespaces, <http://www.ieee.org/22>
- [4] M. Faisal Amjad, M. Chatterjee, O. Nakhila, C.C. Zou, "*An Evolutionary Game Theoretic Framework for Coexistence in Cognitive Radio Networks*", IEEE Global Conference on Signal and Information Processing (GlobalSIP) 2014.
- [5] B. Wang.; K. J. R. Liu, T. C. Clancy, "*Evolutionary cooperative spectrum sensing game: how to collaborate?*" IEEE Transactions on Communications, March 2010.

- [6] P. Sroka, A. Kliks, “*Distributed Interference Mitigation in Two-Tier Wireless Networks Using Correlated Equilibrium and Regret-Matching Learning*”, European Conference on Networks and Communications (EuCNC), 2014.
- [7] J. Zheng, Y. Cai; D. Wu, “*Subcarrier allocation based on correlated equilibrium in multi-cell OFDMA systems*”, EURASIP Journal on Wireless Communications and Networking, 2012.
- [8] J. W. Huang, V. Krishnamurthy, “*Cognitive Base Stations in LTE/3GPP Femtocells: A Correlated Equilibrium Game-Theoretic Approach*”, IEEE Transactions on Communications, 2011.
- [9] S. Maharjan, Y. Zhang, C. Yuen, S. Gjessing, “*Distributed Spectrum Sensing in Cognitive Radio Networks with Fairness Consideration: Efficiency of Correlated Equilibrium*”, IEEE Mobile Adhoc and Sensor Systems (MASS), 2011.
- [10] B. Wang, Z. Han, K.J.R. Liu, “*Peer-to-peer file sharing game using correlated equilibrium*”, 43rd Annual Conference on Information Sciences and Systems, IEEE CISS 2009.
- [11] S. Sengupta, R. Chandramouli, S. Brahma, M. Chatterjee, “*A game theoretic framework for distributed self-coexistence among IEEE 802.22 networks*”, IEEE GLOBECOM 2008.
- [12] R. Etkin, A. Parekh, D. Tse, “*Spectrum sharing for unlicensed bands*”, IEEE Journal on Selected Areas in Communications (JSAC), vol.25, no.3, pp.517,528, April 2007.
- [13] C. Jiang, Y. Chen, Y. Gao, K. J. Ray Liu, “*Joint spectrum sensing and access evolutionary game in cognitive radio networks*”, IEEE Transactions on Wireless Communications, vol.12, no.5, May 2013.
- [14] M. Faisal Amjad, M. Chatterjee, C.C. Zou, “*Inducing Voluntary Cooperation for Optimal Coexistence in Cognitive Radio Networks: A Game Theoretic Approach*”, IEEE Military Communications Conference (Milcom) 2014.
- [15] S. Sengupta, S. Brahma, M. Chatterjee, N. Shankar, “*Self-coexistence among interference-aware IEEE 802.22 networks with enhanced air-interface*”, Pervasive and Mobile Computing, Volume 9(4), August 2013.

- [16] Z. Han, C. Pandana, K.J.R. Liu, “*Distributive Opportunistic Spectrum Access for Cognitive Radio using Correlated Equilibrium and No-Regret Learning*”, Wireless Communications and Networking Conference, IEEE WCNC 2007.
- [17] Google, Inc.'s TV Bands Database System for Operation, ET Docket No. 04-186
<http://www.google.com/get/spectrumdatabase/channel/>
- [18] Show My White Space – TVWS database from Spectrum Bridge Inc.
<http://whitespaces.spectrumbridge.com/whitespaces/home.aspx>
- [19] D. Fudenburg, J. Tirole, “*Game Theory*”, The MIT press, 1991.
- [20] J. Maynard Smith, “*Evolution and the theory of games*”, Cambridge University press, 1982.
- [21] R. Jain, W. Hawe, D. Chiu, “*A Quantitative measure of fairness and discrimination for resource allocation in Shared Computer Systems*”, DEC-TR-301, September 26, 1984.
- [22] Y. Shoham, K. Leyton-Brown, “*Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations*”, Cambridge University Press 2008.

CHAPTER 6: COEXISTENCE IN HETEROGENEOUS SPECTRUM THROUGH DISTRIBUTED CORRELATED EQUILIBRIUM

TV white space (TVWS) channels in the 54-698 MHz frequency range have been made available by the Federal Communications Commission (FCC) [1] for secondary unlicensed access. This is because of a realization that the gap between the demand and supply of wireless spectrum resource is ever increasing and fixed spectrum allocation is causing its severe under-utilization [2]. Strict requirements are placed on the Secondary Users (SU) of the spectrum which is otherwise allocated to licensees called primary users (PU), to continuously sense the spectrum and vacate it when the presence of the PU is detected and not to cause them any interference. This type of spectrum access is intuitively called Dynamic Spectrum Access (DSA). Cognitive Radio Network (CRN) is a paradigm that meets precisely this communication criterion and utilizes DSA to enable secondary, unlicensed access to TVWS spectrum bands in an opportunistic and non-interfering basis [1].

DSA allows CRNs to ensure that their use of spectrum does not cause interference to PUs while at the same time all spectrum opportunities are utilized to the maximum. The decision to select a specific channel for DSA is usually made by a central entity in the CRN such as its base station or some algorithm that enables all SUs in the CRN to reach a consensus in a distributed manner. IEEE 802.22 wireless regional area network (WRANs) [3] is an example of a CRN in which the base station controls all the operation including the choice of spectrum bands for communication. Regardless of how a decision to utilize a specific channel is made, every entity in the CRN is bound to abide by that decision. However, reaching a consensus is non-trivial in the case of multiple collocated CRNs in a given region, all of whom compete for access to the

same set of available channels. This situation is called self co-existence in the context of CRNs which employ coexistence protocols to deal with such situations.

6.1 Motivation and Contribution

Most coexistence protocols work under the assumption that all spectrum bands afford the same level of throughput and do not take into consideration the fact that these channels can be heterogeneous. The heterogeneity of channels can be in the sense that they may vary in their characteristics such as signal to noise ratio (SNR) or bandwidth. Furthermore, a channel whose PU remains idle for most of the time may be more attractive to a CRN as compared with a channel with high PU spectrum usage. This would entail that channels can have an associated *quality* parameter and CRNs may have a preference over the set of available channels for secondary access. Without any incentive for altruism, all CRNs would want to gain access to the highest quality channels making it a conflict condition. Therefore, in the absence of any mechanism to enforce fairness in accessing varying quality channels, ensuring coexistence with minimal contention and efficient spectrum utilization for CRNs is likely to become a very difficult task.

Game theory provides an elegant means to model strategic interaction between agents which may or may not be cooperative in nature. It has been applied to numerous areas of research involving conflict, competition and cooperation in multi-agent systems which also encompass wireless communications. Therefore, by leveraging the mechanisms of game theory, we model the heterogeneous spectrum sharing in CRNs as a repeated, non-cooperative anti-coordination game in which collocated CRNs in a given region are its players. The payoff for every player in

the game is determined by the quality of the spectrum band to which it is able to gain access. We present a detailed mathematical analysis on fairness and efficiency of the solution through the concept of *Price of Anarchy* which is an analysis tool that measures a system's degradation in the presence of selfish behavior from its entities. We also confirm our findings through detailed simulations.

We formulate a heterogeneous spectrum sharing anti-coordination game to come up with a solution that results in fair and efficient utilization of the spectrum resources. Specifically, following contributions are made:

- As potential solutions for the heterogeneous spectrum sharing game, we have derived the game's pure and mixed strategy Nash Equilibria (PSNE and MSNE respectively) as well as its Correlated equilibrium (CE).
- We have analyzed the game's solutions in the context of fairness and efficiency and demonstrated that the traditional solution concepts of Nash Equilibria (NE) are either inefficient or unfair. We also show that the strategies in CE are optimal as well as fair while sharing heterogeneous spectrum resource.
- Finally, to show that CE is scalable, we have demonstrated how CE can be achieved in a 2-player as well as an N-player game with centralized as well as a distributed approach using linear optimization and channel selection learning algorithm, respectively.

6.2 Related Work

In this section we provide an overview of some of the works carried out in the domain of self coexistence in CRNs as well as application of the game theoretic solution concept of correlated equilibrium in the context of communication networks.

A game theoretic approach based on correlated equilibrium has been proposed in [4] for multi-tier decentralized interference mitigation in two-tier cellular systems. Authors of [5] propose a multi-cell resource allocation game for efficient allocation of resources in orthogonal frequency division multiple access (OFDMA) systems based on throughput, inter-cell interference and complexity. The subcarriers are considered as players of the game while the base station acts as the provider of external recommendation signal needed for achieving correlation of strategies of players.

Authors of [6] model the competition among multiple femtocell base stations for spectrum resource allocation in an OFDMA LTE downlink system as a static non-cooperative game. The correlated equilibrium of the game is derived through a distributed resource block access algorithm which is a variant of the No-Regret learning algorithm. CRNs with SUs having variable traffic characteristics are considered in [7] to tackle the problem of distributed spectrum sensing by modeling it as a cooperative spectrum sensing game for utility maximization. The authors have proposed another variant of the no-regret learning algorithm called neighborhood learning (NBL) which achieves correlated equilibrium for the spectrum sensing game. In contrast to the no-regret learning algorithm, NBL is not completely distributed and requires some coordination among players to achieve better performance.

Correlated equilibrium has been employed in [8] for a P2P file sharing non-cooperative game to jointly optimize players' expected delays in downloading files. Not uploading files for others causes an increase in file download time for all players which in turn, forces even the non-cooperative players to cooperate. The authors of [9] tackle the self-coexistence problem of finding a mechanism that achieves a minimum number of wasted time slots for every collocated CRN to find an empty spectrum band for communications. To do so, they employ a distributed modified minority game under incomplete information assumption.

Different punishment strategies have been employed in [10] that form part of a Gaussian interference game in a one-shot game as well as an infinite horizon repeated game to enforce cooperation. Spectrum sharing is however considered within the context of a single CRN. Evolutionary game theory is applied in [11] to solve the problem in a joint context of spectrum sensing and sharing within a single CRN. Multiple SUs are assumed to be competing for unlicensed access to a single channel. SUs are considered to have half-duplex devices so they cannot sense and access a channel simultaneously.

Utility graph coloring is used to address the problem of self-coexistence in CRNs in [12]. Allocation of spectrum for multiple overlapping CRNs is done using graph coloring in order to minimize interference and maximize spectrum utilization using a combination of aggregation, fragmentation of channel carriers, broadcast messages and contention resolution. The authors of [14] achieve correlated equilibrium with the help of No-regret learning algorithm to address the problem of network congestion when a number of SUs within a single CRN contend for access to channels using a CSMA type MAC protocol. They model interactions of SUs within the CRN

as a prisoner's dilemma game in which payoffs for the players are based on aggressive or non-aggressive transmission strategies after gaining access to idle channels.

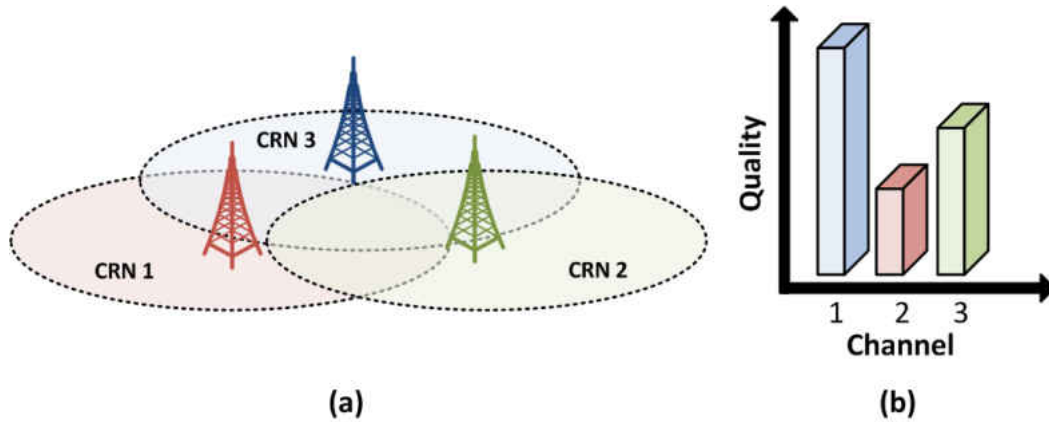


Figure 6.1: Collocated CRNs competing for Heterogeneous channels.

6.3 System Model and Assumptions

6.3.1 System Model

As shown in figure 6.1, we consider a region where IEEE 802.22 WRAN based CRNs represented by the set of $N = \{1, 2, \dots, n\}$ players are collocated and contend for secondary access to the licensed spectrum bands. The set of TVWS channels available for secondary access by the contending CRNs is represented as $K = \{1, 2, \dots, k\}$ channels. The spectrum consists of channels that differ from each other due to various network parameters such as noise, bandwidth or even availability. These differences make the spectrum heterogeneous in nature with channels considered to have some 'quality' parameter determined by the payoff that a CRN may achieve if

it is able to gain access to that channel. The notations and acronyms commonly used in this chapter are shown in table 6.1.

Table 6.1: Notations and acronyms – Chapter 6

Notation	Definition
a_k	CRN's action of selecting channel k
u_k	CRN's utility for gaining access to channel k
N	set of contending CRNs
K	set of available channels
\hat{p}	prob. distribution over set of channels (in MSNE)
EU_k	Expected Utility from accessing channel k
π	joint prob. distribution of available channels (in CE)
t	current time
$\omega_i^t(a'_i)$	utility if all a_i in time slot τ were replaced by a'_i
$\delta_i^t(a'_i, a_i)$	average difference in a CRN's utility up to time t for not selecting every other channel a'_i
$NR_i^t(a'_i, a_i)$	CRN's average regret up to time t for selecting channel a_i instead of every other other channel a'_i that was not selected
p_i^{t+1}	probability of selecting a channel for next time slot
S	Set of strategies in equilibrium
$F(a)$	utility function for all actions in equilibrium
PoA	Price of Anarchy
PU	Primary User
SU	Secondary User
NE	Nash Equilibrium
PSNE	Pure Strategy Nash Equilibrium
MSNE	Mixed Strategy Nash Equilibrium
CE	Correlated Equilibrium

6.3.2 Assumptions

Following are the underlying assumptions for the work presented in this chapter:

- **Time:** A single MAC superframe constitutes one time slot. Every CRN needs to gain access to a channel for which it contends with all other collocated CRNs in every time slot. One superframe's time slot is also treated as one iteration in the spectrum sharing game.
- **Spectrum opportunity and wastage:** A given time slot's spectrum opportunity arises due to a PU being idle in its allocated channel. The opportunity may result in a collision and be wasted if two or more CRNs select the same channel for accessing in the same time slot.
- **Knowledge about PU activity:** In addition to the FCC mandated continuous spectrum sensing to detect PUs' activity, CRNs are also required to periodically access online databases such as [15][16] in order to gain up-to-date information about licensed PUs operating in a given region.
- **Channel quality:** The amount of PU activity, bandwidth and SNR which collectively determine a channel's quality can be learnt from online databases and measured through spectrum sensing over a period of time. Due to the fact that all contending CRNs are collocated in a given region, it is reasonable to assume that a given channel's quality is common knowledge.
- **History of channel access:** As stated above, all CRNs are collocated in a given region and are contending for the same spectrum resource. Therefore, every CRN can

tell which channels other CRNs were able to gain access to in previous time slots and determine channel access history.

- ***Non-cooperative behavior:*** All CRNs are independent as they do not share a common goal and therefore do not cooperate with each other. Being rational about their choices, every player has a clear preference of selecting the best available channel before the start of every time slot. Consequently, if every player tries to access the best channel, it will result in a collision and the spectrum opportunity being wasted.
- ***Payoffs***⁴: Players⁵ that eventually gain access to higher quality channels will gain higher payoffs as compared to the players that end up with lower quality channels. In the subsequent section, we show that our proposed spectrum sharing game can be implemented solely on the basis of a CRN's own payoff observations.

6.4 Equilibrium Solutions for Heterogeneous Spectrum Sharing Game

In this section, we first present the formulation of our proposed spectrum sharing game, followed by the derivation of pure and mixed strategy NE. Next we introduce the concept of CE and demonstrate how it can be achieved in a centralized implementation for a 2-player game using linear optimization. We also demonstrate that CE can be achieved in a distributed manner for an N -player game using a learning algorithm called channel selection learning algorithm which is an adaptation of the No-Regret (NR) learning algorithm [17]. Using these concepts we model the problem of self-coexistence and heterogeneous spectrum sharing in the following

⁴ We use the terms utility and payoff interchangeably.

⁵ Similarly, we use the terms CRNs and players interchangeably.

subsections as an anti-coordination game framework. The game is a non-cooperative repeated game with perfect information because:

- Being rational players, CRNs compete for the best channels available in the spectrum band and are interested only in maximizing their own utility. Therefore, CRNs are not bound to cooperate with each other.
- Utilities are common knowledge since the quality of various network parameters can be measured by every CRN. Also, every CRN can tell which channels other CRNs were able to gain access to in the past hence they know other CRNs' payoffs.

6.4.1 Game Formulation

The heterogeneous spectrum sharing anti-coordination game presented in this chapter is represented as $\mathcal{G} = \langle (N), (A), (U) \rangle$. Players in the game \mathcal{G} are CRNs represented by N . Every player in the game has the same action space represented by $A = \{a_1, a_2, \dots, a_k\}$ and the set of utilities of the channels is $U = \{u_1, u_2, \dots, u_k\}$. Let $K = \{1, 2, \dots, k\}$ denote the set of available channels and there is a bijection between the sets A and K . Also, Let N and K represent the total number of collocated CRNs and the total number of available channels, respectively. Strategy a_k means selecting channel k for communication and a player gets a payoff of u_k if he selected channel k and no other player selected the same channel for a given time slot. The payoff for players playing strategies a_k and a_j when competing against each other is denoted by the ordered pair $u(a_k, a_j) \in U$ and is a function of an individual channel's quality given by:

$$u(a_k, a_j) = \begin{cases} (u_k, u_j), & \text{when } k \neq j \\ (0,0), & \text{otherwise} \end{cases} \quad (1)$$

where the first element of the ordered pair $u(a_k, a_j)$ represents the payoff for player that selected channel k and the second element for player that selected channel j . For the sake of clarity and ease in analysis and without any loss of generality, we assume that $u_k > u_j, \forall u \in \mathbb{R}_{\geq 0}^k$. Initially, we consider a game with 2 players and 2 heterogeneous channels. Later, we present the case with N -players and k -channels in section 6.4.4. The game represented by equation 1 can also be represented in strategic form as table 6.2, which shows the payoffs for two players selecting channels k or j . Since $u_k > u_j$, it is in every CRN's interest to choose channel k instead of channel j for a larger payoff. However, when the players select the same channel it results in a collision, the spectrum opportunity being wasted and both player end up with a payoff of 0. On the other hand, if both players select different channels then their payoffs reflect the quality of the channel to which they are able to gain access. As shown in table 6.2, this game is the reverse of the classic *Battle of the Sexes* game and is classified as an anti-coordination game where it is in both players' interest not to end up selecting the same strategy.

6.4.2 Pure and Mixed Strategy Nash Equilibria

In this subsection we derive the game's solutions in the form of pure strategy Nash equilibria (PSNE) as well as the mixed strategy Nash equilibrium (MSNE) for our spectrum sharing anti-coordination game.

Definition 1: The *Pure Strategy Nash Equilibrium* [18] of the spectrum sharing game is an action profile $a^* \in A$ of actions, such that:

$$u(a_i^*, a_{-i}^*) \succeq u(a_i, a_{-i}^*), \quad \forall i \in K \quad (2)$$

where \succeq is a preference relation over payoffs of strategies a_i^* and a_i . The above definition means that for a_i^* to be a pure strategy NE, it must satisfy the condition that no player i has another strategy that yields a higher payoff than the one for playing a_i^* given that every other player plays their equilibrium strategy a_{-i}^* .

Table 6.2: Strategic form representation of a 2-player anti-coordination game

	a_k	a_j
a_k	$(0,0)$	(u_k, u_j)
a_j	(u_j, u_k)	$(0,0)$

Lemma 1: Strategy pairs (a_k, a_j) and (a_j, a_k) are pure strategy NE of the anti-coordination game.

Proof: Assume player 1 to be the row player and player 2 to be the column player in table 6.2. From equation 1 it follows that both u_k and u_j are positive values and therefore the payoffs for strategy pairs (a_j, a_k) and (a_j, a_k) are greater than the payoffs for strategy pairs (a_k, a_k) and (a_j, a_j) . Consider the payoff for strategy pair (a_j, a_k) from table 6.2. Given that the player playing strategy a_j continues to play this strategy, then from definition 1 for NE, it follows that the player playing strategy a_k does not have any incentive to change his choice to a_j i.e., it will

receive a smaller payoff of 0 if it switched to a_j . Therefore, (a_j, a_k) is a PSNE. The same argument can be applied to prove that the strategy pair (a_j, a_k) is the second PSNE of this game. ■

Definition 2: The *Mixed Strategy Nash Equilibrium* [18] of the spectrum sharing game is a probability distribution \hat{p} over the set of actions A for any player such that:

$$\hat{p} = \{p_1, p_2, \dots, p_k\} \in \mathbb{R}_{\geq 0}^k, \text{ and } \sum_{j=1}^k p_j = 1 \quad (3)$$

which makes the opponents indifferent about the choice of their strategies by making the payoffs from all of their strategies equal. Let α be the probability with which player 1 plays strategy a_k and $\beta = (1 - \alpha)$ be the probability of playing strategy a_j , then from the payoffs of table 6.2, the expected utility of player 2 for playing strategy a_k is given by:

$$EU_2(a_k) = \alpha u(a_k, a_k) + \beta u(a_j, a_k) = \alpha(0) + \beta(u_k) \quad (4)$$

Similarly, the expected utility of player 2 for playing strategy a_j is given by:

$$EU_2(a_j) = \alpha u(a_k, a_j) + \beta u(a_j, a_j) = \alpha(u_j) + \beta(0) \quad (5)$$

According to definition 2, player 2 will be indifferent about the choice of strategies when the expected utilities from playing strategies a_k and a_j are equal, i.e.,

$$EU_2(a_k) = EU_2(a_j) \quad (6)$$

Substituting equations 4 and 5 in equation 6, we have $\beta u_k = \alpha u_j$. Therefore:

$$\alpha = \frac{u_k}{u_k + u_j} \quad (7)$$

$$\beta = 1 - \alpha = \frac{u_j}{u_k + u_j} \quad (8)$$

The mixed strategy NE for the heterogeneous spectrum sharing game is given by the distribution $\hat{p} = \{\alpha, \beta\}$ of equations 7 and 8 which means that when both players select strategies a_k and a_j with probabilities α and β respectively, then their opponents will be indifferent about the outcomes of the play. To generalize, expected utility for every player in a K -channel heterogeneous spectrum sharing game is given as follows:

$$EU_m = \sum_{m=1}^k u_m p_m, \forall m \in K \quad (9)$$

where p_m represents the probability of a CRN selecting channel m and all other CRNs not selecting channel m . We will utilize equation 9 in section 6.5 for the fairness and efficiency analysis of the various game equilibria.

6.4.3 Centralized Correlated Equilibrium for 2-Player Game

Under pure and mixed strategy NE, it is assumed that the players choose their strategies independently and without any prior coordination. However as we demonstrate next, it is in every player's interest to coordinate their actions such that the outcomes are favorable to all players by avoiding. Players would maximize their utilities if somehow they could avoid ending up selecting the same channels. A coordination or the lack thereof, in selecting channels would essentially make it an *anti-coordination* game. Such a coordination to avoid selecting same channels can be achieved with the help of a mutually trusted central entity that can provide all players with a recommendation signal. The external recommendation signals can either be public or private signals or they can even be learnt over a period of time eliminating the need for a central entity making possible its distributed implementation. In this subsection, we present the centralized algorithm to achieve the centralized correlated equilibrium (CE) for a 2-player, 2-

channel game while the distributed algorithm to achieve CE with a channel selection learning algorithm for an N -player K -channel game is presented in the next subsection.

Table 6.3: Joint probability distribution over strategies a_1 and a_2 .

	a_1	a_2
a_1	$p_{1,1}$	$p_{1,2}$
a_2	$p_{2,1}$	$p_{2,2}$

CE is a state in which, when given the availability of an external recommendation signal, none of the players can achieve a greater utility by ignoring that signal when all other players follow the recommended action. In other words, π is a correlated equilibrium if no strategy modification can result in an increase in a player's expected utility. Formally, CE is defined as:

Definition 3: A probability distribution π is a *Correlated Equilibrium* of a game when [19]:

$$\sum_{a_{-i} \in A_{-i}} \pi(a_i, a_{-i}) [u_i(a_i, a_{-i}) - u_i(a'_i, a_{-i})] \geq 0, \quad \forall i \in N \quad (10)$$

$\pi(a_i, a_{-i})$ is the joint probability distribution of players to select a certain strategy pair in the next time slot. The inequality (10) represents that selecting some different strategy a'_i instead of a_i in the next time slot will not result in a higher payoff for a player given that all other players adhere to the recommended strategy. In a centralized implementation of correlated equilibrium for a 2-player 2-strategy game such as the one shown in table 6.3, any external entity e.g., one of

the contending CRNs may be selected as the recommender that calculates and provides the external recommendation signal for all contending CRNs according to the CE joint probability distribution $\pi = (p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2})$. The strategic form of such a correlated strategy pair is shown in table 6.3. A correlated strategy pair means that the action pair (a_1, a_1) is played with probability $p_{1,1}$ and action pair (a_1, a_2) is played with probability $p_{1,2}$ etc.

Here we derive the centralized CE of the heterogeneous spectrum sharing game using a linear optimization approach. CE can be implemented for a multi-player game using linear optimization; however, with this method the number of constraints for CE grows exponentially with the number of players and their strategies and the problem grows at a polynomial rate [20]. Therefore, we derive centralized correlated equilibrium only for a 2-player game and consider the case for an N -player game in the next subsection when we present the case for a decentralized CE. Let the objective function J to find the optimal strategy CE for a 2-player game be defined as:

$$J = \max_{p_{i,j}} \sum_{i=1}^2 \sum_{j=1}^2 [u_1(a_i, a_j) + u_2(a_i, a_j)] \cdot p_{i,j} \quad (11)$$

where the constraints for CE in equation (11) are:

$$p_{1,1} + p_{1,2} + p_{2,1} + p_{2,2} = 1 \quad (12)$$

$$p_{1,1}[u_1(a_1, a_1) - u_1(a_2, a_1)] \geq p_{1,2}[u_1(a_2, a_2) - u_1(a_1, a_2)] \quad (13)$$

$$p_{2,1}[u_1(a_1, a_2) - u_1(a_2, a_2)] \geq p_{2,2}[u_1(a_1, a_2) - u_1(a_1, a_1)] \quad (14)$$

$$p_{1,1}[u_2(a_1, a_1) - u_2(a_1, a_2)] \geq p_{2,1}[u_2(a_2, a_2) - u_2(a_2, a_1)] \quad (15)$$

$$p_{1,2}[u_2(a_1, a_2) - u_2(a_1, a_1)] \geq p_{2,2}[u_2(a_2, a_1) - u_2(a_2, a_2)] \quad (16)$$

$$p_{1,2} = p_{2,1} \text{ and } p_{1,1} = p_{2,2} = 0 \quad (17)$$

For the game of tables 6.2 and 6.3, any correlated equilibrium of the form $\pi = (0, p, 1 - p, 0)$ will maximize the sum of expected payoffs for the players because it eliminates the possibility of the players contending for the same channel. For an egalitarian equilibrium which is fair and maximizes the sum of expected payoffs, we have an additional constraint defined as equation (17).

Having the recommender to provide external signal based on equation (11) and the constraints (12) to (17), ensures that probability of the two players ending up in the same channel is minimized so that the likelihood of spectrum opportunity wastage is also minimized and hence players' utilities can be maximized. It must be noted that the external recommendation signal is not binding and players are free to ignore recommended actions. The efficiency of avoiding the collision condition is achieved only because the players know that they will achieve higher payoffs by following the recommendation signal. This argument is explained with the help of following example.

Consider a situation in which the recommender selects an egalitarian CE probability distribution $\pi = (0, 1/2, 1/2, 0)$ over the payoff matrix of table 6.3 in order for the two players to avoid selecting the strategy pairs (a_1, a_1) and (a_2, a_2) . Suppose the external signal randomly recommends player 1 to select action a_2 i.e., channel 2 which is of lower quality and results in a smaller payoff of 7 compared with a payoff of 9 if channel 1 was selected for next time slot. Player 1 knows that player 2 will follow the recommended action because it has been recommended a higher quality channel. It is however in player 1's interest to select the action

recommended by the external signal since it would yield a higher payoff of 7 instead of 0 if external signal is ignored and both players end up selecting the same higher quality channel.

6.4.4 Distributed Correlated Equilibrium for N-Player Game

CE for a 2-player game was derived in the previous subsection and in this subsection we consider the case for an N -player K -channel game and demonstrate how CE can be achieved in a distributed manner and without the need of any communication among the CRNs or an external recommendation signal. To this end, we propose a novel channel selection learning algorithm which is an adaptation of the No-Regret learning algorithm [17] to achieve CE. Channel selection learning algorithm is based on the concept of minimizing a CRN's regret in the hindsight for not selecting a particular channel in every time slot up to the current time t . Next we detail the working of the channel selection learning algorithm.

Channel Selection Learning Algorithm: Suppose that the heterogeneous spectrum sharing game \mathcal{G} is played repeatedly at every time slot $t = 1, 2, 3, \dots$ and every CRN knows the history of plays h_t of every other CRN up to time t because of being collocated. Given a history of play $h_t = (a_i^\tau)_{\tau=1}^t$ up to time t , every CRN calculates a probability $p_i^{t+1} \in \pi(A_i)$ of selecting the same channel a_i^τ for the next time slot. The probability for selecting a channel for the next time slot is calculated as follows: for every two different channel choices $a_i \in A_i$ and $a'_i \in A_i$ up to time t , if every CRN replaces channel a_i with channel a'_i every time that it was selected in the past then its utility for time τ will become:

$$\omega_i^\tau(a'_i) = \begin{cases} u_i^\tau(a'_i, a_{-i}^\tau) & \text{if } a_i^\tau = a_i \\ u_i^\tau(a_i^\tau) & \text{otherwise} \end{cases} \quad \forall i \in A \quad (18)$$

Then the average difference in a CRN's payoff up to time t is given by:

$$\delta_i^t(a'_i, a_i) = \frac{1}{t} \sum_{\tau=1}^t [\omega_i^\tau(a'_i) - u_i^\tau(a_i^\tau)] \quad (19)$$

and every player's average regret at time t is given by:

$$NR_i^t(a'_i, a_i) = [\delta_i^t(a'_i, a_i)]^+ \quad (20)$$

then the probabilities of selecting channels a_i and a'_i in the next time slot are a function of a CRN's average regret and given by:

$$p_i^{t+1}(a'_i) = \frac{1}{\mu} NR_i^t(a'_i, a_i) \quad (21)$$

$$p_i^{t+1}(a_i) = 1 - p_i^{t+1}(a'_i) \quad (22)$$

The parameter μ determines the amount of inertia that a CRN possesses in deviating from its current choice of a given channel and its value is constrained by $\mu > 2M_i(k - 1)$, such that k is the number of channels available for contention and M_i is the upper bound on $|u_i(\cdot)|$. Its value is independent of time as well as the play's history and also ensures that there is always a positive probability of staying in the same channel as in the previous time slot. As $t \rightarrow \infty$, the empirical probability distribution π over the N -tuples of strategies converges to the CE [20]. A summary of the Channel Selection learning algorithm is given in table 6.4.

Table 6.4: Channel Selection Learning Algorithm

Data: μ, M_i (upper bound on $|u_i(\cdot)|$)
Result: Every channel's prob. of being selected by every CRN for the next time slot.
Initialization: $p_i^1(a_i) \leftarrow \frac{1}{k_i}, \forall a \in A_i, t \leftarrow 1$

while CRNs contend for heterogeneous channels **do**

1. **for** every CRN **do**
2. Compute current Regret NR_i^t up to time t for not selecting channel $a'_i \in A$ as per equation (20);
3. Calculate p_i^{t+1} i.e., prob. of selecting channel a_i and all other channels a'_i for the next time slot as per equations (21) and (22);
4. $t \leftarrow t + 1$
5. **end for**

end while

6.5 Fairness and Efficiency of Derived Equilibria

Having demonstrated how CE can be achieved for an N -player (a_k, a_k) -channel game, we now provide an analysis on the fairness and efficiency of all of the equilibria derived. For the sake of clarity and easy analysis we consider the case of a 2-player 2-channel heterogeneous spectrum sharing game while the same arguments can be applied for analyzing an N -player K -channel scenario. There are three different types of equilibria computed in preceding subsections for the spectrum sharing heterogeneous game:

- Two pure-strategy NE for the anti-coordination game (a_k, a_j) and (a_j, a_k) .
- A mixed strategy NE defined by the probability distribution $\hat{p} = \{\alpha, \beta\}$ given by equations (7) and (8).

- A Correlated Equilibrium defined by the probability distribution $\pi = (0, p, 1 - p, 0)$ over joint strategy pairs of table 6.3 given by equation (11) and constrained by equations (12) to (17).

Price of Anarchy: To analyze the efficiency of these equilibria, we first introduce Price of Anarchy (POA) [21], a measure of degradation due to selfish behavior of non-cooperating players in a system. Let $S \subseteq A$ be a set of strategies in equilibrium such that S_P, S_M and S_C refer to the sets of strategies in pure strategy NE, mixed strategy NE, and CE for the heterogeneous spectrum sharing game, respectively. We define the measure of efficiency of the game as a utility function $F: S \rightarrow \mathbb{R}$ such that

$$F(a) = \sum_{i=1}^{|M|} u_i(a) \quad (23)$$

then POA is defined as the ratio between optimal efficiency and the worst equilibrium efficiency of the game, as follows:

$$POA = \frac{\arg \max_{a \in A} F(a)}{\arg \min_{a \in S} F(a)} \quad (24)$$

where the strategies $a \in S$ represent progressively higher efficiency as POA approaches 1.

Optimal Efficiency: The heterogeneous spectrum sharing game will result in optimum efficiency when all of the contending CRNs always select different channels i.e., they are able to avoid contention for the same channel which would result in a collision and zero payoff. In the presence of selfish players, such optimality is only possible with a correlated choice of strategies as well as fair distribution of spectrum resource. When these conditions are satisfied then the

maximum value of the utility function $F(a)$ is given as the sum of utilities of all channels as follows:

$$\text{arg max}_{a \in A} F(a) = \sum u_m, \forall m \in K \quad (25)$$

Next we discuss the fairness of equilibria as well as their efficiency by deriving the worst equilibrium efficiencies and comparing them with optimal efficiency of the game as per equation (25).

PoA with Pure Strategy Nash Equilibria: As assumed previously in section 6.3.1, channel k is of higher quality than channel j therefore $u_k > u_j$. Then from the payoff matrix of table I, gaining access to channel k brings a larger payoff to a CRN whereas being of comparatively lower quality, channel j brings a smaller payoff. There are two pure-strategy Nash equilibria (a_k, a_j) and (a_j, a_k) , however both of them are unfair because $u_k \neq u_j$ and one player always gets a smaller payoff than the other. Since the game is a non-cooperative game and every player is interested in maximizing its own payoff, all of them will end up selecting the larger payoff channels resulting in contention and collision in every time slot and hence zero payoffs. As a result PoA is not defined in the context of PSNE of this game and therefore, PSNE is not a practical solution for this game.

PoA with Mixed Strategy Nash Equilibrium: MSNE of our spectrum sharing game is the probability distribution $\hat{p} = \{\alpha, \beta\}$ given by equations (7) and (8). Since the expected utilities EU_i given by equation (9) for all players are equal when they mix their strategies according to the distribution \hat{p} , we can conclude that MSNE is fair.

We now derive *PoA* for the game to be able to determine its efficiency under MSNE. There is only one MSNE of the game therefore, minimum value of the utility function $F(a)$ under MSNE is the sum of expected utilities of every player from equation (9) and is given by:

$$\arg \min_{a \in S_m} F(a) = |N| \cdot u_i \sum_{m=1, m \neq i}^{|K|} p_m, \forall i \in N \quad (26)$$

and the price of anarchy under MSNE is given by

$$PoA_M = \frac{\sum_{m=1}^{|K|} u_m}{|N| \sum_{m=1, m \neq i}^{|K|} u_i p_m} \quad (27)$$

by substituting equation (23) and (26) in (24).

PoA with Correlated Equilibrium: The correlated equilibrium (CE) of a 2-player 2-channel spectrum sharing game is defined by the probability distribution of tuple $\pi = (0, p, 1 - p, 0)$ over joint strategy pairs constrained by equation (18). Equations (18) to (22) represent the channel selection learning algorithm implemented to achieve CE for an N -player K -channel scenario. Correlation in the choice of strategies ensures that the probability of players selecting the same channel for contention is minimized so that the spectrum opportunity is not wasted due to collision and players' payoffs are maximized. As demonstrated in next section, the NR algorithm takes some time to converge to CE during which they may select the same channels resulting in collisions. However after convergence, the contending CRNs *never* select the same channel thus wastage of spectrum opportunities is avoided altogether and all channels are utilized to the maximum. Therefore, minimum value of the utility function $F(a)$ under CE is the sum of expected utilities of every player given as:

$$\arg \min_{a \in S_C} F(a) = \sum_{m=1}^{|K|} u_m \quad (28)$$

and PoA under CE is given as:

$$PoA_C = \frac{\sum_{m=1}^{|K|} u_m}{\sum_{m=1}^{|K|} u_m} = 1 \quad (29)$$

Discussion: Under the constraint for the MSNE probabilities of selecting different channels $0 < p_m < 1$ and $\sum_{m=1}^{|K|} p_m = 1$, minimum value of the utility function $F(a)$ in equation (26) will always be smaller than 1. This means that PoA under MSNE of equation (27) will always be greater than 1. On the other hand CE has a price of anarchy equal to 1 which according to its definition is the most efficient case. This is a clear evidence of CE not only being fair but also the most efficient solution for the problem of heterogeneous spectrum sharing game.

6.6 Simulations and Results

6.6.1 Simulation Setup

For the purpose of validating the effectiveness of CE, we implemented our proposed anti-coordination game along with the channel selection learning algorithm. We verify that CE is achievable, fair and efficient as it always yields a higher expected utility per CRN as compared with MSNE. For the purpose of simulation, n represents the number of CRNs and k represents the number of channels in the spectrum available for secondary access by the CRNs. We first carry out the comparison of CE and MSNE with a 2-player 2-channel game i.e., $n = 2$ and $k = 2$ and calculate expected utilities per CRN.

We have also carried out simulations with varying number of CRNs and channels and demonstrate that the game always converges to CE. Since the channel selection learning algorithm approaches CE based solely on a given network's own payoff observations in combination with the common knowledge of the entire CRN population, it allows the distributed implementation of our proposed anti-coordination game. Inertia parameter of the channel selection learning algorithm is μ whose value is kept constant for all simulations except for the simulation of figure 6.3 in which we demonstrate the effect of changing the values of μ . In rest of the simulations, it can be observed that the convergence rate to equilibrium decreases as the number of CRNs increases which is intuitive.

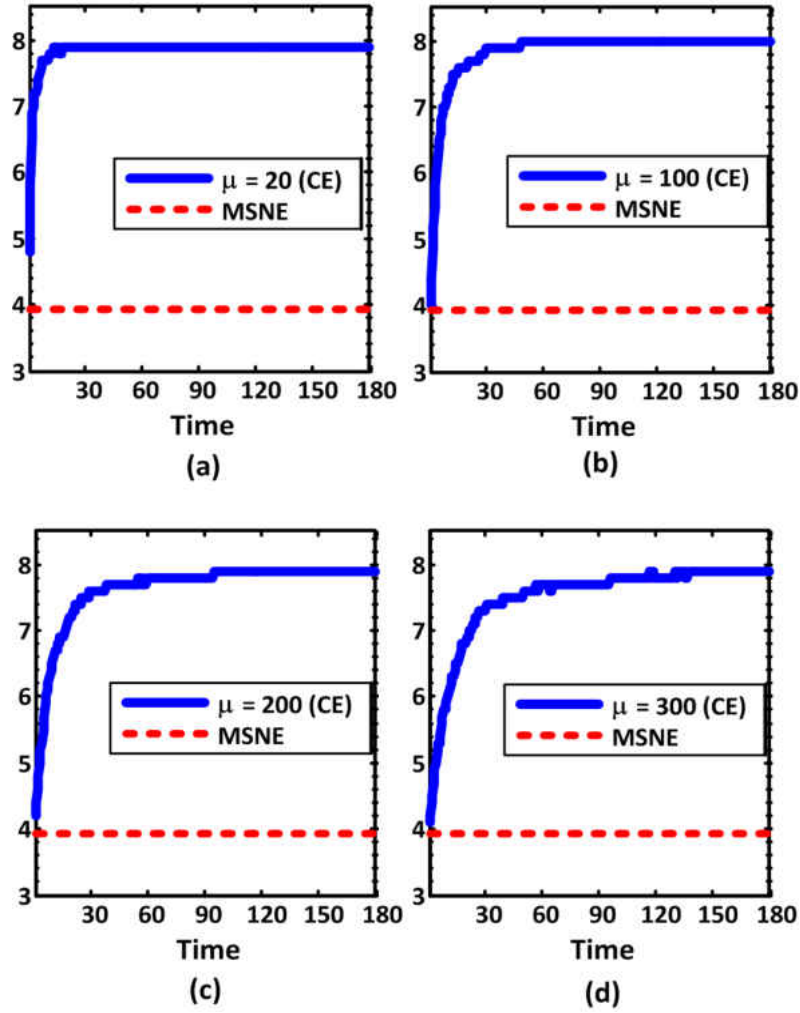


Figure 6.2: Expected utilities per CRN for $n = 2$ and $k = 2$, and utilities from the two channels are: $u_1 = 9$ \$ and $u_2 = 7$ with varying inertia parameter μ . (a) $\mu = 20$, (b) $\mu = 100$, (c) $\mu = 200$ and (d) $\mu = 300$. Different values of μ achieve the same convergence value of expected utility however as inertia increases, it causes a decrease in convergence rate.

6.6.2 Simulation Results

Figure 6.2 shows a comparison of expected utilities per CRN under MSNE and CE with various values for the inertia parameter μ . Payoff value for channel 1 is $u_1 = 9$ while channel 2 has a payoff of $u_2 = 7$. Compared with all the four plots for CE in figure 6.3 where the expected

utilities converge to 8 per CRN, MSNE yields a smaller expected utility of 3.93 per CRN, proving our analysis that CE is more efficient than MSNE. Different values of μ achieve CE at different rates however the convergence values are identical. As evident from figure 6.2, μ being the inertia parameter, reflects a CRN's propensity towards staying in the same channel in next time as the previous one.

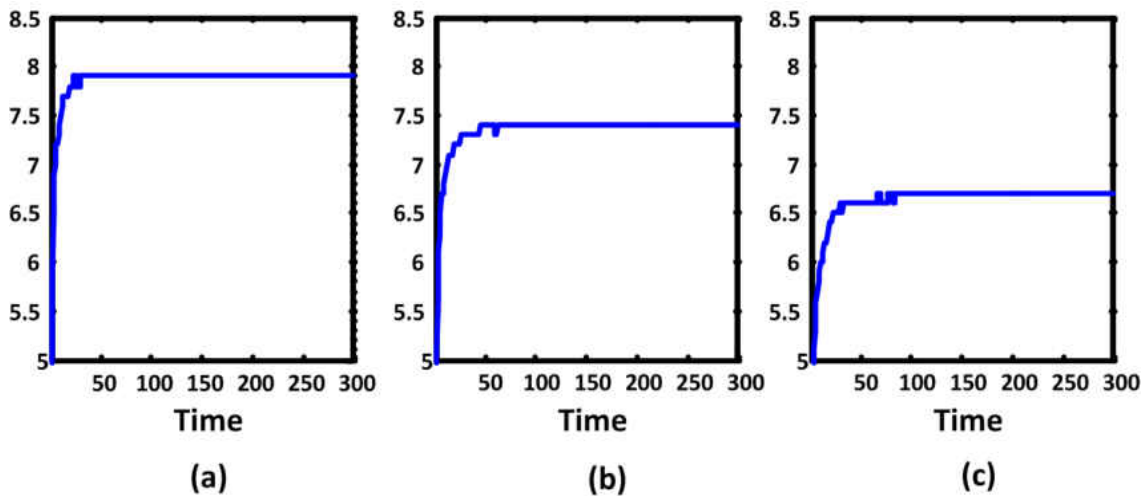


Figure 6.3: Comparison of CE at different values of the number of networks (n) and channels (k). Y-axes represent expected utility per CRN. For this simulation $n = k$ where (a) $n = k = 2$, (b) $n = k = 3$ and (c) $n = k = 4$ such that $u_1 = 9, u_2 = 7, u_3 = 6$ and $u_4 = 5$.

Figure 6.3 shows a comparison of CE at different values of the number of networks (n) and channels (k). For this simulation, the number of CRNs is kept the same as the number of channels available for contention i.e., $n = k$ such that utilities of the channels are $u_1 = 9, u_2 = 7$ and $u_3 = 6$. With every additional CRN, a *lower* quality channel was added to the spectrum resulting in smaller expected utility per CRN and slower convergence to equilibrium.

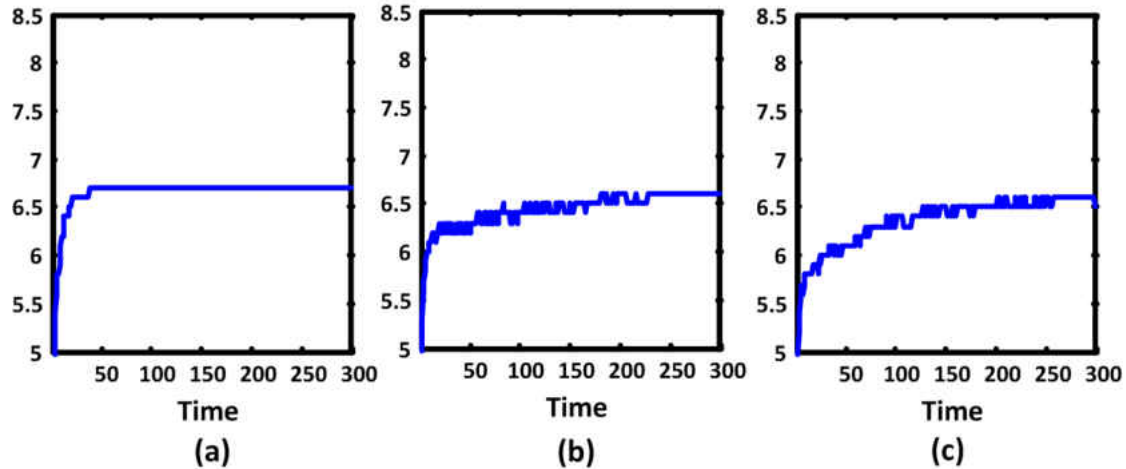


Figure 6.4: Comparison of CE when $k \geq n$ and number of networks is kept fixed. Y-axes represent expected utility per CRN. (a) $k = n = 4$, (b) $k = 5, n = 4$, (c) $k = 6, n = 4$. CRNs always select the best out of the available pool of channels therefore the convergence value of expected utilities are equal however convergence rate increase as $n \rightarrow k$.

Figure 6.4 shows the CE for expected utilities per CRN over time such that $k \geq n$ i.e., increasing the number of available channels from 4 to 6 while keeping the number of contending CRNs constant at 4. Notice that the convergence value for expected utility is the same for all cases. It shows a very important aspect of the channel selection learning algorithm which allows CRNs to always have a fair as well as an efficient distribution of channel resources as players choose the highest quality channels from the pool of available channels. Also, the speed of convergence to CE is fastest when the number of CRNs is equal to the number of available channels i.e., $n = k$. Payoff values for channels 1 through 6 for this simulation are kept at 9, 7, 6, 5, 4 and 3 respectively.

Figures 6.5 (a), (b) and (c) show the CE for expected utilities per CRN over time such that $n \leq k$ i.e., decreasing the number of CRNs from 4 to 2 while keeping the number of available channels constant at 4. Intuitively, expected utility per CRN is lowest at $n = 4$ and $k = 4$ as compared with the situation when the number of contending networks is smaller however, the speed of convergence to CE is fastest when $n = k$. Payoff values for channels 1 through 4 are 9, 7, 6 and 5 respectively.

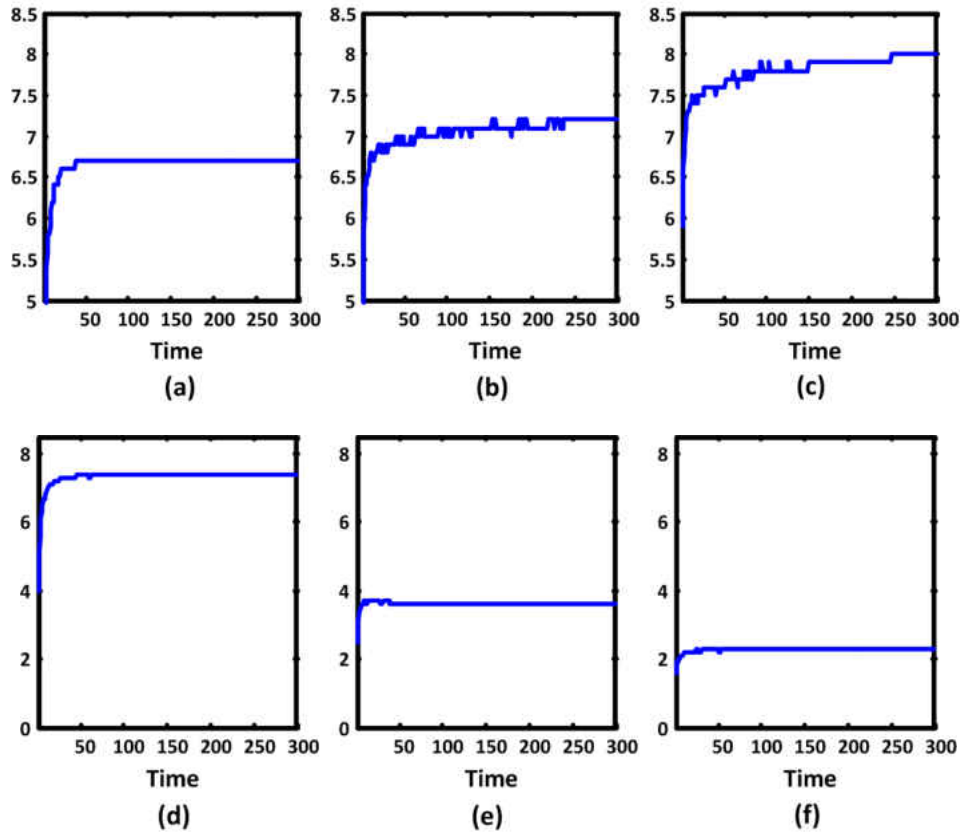


Figure 6.5: (a), (b) and (c) $n \leq k$ and number of networks is kept fixed. Y-axes represent expected utility per CRN. (a) $k = n = 4$, (b) $k = 3, n = 4$, (c) $k = 2, n = 4$. Decrease in number of networks results in an increase in expected utilities and convergence rate decreases as the number of channels increases. (d), (e) and (f) $n \geq k$ and number of channels is kept fixed. Y-axes represent expected utility per CRN. (a) $k = n = 2$, (b) $k = 2, n = 3$, (c) $k = 2, n = 4$. Increase in number of networks results in a corresponding decrease in expected utility per CRN however the convergence rate decreases as the number of channels increases.

Finally, figures 6.5 (d), (e) and (f) show the results of simulation when $n \geq k$ and the number of channels is kept fixed while the number of contending CRNs is increased. It shows that as soon as the number of CRNs contending for channels becomes more than the number of channels available, there will always be at least one collision between two or more CRNs in every time slot making the expected utility per CRN to drop significantly. However, the channel selection learning algorithm still manages to achieve CE despite much degraded expected utilities per CRN.

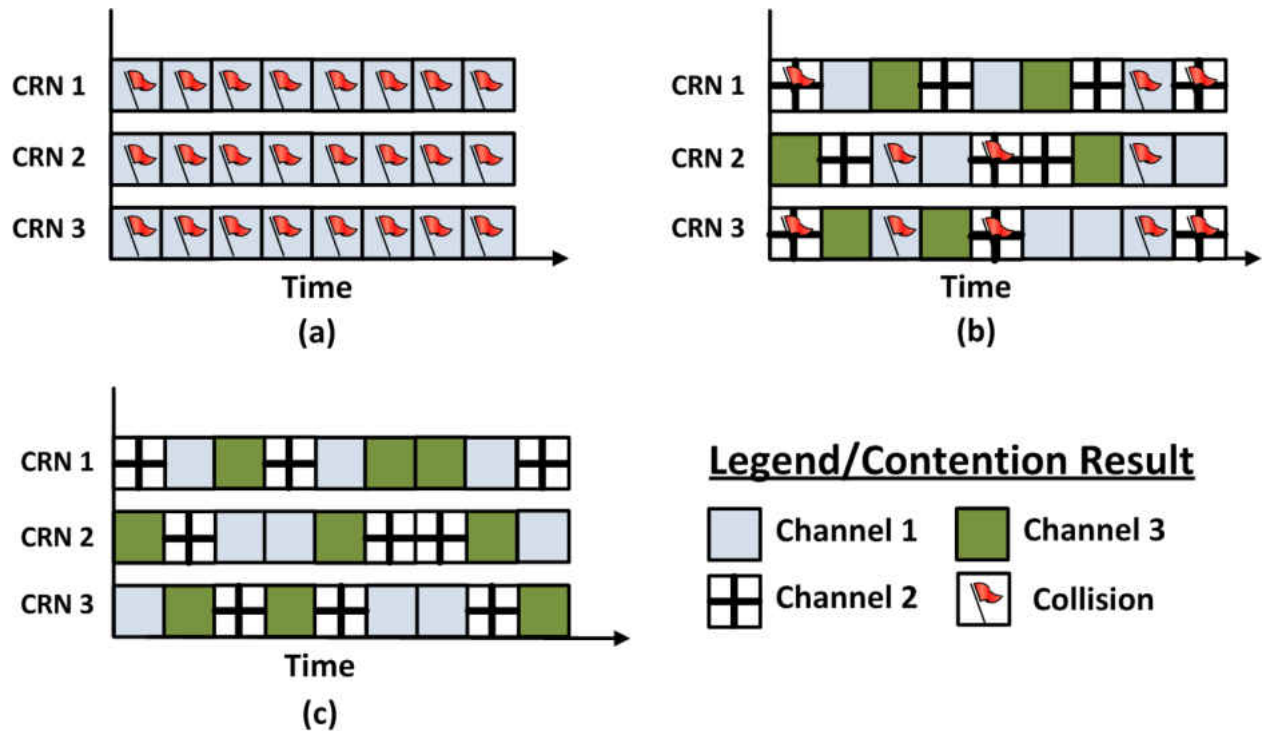


Figure 6.6: Channel access pattern of CRNs. (a) Selfish behavior from CRNs for best quality channel (channel 1) will always result in a collision. (b) Fair distribution of spectrum resource when CRNs mix their choice of channels according to MSNE. However, MSNE is inefficient because of collisions and wasted opportunities. (c) Fair and efficient resource distribution with Correlated Equilibrium.

Figure 6.6 illustrates the non-cooperative behavior from CRNs for self coexistence and the improvement that can be achieved with our proposed channel selection learning algorithm. Figure 6.6(a) shows how selfish behavior may result in collision and wastage of spectrum resource. figure 6.6(b) depicts a scenario where MSNE results in a fair yet inefficient spectrum utilization while figure 6.6(c) shows performance improvement achieved through CE.

6.7 Conclusions

Coexistence protocols employed by collocated CRNs usually do not take into consideration the fact that spectrum bands vary significantly with regards to channel quality thereby making some channels of the spectrum bands more attractive to CRNs than others. We aimed at solving the problem of sharing heterogeneous spectrum by adopting a game theoretic approach. By analyzing the system's efficiency and fairness with the help of *price of anarchy*, we demonstrated that correlated equilibrium solves the problem of inefficiency and unfairness associated with the game solutions of pure and mixed strategy Nash equilibria. Furthermore, to address the problems associated with a centralized implementation, we proposed the use of a novel channel selection learning algorithm that enables the CRNs to achieve correlated equilibrium in a distributed manner.

6.8 References

[1] U.S. FCC, ET Docket 04-186, “*Notice of proposed rule making, in the matter of unlicensed operation in the TV broadcast bands,*” May 25, 2004.

- [2] T. M. Taher, R. B. Bacchus, K. J. Zdunek, D. A. Roberson, “*Long-term spectral occupancy findings in Chicago*,” IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2011.
- [3] IEEE 802.22TM 2011 Standard for Wireless Regional Area Networks in TV Whitespaces, <http://www.ieee.org/22>
- [4] P. Sroka, A. Kliks, “*Distributed Interference Mitigation in Two-Tier Wireless Networks Using Correlated Equilibrium and Regret-Matching Learning*,” European Conference on Networks and Communications (EuCNC), 2014.
- [5] J. Zheng, Y. Cai; D. Wu, “*Subcarrier allocation based on correlated equilibrium in multi-cell OFDMA systems*,” EURASIP Journal on Wireless Communications and Networking, 2012.
- [6] J. W. Huang, V. Krishnamurthy, “*Cognitive Base Stations in LTE/3GPP Femtocells: A Correlated Equilibrium Game-Theoretic Approach*,” IEEE Transactions on Communications, 2011.
- [7] S. Maharjan, Y. Zhang, C. Yuen, S. Gjessing, “*Distributed Spectrum Sensing in Cognitive Radio Networks with Fairness Consideration: Efficiency of Correlated Equilibrium*,” IEEE Mobile Adhoc and Sensor Systems (MASS), 2011.
- [8] B. Wang, Z. Han, K.J.R. Liu, “*Peer-to-peer file sharing game using correlated equilibrium*,” 43rd Annual Conference on Information Sciences and Systems, IEEE CISS 2009.
- [9] S. Sengupta, R. Chandramouli, S. Brahma, M. Chatterjee, “*A game theoretic framework for distributed self-coexistence among IEEE 802.22 networks*,” IEEE GLOBECOM 2008.
- [10] R. Etkin, A. Parekh, D. Tse, “*Spectrum sharing for unlicensed bands*,” IEEE Journal on Selected Areas in Communications (JSAC), vol.25, no.3, pp.517,528, April 2007.
- [11] C. Jiang, Y. Chen, Y. Gao, K. J. Ray Liu, “*Joint spectrum sensing and access evolutionary game in cognitive radio networks*,” IEEE Transactions on Wireless Communications, vol.12, no.5, May 2013.

- [12] S. Sengupta, S. Brahma, M. Chatterjee, N. Shankar, “*Self-coexistence among interference-aware IEEE 802.22 networks with enhanced air-interface,*” *Pervasive and Mobile Computing*, Volume 9(4), August 2013.
- [13] M. Faisal Amjad, M. Chatterjee, C.C. Zou, “*Inducing Voluntary Cooperation for Optimal Coexistence in Cognitive Radio Networks: A Game Theoretic Approach,*” *IEEE Military Communications Conference (Milcom)* 2014.
- [14] Z. Han, C. Pandana, K.J.R. Liu, “*Distributive Opportunistic Spectrum Access for Cognitive Radio using Correlated Equilibrium and No-Regret Learning,*” *Wireless Communications and Networking Conference, IEEE WCNC* 2007.
- [15] Google, Inc.'s TV Bands Database System for Operation, ET Docket No. 04-186 <http://www.google.com/get/spectrumdatabase/channel/>
- [16] Show My White Space –TVWS database from Spectrum Bridge Inc. <http://whitespaces.spectrumbridge.com/whitespaces/home.aspx>
- [17] S. Hart, A. Mas-Colell, “*A simple adaptive procedure leading to correlated equilibrium,*” *Econometrica*, vol. 68, no. 5, pp. 1127-1150, September 2000.
- [18] D. Fudenberg, J. Tirole, “*Game Theory,*” The MIT press, 1991.
- [19] R. J. Aumann, “*Correlated equilibrium as an expression of Bayesian rationality,*” *Econometrica*, vol. 55, no. 1, pp. 1 - 18, January 1987.
- [20] C. H. Papadimitriou, T. Roughgarden, “*Computing correlated equilibria in multi-player games,*” *Journal of the ACM* 55(3), August 2008.
- [21] Y. Shoham, K. Leyton-Brown, “*Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations*” Cambridge University Press 2008.

CHAPTER 7: CONCLUSION

CRNs are a perfect solution to the problems of having a wide gap between the demand and supply of wireless spectrum resource coupled with the fact that fixed spectrum allocation has caused its severe under-utilization. The gap is bridged by CRNs by utilizing DSA to enable secondary, unlicensed access to spectrum bands otherwise licensed to PUs, in an opportunistic and non-interfering basis. This communication paradigm however comes with its own set of challenges and this dissertation has addressed some of them. Specifically, we have provided a wide range of solutions to handle degradation in TCP's throughput resulting from opportunistic spectrum access, SSDF as well as jamming attacks and sharing of heterogeneous spectrum resources among collocated CRNs to induce cooperation among otherwise non-cooperative CRNs.

The contributions of this dissertation are as follows:

- Design of two cross-layer mechanisms to boost TCP's throughput that may be degraded because of network-wide quiet periods enforced for spectrum sensing, opportunistic and dynamic spectrum access, and non-deterministic operation of PUs.
- Design of a novel framework for collaborative spectrum sensing for ad hoc cognitive radio networks under byzantine SSDF attacks. The framework incorporates a spatio-spectral anomaly detection system that functions in conjunction with a reputation system to detect malicious nodes in the CRN.

- Designed a novel adaptive defense framework called DS3 which enables the IEEE 802.22 based CRNs to thwart smart jamming attacks as well as improve spectrum utilization by SUs under noisy channel conditions.
- Designed an evolutionary game theoretic approach to enable collocated and independent CRNs to evolve a strategy that would ensure long term coexistence with *fair* distribution of heterogeneous spectrum resources in a distributed manner.
- Designed another game theoretic approach based on the concept of Correlated Equilibrium which ensures that the distribution of heterogeneous spectrum resources is not only fair but also *optimal* in the long term. To that end, both centralized as well as distributed solutions are presented utilizing linear optimization and machine learning techniques.