Novel Approaches for the Performance Enhancement of Cognitive Radio Networks

Kenneth Ugonna Ezirim

Graduate Center, City University of New York

Recommended Citation
https://academicworks.cuny.edu/gc_etds/916

How does access to this work benefit you? Let us know!
Follow this and additional works at: https://academicworks.cuny.edu/gc_etds

This Dissertation is brought to you by CUNY Academic Works. It has been accepted for inclusion in All Dissertations, Theses, and Capstone Projects by an authorized administrator of CUNY Academic Works. For more information, please contact deposit@gc.cuny.edu.
Novel Approaches for the Performance Enhancement of Cognitive Radio Networks

by

Kenneth Ugonna Ezirim

A dissertation submitted to the Graduate Faculty in Computer Science in partial fulfillment of the requirements for the degree of Doctor of Philosophy,
THE CITY UNIVERSITY OF NEW YORK

2015
© 2015
KENNETH UGONNA EZIRIM
All Rights Reserved
This manuscript has been read and accepted by the Graduate Faculty in Computer Science in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

Professor Ping Ji

__________________________________________
Date Chair of Examining Committee

Professor Robert M. Haralick

__________________________________________
Date Executive Officer

Professor Ping Ji
Professor Theodore Brown
Professor Shweta Jain
Professor Shamik Sengupta
Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK
Abstract

Novel Approaches for the Performance Enhancement of Cognitive Radio Networks

by

Kenneth Ugonna Ezirim

Adviser: Professor Ping Ji

This research is dedicated to the study of the challenges faced by Cognitive Radio (CR) networks, which include self-coexistence of the networks in the spectral environment, security and performance threats from malicious entities, and fairness in spectrum contention and utilization. We propose novel channel acquisition schemes that allow decentralized CR networks to have multiple channel access with minimal spectrum contentions. The multiple channel acquisition schemes facilitate fast spectrum access especially in cases where networks cannot communicate with each other. These schemes enable CR networks to self-organize and adapt to the dynamically changing spectral environment.

We also present a self-coexistence mechanism that allows CR networks to coexist via the implementation of a risk-motivated channel selection based deference structure (DS). By forming DS coalitions, CR networks are able to have better access to preferred channels and can defer transmission to one another, thereby mitigating spectrum conflicts.

CR networks are also known to be susceptible to Sybil threats from smart malicious radios with either monopolistic or disruptive intentions. We formulate novel threat and defense mechanisms to combat Sybil threats and minimize their impact on the performance of CR networks. A dynamic reputation system is proposed that considerably minimizes the effectiveness of intelligent Sybil attacks and improves the accuracy of spectrum-based decision-making processes.
Finally, we present a distributed and cheat-proof spectrum contention protocol as an enhancement of the adaptive On-Demand Spectrum Contention (ODSC) protocol. The Modified On-Demand Spectrum Contention (MODSC) protocol enhances fairness and efficiency of spectrum access. We also show that there is substantial improvement in spectrum utilization with the incorporation of channel reuse into the MODSC protocol.
Acknowledgments

In the vastness of space and immensity of time, it is with tremendous joy that I wish to express my gratitude to all those who helped and supported me on this long but fulfilling path in life.

First and foremost, I am very grateful to my advisor Ping Ji for her thoughtful conversations, advice, and support. Exceptional thanks go to my former advisor, Shamik Sengupta, for all his help, direction and guidance throughout the course of this journey. I cannot express my gratitude enough to other members of my committee, Theodore Brown and Shweta Jain, for their continued support and encouragement. I offer my sincere appreciation for the learning opportunities, guidance and advice that you provided at different times in different capacities.

I would like to recognize David Guy Brizan, Ligon Liu, Peter Terlecky, Vasiliki Mitsou, Milinda Perera, Hannah Aizenman, Kenville Thompson, Deepak Tosh and Tayfun Pay for their great friendship and support. It has been a pleasure sharing graduate student experience with you all.

Finally, the largest serving of gratitude goes to my parents Adolphus and Grace Ezirim, who laid the foundation for my curiosity and pursuit of knowledge. Your parental advice, encouragement and support kept me going, even in toughest times. Your sacrifices are very much appreciated and duly noted. Thanks to my cousin Jennifer and her husband for their moral support.
To all without whose never-failing support and encouragement this dissertation would not have been complete, I say big thank you from the bottom of my heart...
Contents

1 Introduction

1.1 An Overview of Dynamic Spectrum Access 2
1.2 Cognitive Radio Technology 4
1.3 Motivation 6
1.4 Related Works
  1.4.1 Self-coexistence in CR networks 9
  1.4.2 Coalition Formation in Wireless Networks 10
  1.4.3 Spectrum Contention Protocols 11
  1.4.4 Sybil Attacks in Cognitive Radio Networks 12
1.5 Contributions
  1.5.1 Multi-Channel Selection in a Decentralized Network Setting 15
  1.5.2 Self-coexistence using Risk-Motivated Deference Structure 16
  1.5.3 Sustenance against Intelligent Sybil Attacks using Dynamic Reputation System 17
  1.5.4 Modified On-Demand Spectrum Contention Protocol 18
CONTENTS

2 Multiple Channel Acquisition in Decentralized System of Cognitive Radio Networks

2.1 Introduction .......................................................... 20
2.2 Multi-Channel Acquisition Heuristics .............................. 23
   2.2.1 RENO Heuristics .................................. 25
   2.2.2 TAHOE Heuristics .................................. 26
   2.2.3 LINEAR Heuristics .................................. 27
   2.2.4 Dynamic Incremental Heuristics ................. 27
   2.2.5 Find-and-Keep Heuristics ..................... 28
2.3 Channel Ranking Algorithm ..................................... 31
2.4 Estimating Spectrum Contention on a Channel .................. 33
2.5 Experimental Results ........................................... 41
   2.5.1 Experimental Results I ............................ 43
   2.5.2 Experimental Results II ............................ 50
2.6 Conclusion ......................................................... 55

3 Distributed and Cheat-proof Spectrum Contention Scheme for IEEE 802.22 Wireless Regional Area Networks

3.1 Introduction ......................................................... 57
3.2 System Model ...................................................... 59
3.3 On-Demand Spectrum Contention Protocol .................... 61
   3.3.1 Vulnerabilities of ODSC Protocol ................. 63
3.4 Modified ODSC Protocol ........................................ 64
3.5 Spectrum Contention Resolution Schemes .................... 67
   3.5.1 Contention Window Manipulation .................. 68
   3.5.2 MODSC Spectrum Contention Resolution Schemes .... 71
CONTENTS

3.5.3 Non-Cheatability and Collision-Proof of MODSC .......................... 73
3.5.4 Channel Reuse ........................................................................... 75

3.6 Numerical Results ........................................................................ 77
3.6.1 Fairness in ODSC System ............................................................ 78
3.6.2 MODSC Performance in Different Network Topologies .............. 79
3.6.3 Performance Comparison of ODSC and MODSC ...................... 80

3.7 Conclusion .................................................................................... 84

4 Enabling Self-Coexistence through Risk Motivated Deference Structure Formation

4.1 Introduction .................................................................................. 86
4.2 Deference Structure Model ............................................................. 88
  4.2.1 Implementation of Deference Structure ..................................... 90
  4.2.2 Deference Structure Protocol ................................................... 91
4.3 Estimating Utility in Deference Structure Model ............................ 93
4.4 Spectrum Contention Risk Assessment ........................................... 98
  4.4.1 Spectrum Contention Risk ......................................................... 99
  4.4.2 Risk as Expected Loss ............................................................... 100
  4.4.3 Risk-Motivated Channel Selection Scheme ............................... 102
  4.4.4 Deference Structure Coalition Formation as a Game ................. 104
  4.4.5 Stability of Deference Structures .............................................. 109
4.5 Numerical and Simulation Results .................................................. 110
  4.5.1 Impact of Deference Structure Mechanism on System Performance . 111
  4.5.2 Impact of Coalition Size on Average Network Utility and Contention 115
4.6 Conclusions .................................................................................. 118
5 Mitigating against Intelligent Sybil Attacks using a Dynamic Reputation System

5.1 System Model ................................................................. 121
5.2 The Sybil Attacker ........................................................... 122
  5.2.1 Sybil Attacker Learning Strategy .................................... 123
  5.2.2 Identity Ranking Algorithm ........................................... 126
  5.2.3 Identity Sampling Strategies ......................................... 126
5.3 Dynamic Reputation System ............................................ 128
  5.3.1 Reputation Function .................................................. 129
  5.3.2 Spectrum Decision Making .......................................... 131
5.4 Fuzzy Logic Control ....................................................... 134
5.5 Numerical and Experimental Results ................................. 140
  5.5.1 Fuzzy Logic Control of $\lambda$ ...................................... 141
  5.5.2 Comparing Linear and Dynamic Reputation Systems ............ 142
  5.5.3 Comparison of Output Membership Functions .................... 144
  5.5.4 Performance of RL based Sybil Attack ............................ 146
  5.5.5 Comparison of Identity Sampling Strategies ....................... 149
  5.5.6 Comparison of Decision Making Mechanisms ...................... 151
5.6 Conclusions ................................................................. 153

6 Conclusions ................................................................. 154

Bibliography ................................................................. 156
List of Figures

1.1 A cross-section of a channel with multiple spectrum decision [1]. 4

2.1 Channel Acquisition 22
2.2 Cumulative distribution function of $n$ coexisting networks with $m = 12$ channels. 41
2.3 Projected probability distribution function of $n$ coexisting networks with $m = 12$ channels. 42
2.4 The diagram describes the expected system utility in a case where primary users absent in the spectrum. 45
2.5 A plot that illustrates actual to expected ratio of system utility and variations in utilization rate with regards to available spectrum resources. 46
2.6 Performance comparison of INCR heuristics as it applies in the absence and presence of primary users. 47
2.7 Variation of spectrum contention with the number of networks. 48
2.8 An illustration of the utility per contention experienced in the system. This shows that for a large system of networks, utility-per-contention is invariant to the heuristics implemented. 48
2.9 Convergence time of multiple channel acquisition heuristics with primary user absent. 49
2.10 Impact of primary users presence on the convergence times of RENO and LINEAR heuristics .......................... 50
2.11 Comparison of all proposed multiple channel acquisition heuristics with CFL based on convergence time ......................................................... 51
2.12 Comparison of CFL and FAK heuristics with the system having the exact number of channels to satisfy the networks’ channel size requirements ................................................................. 52
2.13 Performance comparison of CFL and FAK algorithms based on convergence time in small network configuration ......................................................... 53
2.14 Performance comparison of CFL and FAK algorithms based on convergence time in large network configuration ......................................................... 53
2.15 Comparison of spectrum contention in CFL to their worst case of spectrum contention ......................................................... 54
2.16 Comparison of spectrum contention in FAK to their worst case of spectrum contention ......................................................... 55
3.1 Finite state machine diagram of spectrum contention in 802.22 WRAN networks ......................................................... 58
3.2 A typical system of WRAN networks ......................................................... 60
3.3 A diagram illustrating conventional ODSC protocol ......................................................... 62
3.4 An illustration of MODSC spectrum contention protocol ......................................................... 66
3.5 Network topologies used in simulating ODSC and MODSC spectrum contention scenarios ......................................................... 77
3.6 Variation of fairness with malicious transition probability ......................................................... 79
3.7 Average system utility derived in MODSC system ......................................................... 80
3.8 An illustration of a typical ODSC spectrum contention scenario ......................................................... 81
3.9 MODSC Spectrum contention scenario ......................................................... 82
3.10 Performance comparison of ODSC and MODSC in cycle network topology ......................................................... 83
3.11 Performance comparison of ODSC and MODSC in wheel network topology. 84

4.1 This diagram illustrate deference structure coalition formation model. The dashed colored lines identifies the different DS coalitions that exist between secondary users in the system. 89

4.2 A finite state diagram illustrating the deference structure coalition formation process. 92

4.3 Deference structure coalition formation process. 94

4.4 Variation of probability of spectrum contention with $n$ and $m$. 109

4.5 An illustration of the difference in performance between systems in DS and NDS modes. In each mode, the number of networks $N = 12$ and networks are free to join any arbitrary deference structure to satisfy channel requirement and mitigate spectrum contention. 111

4.6 An illustration of deference structure formation constraints. Network $N5$ is not allowed to join multiple deference structures formed on channel $CH3$. 112

4.7 A comparison of system performance in DS and NDS mode. A significant improvement is observed for networks that join deference structure. 113

4.8 Percentage increase in network utility with the emergence of DS coalitions. 114

4.9 Comparison of insider and outsider networks performance based on utility rate. 116

4.10 Variation of system’s contention and utility rates with DS coalition sizes. 117

4.11 Performance comparison of different DS coalition sizes with varying $M$, number of spectrum bands. The performance reaches a peak when $\kappa \approx M$. 118

5.1 Sliding Window Identity Sampling Strategy with $k = 3$. 127

5.2 Reputation function curves for different $\lambda$ values $(L = \lambda)$. 130

5.3 Architecture of a fuzzy logic controller for $\lambda$ control. 135

5.4 Membership functions of input variable $\lambda$. 136
5.5 Membership functions of input variable $\mu$. ................................. 137
5.6 BellShape membership functions for output variable $\Delta \lambda$. ........................ 139
5.7 Triangular membership functions for output variable $\Delta \lambda$. ........................ 140
5.8 Time series plot of reputation values of CR nodes as measured by FC using linear reputation system. .................................................. 143
5.9 Time series plot of reputation values of CR nodes, as measured by FC using dynamic reputation system with FL control. ................................. 143
5.10 Time series plot of $\lambda$ values for CR nodes as updated by FC using FL controller during the observation intervals. ................................. 144
5.11 Time series plot of reputation value for output variable with triangular-shaped membership functions. .................................................. 146
5.12 Time series plot of $\lambda$ for output variable with triangular-shaped membership functions. .................................................. 146
5.13 Time series plot of reputation value for output variable with Bell-shaped membership functions. .................................................. 147
5.14 Time series plot of $\lambda$ for output variable with Bell-shaped membership functions. 147
5.15 Comparison of the Performance of RL based Sybil attack and Random action based Sybil attack using SRM mechanism. ......................... 148
5.16 Comparison of the Performance of RL based Sybil attack and Random action based Sybil attack using DRM mechanism. ......................... 149
5.17 Comparison of the Sybil identity sampling strategies based on their Performance with varying $\xi$, with $\epsilon = 0.3$. ................................. 150
5.18 Comparison of the Sybil identity sampling strategies based on their Performance with varying $\xi$, with $\epsilon = 0.8$. ................................. 150
5.19 Comparison of the decision making mechanisms based on their performance with varying $\xi$, $\epsilon = 0.3$. ................................. 152
5.20 Comparison of the decision making mechanisms based on their performance with varying $\xi$, with $\epsilon = 0.8$. ................................. 152
Chapter 1

Introduction

Wireless communication is one of the fastest growing sectors of the telecommunication industry. With successful deployment of cellular networks in licensed bands and wireless networks, such as Wi-Fi, in unlicensed bands, users have anytime, anywhere connectivity with networked systems, leading to the Internet of Things (IoT)[2]. The current static spectrum assignment by government regulatory agencies, such as the Federal Communication Commission (FCC) in the United States, does not support ubiquitous provision of wireless services. The fixed spectrum allocations are usually long-term and wasteful since only about 15% – 80% of the available spectrum resources are actually put to use [3] [4].

Dynamic Spectrum Access (DSA) offered through cognitive radios (CR) is one of the most promising frameworks for alleviating the crunching pressure put forth on the FCC by many of the wireless providers. In contrast to the legacy fixed spectrum allocation policies, DSA allows license-exempt secondary users (SUs) to access the licensed spectrum bands when not in use by the licensed owners, also known as primary users (PUs). DSA is expected to enable more efficient use of frequency channels without impacting the primary licensees [5].

According to the DSA, SUs are practically invisible to the PUs. The SUs are required to observe spectrum etiquette to avoid creating harmful interference to PUs activities. Spec-
trum overlay is one of the DSA approaches that allow SUs to opportunistically sense and detect idle spectrum bands and use them without interference. SUs are required to identify and avoid in timely manner licensed bands that are in use by PUs [6] [7].

However, there are no specifications regarding the coexistence of SUs in the spectral environment. Just like the licensed owners need not to be aware of secondary transmission activities, isolated SUs are practically “blind” to one another. Therefore, they are likely to cause harmful interference to each other’s communication. The interference experienced by SUs is exacerbated by need to dynamically select multiple channels. This results in intense competition among SUs for available spectrum resources. As a result, available spectrum resources are often misused or abandoned in the process of finding free spectrum bands. With all SUs scavenging for available spectrum resources, the system becomes vulnerable to self-coexistence and security issues.

1.1 An Overview of Dynamic Spectrum Access

DSA was proposed as an alternative paradigm to alleviate the crunching pressure on Federal Communications Commission (FCC) to deviate from the practice of fixed spectrum allocation policies. The main goal of DSA, as originally presented at the first IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks [8], is to replace the current static spectrum allocation model with an open spectrum access model or at least allow the identification and exploitation of under-utilized spectrum resources. In other words, license-exempt SUs can access the licensed spectrum bands when they are not in use by the licensed owners (PUs). The DSA approach is expected to alleviate the problem of spectrum scarcity and starvation by providing standards and specifications for opportunistic exploration and exploitation of underutilized spectrum bands. The exploitation of the under-utilized and idle spectrum bands creates numerous opportunities for the provision of a variety of wireless services by
service providers.

DSA spectrum management models are broadly categorized into three models: dynamic exclusive use model, open sharing model and hierarchical model [9]. The dynamic exclusive model maintains the current spectrum regulation policy but allows the licensed owners the flexibility to sell and trade spectrum and to freely choose technology. Another approach of this model suggests dynamic spectrum allocation that involves the exploitation of the spatial and temporal traffic statistics of different spectrum activities to decide whether spectrum is idle or busy. The dynamic exclusive use model does not exclude the presence of TV white spaces resulting from the bursty nature of wireless traffic.

The open sharing model, also referred to as spectrum commons [11] [12], is one of the spectrum management model that proposes the sharing of spectral region among peer users. In contrast to the dynamic exclusive model, open sharing model calls for the elimination of property rights for exclusive use of spectrum. Under this model, the right to access or use the spectrum is shared among users subject to a protocol, etiquette, or framework that supports spectrum management [12]. This model has been successful in wireless applications in the unlicensed industrial, scientific and medical (ISM) radio band (e.g. WiFi). Both centralized [13],[14] and distributed [15]-[16] spectrum sharing strategies have been investigated under the open sharing spectrum management model.

The hierarchical access model proposes the opening of the licensed spectrum to SUs while limiting the interference perceived by PUs. This model considers three approaches - spectrum underlay, spectrum overlay, and interweave. Spectrum underlay approach imposes transmission power constraint on the secondary users that requires them to operate below the noise floor of the primary users. Spectrum overlay allows for concurrent primary and secondary transmission, based on the premise that secondary communication can assist (re-

\[1\] White spaces are large portions of spectrum in the UHF/VHF bands which become available on a geographical basis after digital switchover[10].
CHAPTER 1. INTRODUCTION

Figure 1.1: A cross-section of a channel with multiple spectrum decision [1].

lay) primary transmissions [17]. Interweave approach entails opportunistic spectrum access, first proposed by Mitola [18]. It targets the spatial and temporal white space by allowing secondary users unrestricted access to identify and exploit local and instantaneous spectrum opportunity. Research studies conducted by FCC [19] and the wireless industry show that some part of the spectrum remain unutilized over time. The hierarchical access model seems to be the most compatible with the current spectrum management policies and legacy wireless systems. The implementation of hierarchical model can significantly improve spectrum efficiency.

1.2 Cognitive Radio Technology

Cognitive radios are intelligent radio devices that have the capability to periodically perform spectrum sensing to discover unused frequencies in licensed bands and utilize it for transmission purposes [20]. Cognitive radios were preceded by software-defined radios. Software-defined radios are simply multiband radios that support multiple air interfaces and is reconfigurable via software run on a digital signal processor (DSP) or a general purpose micro-
processors [21]. J. Mitola promoted both cognitive and software-defined radios in the 1990s. The cognitive radios, in contrast, were designed to be aware of the spectrum environment with in-built intelligence to automatically re-configure and adapt to their changing environment. The cognitive ability of radios provides a variety of ways of improving many aspects of communication systems, and addressing important issues such as spectrum scarcity and quality of service. Cognitive radio technology makes it possible to implement the basic features of the opportunistic spectrum model (OSA), which include spectrum opportunity identification, spectrum opportunity exploitation and regulatory policy.

An important regulatory aspect is that SUs must not interfere with the operations in the licensed bands and must identify and avoid such bands in a timely manner [6] [7]. In a case, where any of the bands used by an SU is accessed by the licensed incumbent\(^2\), that SU is required to immediately vacate the spectrum band within the channel move time and switch to another band [22].

With the enhanced capability to switch from one band to another, SUs face yet another serious challenge in the form of spectrum contention. For instance, the 802.11 WLANs are ubiquitous and operate in unlicensed frequency bands with deployments that could be unstructured [23]. Within a band, an 802.11 WLAN network can select one of several available channels without any instruction from the router. This implies that 802.11 WLANs independently decide to remain on the same channel or switch to another channel with better characteristics. Coordinated channel selection is hampered by the fact the interference range of a typical 802.11 device is substantially larger than its communication range [23]. Therefore, the wireless devices can interfere and are unable to implement any specific messaging protocol or even report their positions.

\(^2\)Licensed incumbent refer to a primary user that has the full authority to operate on an FCC-allocated spectrum band.
1.3 Motivation

Self-coexistence poses significant challenge to the performance of cognitive radio (CR) networks [24]. CR networks have to coexist in such a way that allows them optimally exploit the scarce spectrum resources. To reduce spectrum scarcity, CR networks have to dynamically exploit unused licensed bands. However, the activities of the secondary users in the spectrum environment are often uncoordinated, which leads to the wastage of valuable spectrum opportunities. To ensure efficient usage of the available spectrum resources, an efficient spectrum-sharing model that supports coexistence is needed.

We consider a decentralized system of CR networks, where there is no central authority to coordinate spectrum activities. Also, the system lacks secondary-secondary etiquette or protocol that facilitates coordination among the networks. Due to interference and inability to determine their location [23], networks are unable to decode each others messages. As a result, they cannot detect the spectrum activities in their vicinity. A typical example is an emergency situation that requires quick setup of a cognitive radio network in the presence of inter-network communication constraints. In such a case, an end-to-end communication, made possible by the implementation centralized spectrum allocation solutions, might be inapplicable. Our goal is to design heuristics and algorithms that enable CR networks to identify and use spectrum resources in such a way that minimizes contention, improves efficiency of spectrum utilization and reduces the time wasted searching for contention-free channels.

Many protocols and standards have been designed to enable spectrum sharing in centralized networks [25] [26]. Often these protocol designs and standards do not incorporate features that guarantee fairness and security. On-demand Spectrum Contention (ODSC) is the state-of-the-art protocol designed to support spectrum sharing in 802.22 wireless regional area networks (WRAN). The protocol allows networks to contend for available spectrum
bands by comparing randomly generated contention priority numbers (CPN). According to the protocol, the winner of the spectrum contention is the network that generated the largest or smallest CPN depending on the criteria adopted by the contending networks. Although ODSC is design to address the self-coexistence problem, the protocol design and standards do not incorporate features that guarantee fairness and security of the spectrum contention process. For instance, the arbiter of the spectrum contention is the network that is currently occupying the contended channel, also referred to as the contention destination. The protocol assumes that the spectrum contention arbiters are unbiased and adhere strictly to the protocol specifications. Even though ODSC supports distributed and real-time spectrum sharing, the design flaws expose the spectrum contention process to cheating and gives unfair advantage to the contention destinations. Our main objective is to design a self-coexistence protocol that guarantees fairness and security of the spectrum contention process.

The “open access” philosophy of the FCC-proposed DSA paradigm makes cognitive radio networks susceptible to various unforeseen attacks by smart malicious radios. The effect of malicious disruptions can be even more fatal as there is no way to understand whether the disruptions are intentional or not. The motivation for such shadow-disruptive attack behavior can be either monopolistic — to capture as much spectrum as possible for themselves without maintaining any spectrum sharing etiquettes and make other secondary users starve [27]; or adversarial — to disrupt other secondary users communications and shut them down (particularly applicable in environments filled with adversary users/networks) [28]. The current DSA paradigm lacks the protocols to handle most of the security issues arising in a cognitive network [29], [30]. The Sybil attack, which is classified as an identity spoofing attack, is one of the most common security issues in cognitive radio network. During a Sybil attack, a malicious attacker operates with multiple identities, pretending to be multiple distinct entities [31]. Sybil attacks are possible because of the ability of a cognitive radio device to reconfigure operating parameters, including its identity. The malicious attacker can
then make several false sensing reports with different identities. The false sensing reports, if considered, can alter the results of major spectrum decision making processes [32]. The Sybil threats using malicious cognitive radio(s) in DSA networks are even more prevalent and dangerous for several reasons:

1. They are highly “mobile” in every possible aspect due to the characteristics of software re-configurability;

2. DSA networks are susceptible to attacks ranging from passive eavesdropping to active interfering, frequent break-ins by adversaries due to their open, ubiquitous and interoperable nature [33];

3. Due to the open source nature of DSA networks, it is practically impossible to establish a standard database to record the identity of every CR [34].

This work also considers the problem of intelligent and context-aware Sybil attacks in cognitive radio networks. The most important aspect being the capability of an attacker to learn its environment and use the knowledge obtained to carry out intelligent and sophisticated attacks.

1.4 Related Works

This dissertation is a compendium of published works [35] [36] [37] [38] and a book chapter [39]. The discussion of the related works is logically organized into the following subsections: 1) Self-coexistence and spectrum allocation challenges faced by CR networks; 2) Coalition formation in wireless networks, 3) Spectrum Contention protocol, and 4) Sybil attacks in CR networks.
1.4.1 Self-coexistence in CR networks

Most overlapping cognitive radio networks face the challenge of self-coexistence. In the absence of a central authority that coordinates spectrum activities, the networks are exposed to conflicts that degrade performance and reduce spectrum utilization.

Sengupta et al. [24] addressed the problem of self-coexistence between cognitive radio networks from a game theoretical point of view. The model used in their study is a modified version of Minority game model (MMG), and assumed that networks select a channel without the knowledge of the channels selected by other networks. They suggested a Nash equilibrium switching probability that guarantees convergence of the system when decisions made by networks to find contention-free channels are modeled as a mixed strategy game. This approach suffers from its limitation to single channel acquisition problem and does not address convergence time.

Self-coexistence problem is often addressed as a spectrum allocation problem. Recent works by Cao et al. [40] and Anand et al. [41] addressed self-coexistence problem from a graph theoretical perspective as a graph coloring problem. They assumed a centralized network setting where networks require single channel to operate. Sengupta et al. [42] introduced Utility Graph Coloring (UGC) with primary focus on the improvement of spectral efficiency and spectrum utilization in cognitive radio-based networks such wireless regional area networks (WRANs). UGC, by design, is constrained to work only in centralized system that implements broadcast messaging, aggressive contention resolution scheme and other techniques.

Recently, efforts have been made to address self-coexistence problem in a decentralized network setting. Barcelo et al. [43] suggested the learning-BEB algorithm for collision-free scheduling in 802.11 networks. The algorithm is a modified version of the CSMA/CA mechanism with truncated exponential back-off. The algorithm is simple to implement but suffers
from slow convergence rates [44]. Duffy et al. proposed the Communication Free Learning (CFL) algorithm. The CFL algorithm implements a stochastic learning mechanism to update the probability of selecting a channel based on local information. The CFL algorithm is quite adaptive to changes in topology and quite fast in convergence. All the afore-mentioned decentralized algorithms assume single channel requirement by the networks. A modified version of the CFL algorithm, known as the simplified CFL (SCFL) [45], gives similar convergence rate performance like the CFL algorithm but with less memory and processing power.

As Duffy et al. (Duffy, 2013) correctly identified in their work on decentralized constraint satisfaction, it is possible to have limited communication between entities in system, especially in wireless network settings. Most of the algorithms for channel selection assume the existence of an end-to-end communication for centralized solutions, for control messaging solutions or some sort of global coordination in simulated annealing proposals [46] [47] [48] [49]. Algorithms proposed for distributed systems can be found in works by Mishra [50], Zhao [51] and Nie [52]. These algorithms exploit control messaging to support communication based on learned spectral trends. However, the algorithms introduce a great deal of overhead messaging cost. A number of protocol designs for self-coexistence in both centralized and distributed networks can be found in [53] [54] [22] [9]. The performance of these protocols in a decentralized setting degrades with persistent interference caused by the lack of unified messaging interface. As a result, there are often no incentives for networks to implement one type of protocol in preference to another in order to sustain the coexistence of the CR networks.

1.4.2 Coalition Formation in Wireless Networks

Saad et al. [55] and Hao et al. [56] made notable contributions to the concept of coalition formation in wireless networks. Both works address coalition formation from a game-theoretical
point of view. The main problem lies in finding the optimal partitioning that maximizes utilities of the emergent coalition.

Saad et al. suggested a distributed merge-and-split algorithm that allows networks to form coalitions in order to maximize utilities. The model measured utility in terms of power needed to broadcast and the number of users in a given coalition. In terms of broadcast power, the farther apart the networks, the more the cost incurred to cooperate. Likewise, cost also increases with the increasing cumulative cost of maintaining connectivity with members of the coalition. The proposed algorithm assumes that the resulting self-organization of the entities in the system is guided by their interest to improve individual user’s payoff. The stability of the network coalitions formed is supported by the concept of defection function. That is, using the merge-and-split algorithm, the networks are partitioned such that there is no incentive for a network to switch to another coalition.

Hao [56] studied coalition formation among networks to enhance collaborative spectrum sensing. The formation of coalition is lead by the need by the networks to sense accurately and enhance energy efficiency. Therefore, the utility function dependent on sensing accuracy and energy efficiency of the coalitions. Each coalition is tasked to sense a particular channel; therefore the number of coalition is equivalent to the number of channels available. A distributed algorithm was proposed to find the optimal partition that maximizes the aggregate utility of all coalitions in the system.

1.4.3 Spectrum Contention Protocols

Several primary user protection mechanisms have been suggested in [57], which addresses primary-secondary spectrum etiquette. However, the issue of secondary-secondary spectrum etiquette that deals with the ability of secondary users to coexist in same spectrum environment receives little attention. The introduction of the on-demand spectrum contention (ODSC) protocol was part of the several effort to address the issue of spectrum scarcity as
it relates to self-coexistence [58] [59].

Hu et al. [58] first proposed an adaptive ODSC protocol, a self-coexistence oriented protocol designed specifically for 802.22 WRAN networks. The ODSC protocol leverages the MAC messaging on the inter-network communication channel to provide inter-network spectrum sharing opportunity among coexisting WRAN networks. The protocol allows WRAN networks to compete for shared spectrum by simply exchanging and comparing randomly generated contention priority numbers (CPNs).

Lin et al. [60] addressed the cascading spectrum contention problem associated with ODSC. The problem was studied using the percolation-based model in the context of the cognitive radio networks. Lin suggested a biased model that prevents a starved network from triggering successive spectrum contentions and limits the spatial cascading impact of the spectrum contentions. Other flaws have been identified with the ODSC protocol but have since received little or no attention. The protocol assumes that all participants in the spectrum contention process are honest and CPN cannot be manipulated. These assumptions makes it possible for a very few of the networks to “hijack” the spectrum contentions, thereby leaving others to starve.

1.4.4 Sybil Attacks in Cognitive Radio Networks

Several approaches have been proposed to prevent or mitigate Sybil attacks. These approaches range from the use of cryptographic methods to the simply approach of monitoring the MAC layer for malicious activities. A lot of studies of wireless security use traditional cryptographic tools that are normally based on computational assumptions and maybe equally invalid in the future [61]. The use of reputation systems in counteracting Sybil attacks has been suggested in many works on Sybil attacks [62]. Cheng and Friedman [63] evaluated the vulnerability of reputation systems to Sybil attacks. Reputation systems were broadly classified into symmetric and asymmetric reputation systems. Cheng
and Friedman [63] also proved that symmetric reputation systems, such as EigenTrust [64], PageRank [65] and [66], are more vulnerable to Sybil attacks. In contrast, asymmetric reputation systems are more resilient to such attacks. Asymmetric reputation system relies on some trusted nodes from which all reputation values are propagated. Such systems raise the cost of fomenting a Sybil attack because the attacker is forced into building enough reputation before any successful attack can take place [62].

Tan et.al. [67] discussed the feasibility of Sybil attacks in CR networks. Beside being capable of launching primary user emulation (PUE) attacks, a Sybil attacker can use multiple identities to compromise spectrum decision making process. A detail analysis on how a reputation system can be used to mitigate against Sybil attacks in CR networks can be found in [67], [36]. In [68] and [69], a received signal indicator (RSSI) based solution was proposed. The solution requires the collaboration of trusted nodes to enhance the accuracy of the approach. The approach suffers serious drawbacks due to overhead cost arising from extra computational and memory costs.

The authors of [70] suggests the MAC level monitoring to differentiate between a single attacker spoofing multiple addresses and a group of nodes that are at close proximity. While some approaches proposed in these works assume static nature of Sybil attacks, some of them are not adaptable to the CR network scenario. An effective solution to the problem of Sybil attacks in CR networks must not only be applicable in CR networks but also lightweight, scalable and robust to intelligence-based Sybil attacks.

There are also many works devoted to the design of reputation management systems that enforce cooperation of entities in a network setting [71], [72], [73], [74]. According to [71], the main functions of a reputation management system must include behavior evaluation, behavior detection and reaction to the detected behavior. The evaluation function involves the use of a metric to score node based on their behavior. The detection function focuses on distinguishing between honest nodes and malicious nodes based on their reputation. The
reaction function takes action against or in favor of nodes based on their reputation. For a reputation management system to be effective, the evaluation criteria, detection decision factors and reactive measures should be adaptive to changes in the network in time and space [71].

Fuzzy logic controllers (FLC) have found widespread acceptance in systems that require robust control of parameters especially in responding to sudden critical changes. Fuzzy logic techniques have been successfully applied in wireless networks to improve security [75], to manage vehicle movement at intersections [76], to implement traffic adaptation in Wireless Mesh Networks (WMNs) [77], to implement intelligent network selection in 4G networks [78], to control transmission rate in wireless multimedia sensor networks [79]. FLC is known to be a non-linear intelligent and adaptive control based on artificial Intelligence [80]. FLCs rely on fuzzy membership functions and rules for smooth control of a system’s parameters. We implemented an FLC with the intention of intelligently and dynamically controlling the reputation function parameters of nodes. The reputation function parameters leverages the FLC to control $\lambda$ values of reporting nodes based on their observed spectrum reporting behavior.

1.5 Contributions

In this section, we discuss the main contributions of this research work. Not many researches have been done to address some of the self-coexistence issues discussed in this work, as they pertain to spectrum sharing and spectrum contention. We also highlight the efforts made to enhance efficiency of spectrum utilization and address security issues surrounding spectrum decision and the implementation of spectrum contention protocol.
1.5.1 Multi-Channel Selection in a Decentralized Network Setting

In a decentralized setting, control-messaging techniques cannot fully address the challenges faced by networks during channel selection. Communication constraints make it difficult for networks to know the channels selected by their neighbors and avoid transmitting over them. With increasing demand for spectrum resources, it becomes inefficient and expensive to maintain control channels that could have been used for actual data transmission. In fact, reserving some channels for control messaging, in a system where networks are already starved of spectrum resources, will only exacerbate the spectrum scarcity. Therefore, instead of relying on control messaging to coordinate spectrum activities, a decentralized approach that allows networks to select channels with minimal interference can be implemented.

We propose channel acquisition heuristics that facilitate selection of multiple channels by networks. The implementation of the channel acquisition heuristics is suited for a decentralized system, where communication between networks is constrained by interference and lack of unified communication protocol. The channel acquisition heuristics provide alternative means for networks to select channels for transmission with minimal or zero coordination. The heuristics implements mechanisms that minimize spectrum contention and facilitates fast convergence - networks settling on preferred channels in short period of time.

As part of the multiple channel acquisition heuristics, we suggest a channel-ranking algorithm that facilitates decision making by networks during spectrum contention. Basically, networks have to make decision to “stay” or “switch” on multiple channels. By aggregating channel profile history, networks can use the proposed algorithm to determine and select less contentious channels for transmission purposes. The channel-ranking algorithm is a modified version of the merge sort algorithm, where the rates of successful and failed transmissions are used as the comparison criteria. To capture the actual performance of channels during the early stages of multiple channel acquisition, the normalized success rate is used up until
enough channel profile information have been gathered.

We analyze spectrum contention problem in decentralized system of cognitive radio networks as a birthday paradox problem. The analysis shows that the possibility of at least two networks contending the same channel follows an exponential distribution. We approximated the probability $Pr\{D_n\}$ of $n \geq 2$ networks contending the same channel as $Pr\{D_n\} \geq 1 - e^{-n(n-1)/2m}$, where $n$ is the number of networks and $m$ is the number of available channels. The analysis also shows that an increase in spectrum scarcity, with fixed number of contending networks, increases the frequency of spectrum contentions, and vice versa. A general definition of expected number of contending pairs on a given channel in terms of $n$ and $m$ is presented. By showing that $F_X(n) = Pr\{D_n\}$ where $F_X(n)$ is the cumulative distribution function (CDF), a non-decreasing function, the probability distribution function (PDF) $f_X(n)$ of networks contending on a particular channel is derived.

Finally, a detail comparison of the channel acquisition heuristics based on simulation results is given. The results show that the find-and-keep (FAK) algorithm out-performs the state-of-the-art communication-free learning (CFL) algorithm in multiple channel selection irrespective of the scale of the network. Utility, convergence and frequency of spectrum contention are used as metrics to evaluate the performance of the algorithms.

1.5.2 Self-coexistence using Risk-Motivated Deference Structure

In our work, we are interested in the dynamic spectrum access with focus on secondary-secondary spectrum etiquette and self-coexistence mechanism that can foster better performance of cognitive radio networks and reduce the amount of contention they experience. In the face of spectrum scarcity, cognitive radio networks incur huge amount of losses while competing for available spectrum resources.

As a way to minimize these losses we present a self-coexistence mechanism that allows cognitive radio networks to coexist with each other. This mechanism involves a channel se-
lection heuristics that takes into consideration the amount of spectrum contention risk faced by a CR network. The system model is such that CR networks form deference structure (DS) community to have more efficient access to a channel of interest. Networks can defer transmission to another on deference channel, thereby minimizing their chances of conflicting on the same channel. The DS model relies on the ability of CR networks to adhere to DS agreement which supports the idea of networks sharing and deferring transmission opportunities to other member networks in urgent need. DS model supports reciprocity to promote fairness with the primary goal of mitigating spectrum contention between networks belonging to the DS coalition.

As part of the decision making process to join a DS community, CR networks rely on a risk-motivated channel selection scheme to evaluate the tentative deference structure channel. We provide numerical and simulation results that demonstrates the benefits of the proposed self-coexistence mechanism. We also show how the mechanism can help networks to coordinate their spectrum activities, minimize the number of contentions and improve spectrum utility. We also highlighted the impact of DS community size on expected performance of member networks.

1.5.3 Sustenance against Intelligent Sybil Attacks using Dynamic Reputation System

This work presents an overview of intelligent and context-aware Sybil attack in a CR networks. We model Sybil attacks as intelligence-based attacks that apply the reinforcement learning technique, Q-learning, in selecting false identities for spectrum reporting. The most important aspect of the model is capability of an attacker to learn its environment and use the knowledge obtained to carry out intelligent and sophisticated attacks.

We propose a novel reputation system that tracks the reputations of CR nodes reporting
spectrum state. We present the dynamic reputation system with security framework to mitigate the impact of malicious Sybil nodes on spectrum decisions made by the fusion center (FC). The dynamic reputation system controlled by FC relies on non-linear reputation functions to compute reputations of CR nodes. The reputation system is shown to be flexible but robust to the accuracy of spectrum reports.

We suggest the use of a fuzzy logic controller (FLC) to control reputation function parameter $\lambda$ was suggested. The FLC plays very important role in reputation evaluation as it implements built-in logic required to control the quantum of change $\Delta \lambda$. This provides the reactionary mechanism that is needed to respond to changes in reporting behavior of CR nodes by dynamically adjusting the reputation growth rate $\lambda$.

### 1.5.4 Modified On-Demand Spectrum Contention Protocol

Here, we address some of the vulnerabilities of ODSC protocol. We propose a modified version of the ODSC that addresses security loopholes associated with the protocol. Modified ODSC does not rely on min-max criteria to decide winner of spectrum contention. Rather it exploits the zero-knowledge principle to prevent the exposure of contention priority numbers (CPNs) prior to the decision-making stage in the spectrum contention process. Winners of spectrum contention are computed in a distributed manner, denying the current occupant of a contended channel the autonomy to decide the outcome of the spectrum contention process.

We show that the decision function used in MODSC is non-cheatable and collusion proof. This guarantees fairness, eliminating the possibility of a group of colluding contenders to “hijack” spectrum resources. The decision function is computationally simple and collision-free. This is because the distributed computation of the function produces the same result. As a result, exactly one winner emerges at the end of the contention and all participants are instantly aware of the outcome.
We show that the protocol’s support for repeated spectrum contention can lead to channel reuse. This increases the number of networks that can exploit the available spectrum resources, thereby reducing starvation and increasing spectrum utility. However, channel reuse is constrained by the network topology and depends on the average degree of the conflict graph formed by the networks.
Chapter 2

Multiple Channel Acquisition in
Decentralized System of Cognitive
Radio Networks

2.1 Introduction

This chapter discusses coexistence of cognitive radio (CR) networks with multiple channel requirements in an uncoordinated decentralized system. The study falls into a neglected aspect of cognitive radio technology, involving secondary-to-secondary etiquette, commonly referred to as self-coexistence. Our goal is to develop strategies and algorithms to enhance self-coexistence in an uncoordinated spectrum environment where communication between secondary networks is incapacitated by factors such as interference constraints and the absence of common communication protocol.

We address such situations where CR networks are in need of multiple channels to operate in order to meet quality of service requirements. A typical example is the case where interference networks exceed transmission ranges between networks. The outcome is such
that networks cannot coordinate their activities in the spectrum environment, and therefore risks interfering with each other’s operation. This constitutes a self-coexistence problem since it involves the search of an optimal spectrum assignment with no conflicts between the operating cognitive radio networks. Previous efforts have been made using graph coloring techniques to ensure that an optimal spectrum assignment is achieved in a cooperative network setting. However, in a decentralized network setting with no communication between networks, coordination via message exchange becomes a major challenge. Since there is no coordinated access to spectrum resources, spectrum contention intensifies, leading to interference and poor spectrum utilization.

We propose multi-channel acquisition heuristics that allows networks to contend and acquire spectrum bands to satisfy their needs. The main challenge in designing such heuristics is the need to have coordinate pattern of searching for free bands without coordination between networks. This implies that spectrum decisions are made by the networks are independently by each network and thus do not constitute common knowledge. The decision to select a subset of spectrum bands in preference to other available spectrum bands is also carried out independently of surrounding neighbor networks. Thus, the possibility that the interests of two given networks will conflict is quite significant.

A channel acquisition heuristic can be seen as a strategy that can be used by cognitive radio networks operating in wireless medium to acquire idle channels with minimal spectrum contention. Networks contend basically because they anticipate other contenders to select or switch to a different channel. As we know, continued contention between networks would lead to reduced spectrum utilization and poor system performance. Since there is no unilateral or prior agreement between the networks, spectrum contention remains the only way to secure one or more channel for transmission purposes in a communication-constrained system as described above.

A typical example of a contention avoidance mechanism can be found in [81]. To re-
solve contention among cognitive radios, a carrier sense multiple access (CSMA) scheme is used to allocate channel time among competing cognitive radios based on a reserve system. According to the scheme, radios use a back-off mechanism to determine which time slot to transmit. The back-off time is chosen according to a uniform distribution on a given interval of time. Such back-off mechanism is not compatible with a decentralized system of cognitive networks with multiple channel demand. The networks would have to maintain separate back-off mechanisms for different channels. More so, the system architecture under consideration does not support fragmentation of spectrum opportunity into time slots, which is common with most CSMA schemes.

The open nature of the wireless medium makes it rather difficult to implement communication protocols effectively. So far, there are few cognitive protocols that addresses the

---

1Channel acquisition in this context implies a network selecting an idle channel and maintaining control of it as a preferred channel for transmission purposes while observing primary-secondary etiquette.
problem of spectrum contention without significant message overhead and time delay due to synchronization. In [22], 802.11 networks that are within radio range of each other are required to synchronize their super frames. Via the transmission of coexistence beacons with time stamps, the networks are able to adjust their super frames’ start times according to an earlier agreed rules. A survey of MAC protocols for cognitive radio networks can be found in [82]. The design of these proposed MAC protocols rely on control message exchange and coordination to mitigate conflicts and boost performance. For instance, the adaptive MAC (AMAC) protocol proposed in [54], with the ability to switch between CSMA and TDMA schemes, involves significant control information overhead and latency. The goal of AMAC is to improve performance relative to conventional system of static spectrum assignment. In general, these protocols are not adaptive to a decentralized system with incomplete information about various protocols implemented by the networks.

2.2 Multi-Channel Acquisition Heuristics

Since the application control messaging based protocols is inapplicable to decentralized system of cognitive radio networks, we resolve to develop heuristics and mechanisms that will enable networks to operate independently in a communication-free system. We borrow some ideas from the TCP congestion control schemes which implements slow start and fast transmit approaches. The design of TCP protocol is known support end-to-end connection but does not provide means for end users to communicate congestion levels to one another [83]. Instead, the end users estimate congestion based on the feedback from the network and take measures to reduce congestion. Just like the adjustment of the congestion window can help control congestion in the network, we surmise that adjustment of the number of channels acquired by a network could minimize contention and increase convergence. Also, the reduction in the number of channels sought for is carried out only after contention is detected.
and creates an opportunity for the network to “back-off” and consolidate its hold on channels with lesser contention. In the multi-channel acquisition scenario, we assume that the networks maintain synchronized clocks. During the operational phase, otherwise known as transmit phase, the networks “probe” the channels and record the feedback it receives about their states.\(^2\)

The general pseudocode for our multi-channel acquisition heuristic is presented in Algorithm 1. At the beginning of any operational phase, a network selects a set of channels \(s_i\), consisting of \(k\) channels, to contend. Depending on the outcome of operation phase, the network decides whether to increase or decrease \(k\). An important feature of the heuristic is the decision to either increase or decrease \(k\). The channel requirement threshold \(\tau\) is used as a criteria in making this decision. It serves as a threshold to increase \(k\) linearly or exponentially. The back-off mechanism is implemented by adjusting \(k\) whenever a network experiences conflict with another network. The entire process of channel acquisition terminates only when all networks have settled on their preferred channels or otherwise met their channel requirement \(m_i\) with zero interference. When the networks have satisfied their channel requirement, we say that the system has converged. The time required for the system to converge is referred to as convergence time. It is an important parameter to ascertain the performance of any given heuristic. We proceed to discuss the channel acquisition heuristics and their characteristics.

We considered the following channel acquisition heuristics in our study: RENO, TAHOE, Dynamic Incremental and Find-and-Keep heuristics. The first two heuristics are similar and implements channel acquisition as described in algorithm 1. However, they differ in the way spectrum contentions are handled.

---

\(^2\)We assume that a channel can be in two different states - free and busy. A busy state indicates that a channel is contended by an SU and not occupied by a PU.

\(^3\)We assumed that the channels were homogeneous
Algorithm 1 Multiple Channel Acquisition Heuristics

1: procedure CHANNELACQUISITION(s: set of available channels)
2:     repeat
3:         $s_i \leftarrow$ select best channels from $s$, where $|s_i| = k < m_i$
4:         Transmit on $s_i$
5:         if $s_i \cap s_{i-1} \neq \emptyset$ then
6:             $k \leftarrow$ adjust by reducing $k$
7:         $\tau \leftarrow$ channel requirement threshold $\tau$ (optional)
8:         else
9:             if $k < \tau$ then
10:                Adjust by increasing $k$ exponentially
11:         else
12:             $k \leftarrow$ adjust by increasing $k$ linearly
13:     until $k = m_i$ and $\Phi_a(s)$ /* condition for convergence */

2.2.1 RENO Heuristics

The heuristics used in RENO heuristics is adopted from the TCP RENO congestion control and avoidance mechanism. RENO mechanism defines the behavior of the network when it does experience contention and when there is no contention. Upon experiencing contention on any of the idle channels selected in the previous phase of channel selection, the network reduces the number of channels it accesses in the current phase.

The manner in which the networks populate their channel set $s_i$ depends on $\tau$. As mentioned above, the value of $k$ is controlled by $\tau$. As part of the heuristics the number of channels acquired is increased exponentially until $k < \tau$. The exponential acquisition enables a network to build up quickly its channel set $s_i$ with fewer steps with $k = 1$ at initialization. $k$ is increased linearly after the channel requirement threshold has been reached until $k = m_i$ and zero conflict with other networks.

According to RENO heuristics, until the channel requirement threshold is reached, the value of $k$ is doubled, otherwise it is increased by 1. Therefore,
\[ k = \begin{cases} 2k & \text{if } k < \tau \\ k + 1 & \text{otherwise} \end{cases} \] (2.1)

Assuming that \( Q(k) \) is a function that determines whether the channel threshold has been exceeded, then we have that the next \( k \) is equivalent to

\[ k \leftarrow 2k \cdot Q(k) + (k + 1) \cdot (1 - Q(k)) \] (2.2)

The outcome of the process of channel acquisition terminates when \( k = m_i \). In an attempt to ensure quick convergence of the system, that is \( \Phi_a(s) = 1 \), networks select the channel(s) with the least potential of contention for transmission purposes. Later, we will present the channel-ranking algorithm used by networks to select the best channels for transmission.

RENO heuristics handles contention by halving the number of channels \( k \), that is \( k = 2^{-1}k \). The channel requirement threshold of the network is likewise reduced in the same way \( \tau = 2^{-1}k \) such subsequent channel acquisition will carried out in a linear fashion. This implies that upon the first incident of contention, the exponential increment would no longer take place.

### 2.2.2 TAHOE Heuristics

TAHOE heuristics is very similar to that of RENO, except that it inherits some of its specifics from TCP TAHOE collision avoidance algorithm. TAHOE mechanism implements the same channel acquisition heuristics except that it handles contention differently. TAHOE handles contention by reducing the number of channels that it currently has to one, that is \( k = 1 \). The channel requirement threshold is set to \( \tau = 2^{-1}k \). This means a network implementing this heuristics restarts channel acquisition process with a single channel once it encounters contention. If \( \tau \) is still significant, then the network have a chance to increase
CHAPTER 2. CHANNEL ACQUISITION IN COGNITIVE RADIO NETWORKS

$k$ exponentially. Note that this type of back-off mechanism implemented in TAHOE is quite extreme. However, unlike RENO where exponential increment of $k$ is no longer possible after the first contention, TAHOE heuristics allows for quick recovery from spectrum contention since $k < \tau$. In some special cases, $\tau$ can be fixed and left unmodified even with a network experiencing contention.

2.2.3 LINEAR Heuristics

This channel acquisition heuristics does not make use of the channel requirement threshold $\tau$. Using this mechanism, a network acquires channel one at a time. An incident of contention is followed by the relinquishment of a single channel. The heuristics may not guarantee quick convergence but the steady pace of the acquisition process might help the network avoid unnecessary conflict with other networks. LINEAR mechanism can be summarized as follows

$$k \leftarrow \begin{cases} 
  k - 1 & \text{if } s_i \cap s_{-i} \neq \emptyset \\
  k + 1 & \text{otherwise} 
\end{cases} \quad (2.3)$$

2.2.4 Dynamic Incremental Heuristics

Unlike the previously discussed heuristics, dynamic incremental heuristics relies on a randomized process to decide the number of channels contended in every stage of the channel acquisition process. The value of $k$ for the next phase is dependent partly on the current value of $k$ and the difference in $m_i - k$ channels required to attain convergence. Suppose there is a random function with uniformly distributed outcomes $\lambda(\cdot)$ such that $\lambda(x) \in \{0, x - 1\}$. Then, the value of $k$ is updated like this,

$$k = k + \Delta k \quad (2.4)$$
where $\Delta k = \delta k \pm \lambda(\delta k)$ and $\delta k = m_i - k$. In a case where the network is greedy, we have $\Delta k = \delta k + \lambda(\delta k)$. With such configuration and $k = 0$, the network is likely to contend for a number of channels bounded by the following inequality $m_i \leq k < 2m_i$. So equation (2.4) can be re-written as

$$k = m_i + \lambda(m_i - k) \quad (2.5)$$

By the equation, it becomes evident that the network goes for more channels that is required. This approach might be greedy but it allows the network to probe the available channel and discover which ones are left vacant. By this means, the network would be able to gather more information about spectrum utilization. We can also observe that as $k \to m_i$, the number of extra channels probed by the network decreases. Given a function $\phi(k)$ that defines the outcome of every channel’s probe transmission, we have that the network becomes satisfied only when $\phi(m_i \pm \lambda(m_i - k)) \geq m_i$. With this heuristics, the networks are not concerned about the amount of spectrum contentions before convergence. Rather they are interested in satisfying channel requirement in every operational phase.

### 2.2.5 Find-and-Keep Heuristics

The approach used in Find-and-Keep (FAK) heuristics exploits the persistence of networks to remain on a channel once found to be free. Technically, we assume cognitive radio networks can detect spectrum contentions with neighbors and make decision to switch or stay. Equipped with this capability, networks are still unable to identify the source(s) of the contentions experienced on a particular channel. As a result of this, networks have to make proactive decision to remain on a channel or switch to another.

Sengupta et al. suggested a Nash equilibrium switching probability $p$, which if all networks switch with $p$ upon experiencing contention, can lead to the convergence of the system.
Making a decision to stay or switch for a multiple number of channels is expensive, considering the switching cost. The approach involves networks hopping aimlessly over the available channels with no preference for any particular channel.

The FAK heuristics is designed to minimize the cost of switching and encourages the maintenance of preferential list of channels, just like the aforementioned heuristics. Thus, when a network finds a idle channel, it stays on the channel with a probability \( q \approx 1 \), and switches with \( p \approx 0 \), where \( 0 \leq p, q \leq 1 \) and \( p + q = 1 \). Any time when contention is recorded on a particular channel, \( q \) undergoes an exponential decay. Suppose \( q_o \) is the initial probability of selecting a newly found idle channel. After \( \tau \) spectrum contentions on that channel, we may have the probability to stay updated as follows:

\[
q_\tau = q_o \cdot e^{-\lambda \tau} = q_o \cdot e^{-\tau/T}
\]

And in a case, where we substitute \( q_o \) with \( q_\tau \) after every update, we have

\[
q_\tau = q_o \cdot e^{-\tau(\tau+1)/T}
\]

Note that \( \lambda = 1/T \) is the decay rate of the stay probability \( q \) and the \( T \) is the time required for \( q \) to decay to an amount equivalent to \( 1/e \) of its initial value \( q_o \). Equation (2.7) is more appropriate for cases where a network is sensitive to contentions and want \( q \) to decay faster with fewer contentions. This allows the network to explore other channels without having to be strictly attached to the first discovered channel(s). A necessary criteria for the convergence of the system is that \( m \geq n \), otherwise the system will never converge. When \( m < n \) and each network needs a channel to operate, then the system needs at least \( n - m \) channels to ensure that each network gets at least a single channel to operate.

FAK heuristics has numerous advantages, which favors convergence time of the system. The mechanism operates on the first come first serve principle. The first network to identify
Algorithm 2 Find-and-keep heuristics

1: procedure FINDANDKEEP
2: Initialize $\vec{q} \leftarrow 0$
3: repeat
4: \hspace{1em} \text{- - Channel Selection Phase}
5: \hspace{2em} for $N_i \in \mathcal{N}$ do
6: \hspace{3em} if $s_i^t$ is Empty then
7: \hspace{4em} $s_i^{t+1} \leftarrow$ select $m_i$ channels u.a.r from $\mathcal{C} = \{c_j : j = 1, 2, \ldots, m\}$
8: \hspace{3em} else
9: \hspace{4em} $s_i^{t+1} \leftarrow$ select $c_j$ from $s_i^t$ with $q_{ij}$
10: \hspace{3em} if $|s_i^{t+1}| < m_i$ then
11: \hspace{4em} $s_i^{t+1} \leftarrow s_i^{t+1} \cup$ select $k = m_i - |s_i^{t+1}|$ channels u.a.r from $\mathcal{C} \setminus s_i^t$
12: \hspace{2em} end
13: \hspace{1em} \text{- - Channel Stay Probability Update Phase}
14: \hspace{2em} for $N_i \in \mathcal{N}$ do
15: \hspace{3em} for $c_j \in s_i^{t+1}$ do
16: \hspace{4em} if $I(c_j) == 0$ then \hspace{1em} \text{- - zero interference/contention}
17: \hspace{5em} $\tau_{ij} \leftarrow 0$
18: \hspace{5em} $q_{ij} \leftarrow 0.99$
19: \hspace{4em} else
20: \hspace{5em} $\tau_{ij} \leftarrow \tau_{ij} + 1$
21: \hspace{5em} $q_{ij} \leftarrow q_{ij} \cdot e^{-\lambda \tau_{ij}}$
22: \hspace{3em} end
23: \hspace{2em} end
24: \hspace{2em} until $\bigcap_{i=1}^n s_i^{t+1} = \emptyset$

an idle channel literally sticks to it but with an exponentially decreasing probability $q$. This makes it difficult to displace the first network to arrive on the channel with fewer contentions. The number of contentions required to displace a network is equivalent to the inverse of the decay rate $1/\lambda$. Spectrum contenders that are yet to satisfy their channel requirement must then perform channel hopping to find idle channels that are yet to be acquired. Assuming that there are $n$ networks in the system. In the first round of channel acquisition process, half of the network could have settled on some idle channels. Assuming that in every round approximately half of the networks find a channel idle and settle on them, then it will take approximately $O(\log(n))$ time for the system to converge.

FAK heuristics is also robust to the emergence or departure of a network during the
channel acquisition process. The first come first serve principle ensures that the emergence of new networks in the spectrum environment does not disrupt or displace already settled networks. An incoming network have to hop over the channels, probing for the idle bands, thereby minimizing the number of spectrum contentions needed to stabilize the system. The departure of a network from spectrum environment does not affect disrupt normal spectrum operation. Rather, it creates an opportunity for unsatisfied networks to acquire those channels left by the departing networks. The FAK heuristics is memory-less. Once a channel is found to be idle, the probability of a network remaining on the channel becomes significant. Previous information about secondary users activities on the newly found channel are overridden by the fact the channel is available for use in transmission.

2.3 Channel Ranking Algorithm

The channel ranking algorithm is used during the acquisition process to determine which channels to select for the acquisition process. The decision to operate on a certain set of channels must be based on how successful operations on those channels have been in the recent past. Contention is likely to occur on any of the $m$ available channels since selections made by neighboring networks are not communicated. In that case, it would be important to choose channels with high success rate. Success rate can be measured in terms of the number of successful probe transmissions carried out by the network after sensing a channel to be idle.

We have made the assumption that channels are homogeneous in terms of spectrum capacity, so no one channel is better than the other. By probing the spectrum environment, the networks are able to gather profile information about available set of channels. Profile information gathered are marked by channel identity $C_j$, number of successful attempts $u$, and number of failed attempts $v$. The number of failed attempts $v$ also includes the frequency
of PU activity on the channel on the select channel.

We proceed to describe how the channel-ranking algorithm works. The algorithm is designed such that normalized success rate \( \mu \) is used in sorting the channel ids until enough channel profile information have been gathered. Sorting is carried out in descending order such that the first channel id has the best success rate. If there are \( m \) channels, \( \mu_j \) would denote the success rate of channel \( C_j \). Initially, for all channel \( u_j = 1 \) to avoid division by zero during the normalization. A network decides the length of time in time slots \( T \) during which it will be using the normalized approach for channel ranking. After \( T \) time slots, subsequent ranking is based on the ratio of \( u_j \) to the \( u_j + v_j \). A summary of the channel ranking rules are presented below:

1. At any time \( t < T \), success rate \( \mu_j \) is defined as \( \mu_j = u_j / \sum_i u_i \)

2. At any time \( t \geq T \), success rate \( \mu_j \) is defined as \( \mu = u_j / (u_j + v_j) \).

3. Channel \( c_j \) is prioritize over channel \( c_k \), if \( \mu_j > \mu_k \).

4. In case \( \mu_j = \mu_k \), channels according to the uniformly at random order of selection from the resulting channel set \( \{c_j, c_k\} \).

The parameter \( T \), indicating the length of the probing period, is strictly network-defined. Depending on the priority of the network, \( T \), whether to learn more about the channels, it can decide to set the value of \( T \) to be small or large. According to the first rule, \( \mu_j \) measures the relative performance or the availability of \( C_j \) with respect to other channels. The second rule, on the other hand, treats \( \mu_j \) as a measure strictly based on history of actual experience on \( C_j \). Both measures can be combined to get global view about the performance of a particular channel. In that case, we have \( \mu_j \) defined as follows,

\[
\mu_j = \alpha \cdot \frac{u_j}{\sum_j u_j} + (1 - \alpha) \cdot \frac{u_j}{u_j + v_j} \tag{2.8}
\]
where $\alpha \in 0$ and $a \in \mathbb{R}$ is a coefficient of relative importance of the two measures. As a matter fact, when there is lack of history on the channel set, the relative performance takes precedence over individual channel performance, so $\alpha = 1$. As a result, a network can decide to keep $\alpha = 1$ up until $T$ time slots has elapsed and then switch to individual performance assessment by setting $\alpha = 0$. As an alternative approach, the value of $\alpha$ can be allowed to decay gradually by a certain quantum of change. Using this approach, the significance of the relative performance measure diminishes gradually until enough channel profile information has been gathered. The channel ranking scheme ensures that channels with high $\mu$ values are selected in preference.

### 2.4 Estimating Spectrum Contention on a Channel

As part of our studies, we analyzed spectrum contention as it pertains to conflicts experienced in cognitive radio systems. Since cognitive radios rely on opportunistic access of idle frequency bands, they often encounter conflict during spectrum access. It is therefore imperative to estimate the severity of spectrum contention based on important features of the system such as the number of networks and available frequency bands in the system. When spectrum contention takes place between two networks knowingly or unknowingly, it produces interference, which does not benefit any of the networks. We mentioned earlier that spectrum contention could be used as a strategy to maintain control of a channel. However, the effectiveness of such strategy depends on the homogeneity of the frequency bands as well as the system characteristics.

Given certain information, such as number of networks in the system and number of available channels, we can probably estimate the chances of spectrum contention occurring. We proceed to derive the probability of two or more networks contending on the same channel.
Theorem 2.4.1. Given \( m \) and \( n \) as positive discrete integers and \( D_n \) denoting an event where 2 or more cognitive radio networks contend a single channel, then probability that event \( D_n \) occurs is defined

\[
Pr\{D_n\} \geq 1 - e^{-\frac{n(n-1)}{2m}}
\]

Proof. To prove this theorem, we resort to the well-known birthday paradox problem. The birthday paradox problem addresses the probability that, in a given set of individuals, some pair of individuals were born on the same day. We used the same approach used in T. H. Cormen et. al, to derive the probability \( Pr\{D_n\} \) of two or more networks contending the same channel. Let \( c_i \) denote the identity of the channel accessed by \( N_i \) out of \( m \) available channels. The probability that any two networks \( N_i \) and \( N_j \) contends on a given channel with identity \( c \), assuming independence of the choices made by the networks, is given as

\[
Pr\{c_i = c, c_j = c\} = Pr\{c_i = c\} \cdot Pr\{c_j = c\} = \frac{1}{m^2}
\]  

(2.9)

Therefore, the probability that any choice made by the two networks coincide is

\[
Pr\{c_i = c_j\} = \sum_{c \in C} Pr\{c_i = c, c_j = c\} = \sum_{c \in C} \frac{1}{m^2} = \frac{1}{m}
\]  

(2.10)

Further, we can analyze the probability of at least two out of \( n \) contends on the same channel by looking at the complimentary events. The probability of at least two networks contending is same as one minus the probability that no network contends with another, that is zero contention. We define an event \( A_i \) that \( N_i \)’s choice is distinct from any other \( N_j \) given that \( j < i \). Therefore, event \( B_n \) that \( n \) networks select distinct channels is defined as

\[
B_n = \bigcap_{i=1}^{n} A_i
\]  

(2.11)

According to Bayes theorem and applying the commutative law for two events with non-
zero probability, we can write $B_n = A_n \cap B_{n-1}$ as a recurrence

$$Pr\{B_n\} = Pr\{B_{n-1}\} \cdot Pr\{A_n|B_{n-1}\}$$

(2.12)

where we take the base case as $Pr\{B_1\} = Pr\{A_1\} = 1$. Therefore, the choices made by the $n$ networks are distinct only if the sequence $c_1, c_2, \cdots, c_n$ are distinct. This is equivalent to the probability that $c_n \neq c_i$ for $i = 1, 2, \cdots, n-1$ times the probability that the $c_1, c_2, \cdots, c_{n-1}$ are distinct. This is possible only if $Pr\{A_n|B_{n-1}\} = (m - n + 1)/m$, since out of $m$ channels, $m - n + 1$ channels have already been selected by $n-1$ networks. Upon expanding the recurrence, we have

$$Pr\{B_n\} = 1 \cdot \left(1 - \frac{1}{m}\right) \cdot \left(1 - \frac{2}{m}\right) \cdots \left(1 - \frac{n-1}{m}\right)$$

(2.13)

For all $x \in \mathbb{R}$, we have $e^x \geq 1 + x$. Thus,

$$Pr\{B_n\} \leq e^{-1/m} e^{-2/m} \cdots e^{-(n-1)/m} = e^{-n(n-1)/2m}$$

(2.14)

From the above expression, we can state that the probability of contention $Pr\{D_n\}$, given that $D_n$ is the event that at least two networks contends, is

$$Pr\{D_n\} \geq 1 - e^{-n(n-1)/2m}$$

(2.15)

From inequality 2.15, we can observe that to minimize contention amounts to minimizing $Pr\{D_n\}$. This, in turn, implies maximizing the exponential component that is $-n(n-1)/2m = 0$. Solving the equation shows that contention is inevitable, except when there is zero or a single network present in the system.

**Corollary 2.4.2.** Suppose that $m_1$ and $m_2$ are distinct non-zero positive integers such that
Also, suppose that \( n \) is constant and \( \Pr\{D_n^k\} \) denotes \( \Pr\{D_n\} \) for a case where there are only \( k \) channels available. Then,

\[
\Pr\{D_n^{m_1}\} > \Pr\{D_n^{m_2}\}
\]

**Proof.** From equation (2.15), we can approximate \( \Pr\{D_n\} \) to be

\[
\Pr\{D_n\} = 1 - e^{-n(n-1)/2m}
\]

which in other words can be simply interpreted as the lower bound for spectrum contention probability. With \( n \neq 0 \), it is easy to see that

\[
\lim_{m \to \infty} \Pr\{D_n\} = 0
\]

This implies that with more channels, the probability of spectrum contention tends to zero. Therefore, a system with just \( m_1 \) channels is likely to experience more spectrum contention than a system with \( m_2 \) available channels, given that \( m_2 > m_1 \). Thus, it is valid to state that

\[
\Pr\{D_n^{m_1}\} > \Pr\{D_n^{m_2}\}
\]

Corollary 2.4.3. Suppose that the number of networks \( n \) is variable, with entry or departure of \( k \) networks, amid fixed spectrum resources \( m \). For any \( 0 < k \leq n \)

1. \( \Pr\{D_n\} \geq \Pr\{D_{n-k}\} \)

2. \( \Pr\{D_n\} < \Pr\{D_{n+k}\} \).

**Proof.** To prove the above statement, we begin by looking at the first case. We can interpret this case as being similar to a scenario of \( k \) networks leaving the system. This is an indication
that only \( n - k \), instead of \( n \), networks are left to contend for \( m \) channels. And we have that,

\[
\lim_{{n \to 0}} Pr\{D_n\} = 0
\]

So a reduction in \( n \), actually reduces the level of spectrum contention to expect in the system,

Considering the constraints stated earlier, we have that \( n(n - 1) > (n - k)(n - k - 1) \) and subsequently \(-n(n - 1) < -(n - k)(n - k - 1)\). This implies that

\[
e^{-n(n-1)/2m} < e^{-(n-k)(n-k-1)/2m}
\]

\[
1 - e^{-n(n-1)/2m} > 1 - e^{-(n-k)(n-k-1)/2m}
\]

With the transformation, it leads us to conclude that

\[
Pr\{D_n\} \geq Pr\{D_{n-k}\}
\]

The equality sign, seen in the above inequality expression, explains the possibility of the departure not contributing to significant improvement in spectrum contention. This is very likely to happen in a system where \( k \ll n \).

In a similar way, we can show that \( Pr\{D_n\} < Pr\{D_{n+k}\} \), since an increase in the number of networks by \( k \) would create more demand for spectrum resources.

\[\square\]

**Theorem 2.4.4.** Assuming a cognitive radio network system is characterized by \( n \in \mathbb{Z}^+ \) networks and \( m \in \mathbb{Z}^+ \) channels and a random variable \( Z \) that denotes the number of contending network pairs registered, then

\[
E[Z] = \frac{n(n - 1)}{2m}
\]

defines expected number of contending network pairs involved in spectrum contention.
Proof. We can analyze the expectation of spectrum contention in a given cognitive radio network system by taking into account the expected number of networks that will choose the same channel, given the homogeneity of the channels. Let us represent the choices made by any two independent networks $N_i$ and $N_j$ with an indicator random variable $Z_{ij}$, defined as

$$Z_{ij} = I\{c_i = c_j\} = \begin{cases} 1 & c_i = c_j \\ 0 & \text{otherwise} \end{cases}$$

where $c_i$ and $c_j$ are the choices of $N_i$ and $N_j$ respectively. Considering equation (2.10), we have the expectation of the random variable $Z_{ij}$ being $E[Z_{ij}] = 1/m$. Let the number of such possible pairs of networks that select the same channel be denoted $Z$, we have

$$Z = \sum_{i=1}^{n} \sum_{j=i+1}^{n} Z_{ij} \quad (2.17)$$

Applying expectation to both sides and extending the linearity, we have that

$$E[Z] = E\left[ \sum_{i=1}^{n} \sum_{j=i+1}^{n} Z_{ij} \right] = \sum_{i=1}^{n} \sum_{j=i+1}^{n} E[Z_{ij}] = \binom{n}{2} \frac{1}{m} = \frac{n(n-1)}{2m} \quad (2.18)$$

$$E[Z] = \frac{n(n-1)}{2m} \quad (2.19)$$

Thus, if $n(n - 1) \geq 2m$, then $E[Z] \geq 1$. This implies that at least two networks will be contending for a single channel. \qed

In a case, where $n = m$ with single channel requirement per network, we have that the expected number of pairwise contention is equal to $(m - 1)/2$. This shows that even in the face of adequate number of channels to satisfy the networks’ channel requirements, they can still experience contention if the system is decentralized. Even when there are $\sqrt{2m} + 1$ networks in the system, we can still expect that at least two networks will contend for the
same channel.

Earlier, we described the event $D_n$ as an event where at least two networks contend
the same channel. Thus, $Pr\{D_n\}$ describes the probability that at least two networks will
conflict in an attempt to acquire a channel. To determine the distribution of the spectrum
contention, we define a random variable $X$ that denotes the number of networks contending
for the same channel. Thus, equation (2.15) can be rewritten as follows:

$$Pr\{D_n\} = Pr\{1 < X \leq n\}$$

(2.20)

We recognize that $Pr\{D_n\}$ is defined for a closed range $[1, n]$ and fits into the definition
of a cumulative distribution function $F_X(x)$, where $\sup\{x \in \mathbb{Z}^+\} = n$, given that

$$Pr\{1 \leq X \leq n\} = F_X(n) - F_X(1) = \int_1^n f_X(t)dt$$

(2.21)

We note also that $F_X(x) = 0$ for all $x \leq 1$, since in the context of our spectrum contention
analysis, contention can take place with the involvement of at least two networks.

**Definition 1.** A function is a cumulative distribution function (CDF) of a random variable $X$ if i) non-decreasing ii) right continuous iii) $\lim_{x \to 0} F(x) = 0$ and iv) $\lim_{x \to \infty} F(x) = 1$.

**Lemma 2.4.5.** The function $F_X(x) = 1 - e^{-\frac{x(x-1)}{2m}}$ is the cumulative distribution function of
the random variable $X$, where $x \in [0, +\infty]$ and $m$ is a constant.

**Proof.** The function $F_X(x)$ is inherently a non-decreasing function, because for any given
pair of numbers $a$ and $b$, with $b > a$, $F_X(b) > F_X(a)$. Likewise, we can show that $F_X(x)$ is
right continuous. For any given $c \in [2, +\infty]$, we have that

$$\lim_{x \to c} F_X(x) = 1 - e^{-\frac{c(c-1)}{2m}} = F_X(c)$$

(2.22)

This implies that the limit of $F_X(x)$ as $x$ approaches $c$ exists and equals to the value of $F_X(x)$
at $x = c$. And we can easily show that the limit of the function as $x$ approaches zero is

$$
\lim_{x \to 0} F_X(x) = \lim_{x \to 0} 1 - e^{-\frac{x(x-1)}{2m}} = 0
$$

and as $x$ approaches infinity that the limit of the function

$$
\lim_{x \to 0} F_X(x) = \lim_{x \to \infty} 1 - e^{-\frac{x(x-1)}{2m}} = 1
$$

Theorem 2.4.6. The probability density function (PDF) of the random variable $X$ can be expressed as

$$
f_X(x) = \frac{2x - 1}{m} e^{-\frac{x(x-1)}{2m}}
$$

Proof. The CDF of a random variable $X$ can be represented as

$$
F_X(x) = \int_{-\infty}^{x} f_X(t)dt
$$

such that $f_X(x) = F_X'(x)$. Since the CDF is right continuous, we can rewrite, equation (2.25) to derive the PDF function for $X$ as follows

$$
F_X(n) - F_X(1) = \int_{1}^{n} f_X(x)dx
$$

To derive $f_X(n)$ we need to differentiate L.H.S of equation (2.15), assuming that the CDF
Figure 2.2: Cumulative distribution function of $n$ coexisting networks with $m = 12$ channels.

is approximated to the lower bound of that expression. So,

$$f_X(n) = \frac{d}{dn} \left( 1 - e^{-\frac{n(n-1)}{2m}} \right)$$

$$= -e^{-\frac{n(n-1)}{2m}} \frac{d}{dn} \left( -\frac{n(n-1)}{2m} \right)$$

$$= \frac{2n-1}{m} e^{-\frac{n(n-1)}{2m}}$$

(2.27)

2.5 Experimental Results

To test and compare the performance of the proposed mechanisms for multiple channel acquisition, we conducted extensive simulation experiments. The goal of the experiments was to generate and test spectrum contention model that resemble real-world scenario. The simulation model was programmed to emulate the sensing and transmission operations per-
formed by cognitive radio transmitters during normal spectrum activity. Spectrum access is synchronized in frames. Each frame is partitioned into beacon phase and data transmission phase. Networks perform sensing during the beacon phase and transmit during the data transmission phase. Spectrum sensing is enabled to ensure that all networks adhere to spectrum etiquette and avoid any interference with primary users. During the data transmission phase, network attempts transmission over one or more channels. Transmission fails when at least two networks transmit over the same channel. We assume that networks have the ability to detect such failed transmissions, and consequently infer spectrum contention.

The main performance metrics used in comparing the mechanisms are convergence time, average system utility and contention. Convergence is achieved when all networks in the system have settled on their preferred channels or spectrum bands and are no longer contending each other. Convergence time is thus defined as the number of time slots or frames required for the system to attain stability. Depending on primary user rate of activity and
available spectrum, we anticipate an exponential increase in convergence time as the number of networks increases. The average simulation time for our experiment was limited to 1000 time slots/frames. In order to capture the average performance trend for each mechanism, we repeated the experiment 1000 times.

To provide a fair comparison of the different mechanisms, we adopt the same network setting throughout the experiment. In our experimental setup, we assume an average channel requirement for each network and ensure that the available channels are sufficient enough to satisfy the networks. As a result, the experiments were conducted in two different network settings - small and large network. For small network setting, the configuration is such that the average channel requirement $k = 2$ and the total number of available channels $m = 20$, with at most $n = 10$ independent networks. The large network setting, on the other hand, has $k = 5$ and $m = 200$, with at most $n = 30$ independent networks.

We present the results obtained from our experiments in two sub-sections. First, we present results obtained during our earlier investigation into multiple channel acquisition in DSA systems. The heuristics studied and analyzed at that stage include RENO, TAHOE, LINEAR and Increment Probabilistic heuristics (INCR). Later, we present the find-and-keep heuristics, which is the latest addition to the pool of heuristics for multiple channel acquisition heuristics. We compare find-and-keep heuristics to the communication-free learning algorithm using the convergence time performance metric.

### 2.5.1 Experimental Results I

In this section, we present the results obtained from our investigation into the nature of multiple channel acquisition in cognitive radio networks. The experimental setup had the following configuration. Networks shared a total of $m = 225$ channels with an average channel requirement per network $k = 5$. Each network has channel size requirement, which serves as a threshold to acquire channels linearly or exponentially. We configure the networks
to have the same channel size requirement. RENO and TAHOE heuristics make use of this parameter in their respective implementations. However, the threshold parameter is not used in LINEAR and INCR heuristics.

The simulations were conducted in two different modes: primary users present and primary users absent. In the simulation involving primary users, primary user activity was modeled using Markov chain. A channel goes from idle to busy due to primary user activity with a probability of 0.1. The average channel occupancy follows Poisson distribution with a mean value of 10 time slots/frames. The performance metrics used in the experiment are utility, convergence time and contention based on the number of networks or available channels. All metrics are measured in time slots.

**System Utility**

System utility is measured in terms of the number of time slots or frames during which a network was able to operate in an interference-free channel. We assume that the transmitted information is delay tolerant but has to retain its data integrity. Therefore, any form of interference during active transmission on the channel renders the information inaccurately, thereby reducing the utility to zero. This implies that no partial benefit can be derived even if part of the transmitted data were delivered.

Performance comparison of the heuristics, based on system utility in the absence of the primary users, is illustrated in Figure 2.4, where x-axis denotes the number of networks in the system and the y-axis denote system utility, measured in time slots. We can observe that the INCR heuristics gives the best performance. Performance of INCR heuristics can be attributed to its slightly greedy approach in channel acquisition. Networks implementing this mechanism consistently select a random number of channels to contend. In some cases, the number of channels selected might actually exceed the channel requirement. The other heuristics (TAHOE, RENO, LINEAR) apply a step-wise approach in selecting channels,
and implement back-off mechanism by slicing the channel size requirement upon experiencing contention. LINEAR gives a better performance than RENO and TAHOE mechanisms because the mechanism adopts a “slow and steady” approach in acquiring channels. The poorer performance of RENO and TAHOE can be attributed to the contention avoidance measure of halving channel size whenever there is contention. TAHOE mechanisms poor performance can be attributed to the drastic reduction in the number of acquired channel after contention. Even though with subsequent successful transmissions, followed by an exponential increase in channel size (up until channel size threshold is reached), the mechanism may not be effective in helping the network recover as fast as RENO.

![System Utility Diagram](image)

Figure 2.4: The diagram describes the expected system utility in a case where primary users absent in the spectrum.

Generally, we can observe that system utility increases as the number of networks increases. However, the observable trends are accounted for by the sufficient supply of channels and not as a result of number of networks. With sufficient supply of channels, the convergence time is shorter and therefore networks able to begin interference-free transmission
earlier. Given a certain number of networks $n$, we expect that with an average channel size requirement $k$, the expected system utility is equivalent to $n \cdot k \cdot T$, where $T$ is the number of observed transmission time slots/frames. We examine the ratio of the actual system utility derived to the expected system utility and how it relates to $n$ and the utilization rate of the available channels.

![Figure 2.5: A plot that illustrates actual to expected ratio of system utility and variations in utilization rate with regards to available spectrum resources.](image)

An illustration of the ratio of actual system utility to expected system utility can be seen in Figure 2.5. We expect actual system utility to be less than or equal to the expected utility. However, this condition does not hold for INCR heuristics. This is because networks might end with more channels than the channel size requirement. We can also observe that as the utilization rate increase, the possibly of system implementing INCR to achieve a ratio greater than one diminishes.

The presence of primary user in the system has negative impact on the system utility. In Figure 2.6, we compared the performance of INCR heuristics in the absence and presence of primary users. We can observe a decrease in system utility as a result of primary presence. The system utility decreased by average of 8%.
Figure 2.6: Performance comparison of INCR heuristics as it applies in the absence and presence of primary users.

**System Contention**

While the system utility is an important performance measure, it is also important have an insight on the number of spectrum contentions observed in the system. In our simulation settings, contention is measured in terms of the number of time slots wasted when networks select the same channel. In other words, spectrum contentions are measured in terms of the number of channels with records of conflicts and not the number of conflicting networks. Spectrum contention ceases when networks have acquired the channel size requirement and no longer contending with other networks. Figure 2.7 illustrates the variation spectrum contention with $n$.

We observe that as the network density increases, with limited supply of channels, the number of spectrum contentions in the system increases. Figure 2.7 shows that the INCR does better than other heuristics, until $n > 27$. RENO and TAHOE outperforms LINEAR
for $n > 20$, and even better than INCR when $n \geq 28$. The backoff-mechanism employed by RENO and TAHOE pays off, with the networks encountering less conflicts than LINEAR and INCR. The persistent nature of INCR makes it highly vulnerable to contentions as $n$ increases. By comparing the utility derived per contention experienced in the system, we have a completely different picture of the performance of the heuristics.

In Figure 2.8, we observe that the utility per contention decreases and converges towards
zero as $n$ increases. The causative factor for such trend is the increased utilization rate, which reduces the abundance of spectrum resources exists with smaller $n$. With increasing channel requirement, the networks have to contend as much as the amount of utility that they derive from available fixed spectrum resources. This implies that the utility per contention measure is invariant to the heuristics implemented in the system. However, INCR offers the best performance when compared to other networks when $n \leq 25$.

**Convergence Time**

Convergence time is the number of time slots/frames that elapsed before the networks satisfied the channel size requirement. Convergence time is dependent on a number of factors, including the presence of primary users and the number of available channels, and the density of the system with regards to the average allocation per network.

![Figure 2.9: Convergence time of multiple channel acquisition heuristics with primary user absent.](image)

Figure 2.9 illustrates the dependency of convergence time on the number of networks. We can observe that convergence time is a non-decreasing function of $n$. As the number of networks in the system increase, it becomes rather difficult for networks to satisfy their channel requirement. In our simulation settings, the number of available channel is set to
$m = 225$. With some heuristics, the system never converges within the simulation time $T = 1000$ with 50% utilization rate. The INCR heuristic gives the fastest convergence time.

![Convergence Time](image)

**Figure 2.10:** Impact of primary users presence on the convergence times of RENO and LINEAR heuristics.

Depending on the rate of primary user activities, it might take the system additional time to converge. With networks getting displaced from acquired channels, and near-stable state of the system can be upset. We show the impact of primary user presence by comparing the convergence times of RENO in the absence and presence of primary users. The convergence time curve is shifted to left, indicating a slower convergence rate.

### 2.5.2 Experimental Results II

#### Convergence Time

Experiments were conducted to compare the performance of the multiple channel acquisition heuristics discussed in section 2.5.1, the find-and-keep (FAK) heuristics and the communication-free learning (CFL) algorithm. In comparing the heuristics, we ensured that the configurations were the same for all experimental setup. For instance, the simulation time was set at 1000 time slots, the average channel size requirement $k = 5$ and the number
of available channels $m = 225$. We observed the performance as the system’s size increases. Figure 2.11 shows the convergence time trend for all heuristics discussed.

![Figure 2.11: Comparison of all proposed multiple channel acquisition heuristics with CFL based on convergence time.](image)

Based on the illustration, we observe that FAK outperforms all heuristics with fast convergence time. Provided the available channel supply is sufficient to satisfy each network’s channel size requirement, a system implementing FAK is guaranteed to converge. FAK converges very fast with convergence time under 100 time slots. This performance is attributed to the basic idea of the heuristics. According to the heuristics, a network to hold onto a channel after discovering it as contention-free. It relinquishes the channel with a probability that only increases (exponentially) when contention is being experienced on that channel increases. Unlike in the CFL algorithm, where the probability distributions’ updates are followed by normalization, FAK employs exponentially decay approach during updates and do not normalize across distributions. It is worth noting that INCR competes with CFL, producing almost the same convergence time trend as CFL.

In Figure 2.12, we present a strict performance comparison of the CFL and FAK with a constraint such that $m = k \cdot n$. This implies that the exact number of channels required to satisfy each network is available or the utilization rate is 1.0. We studied cases where $k = 1$
and $k = 2$ to show the strengths of the two heuristics being compared.

Figure 2.12: Comparison of CFL and FAK heuristics with the system having the exact number of channels to satisfy the networks’ channel size requirements.

We can observe that CFL is more suitable for channel acquisition than FAK when $k = 1$. While CFL converges faster when $k = 1$, FAK converges faster than CFL when $k = 2$. For the case where $k = 2$, CFL’s convergence becomes non-deterministic when $n > 20$. On the contrary, FAK is more scalable, converging faster and even further up until $n > 25$. For single channel acquisition, both FAK and CFL guarantee convergence of the system, irrespective of the increase in system size.

**Impact of System Size on Convergence**

In previous section, we provided results for multiple channel acquisition for large system of networks. Here, we show the results obtained for both small and large system of networks. The results show the comparisons of our FAK heuristics with CFL, which is self-acclaimed as the fastest channel selection heuristics in recent works. As a result, our focus will be based more on convergence time and the amount of contentions experienced in the system. The small network setting has a configuration where $k = 2, m = 20$ and $5 \leq n \leq 10$, while the large network setting has $k = 5, m = 200$ and $5 \leq n \leq 30$. 
Figure 2.13: Performance comparison of CFL and FAK algorithms based on convergence time in small network configuration.

Figure 2.14: Performance comparison of CFL and FAK algorithms based on convergence time in large network configuration.
Figure 2.15: Comparison of spectrum contention in CFL to their worst case of spectrum contention

**Spectrum Contention**

We investigated how CFL and FAK heuristics performed in terms of the number of spectrum contentions observed during implementation. The actual number of spectrum contentions is compared to the expected number of spectrum contention in the worst-case scenario. The expected number of spectrum contentions in the worst scenario is derived by assuming that contentions occurred throughout the time that it would normally take the system to converge. We observed that in the case of FAK, the system registered far less number of spectrum contentions with only 9% of expected number of spectrum contention in the worst case scenario. On the other hand, the system, implementing CFL, registered high level of spectrum contentions and experienced, on average, 16% of expected number of spectrum contentions in the worst case scenario.
CHAPTER 2. CHANNEL ACQUISITION IN COGNITIVE RADIO NETWORKS

Figure 2.16: Comparison of spectrum contention in FAK to their worst case of spectrum contention.

2.6 Conclusion

In this chapter, we discussed heuristics for multiple channel acquisition. The proposed heuristics offers decentralized solution to the problem of self-coexistence of cognitive radio networks. CR networks that operate in a spectral environment where communication is constrained can implement any of the proposed heuristics. We have presented an argument that control messaging is inapplicable in a decentralized system that lacks centralized control and embodied with communication constraints. Networks operating in such systems do not have sufficient knowledge of spectrum choices made by their neighbors. Given the dynamic nature of the spectrum and the cost of setting up control channels, a befitting solution for channel selection or acquisition should employ a decentralized approach.

The proposed multiple channel acquisition heuristics implement decentralized mecha-
nisms that require no coordination among networks in the system. Our proposed channel selection scheme ensures that the best channels are selected based on channel profile history. Some of the heuristics like RENO and TAHOE implement back-of mechanisms that allow them to avoid contention and maintain system utility. We also show that the performances of the heuristics are quite consistent and fairly robust to rare primary user presence in the spectrum.

We compared the performance of our heuristics to the CFL algorithm. We found INCR and FAK heuristics can contend with the CFL algorithm in terms of convergence time. CFL algorithm is best suited for single channel acquisition cases, while FAK converges faster in multiple channel acquisition. FAK algorithm is also scalable with respect to the number of networks, showing better convergence compared to CFL. FAK algorithm guarantees the convergence of the system, provided there exists a spectrum allocation that satisfies the channel size requirements of the contending CR networks.

In conclusion, we emphasize that the multiple channel acquisition heuristics are well suited for such wireless network scenarios where there is no prior knowledge of channel availability and no history profile about both primary and secondary users activities. The heuristics are also adaptable to scenarios where cognitive radio networks cannot exchange control messages to avoid contention with one another. The heuristics are quite simple to implement, efficient and inexpensive. There is no overhead cost due to messaging, and the memory cost is quite insignificant.
Chapter 3

Distributed and Cheat-proof
Spectrum Contention Scheme for
IEEE 802.22 Wireless Regional Area Networks

3.1 Introduction

The adaptive On-Demand Spectrum Contention (ODSC) protocol is a self-coexistence oriented protocol, designed specifically for WRAN networks [58] [59]. The ODSC protocol leverages the MAC messaging on the inter-network communication channel to provide inter-network spectrum sharing among coexisting WRAN networks. The protocol is designed to allow WRAN networks to compete for shared spectrum by simply exchanging and comparing randomly generated contention priority numbers (CPNs). Several flaws have been identified with the ODSC protocol, which can jeopardize the fairness guarantees and also impact negatively on system performance. ODSC protocol is prone to random number gen-
Figure 3.1: Finite state machine diagram of spectrum contention in 802.22 WRAN networks.

The vulnerability in the ODSC protocol allows for possible CPN manipulation, where participants can manipulate the generated CPNs in order to win the contention process. The contention destination can easily ignore or overlook the ODSC request sent by contention sources and declare itself the winner of the contention process. Given the above scenarios, it becomes possible for one or more participants to “hijack” available spectrum resources, thereby eroding the fairness that the ODSC protocol was designed to provide.

In this chapter, we address vulnerabilities associated with the ODSC protocol. We propose a modified version of the protocol that mitigates the possibility of CPN manipulation by
spectrum contenders, thereby promoting fairness and self-coexistence. We also investigate and propose ways to improve system utility, leveraging the proposed spectrum contention scheme.

3.2 System Model

Consider a typical deployment scenario of multiple WRAN networks, each consisting of a base station (BS) and related customer premise equipment (CPE). The communication range of a WRAN network could extend up to 100 km [26] [84] and may overlap with other WRAN networks in its vicinity. Spectrum resources that are not being used by the licensed incumbents are allocated in such a way as to mitigate interference during the operation of the WRAN networks. A typical deployment of WRAN networks is illustrated in Figure 3.2. Suppose there are \( n \) IEEE 802.22 WRAN networks in the system. The BSs of these networks participate in spectrum contention to gain access to a specific channel. The system of WRAN networks can be represented as an undirected interference or conflict graph \( G = \{N, E\} \) where \( N = \{N_i\} \) is the set of vertices denoting the WRAN networks and \( n = |N| \). \( E \) is a set of undirected edges denoting the existence of interference constraints existing between any given two networks. For instance, if an edge \((i, k)\) exists in \( E \) for a channel \( C_j \), then both \( N_i \) and \( N_k \) cannot operate simultaneously on channel \( C_j \) without interference. Assuming \( N_k \) is the contention destination currently occupying channel \( C_j \), then possible contenders or set of contention sources is defined as the set \( N^c = N \setminus N_k \cup \{N_i : (i, k) \in E\} \).

We assume that in the system, there are \( m \) available channels. Each channel is partitioned into synchronized superframes which is further partitioned into 16 frames of fixed length. Each frame is further divided into Data Transmission Period (DTP) and Beacon Period (BP) just like in CBP protocol [26]. Availability of the channels is time-variant and largely dependent on the activities of the licensed incumbents. Without loss of generality, we assume
that all WRAN networks are aware of the system topology that imposes the operational constraints on the use of the available frequency bands. Primary-secondary etiquette is strictly observed in the system. The secondary-secondary etiquette is enforced by allowing WRAN networks to request spectrum contention instead of blindly grabbing any available channel for transmission. Utility derived by WRAN networks is dependent on the throughput obtained while operating on the channels. We assume that when two WRAN networks are in close proximity and transmitting on the same frequency band(s), interference will occur.
As a result, no utility is derived since the interference could exceed the signal to interference and noise ratio (SINR) requirements, causing the transmissions to fail [59].

### 3.3 On-Demand Spectrum Contention Protocol

On-demand spectrum contention (ODSC) protocol is a distributed, cooperative, and real-time spectrum sharing protocol. The fundamental idea of the protocol is based on allowing BSs of coexisting WRAN networks to contend for shared spectrum resources on an on-demand basis [26]. Figure 3.3 shows the conventional ODSC protocol as described by Hu et al. in [26].

The ODSC scheme works as follows. An occupant of a channel, referred to as contention destination (DST), regularly send ODSC announcement messages (ODSC ANN), informing neighbors of the occupied channel. A spectrum-demanding network, also known as contention source (SRC), upon receiving such announcements prepares an ODSC request message (ODSC REQ) and forwards it to a randomly selected DST.

The ODSC REQ message includes a CPN which can be either a real number uniformly selected from the range \([0, 1]\) or an integer selected uniformly at random from the range \([0, 2^x - 1]\) with \(x\) being an arbitrary integer generally accepted in the system. DSTs also maintain an ODSC REQ window during which they expect to receive ODSC REQ from channel contenders. At the end of the ODSC REQ window, if any ODSC REQ was received, a DST network generates a CPN and compares it with the CPNs from other SRCs.

When a DST network receives the CPNs, it proceeds to aggregate them and decide the winner based on the spectrum contention resolution scheme adopted in the system. Once the spectrum contention decision is made, DST network sends out an ODSC response message (ODSC RSP), appending the identity of the spectrum contention winner. Suppose that the criteria for winning spectrum contention in the system are based on contender with the
smallest CPN wins. If a DST network’s CPN is the smallest (highest priority) among all CPNs compared, then it will send an ODSC_RSP message to all SRC networks indicating contention failure. Otherwise, winner SRC network will receive an ODSC_RSP indicating contention success while other SRC networks receives messages indicating contention failure. The winner SRC then sends an acknowledgement message (ODSC_ACK) indicating the time when it intends to acquire the contended channel. A channel release is scheduled by all DST networks operating within operating range of the winner SRC network via an ODSC release message (ODSC_REL). ODSC_REL specifies the channel to be released, the channel release time and winner SRC network’s identification.

Figure 3.3: A diagram illustrating conventional ODSC protocol.
3.3.1 Vulnerabilities of ODSC Protocol

ODSC protocol is far from a perfect protocol for fostering self-coexistence of WRAN networks. We can identify some of the loopholes in the protocol design that could jeopardize self-coexistence among the networks. Some of the assumptions made in ODSC protocol include:

1. CPNs are actually generated uniformly at random from the range specified and agreed upon by the system of WRAN networks;

2. DSTs, serving as arbiters during spectrum contention processes, are honest and unbiased;

3. CPN collisions are rare or practically impossible.

The first assumption deals with the generation of the CPNs used in spectrum contentions. Prior to the deployment of the WRAN networks, a decision is reached on the criteria used in deciding the winner of a spectrum contention. With this information, the BSs might be tempted to manipulate their CPNs in order to win the contention. The second assumption grants unlimited authority to incumbent DSTs to decide the outcome of spectrum contentions. DSTs can reach decisions in favor of themselves, regardless of the CPNs sent by SRCs. Even though the possibility of CPN collisions is quite negligible depending on the range $w = 2^x$, it is still important to address such situations. In the ODSC system, a criterion is usually adopted for spectrum contention resolution; for instance the owner of the smallest CPN wins. With this knowledge, some contenders might decide to generate the smallest possible CPN value in order to win a spectrum contention. This makes CPN collisions more frequent. The best approach to conduct spectrum contention is to hide the criterion for spectrum contention resolution from participants, thereby forcing them to use random CPN generators. However, this approach still leaves loopholes in ODSC because
DSTs still reserve the right to: 1) decide the criterion; and 2) announce the winner of the spectrum contention. Also the protocol fails to consider repeated spectrum contentions that can lead to channel reuse, which can improve efficiency of spectrum utilization.

### 3.4 Modified ODSC Protocol

We propose a distributed and cheat-proof spectrum contention protocol, otherwise known as Modified ODSC. MODSC addresses issues related to the ODSC protocol. Our approach supports an open and distributed decision-making process, which involves every network contender. Also, it eliminates the need for a fixed range in generating CPN numbers, such that CPNs can be any number within the interval \([0, \infty]\). As we have stated earlier, spectrum contentions are conducted to decide which network gets the opportunity to operate on a contended channel. To encourage self-coexistence among the WRAN networks, the spectrum contention process must be fair to all participant networks. This means that the process must be devoid of bias and cheating. Therefore, all networks participating in spectrum contention should be able to determine the winner in a distributed manner. This eliminates the monopoly enjoyed by DSTs in making spectrum contention decisions.

MODSC protocol is designed to support distributed spectrum contention. One of the weaknesses of ODSC protocol is that spectrum contention is centralized and introduces bias in the spectrum contention. In MODSC, all networks participating in the spectrum contention take part in the spectrum contention decision process. Networks exchange their CPNs with one another and each network uses a global spectrum contention resolution scheme to decide the winner. The spectrum contention resolution scheme shall be discussed later in this section. With MODSC, no one DST network is reserved the monopoly to decide the outcome of a spectrum contention process. All contenders make decisions simultaneously and are expected to have the same outcome.
In ODSC protocol, the DST networks exercise monopoly in deciding the outcome of every spectrum contentions they conduct. As a result, the spectrum contention process can be biased towards the potential DST networks, giving them an edge to occupy the available channels. Our proposed solution intends to prevent the type of cheating and afford every spectrum contender equal opportunity to the available spectrum resources. First, we suggest that each contending network, including DST networks, to exchange CPNs at the same time. The exchange introduces transparency in the spectrum contention process, as SRC networks are able to know the CPNs of the DST networks, which in ODSC protocol is hidden from the SRC networks. The spectrum contenders can then apply the spectrum contention resolution scheme to decide the winner.

However, while exchanging CPNs, a malicious BS may delay sending a CPN in order to first read the CPN of fellow contender. Reading a contender’s CPN gives the BS an opportunity to manipulate its CPN. To resolve this delay-induced cheating problem described above, we apply the zero knowledge proof (ZKP) technique [85]. The ZKP technique is a method by which parties can prove to one another that their declarations are true without conveying any extra information apart from the declarations themselves.

To implement this technique, spectrum contenders are required to exchange irreversibly hashed values of their CPNs before their actual CPNs are exchanged. The hashed CPNs can prove generation time of the later-to-be-exchanged CPNs without exposing their actual values. The hash function used for this purpose can be any irreversible hash function with no known collisions beyond certain input size, such as SHA1 and SHA256. An additional requirement due to the use of hash functions is the need for CPNs to be sufficiently long to prevent dictionary attacks and minimize the rare possibility of collisions. A digest size of 128 bits has been shown to be sufficient to protect the hash value of the CPNs from collisions [86]. BSs should have a fixed broadcast window to exchange their hashed CPNs with each other. Spectrum contenders exchange their actual CPNs after all hashed CPNs
have been received. Then validation of CPNs follows, with each contender comparing hashes of the received CPNs with the hashed CPNs received earlier on. At the end of the comparison, the decision function is applied to determine the winner. If the validation process fails, then other contenders are notified and the spectrum contention is annulled by majority vote.

An illustration of MODSC message exchange is shown in Figure 3.4. MODSC scheme starts with the broadcast of announcement message ANN by the DSTs. DSTs are required to broadcast their current channels at the beginning of each frame. The ANN messages are piggy-backed with the hash CPN of broadcasting DSTs. Leveraging the spectrum contention request message REQ, SRCs declare their interest to contend with DSTs. REQ message contains SRC identity, contended channel and hash CPN for spectrum contention. Following the exchange of the hash CPNs, the participants exchange their actual CPNs, which is encapsulated in MSG messages. Hashed CPNs are exchanged before actual CPNs to prevent
CPN manipulation. Each network checks the received hash CPNs against the actual CPNs. Using the spectrum contention resolution scheme, each network computes the winner of the spectrum contention. Since the output is expected to be the same, the networks will know the winner with no need for message exchange. The contended channel is then released to the winner network.

### 3.5 Spectrum Contention Resolution Schemes

In ODSC, the source network is arbiter that decides the winner of a spectrum contention. Inherent in the assignment of the responsibility to the source are the assumptions that the source network is an honest arbiter and not biased towards any of the contending network. The decision is reached by combining randomly generated contention priority numbers provided by the contending the networks. Assuming we have a set of networks $N^{(j)}$ contending for channel $j$, with one of the networks as the contention source. The decision function $D$ used by the source network is defined as

$$D(x) = \arg\max_{N_i \in N^{(j)}} \{x_i\} \quad (3.1)$$

where $x = \{x_i : i \in |N^{(j)}|\}$ is the set of CPNs of channel contenders. Based on the agreement reached among the networks, the criteria for selecting the winner can be flipped such that the network that generates the smallest CPN wins the spectrum contention. However, losers (contention destinations) may be unsatisfied by the decision reached by the contention source because the decision process is not transparent and is prone to manipulation.

In some case, the decision about the winner of the spectrum is conducted in a pair-wise manner [87]. With pair-wise spectrum contention, the contention source can win with a probability of $1/2$. A contention source is declared the winner only if it wins all pair-wise spectrum contentions. The problem with pair-wise contention is that it can lead to cascading
spectrum contention problem addressed in [60]. Unsatisfied contenders can trigger a series of spectrum contention instances that spreads across the network and waste spectrum resources.

3.5.1 Contention Window Manipulation

Spectrum contention resolution scheme of ODSC assume that all contending networks have equal probability to win. This is based on the assumption that all contending networks generate unique CPN numbers, thereby making CPN collision impossible. Even if the CPN numbers are uniformly generated real number between 0 and 1, the possibility of a collision cannot be completely ignored.

We proceed to show that the probability of winning to both source and destination networks is not exactly $1/2$, especially in a case where CPN is an integer. Actually, the chance of winning is dependent, among other factors, on the contention window $W \in \mathbb{Z}^+$, which specifies the range of CPN numbers generated by a network’s pseudo-random generator. We assume that all networks generate CPN number from the range $[1, W]$. We show that it is possible to manipulate the outcome of a spectrum contention by simply shrinking or extending $W$. This implies manipulation of the pseudo-random generator to produce winning CPNs.

We consider a case where there are two overlapping WRAN networks $N_i$ and $N_k$ in involved in a pairwise spectrum contention. $N_i^{(j)}$ denotes that network $N_i$ is contending channel $j$. Suppose we denote the windows used by both networks as $W_i$ and $W_k$ and random CPN variables as $r_i \in [1, W_i]$ and $r_k \in [1, W_k]$. Assuming $N_k$ can select CPN $w \in [1, W_k]$, then the chances of $N_i$ winning the contention will depend on whether it is able to generate CPN within the range $[w + 1, W_i]$. This is the joint probability of $N_j$ picking CPN $r_k$ and $N_i$ picking $r_i$ from $[r_k + 1, W_i]$. Thus, probability that $r_i$ greater than $r_k$ is
Pr\left( S_{i>k} \right) = \sum_{w=1}^{W_k} \frac{1}{W_k} \cdot \frac{W_i - w}{W_i} = \frac{1}{W_i \cdot W_k} \sum_{w=1}^{W_k} W_i - w \quad (3.2)

where $S_{i>j}$ denotes the event that $N_i$ wins the spectrum contention over $N_j$. We expect that when $W_i = W_k$, then $Pr(S_{i>k}) = Pr(S_{k>i})$. Hence,

$$Pr(S_{i>k}) = Pr(S_{k>i}) = \frac{W - 1}{2W} \quad \text{where } W = W_i = W_k \quad (3.3)$$

Considering that the spectrum contention might end up in a tie, we have $Pr(S_{i>k}) + Pr(S_{k>i}) + Pr(S_{i=k}) = 1$, where $S_{i=k}$ denotes an event where there is a tie. Solving for $Pr(S_{i=k})$, we have that,

$$Pr(S_{i=k}) = \frac{1}{W} \quad (3.4)$$

The significance of this result is that the probability of having tie is non-zero and very much dependent on the value $W$, which is likely to be fixed for all contending networks. However, it is a serious assumption to make, considering the possibility that contenders might use different window sizes. Alteration of the window sizes introduces bias whether $W_i > W_k$ or $W_i < W_k$. So in a case where $W_i \neq W_k$, we have

$$Pr(S_{i>k}) = 1 - \frac{W_k + 1}{2W_i} \quad (3.5)$$

and also,

$$Pr(S_{k>i}) = 1 - \frac{W_i + 1}{2W_k} \quad (3.6)$$

It is not hard to observe that when $W_i > W_j$ then $N_i$ has undue advantage over $N_k$ because it can generate larger numbers. So we have,

$$Pr(S_{i>k}) = \sum_{w}^{W_k} \frac{1}{W_k} \cdot \frac{W_i - w}{W_i} \quad (3.7)$$
and also,

$$\text{Pr}(S_{k>i}) = \sum_{w}^{W_i} \frac{1}{W_i} \cdot \frac{W_k - w}{W_k}$$  \hspace{1cm} (3.8)$$

Equation 3.7 reduces to equation 3.5 on further simplification. Expanding equation 3.8 we have

$$\text{Pr}(S_{k>i}) = \sum_{w}^{W_k} \frac{1}{W_i} \cdot \frac{W_k - w}{W_k} + \sum_{w=W_k+1}^{W_i} \frac{1}{W_i} \cdot \frac{W_k - w}{W_k}$$  \hspace{1cm} (3.9)$$

The second component on the R.H.S. of equation 3.9 reduces to zero, since $N_k$ cannot generate such $r_k > W_k$. As a result $\text{Pr}(S_{k>i})$ becomes

$$\text{Pr}(S_{k>i}) = \frac{W_k - 1}{2W_i}$$  \hspace{1cm} (3.10)$$

It is easy to show that $\text{Pr}(S_{i>k}) > \text{Pr}(S_{k>i})$, which implies that the spectrum contention resolution is biased towards $N_i$. Suppose $N_i$ has zero probability of winning, that is, $\text{Pr}(S_{i>k}) = 0$. This implies that $W_i = (W_k + 1)/2$ (see equation 3.5), which is a contradiction since we started off with the assumption that $W_i > W_k$. So $N_i$ has a non-zero probability of winning the contention. Likewise, if we suppose that $\text{Pr}(S_{k>i}) = 0$, then we have $W_k = 1$. Plugging this into equation 3.5, we have $\text{Pr}(S_{i>k}) = (W_i - 1)/W_i$. This means that the best outcome of spectrum contention between $N_k$ and $N_i$ is a tie, which happens with a probability equivalent to $1/W_i$. Fairness can be achieved only when $\text{Pr}(S_{i>k}) = \text{Pr}(S_{k>i})$. Solving equality, we have,

$$1 - \frac{W_k + 1}{2W_i} = \frac{W_k - 1}{2W_i}$$

$$2W_i - W_k - 1 = W_k - 1$$  \hspace{1cm} (3.11)$$

$$W_i = W_k$$
This represents the condition that must be satisfied for a spectrum contention to be declared fair. The significance of the bias that exists when $W_i > W_k$ can be seen by simply plugging in real numerical values. For instance, when $W_i = W_k + 1$ and $W_k = 256$, $\Pr(S_{i>k}) = 0.5$ and $\Pr(S_{k>i}) = 0.496$.

Consequently, a contending network with the largest $W_{max}$ has an undue advantage of winning over others when the decision function $D$ is defined as in equation 3.1. The reverse is the case when the contention resolution rule is such that the network with the smallest CPN wins. In such a case, a contending network with $W_{min}$ will win most of the time.

### 3.5.2 MODSC Spectrum Contention Resolution Schemes

We suggest two spectrum contention resolution schemes for pairwise and $n$-wise spectrum contention. With these resolution schemes, all participating networks unanimously reach a decision on the winner of a spectrum contention. There are no criteria involved (min or max) and all participants arrive at the same conclusion using a common decision function in a distributed manner.

**Pairwise Spectrum Contention Resolution**

Pairwise spectrum contention entails that only two BSs are involved in the contention process. The process initiated by a contention source interested in an advertised channel. Suppose two BSs $N_i$ and $N_k$ generated and exchanged CPNs $x$ and $y$ respectively. The decision function $D(x, y)$ for the spectrum contention resolution is given as

$$D(x, y) = F(x, y) \oplus G(x, y)$$  \hspace{1cm} (3.12)

where $\oplus$ is an XOR logical operator. The function $F(x, y) \in \{0, 1\}$ is defined as $F(x, y) = (x + y) \text{ mod } 2$ and $G(x, y) \in \{0, 1\}$ is defined such that $G(x, y) = 0$ when $x < y$, and $G(x, y) = 1$ when $x > y$. In a case where $x = y$, the spectrum contention is repeated.
The function $G(x, y)$ introduces uncertainty in $D(x, y)$ by taking into consideration the relative values of $x$ and $y$. The computation of $D(x, y)$ is carried out independently by the BSs and the outputs expected to be the same, provided CPNs are not manipulated. We assume that prior to the spectrum contention, contenders have agreed to an injective function $f : N_i \rightarrow \{0, 1\}$ that uniquely maps each contender to an element in $\{0, 1\}$. By this means, each participant will know who won the contention after computing $D(x, y)$.

### N-wise Spectrum Contention Resolution

Given a scenario where spectrum contention can involve more than two BSs, the decision function derived for pairwise spectrum contention resolution cannot be used. If the pairwise spectrum contention resolution is used, at least $O(\log n)$ spectrum contentions would be required to decide the winner, with $n$ being the number of contending BSs. The decision function for $n$ contenders will be a function with $n$ input parameters denoted as $x = \{x_i \mid x_i \in \mathbb{Z}^+\}_{i=1}^n$. We define the function as

$$D(x) = D(\{x_1, \cdots, x_n\}) = \left[ \sum_{i=1}^n x_i \right] \mod n \quad (3.13)$$

$D(x) \in \{i\}_{i=0}^{n-1}$ is inherently uniformly distributed assuming that the randomly generated CPN values were also uniformly generated, that is, $D(x) \sim U(0, n - 1)$. The earlier decision function cannot be applied because $F(x) \oplus G(x) \sim U(0, n - 1) \ \forall x_i \in \mathbb{Z}^+$. With the help of the decision function $D(x)$ and a predefined mapping function $f : i \rightarrow N_i$, each participant has an equal chance to emerge as the winner of a spectrum contention. The simultaneous and independent computation of $D(x)$ to reach a unanimous decision in a distributed manner rids the malicious DSTs of the capability of altering spectrum contention outcomes.
3.5.3 Non-Cheatable and Collision-Proof of MODSC

The design of MODSC emphasizes non-cheatability in terms of CPN manipulation. Spectrum contention processes should also be collusion-proof. This means that no group of WRAN networks can collude to alter the outcome of spectrum contention in their favor. Suppose that spectrum contention is a game and each network selects a CPN independently of the other networks. We can consider the choice of a particular CPN $x_j$ as a pure strategy such that $x_j \in [x_{\text{min}}, x_{\text{max}}]$ is a pure strategy. Using a random CPN generator with a probability mass function $\Pr(x)$, a mixed strategy of these pure strategies can be derived. Regardless of strategies (pure or mixed) implemented by the players (BSs), no player should have an advantage over another in winning the spectrum contention game. The spectrum contention should present to every player with equal opportunity to win, provided the CPNs are not tampered with. Therefore the decision function must meet the non-cheatability and collusion-proof criteria to be considered applicable in deciding winners of spectrum contentions.

**Definition 2.** A non-cheatable decision function $D(x)$ need to satisfy the following condition: Each player has a strategy $s_0$ that guarantees at least $\frac{1}{n}$ to win regardless of other players’ strategies i.e. $\Pr(D(x) = k) \geq \frac{1}{n}$ when $x_k \sim s_0$.

**Definition 3.** A collusion-proof decision function $D(x)$ need to satisfy the following condition: For a colluding set of players, $C \subset \{N_1 \ldots N_n\}$, regardless of the collusion scheme $\Pr(\{x_k \in C\})$, $\Pr(D(x) \in C) \leq \frac{|C|}{n}$.

**Proposition 3.5.1.** Any non-cheatable decision function is collusion-proof, and vice versa.

Proposition 3.5.1 is quite obvious. Since $D(\{x_k\}_{k=0}^{n-1})$ is non-cheatable, all players not belonging to the colluding set $C$ use strategy $s_0$, such that $\Pr(D(\{x_k\} \notin C)) \geq \frac{n-|C|}{n}$. This also implies that $\Pr(D(\{x_k\} \in C)) \leq 1 - \frac{n-|C|}{n} = \frac{|C|}{n}$.
CHAPTER 3. SPECTRUM CONTENTION SCHEME FOR IEEE 802.22 WRANS

The non-cheatability condition assures that regardless of the strategy employed by players, the probability of winning remains the same for all. Collusion-proof condition ensures that collusion among players cannot increase their chances of winning the game. This condition is obviously necessary for every individual player. Thus, for every individual player $N_i$, there exists a strategy $s_0$ such that if all other players are to collude, $s_0$ still guarantees a fair winning probability $\frac{1}{n}$ to the individual players. That is, $\Pr(D(x) = N_i) \geq \frac{1}{n}$ if $x_i \sim s_0$.

We proceed to give the proof of non-cheatability and collusion-proofness of the decision function stated in equation 3.13. We recall that the domain for the set of CPNs $\{x_k\}$ is all integers from 0 to $W - 1$, where $r \gg W$.

**Proof.** Suppose we have a certain player $N_i, i \in 1 \cdots n$. If player $N_i$ uses the strategy

$$\Pr(x_i = a | a \in 0 \cdots W - 1) = \frac{1}{W}$$

Then the probability of $N_i$ winning among $n - 1$ other contenders can be expressed as

$$\Pr((a + \sum_{k \in 1 \cdots n \setminus \{i\}} x_k) \mod n = i)$$

Suppose other players adopted a joint strategy such that $\Pr(\{x_k\}_k \in 1 \cdots n \setminus \{i\})$ with a certain probability mass function $p_y(y)$ such that $y = \sum_{k \in 1 \cdots n \setminus \{i\}} x_k$. Obviously, $y \in 0 \cdots (n - 1)(W - 1) - 1$ and $\sum_{y=0}^{(n-1)(W-1)-1} 1 = 1$ (fairness within collusion). Therefore, for a specific $y_0$ we have that

$$\Pr((y_0 + x_i) \mod n = i) = \Pr(x_i \mod n = (i - y_0 \mod n) \mod n)$$

We know that the $x_i$ is uniformly distributed within the range $[0, \cdots, W - 1]$ and $W \gg n$. Then $\forall m \in 0 \cdots n - 1$, $\Pr(x_i \mod n = m) \approx \frac{1}{n}$. So the probability of player $N_i$ to win,
given that \( y \) is distributed according to \( p_y(y) \), becomes

\[
\Pr((y + x_i) \mod n = i) = \sum_{y=1}^{(n-1)(r-1)-1} p_y(y) \cdot \Pr(x_i \mod n = (i - y \mod n) \mod n) \\
= \frac{1}{n} \cdot \sum_{y=1}^{(n-1)(r-1)-1} p_y(y) \\
= \frac{1}{n}
\]

\[\square\]

### 3.5.4 Channel Reuse

We can represent the WRAN networks as a conflict graph \( G(N, E) \) defined by a set of nodes (networks) \( N = \{N_i\} \) and a set of conflict edges \( E = \{(i, k) : i \neq k \land N_i, N_k \in N\} \). Two networks cannot simultaneously operate on the same channel without interference if there is an edge between them. To decide who operates on a contended channel, neighbors participate in spectrum contention.

Consider a complete conflict graph \( G(N, E) \) with a set of variable neighbor degrees \( \{d_i\} \) with a single channel \( j \) available for all networks. Isolated spectrum contention can cause cascading spectrum contention problem, which leads to wastage of spectrum resources. As an alternative, we suggest a spectrum contention, involving all interested networks. At the end of the spectrum contention, one winner emerges that can operate without interference. However, some networks that do not share an edge with the winner network are deprived of spectrum opportunity. By conducting another spectrum contention, at least one network might benefit from the shared channel.

Suppose the winner of a spectrum contention on channel \( j \) is network \( N_k \). We denote the set of networks that are qualified to participate again in spectrum contention as \( N^c \). We express \( N^c \) as
\[ N^c = N \setminus N_k \cup \{N_i : (i, k) \in E\} \]

Provided that \( N^c \neq \emptyset \), repeated spectrum contention leads to channel reuse, which enhances spectrum utilization.

Although repeated spectrum contention enhances spectrum utilization, not every network receives fair share of the spectrum opportunity. The high neighbor degree reduces the chances of a network winning the spectrum contention. Assuming in the \( t \)-th round, \( N_i \) participates in a spectrum contention involving \( n_t \) contending networks. We define the event that \( N_i \) wins as \( S^t_i \). Obviously, the probability \( \Pr(S^t_i) \) wins in the current round \( t \) is \( 1/n_t \), provided that the spectrum contention was fair.

However, \( N_i \) might not win in round \( t \) but have a chance to win in subsequent rounds. It is important to know that the chances of \( N_i \) winning in the next round of spectrum is dependent on its position in the conflict. If \( N_i \) shares a link with the last winner, then \( N_i \) automatically excluded from the next contest. This implies that the probability of \( N_i \) winning in the next round is the joint probability of \( N_i \) losing in current round, not sharing an edge with the winner and being the winner of the next round of spectrum contention. Thus, the probability \( \Pr(S^{t+1}_i) \) that \( N_i \) wins the next round of spectrum contention, with a neighbor degree \( d_{i,t} \) is defined as

\[
\Pr(S^{t+1}_i) = \left(1 - \frac{1}{n_t}\right) \cdot \left(1 - \frac{d_{i,t}}{n_t - 1}\right) \cdot \frac{1}{n_t - d_{i,t} - 1} 
\]

(3.14)

where \( n_{t+1} = n_t - d_{i,t} - 1 \).
3.6 Numerical Results

In this section, we present a numerical analysis and performance evaluation of ODSC and MODSC spectrum contention schemes. The network topologies shown in Figure 3.5 are used in our analysis. We assume that there is a single channel for the entire system of WRAN networks. We adopt the Beacon Period Framing (BPF) protocol that guarantees reliable, efficient and scalable internetwork communication [26]. Jain’s fairness index is used in quantifying the degree of fairness in the system. System utility is measured in terms of the number of superframes used by networks without any interference.

Depending on network topology, an additional spectrum contention can be conducted before the end of a superframe. This leads to reallocation of the same channel to another non-interfering WRAN network, which we refer to as channel reuse. Channel reuse is possible if there is at least a single WRAN network, whose operations on the contended channel will not interfere with the operations of the winner network from the previous contention(s). It is important to note that since the winner of a spectrum contention is decided simultaneously, losers will know instantly whether to initiate another spectrum contention for a possible channel reuse. The knowledge of network topology also helps losers to ascertain conflicting scenarios and avoid initiating spectrum contention. We denote channel reuse as the

Figure 3.5: Network topologies used in simulating ODSC and MODSC spectrum contention scenarios.
CHAPTER 3. SPECTRUM CONTENTION SCHEME FOR IEEE 802.22 WRANS

parameter \( r \), which represents the number of spectrum contentions that can be conducted or allocations that can be made for the same channel. For instance, \( r = 3 \) indicates that it is possible to conduct 3 spectrum contentions in a superframe.

3.6.1 Fairness in ODSC System

Simulation results show that fairness in a system of WRAN networks implementing the ODSC protocol depends on network topology. We use the well-known Jain’s Fairness Index (JFI) to measure fairness in the system. Given that the ODSC scheme is highly vulnerable, we simulated the impact the presence of malicious contenders will have on fairness in the system. We assume that the malicious contenders can make transitions between two states: active and inactive states. We note that an active malicious DST always declares itself the winner of any spectrum contention process. On the other hand, an inactive malicious DST follows the specified guidelines of the protocol in determining the winner of any spectrum contention process. For experimental purposes, we assume a malicious DST makes a transition from inactive state to active state with a probability \( p \) and makes a reverse transition with a probability \( 1 - p \). Simulation results are presented in Figure 3.6. The results show how fairness in the system varies with \( p \) for the select network topologies.

In this experiment, we set the number of WRAN networks \( n = 20 \). Also a malicious contender is selected randomly at the beginning of the simulation, invariant to the contender’s position in the network topology. We observed that with low malicious transition probabilities, the ODSC protocol achieves near-optimal fairness. As we know the network topology reflects the coexistence constraints existing in the system. This explains the difference in fairness under the different network topologies. In a complete network topology, all participants are aware that only one network can operate at any time, despite the possibility of cheating occurring in the system. When \( p \) is high, we have a scenario where one network can highjack the contended channel and refuse to release it. Fairness in wheel and cycle
network topologies are purely affected by the fact that more than one network can win the right to operate on the channel. This creates the possibility of adjacent winners of spectrum contention that could interfere and lay wastage of the spectrum opportunity. The winners are thus denied of their fair share of the spectrum opportunities that might arise. In general, scenarios with high $p$ and either cycle or wheel network topology are far better and more stable in terms of fairness than scenarios with complete network topology.

### 3.6.2 MODSC Performance in Different Network Topologies

Performance of the MODSC system under the three selected network topologies using the average system utility metric is illustrated in Figure 3.7. Average system utility is best in a system with cycle network topology, where each WRAN network has at most two neighbor WRAN networks. In a complete network topology, even though spectrum opportunity is stable, we observe a steady decline in average system utility with increasing number of networks. The results obtained emphasize the importance of placement of the WRAN networks...
in the expected system performance. To maximize system performance, WRAN networks have to be setup at locations where they have minimal number of neighbors. In cases where this requirement cannot be met, especially in a complete network topology scenario, MODSC ensures that self-coexistence among networks is maintained. The in-built features of the protocols mitigate against CPN manipulation and eliminate the possibility of cheating during spectrum contentions.

### 3.6.3 Performance Comparison of ODSC and MODSC

ODSC protocol stipulates that SRCs send spectrum contention requests on demand to contention destination DSTs. With this approach, SRCs need at least one DST to commence any spectrum contention process. Even if by chance, one or more SRCs discover that their operations on the contended channel will not interfere with the winner of the just concluded spectrum contention, no spectrum contention can be conducted until the next superframe when the winner DST sends out an ODSC\_ANN message. This leads to the wastage of the

![Graph](image)

**Figure 3.7:** Average system utility derived in MODSC system.
spectrum opportunity, which one of the SRCs could have benefited from. Furthermore, the fact that SRCs have to randomly or systematically select a DST to contend with creates a self-coexistence problem. Consider a WRAN network with a wheel network topology depicted in Figure 3.8. Before spectrum contention, there is a set of DSTs \( \{C, E\} \). During the contention process, the SRCs \( \{A, B, F, D\} \) have to select independently one DST to contend with. Suppose those that decided to contend \( C \) are \( Y_C = \{A, F\} \) and those that decided to contend with \( E \) are \( Y_E = \{D, B\} \). If after the spectrum contention, \( F \) and \( D \) emerge as winners of their respective contention processes, then both BSs cannot operate without interfering with one another. According to the provisions of ODSC no spectrum contention takes place until the next superframe. As a result of this restriction, the entire spectrum opportunity is wasted.

![Figure 3.8: An illustration of a typical ODSC spectrum contention scenario.](image)

However, with MODSC, the procedure is quite different. When a BS initiates spectrum contention request for a specific channel, all interested BSs will participate in the process. Their participation allows them to know the winner of the spectrum contention simultaneously. Then, with the help of this information and the network topology, the BSs will know exactly whether to initiate another spectrum contention before superframe ends. The BP frame size and the number of BPs in a superframe limit channel reuse, which is the same as the number of spectrum contentions that can be conducted in a given superframe. Using
illustration in Figure 3.9 as an example, we see that in the worst case, \( r = 1 \) and exactly one BS emerges a winner at the end of the first round of contention. Let us assume that the winner BS is \( B \). None of \( B \)'s neighbors \( \{A, F, E\} \) can initiate another spectrum contention. The remaining BSs \( \{C, D\} \), with the knowledge about the network topology and winner BS, can conduct another spectrum contention. The operation of the winner of this later spectrum contention will not interfere with \( B \)'s. The fact that MODSC supports channel reuse improves the efficiency of spectrum utilization and reduces spectrum starvation.

Consider a system of WRAN networks with \( n = 5 \) and \( r = 2 \) for \( T \) superframes. In a system with cycle network topology, each BS has equal opportunity to win either first or second round of spectrum contention. Thus, the expected system utility \( E[U] \leq 2T \). In a system with a wheel network topology, the scenario is different. When the central BS, denoted as \( N_m \), wins the expected payoff is \( T \). However, when any other BS \( N_i \neq N_m \) wins
the spectrum contention the expected payoff is $2T$. Therefore, expected utility $E[U]$ in this scenario is $E[U] = \frac{(2n-1)T}{n}$. Substituting $n = 5$ in the equation and computing expected channel reuse using the expression $E[r] = E[U]/T$, we find that $E[r] < r$, which is confirmed by simulation results illustrated in Figure 3.11. Comparison of the performances of ODSC and MODSC based on channel reuse under wheel and cycle network topologies are shown in Figures 3.11 and 3.10 respectively.

![Figure 3.10: Performance comparison of ODSC and MODSC in cycle network topology.](image)

We can clearly see that MODSC, in contrast with ODSC, guarantees more channel reuse with increasing number of WRAN networks in both cycle and wheel network topologies. Contrary to this trend, the ODSC system shows a continuous decline in channel reuse as the number of networks increase. This trend observed in ODSC system can be explained by the independent spectrum contentions conducted, which may end up in winners conflicting on the same channel. Comparing the trends in Figures 3.11 and 3.10, we can say that channel reuse is better in cycle network topology than in wheel network topology. This is also anticipated because the central WRAN network, in system with a wheel network topology,
In complete network topology, channel reuse is bound to $r = 1$. Considering interference constraints, only one spectrum contention can be conducted in a superframe and only one network can emerge as the winner of the process. Therefore, in a complete network topology, channel reuse is constant even with increasing number of WRAN networks, and regardless of the type spectrum contention protocol implemented in the system.

### 3.7 Conclusion

In this work, we address some of the vulnerabilities of ODSC protocol and proposed a modified version of the protocol that addresses the security vulnerabilities. We have shown that by shrinking or expanding the contention window, one contender may have undue advantage over others during spectrum contention depending the criteria for deciding the winner. The ODSC also grants the DST network the laxity to manipulate spectrum contention outcome.
to its favor. By modeling the behavior of a malicious DST network as dependent on the frequency of transitions between honest and malicious state, we are able to show how fairness in spectrum contention is impacted. ODSC lacks the mechanism to verifying DST’s decision and as a result fairness is guaranteed. On the other hand, MODSC is a protocol that guarantees fairness by eliminating the possibility of cheating by malicious spectrum contenders. The protocol also gives better system performance with the implementation of n-wise spectrum contention, which can increase channel reuse.
Chapter 4

Enabling Self-Coexistence through Risk Motivated Deference Structure Formation

4.1 Introduction

Coalition formation in cognitive radio networks is sometimes approached as a covert attempt by a group of networks trying to exploit spectrum resources in a way that is disadvantageous to other networks in the system. Tan’s work on the effect of parochialism in cognitive radio networks [88] deemed the formation of parochial community as malicious because such coalition can deviate from the Nash equilibrium (N.E.) switching probability to benefit more than others. On one hand, such change in strategy does not promote self-coexistence in the system. Tan et al. argued that the existence of parochial community favors only the members of the community known as the insiders more than non-members known as the outsiders. As a result, the system changes from a state of equilibrium to an unstable state.

On the contrary, a deviation from N.E. strategy could mean the search a better strategy
that benefits the coalition, which is not necessarily malicious. More so, the formation of coalitions or communities to access spectrum resources could be initiated by different factors other than the greedy predisposition or parochialism. In the midst of intense competition for spectrum opportunity, it is actually difficult for networks to agree to a fixed switching strategy, expressed in terms of switching probability. Naturally, an alternative option to reduce spectrum contention and improve spectrum utilization is by forming coalition, where networks defer transmission to one another. Such cooperation to defer transmission to another network leads to coordinated access that enhances self-coexistence in the spectrum environment. We refer to such coalitions as deference structure. A more formal definition is given below:

**Definition 4.** A deference structure (DS) is a coalition formed by the CR networks to have coordinated access to a specific channel or spectrum band of interest. The selected channel of interest is referred to as DS channel.

Although deference structures are formed per channel or spectrum, it is possible to have multiple deference structure formed independently to access the same channel. With limited supply of spectrum resources limited, it is impossible for the system to attain an absorbing state (convergence). Formation of deference structures offers an opportunity for networks to collaboratively access available resources, which can increase the efficiency of spectrum sharing. The formation of such network structures is guided by network’s perception of risk of spectrum contention and interest to mitigate loss of transmission opportunities to spectrum competition. Therefore, the motivating factor for all participant networks is to reduce spectrum contention risk rather than promote parochialism.
4.2 Deference Structure Model

Consider a system consisting of \( n \) CR networks constrained to operate over a fixed number \( m \) of spectrum band (channels). All the CR networks are stationary and able to communicate over a common control channel. Since the focus is on coalition formation, we assume that the primary users (PU) are rarely present. Two or more CR networks conflict if they attempt to transmit over the same channel. The set of all CR network is denoted as \( N = \{ N_i : i \in [1, n] \} \).

The system’s initial mode is non-cooperative.

In order to minimize the risk of spectrum contention, CR networks merge to form DS coalition. Each coalition formed \( S \subseteq N \) choose a preferred channel \( C_j \) that all members will collaboratively access without conflicts. With each coalition, networks can defer transmission to a later time for other members to transmit urgent information. The initiator of the DS formation process is automatically assigned the role of DS coalition head. The DS coalition head is responsible for coordination of all activities, including transmission deference, within the coalition.

With high levels of spectrum contentsions, CR networks are triggered to broadcast DS requests neighboring networks to engage in coalition formation for improved spectrum access. Some networks might be truly altruistic in nature and willing to form a DS coalition for general performance improvement across the system [89]. It is possible also to have a category of networks that are willing to participate in coalition formation only because of the benefit they will derive from the collaborative process. The remaining group of networks maybe opposed to any collaborative effort to mitigate spectrum contention. These networks are optimistic that they will find contention-free channels for their operations. A CR network that joins a DS coalition is referred to as an insider network. Other networks that refuse to join a deference structure are referred to as outsider networks.

DS coalition formation could be preceded by negotiation between networks on the allo-
Figure 4.1: This diagram illustrate deference structure coalition formation model. The dashed colored lines identifies the different DS coalitions that exist between secondary users in the system.

DS coalition formation is initiated by a CR network that has assessed the level of spectrum contention risk on a preferred channel to be above acceptable threshold. Other networks, contending for control of the channel, also assess the risk before responding to requests to form a deference structure. Given this type of scenario, networks participating in the deference structure formation anticipate a reduction in risk and an improvement in average
system utility.

### 4.2.1 Implementation of Deference Structure

The implementation of deference structure is a measure taken to mitigate the wastage of spectrum opportunities that are available in the absence of the licensed band owners. Spectrum resources are limited and scarce. To survive the crunch on the available spectrum resources, effort must be made within the CR system to implement measures that enable effective and efficient spectrum utilization. CR networks, equipped with their cognitive ability should be able to initiate and sustain coordinated access to vacant licensed bands.

A CR network that urgently needs to improve its utility by reducing risk of contention initiates deference structure formation. The initiator of the process broadcasts a request message, announcing its interest to form a deference structure for access to a channel of interest. It is possible that more than one network could make the announcement, given that each network in the system may have different level of tolerance threshold for spectrum contention risk. Such a scenario can bottleneck coalition formation because of multiple initiators. Bottlenecks can be resolved by networks choosing to respond to request with earliest timestamp or from a network with the least identifier.

As we have already mentioned earlier, response to a request may depend on the relatedness of the CR networks, urgency to operate in a contention-free spectrum band or altruistic predisposition of CR networks. In the current implementation of deference structure, response is motivated by the desire to minimize contention risk. Networks use a risk-motivated channel selection scheme (RCSS) to evaluate the risk of contending in the advertised channel with respect to other available channels in the spectrum. Networks respond if the risk is well above a tolerable level. The RCSS scheme will be discussed later.

Upon forming a deference structure, networks reach an agreement on how to opportunistically access the deference channel. The channel is time-sliced to accommodate all members.
CHAPTER 4. RISK-MOTIVATED DEFERENCE STRUCTURE FORMATION

of the coalition. Networks are prohibited from forming a deference structure on the same deference channel with outsiders. Coordinated access to the deference channel is enforced by means of shared spectrum access list, specifying the order in which the networks access the channel. Besides the goal of minimizing contention risk, the sharing of spectrum resources among CR networks in a deference structure community must be fair. A way of ensuring fairness in the coalition would be to assign each participating member network equal transmission time slots. In the case, where a member needs to transmit time-sensitive information, other members can defer their transmission operation to a later time.

4.2.2 Deference Structure Protocol

The formation and coordination of a deference structures rely on message exchanges among the CR networks. Specifically MAC messaging is of paramount importance for these coalitions to exist. Deference structure protocol is built on top of 802.11 MAC protocol and inherits most of its features including contention-handling mechanism needed to mitigate congestion.

Communication in our DS model is conducted via a common control channel (CCC) during a beacon period (BP). We consider BP as a period in the super frame when networks communicate and coordinate activities within their respective DS coalitions. In contrast with the beacon periods implemented in [90] [91] [92], BP in deference structure model can be of variable of length and can extend to overlap with the data transmission period. The deference structure formation process continues until a final agreement is reached among the participating networks. This helps to avoid scalability issues associated with fixed BP and allows communication to continue by using part of the transmission slot time.

At the beginning of the deference structure formation, an initiator broadcasts a request (REQ) message to all CR networks, advertising the channel that it desires to form a deference structure on (see Figure 4.3). The REQ message contains, among other information,
the identifier of the initiator network, the advertised channel identifier (frequency), and the priorities (high data rate, long range transmission etc.). REQ messages also contain request expiration time, also known as Time To Live (TTL). When TTL expires no subsequent responses are ignored. Interested CR networks respond by sending to the initiator a response (RSP) message, which contains the responding network’s identifier as well as its spectrum requirements (desired duration to use the channel, time-sensitive data transmission needs etc.). The initiator, upon receiving the RSPs from interested networks, schedules the networks according to their various requirements in a manner that ensures fairness to all participating networks. In some cases, scheduling might be accompanied by negotiation between the networks on the fraction of time slots or frames assigned to them. This will require the initiator to issue a negotiation message (NEG), to which a potential member can
either respond to or ignore completely. The criteria for terminating the DS formation at this stage ranges from partial responses to complete refusal to ACK the NEG message by the participating CR networks. The refusal comes as a result of the networks refusing the imputation offered to them. The initiator later multicasts the deference structure message (DSM) to member networks. DSM contains the deference order, which specifies the order in which networks access the deference channel. The order is expressed using a prioritized list which members adhere to assuming they are all honest networks. Multicast of DSM is followed by an acknowledgment (ACK) from the recipients, which marks the completion of the DS formation cycle.

### 4.3 Estimating Utility in Deference Structure Model

In a typical DSA scenario, CR networks are devoid of the knowledge of the particular channel that their neighbors are going to access. With a limited supply of spectrum resources, there is a potential risk of networks contending one or more channels in attempt to carry out transmission. In chapter 2 we derived an expression that describes the potential of spectrum contention on a given channel. The probability of spectrum contention \( Pr\{D_n^m\} \) on a given channel \( j \), supposing that there are \( n \) CR networks contending for \( m \) channels, was defined as

\[
Pr\{D_n^m\} \geq 1 - e^{-\frac{n(n-1)}{2m}}
\] (4.1)

To emphasize the significance of the spectrum contention experienced on channel \( j \), we rewrite \( Pr\{D_n^m\} \) as \( p_j^{(n,m)} \). The tuple \((n, m)\) is another way of representing system configuration. Based on the results obtained in the previous chapter, we know that the probability of spectrum contention can increase either with an increase in \( n \) or a decrease in \( m \).

Suppose that network \( N_i \) in the system is capable of deriving a utility of \( u(C_j) \) by op-
Figure 4.3: Deference structure coalition formation process.

We assume that the channels have equal spectrum capacity as specified earlier in the system model. Thus, the utility \( u(C_j) \) per channel is uniform and proportional to the number of bits \( W \) that can be delivered to a potential destination during a synchronized transmission slot of length \( \tau \) seconds. Gupta and Kurmar [93], through their extensive work on capacity of wireless networks, established that the throughput capacity of a random ad-hoc networks is equivalent to \( \Theta(W/\sqrt{n \log n}) \) bits per second. We can choose to define \( u(C_j) \) in terms of number of bits transferred during a transmission slot \( \tau \),
\[ u(C_j) = W \cdot \frac{\tau}{\sqrt{n \log n}} \]  

(4.2)

This model suggests that utility derived from channel diminishes as the number of networks operating on that channel increases. This goes with the assumption that there is zero interference during the transmission period of \( \tau \) slots. Contending for spectrum opportunity does lead to interference which impacts on the utility derived. As a result of interference, affected networks incur a loss or interference cost \( \nu(C_j) \) that is measurable in terms of the utility \( u(C_j) \). Since there could be partial loss of transmittable bits, \( \nu(C_j) \) is defined as

\[ \nu(C_j) = -u(C_j) \cdot \alpha_t \quad 0 \leq \alpha_t \leq 1 \]  

(4.3)

where \( \alpha_t \) is the fraction of the utility (transmittable bits) that was lost due to interference resulting from spectrum contention and nearby transmission activities. We assume \( \alpha_t \) is only time dependent. However, \( \alpha_t \) could be dependent on other external factors such as the nearby transmission activities as well as on the number of contending networks and their proximity to each other. The channel degradation worsens with increasing number of networks generating the interference. Therefore, we cannot attribute interference only to channel contenders. The activities of nearby primary users do significantly contribute to the degradation of channel quality. As a result of degradation in channel quality, the amount of utility derived by operating networks will reduce significantly. Since we do not know the exact distribution of these external factors and the mapping of networks’ transmission attempts to the set of available channels, we simply denote \( \alpha_t \) as a function of time \( t \).

Therefore, the utility derived by operating on a channel that is susceptible to such channel disturbances is given as

\[ u_t(C_j) = u(C_j) + \nu(C_j) = u(C_j) \cdot (1 - \alpha_t) \]  

(4.4)
Since \( u_t(C_j) \) is the utility derived by a lone network operating on channel \( j \) at time slot \( t \), the cumulative utility derived over \( T \) transmission slots can be expressed as

\[
U(C_j) = \int u_t(C_j) \cdot \delta t = u(C_j) \int (1 - \alpha_t) \cdot \delta t
\]  

(4.5)

The cumulative utility \( U(C_j) \) is an estimate of the total utility derived with zero interference. In fact, it is more comprehensive to consider the impact of expected spectrum contention on the utility derived from channel \( j \). By taking this into consideration, we can derive the expected utility with the assumption that the probability of spectrum contention involving \( n \) networks is equivalent to \( p_j^{(n,m)} \in [0,1] \). We concisely represent \( p_j^{(n,m)} \) as \( p_j \). Thus, the expected utility becomes

\[
E[U(C_j)] = \sum_{t \in T} [(1 - p_j) \cdot u(C_j) - p_j \cdot \alpha_t \cdot u(C_j)]
\]

(4.6)

The limits of \( E[U(C_j)] \) with respect to the upper and lower bounds of \( p_j \in [0,1] \) are given as

\[
\lim_{p_j \to 0} E[U(C_j)] = u(C_j)T
\]

\[
\lim_{p_j \to 1} E[U(C_j)] = -u(C_j) \sum_{t \in T} \alpha_t
\]

The expression above depicts expected utility by considering cases where channel \( j \) is either completely devoid of spectrum contention or is severely contended by two or more networks. Even though equation 4.6 is a statement about estimated utility, both parameters \( p_j \) and \( \alpha_t \) are unknowns and remains to be estimated by the networks based on prior experience.

Based on the conjecture in chapter 2 about estimating \( p_j \), we expect \( E[U(C_j)] \) to diminish
with the formation of a DS coalition. Assuming $k \in [1, n]$ is the size of an arbitrary DS coalition, the number of contenders decreases such that the system $k$ less spectrum contenders. This implies $n \rightarrow n - k + 1$ and less conflict for the DS coalition. Members of the DS would anticipate spectrum contention from the subset of non-member networks that may want to access the same channel with them. To show that this event leads to a reduction in contention, we compare the probability of spectrum contention on channel $j$ before and after the deference structure formation. Before the formation, there are $n$ networks that are possible contenders of channel $j$ with the probability denoted as $p^b_j = p^{(n)}_j$. After the formation of the deference structure of $k$ networks, then there are $n - k + 1$ contenders with probability of contention denoted as $p^a_j = p^{(n-k+1)}_j$. Based on previous analysis in chapter 2, we know that $\inf\{p^a_j\} < \inf\{p^b_j\}$ since $n > n - k + 1$ with $k \neq 0$. Suppose that $E[U(C_j)] \sim E[U^a_j]$ then

\begin{align*}
E[U^a_j] &= u(C_j)T - p^a_j u(C_j) \cdot \sum_{t \in T} (1 + \alpha_t) \quad \text{(I)} \\
E[U^b_j] &= u(C_j)T - p^b_j u(C_j) \cdot \sum_{t \in T} (1 + \alpha_t) \quad \text{(II)}
\end{align*}

\[ (4.7) \]

Here, we assume that both strategies are implemented for $T$ transmission slots. Subtracting (II) from (I), we have

\begin{align*}
E[U^a_j] - E[U^b_j] &= (p^b_j - p^a_j) \cdot u(C_j) \sum_{t \in T} (1 + \alpha_t) \\
&= \Delta p \cdot u(C_j) \sum_{t \in T} (1 + \alpha_t)
\end{align*}

\[ (4.8) \]

where $\Delta p = p^b_j - p^a_j$ is change in the probability of spectrum contention with reduction in the number of contending networks. In other words, $\Delta p \geq 0$ captures the reduction in the susceptibility of a channel to spectrum contention, given the decrease in the number of possible contenders. Actually $\Delta p$ is equivalent
\[ \Delta p = e^{-(n-k+1)(n-k)/2m} - e^{-n(n-1)/2m} \] 

With no change in \( p_j \) then \( \Delta p = 0 \). Assuming \( k = \gamma n \), where \( \gamma \) is the fraction of \( n \) networks that are forming DS coalition. It is interesting to observe that the condition \( \Delta p = 0 \) holds only when \( \gamma = 1/n \) or \( \gamma = 2 \) with \( m \neq 0 \). However, the later is unrealistic since \( k \leq n \). If \( \alpha_t \) is insignificant that is \( \alpha_t \to 0 \) then

\[ E[U_j^a] - E[U_j^b] = \Delta p \cdot u(C_j)T \]  

Depending on the number of networks that merge to form a DS coalition, the increase in expected utility of that coalition is quite significant. In the face of severe spectrum scarcity, especially in a case where \( n > m \), \( p_j^b \) is much closer to 1. The formation of the coalition leads to \( p_j^b \to p_j^a \). It is interesting to observe that as \( p^b - \Delta p \to 0 \), \( E[U_j^a] \to u(C_j)T \), which signifies an improvement in expected utility over time \( T \).

By joining a DS coalition, each of the \( k \) network in the coalition is expected to receive a fair share of the spectrum opportunity on the deference channel. Fair share of the transmission frame could mean either an equal transmission slots or enough transmission slots to meet channel requirement. Assuming each member receives equal number of transmission slots, then we expect that the average utility is equivalent to \( \bar{U}_j = U_j^a/k \). From the perspective of self-coexistence, this is far more beneficial to the networks than the risk of spectrum contention they face operating as singletons.

### 4.4 Spectrum Contention Risk Assessment

Estimating the risk of spectrum contention is important for networks to reach a decision to participate in deference structure formation. Continued spectrum contention poses signifi-
cant risk to conduct interference-free transmission. Here, we present a way for networks to estimate the risk of spectrum contention.

4.4.1 Spectrum Contention Risk

Risk is the possibility of experiencing loss or the possible cost of experiencing a loss. In economics, risk is measured as the standard deviation of historical performance or the average performance of an investment. A large deviation from a normal or expected trend would normally serve as an indicator of high risk associated with the observed process. Similarly, in the context of spectrum access, the record of the frequency of spectrum contentions can be used as an indicator of the level of risk associated in transmitting over a select channel. Consequently, the risk of selecting a contended channel is heightened by the absence of secondary-to-secondary etiquette, common in decentralized network settings. High risk introduces the anticipation of low throughput and huge losses due to re-transmissions and channel switching costs. Therefore, it is important for networks to measure the risk they face and incorporate it in decision-making regarding coalition formation. Huge losses incurred as a result of repeated failure to transmit can be avoided and at least, a fraction of the expected spectrum utility can be beneficial to the network.

When a network selects a channel to operate on, it expects to receive a certain amount of utility, provided no interference occurs within the transmission frame. For simplicity, we denote this expected utility as $\bar{b}$ which represents the fraction of transmission frame with zero interference. Hence, $\bar{b}$ can be treated as a real number in the interval $[0, 1]$. We denote the actual utility derived at the end of the transmission frame as $b$. Assuming no utility is derived if there is slight interference, then $b$ and $\bar{b}$ can be treated as binary variables such that $b, \bar{b} \in \{0, 1\}$. 
4.4.2 Risk as Expected Loss

We define spectrum contention risk as an expected loss due to failed transmission. We proceed to derive an expression for this risk measure in terms of the loss incurred as a result of failed transmission caused by spectrum contention. The loss incurred by a network over a select channel at time \( t \) is measured by \( L(b_t, \bar{b}_t) \), where \( L \) is the loss function with range \([0, \infty)\). We adopt the absolute loss function \( L_{abs} \), such that \( L = L_{abs} \). Therefore, loss of spectrum opportunity in time slot \( t \) is defined as

\[
L(b_t, \bar{b}_t) = |b_t - \bar{b}_t| \tag{4.11}
\]

By virtue of selecting a channel, a network anticipates to derive \( \bar{b} \) from the channel. Therefore, the loss function associated with such a selection can be expressed as

\[
L_{\bar{b}} = L(b, \bar{b}) \tag{4.12}
\]

Since the decision to select a channel is binary, then \( \bar{b} \) can be treated as a prediction, with a probability \( p = 1 \) that \( b = \bar{b} \). The outcome of this decision is the unknown parameter \( b \) which can be either a loss or a benefit. With that in consideration, we resolve \( L_{\bar{b}} \) into two independent functions \( L_1(b) = L(b, 1) \) and \( L_0(b) = L(b, 0) \). \( L_1(b) \) is associated with the decision of the network to pick the select channel for transmission and \( L_0(b) \) is associated with the decision of the networks not to pick the channel.

Here, we introduce \( Q \) as a probability measure on the set of binary outcome \( \{0, 1\} \), such that \( \Pr_{b\in Q}[b = 0] = q \). The expected loss for the probability measure \( Q \), for an outcome \( b \in [0, 1] \) is defined as

\[
\mathbb{E}_{b\in Q}[L(b, \bar{b})] = q \cdot L_1(b) + (1 - q) \cdot L_0(b) \tag{4.13}
\]
With the selection an arbitrary channel selected, a network risk losing the time slot with probability $q$. The main goal is to minimize the amount of loss incurred. Based on the loss equation, no loss is incurred if the channel was interference-free. Therefore the expected loss in that case results to zero. On the other hand, the network’s refusal to pick a channel could result to a loss. This happens with a probability $1 - q$ when the channel is interference-free. Note that no loss is incurred if the channel turns out to be busy. In fact, if the networks are not interested in verifying the resulting state of a rejected channel, then the equation 4.13 simply reduces to

$$E_{b \in Q}[L(b, \bar{b})] = q \cdot L_1(b)$$  \hspace{1cm} (4.14)

Risk has no scale of measurement and can be expressed in terms of expected loss. The general representation of risk is a function mapping a random variable, which belongs to a set of possible real outcomes $\omega$, to a set of real numbers $\mathbb{R}$. The general form of the function is given below,

$$\rho : X \rightarrow \mathbb{R} \cup \{\infty\}$$  \hspace{1cm} (4.15)

We denote the risk as a certain measurable quantity of loss associated with a channel $C$ as $\rho(C_j)$. The function $L$ allows the networks to measure the quality of $C_j$ by quantifying it in terms of the cumulative loss recorded while transmitting over channel $C_j$. The cumulative loss is the sum of instantaneous losses over $T$ time frames

$$L(C_j) = \sum_{t \in T} L(b_t, \bar{b}_t)$$  \hspace{1cm} (4.16)

If the quality of $C$ is degrading, we expect $L(C_j)$ to increase significantly, thereby increasing the risk of operation. Hence, we can define a risk function as $\rho(C_j) = E[L(C_j)]$. With this
definition, $E[L(C_j)]$ becomes a measurable quantity in retrospect of past failed attempts to transmit over channel $C_j$.

Precisely, we can define risk as a measure that quantifies the vulnerability of a network to experience spectrum contention while transmitting over a channel. This measure of risk does take into consideration the frequency of spectrum contentions as well as the persistence of conflicts on each channel. Based on channel profile information accumulated by a network, we can make inference on the probability of selecting a specific channel. The probability of selecting channel $j$ can be approximated, according to the law of large number, to the frequency $f_j$ of channel $j$’s selection divided by the total time slots of network activity $T_A$. Likewise, the probability of spectrum contention can be approximated as the frequency of contention $f^c_j$ on channel $j$ divided by usage frequency $f_j$ of channel $j$. The network risks recording a cumulative loss (cost of spectrum contention), $L(C_j) = \sum_{t=1}^{T_A+1} L(b_t, \bar{b}_t)$ if it selects channel $j$ for the next transmission round. Therefore, the risk $\rho(C_j)$ associated with selecting channel $j$ for transmission is

$$\rho(C_j) = \frac{f_j \cdot f^c_j \cdot L(C_j)}{T_A} = \frac{f^c_j \cdot L(C_j)}{T_A} \quad (4.17)$$

If we assume a unit cost for each loss incurred, then $L(C_j)$ sums up to $f^c_j$. Thus, we can rewrite equation 4.17 as

$$\rho(C_j) = \frac{f^c_j \cdot (f^c_j + 1)}{T_A} \quad (4.18)$$

4.4.3 Risk-Motivated Channel Selection Scheme

During channel selection, networks pick channels to operate on based on the channel characteristics. A rational network’s choice should be guided by accumulated knowledge about the activities of the channel. In our model, we consider that primary users are absent and
only secondary users are operating on the available channels. Therefore, the competition for the available channels is strictly between secondary users, with no prior agreement on the order of spectrum access.

At the beginning of a transmission period, a network has to pick the best channel(s). We propose a channel selection scheme that involves ranking of channels based on their levels of perceived spectrum contention risk. As discussed above, high risk of spectrum contention indicates a potential for low throughput, excluding the losses incurred due to the presence of licensed owners. Channel ranking is carried as follows:

- Rank $C_i$ above $C_j$ if $\rho(C_i) < \rho(C_j)$
- In case of $\rho(C_i) = \rho(C_j)$, rank $C_i$ above $C_j$ if $u(C_i) > u(C_j)$
- Otherwise, break tie via coin toss.

A network initiates deference structure formation once the risk $\rho(C_j)$ of the highest ranked channel exceeds acceptable level of spectrum contention risk, denoted as $\rho_o$. In our model, each network is constrained to pick the best channel for transmission. Assuming that $C_j$ is the best channel and $\rho(C_j) > \rho_o$, then there is no incentive to select an arbitrary channel $C_i$ for transmission, where $\rho(C_i) \geq \rho(C_j)$. Spectrum contention risk on the best channel exceeds $\rho_o$ and this motivates the network to initiate the deference structure formation process. The network that starts the process is referred to as the initiator network. It starts by sending out the REQ message, advertising the preferred deference channel for collaborative access.

Any network that receives the REQ message makes a rational decision to accept or ignore the request. Since the received REQ packet contains information about the potential deference channel, network can compare the risk associated with the advertised channel with the risks of other channel. Let $C_j$ denote the advertised channel and $\rho(C_j)$ as the risk associated with it. A response is issued if
\( \rho(C_j) > \rho_o \) or \( \forall C \neq C_j \), \( \rho(C) \leq \rho(C_j) \), and

\( \rho(C_j) \geq \rho(S_j) \)

where \( \rho(S_j) \) is the risk of the potential deference structure \( S_j \) to be formed.

### 4.4.4 Deference Structure Coalition Formation as a Game

Coalition formation in cognitive radio networks have been studied from a game theoretical perspective [94] [95]. One of the notable works on coalition formation is the work done by Khan et al. on selfish and altruistic formation in cognitive radio networks. The coalition formation problem was formulated as a sensing-throughput tradeoff problem in distributed cognitive radio networks. A value decision function was introduced to encourage collaborative networks to join coalitions to minimize their false alarm probabilities.

Along the same line, we argue that CR networks can be encouraged to form deference structures to minimize the amount of spectrum contention risk they face in the spectral environment. The risk measure is used as an incentive to encourage networks to join deference structures to minimize conflicts. Let \( N \) denote the set of players (networks) participating in the coalition game to access a set of available bands \( M \). Each player \( i \in N \) seek to minimize spectrum contention risk on preferred channel \( j \in M \). A player \( i \) choose to transmit on \( j \) if

\[
    j = \arg \min_{m \in M} \rho(C_m) \tag{4.19}
\]

Thus, deference structure coalition \( S_j \) is set of players such that \( S_j \subseteq N \), where \( N \) is the grand coalition. An individual network \( i \) that does not belong to any deference structure is a singleton deference structure, denoted as \( S_j^{(i)} \). The valuation of a given deference structure coalition \( v(S_j) \) can be measured in terms of cumulative utility derived by DS coalition \( S_j \) by transmitting over channel \( j \). The definition of utility have been given earlier in section 4.3.
Definition 5. A coalitional game $((N,v,\rho))$ has a transferable utility if the value $v(S_j)$ of a coalition $S_j$ can be distributed among players in any conceivable way. In a case, where each player has its own utility within the $S$, then the coalition game is said to have non-transferable.

Proposition 4.4.1. In the proposed deference structure game model, the utility derived by $S_j$ is equal to the utility derived by each individual player $N_i$, i.e.

$$v(S_j) = \sum_{N_i \in N} u_i(C_j)$$

Consequently, deference structure game model has transferable utility.

Proof. Without any external disturbance, utility derived by the DS coalition $S_j$ is measurable in terms of the utility obtainable while operating on $C_j$. Suppose that duration of active operation by members of $S_j$ can be partitioned into transmission time slots. Then, each network receives a certain amount of time slots by virtue of its membership to $S_j$. The total utility derived by the coalition $S_j$ is given as $v(S_j) = \sum_{N_i \in N} u_i(C_j)$, where $u_i(C_j)$ is the utility derived by $N_i$ from assigned time slots. Hence, the DS coalition value $v(S_j)$ can be arbitrary apportioned among members. This coincides with the premise of DS coalition formation, which is based on the ability of CR networks to defer transmission to one another.

Definition 6. A coalition game $(N,v,\rho)$ has a transferable risk if $\rho(S_j)$ of a coalition $S_j$ can be distributed among players in any conceivable way. Otherwise, a risk-motivated coalition game has non-transferable utility if each player faces an individual risk by virtue of its membership to $S_j$.

Proposition 4.4.2. The deference structure game model has non-transferable risk.
Proof. By agreeing to form a DS coalition $S_j$, any network $N_i \in S_j$ pledges not to interfere with the operations of a member network $N_k \in S_j \setminus N_i$. Thus, $S_j$ as a unit can only contend with any other coalition $R_j$ where $R_j \subset N$ and $R_j \cup S_j = \emptyset$. The spectrum contention risk faced by $S_j$ is denoted as $\rho(S_j)$. By virtue of membership to $S_j$ to operate uninterrupted on channel $C_j$, the risk $\rho_i(S_j)$ faced by $N_i$ equals the risk faced by the DS coalition $S_j$ i.e. $\rho(S_j) = \rho_i(S_j)$ and vice versa. Irrespective of the division of DS coalition utility, members share the same risk of spectrum contention $\rho(S_j)$. Hence, deference structure game model has non-transferable spectrum contention risk.

We denote the spectrum contention risk, associated with a given deference structure $S_j$ formed on channel $j$, as $\rho(S_j)$. We envision a coalition game where each member $i$ of $S_j$ faced a certain risk of spectrum contention $\rho(S^{(i)}_j)$ prior to its formation. The risk faced by $N_i$ after the formation of $S_j$ is denoted as $\rho_i(S_j)$. The minimized risk $\rho_{\text{min}} = \sup_{S_j \subset N} \rho(S_j)$ serves as an incentive for networks to join a DS coalition on a particular channel.

**Proposition 4.4.3.** A sufficient incentive for the emergence of DS coalition is the reduction in spectrum contention risk.

*Proof.* Assume that there is sufficient supply of spectrum resources and zero contention in the system. Then no rational CR network joins a DS coalition to minimize spectrum contention risk. However, this is contradictory to the case of spectrum scarcity where $n > m$.

Players are better off sharing than competing for the spectrum resources because competition generates no utility and leads to wastage of spectrum opportunity. The formation of deference structure should also take into consideration the cost of coordinating a DS coalition. The coordination cost increases as the size of the deference structure $|S_j|$ increases. The motivating criteria for a player $i$ to form or join a deference structure on channel $j$ are:

1. The spectrum contention risk $\rho(C_j)$ exceeds acceptable risk threshold $\rho_o$. 
2. Player \( i \) anticipates that joining \( S_j \) changes \( \rho(C_j) \) to \( \rho(S_j) \) faced by the members of \( S_j \), where \( \rho(S_j) \leq \rho(C_j) \).

A selfish deference structure is formed when players respond to request, seeking to minimize spectrum contention risk and consequently maximize throughput. Given two deference structures \( S_i \) and \( S_j \), the emergence of a selfish deference structure is possible if only

\[
\rho(S_i \cup S_j) < \min\{\rho(S_i), \rho(S_j)\}
\]

Due to the condition above, whenever a request to form deference structure is sent out, the networks might have no incentive to remain as singleton deference structures. As rational entities, minimizing the spectrum contention risk is important to keep the spectral environment fairly stable for transmission purposes.

In some cases, the formation of a deference structure may not be entirely motivated by selfish interest of the network maximize utility. Networks can be altruistic with the risk they face in their coalition. Consider the emergence of an outsider network \( i \) in the spectral environment, with interest to form a deference structure of channel \( j \). Prior to the appearance of network \( i \), a deference structure \( S_j \) existed on the deference channel \( j \). The presence of network \( i \) does not pose significant risk to the existence of \( S_j \), since network \( i \) might be hopping from one channel to another seeking to find the best channel for transmission. If \( S_j \) accepts to merge with \( i \) to form a deference structure, then the resulting coalition could be said to be altruistic in nature. Therefore, the condition for the emergence of an altruistic deference structure \( S_j \cup S_j^{(i)} \) is as follows

\[
\rho(S_j) \leq \rho(S_j \cup S_j^{(i)}) < \rho(S_j^{(i)})
\]

The contribution made by \( S_j \) is measurable in terms of the change in risk \( \Delta \rho = \rho(S_j \cup S_j^{(i)}) - \rho(S_j) \). The condition given above is valid, if and only if we assume that there could
be an increment in risk with an increase in the size of the deference structure. On the other hand, the merging of deference structures should generally remove the competition that exists between the structures, and thereby reduces the risk of contention. Taking this into consideration, $S_j$ might be still be considered to be altruistic, provided it is indifferent to the gains in terms of reduction in risk. Therefore, the following inequality,

$$\rho(S_j \cup S_j^{(i)}) \leq \rho(S_j) < \rho(S_j^{(i)})$$

holds only if and only if $S_j$ is indifferent to the improvement in spectrum contention risk.

**Proposition 4.4.4.** For a given collection $\{S_i\}$ of disjoint DS singletons, the joint spectrum contention risk of an emerging DS coalition $S = \bigcup_{i \in [1,n]} S_i$ is such that,

$$\rho(S) < \min_{i \in [1,n]} \{\rho(S_i)\}$$

provided $\forall S_i$, $S_i \neq \emptyset$ and $\rho(S_i) \neq 0$.

**Proof.** By the inspecting the equation $p = 1 - e^{-n(n-1)/2m}$, we observe that as the number of contenders $n$ decreases, $p$ decreases which implies a reduction in $\rho(C_j)$ for any arbitrary selected channel $j \in [1,m]$. With the emergence of the new DS coalition $\bigcup_i S_i$, the number of potential contenders of $C_j$ decreases from $n$ to $n - \sum_i |S_i| + 1$. This signifies a decrease in probability of spectrum contention and corresponding decrease in risk of spectrum contention. Suppose $n = 4$ with fixed $m$, then after the emergence of the DS coalition involving $n/2$ of the CR networks present, the probability of spectrum contention reduces by approximately $e^{-3/m} - e^{-6/m}$. This is a quite significant improvement, depending on the number of channels $m$ that is available.  

$\square$
4.4.5 Stability of Deference Structures

A DS coalition is expected to last as long as the condition for its formation remains valid. That is, provided $\rho(S_j)$ is maintained below each member’s risk threshold $\rho(S_j^{(i)})$. However, this might not be the only incentive for deviation by the members. The discovery of idle channel(s) could force networks to abandon already negotiated resources for the anticipation of contention-free transmission. A network decision to switch from one channel is accompanied by the notion that the target channel has lesser spectrum contention risk. Another important factor that can make DS unstable is the return of the primary user to the defer-
ence channel. This implies that members have to renew their search for a new coalition for a contention-free transmission. Otherwise, the DS coalition will have to be dormant until the occupied channel becomes free. In a case, where transmitted data are time-sensitive information, it is more beneficial for networks to switch to another available channel. Analytically, the instability of DS coalitions is the consequence of

1. a singleton deference structure $S_j^{(i)} \subset S_j$ discovering an alternative channel $C_k$ such that the spectrum contention risk of operating on $C_k$ is strictly less than the spectrum contention risk on $C_j$ i.e. $\rho(C_k) < \rho(S_j)$.

2. activities of an adversary DS coalition or singleton deference structure $R_j$, that increases $\rho(S_j)$ beyond acceptable threshold.

### 4.5 Numerical and Simulation Results

We modeled experiments to show that the benefit of having deference structure in a system of networks. In the simulations, we assumed that the spectrum resources are limited in supply and some CR networks are willing to form deference structure coalition with other networks while others are not. The networks that eventually form a deference structure coalition are regarded as insider networks. The networks that prefer to operate independently are regarded as outsider networks. Systems, consisting of insider networks, are described as deference structure (DS) system. A system is referred to as non-DS (NDS) system, if it has no insider networks. We consider a distributed system where networks can communicate over common control channels assigned to the system. As part of the system requirement, message exchanges are conducted over a control channel implementing cognitive radio MAC protocol such as CR-MAC [96] and C-MAC [97] protocols. Both protocols are time-slotted with synchronized frame. In our case, the control channel was implemented like rendezvous channel in C-MAC [97] and are available throughout the duration of the simulation.
Figure 4.5: An illustration of the difference in performance between systems in DS and NDS modes. In each mode, the number of networks $N = 12$ and networks are free to join any arbitrary deference structure to satisfy channel requirement and mitigate spectrum contention.

### 4.5.1 Impact of Deference Structure Mechanism on System Performance

In our experiment, we observed that the formation of deference structures in the system impacted positively on the system performance. The simulated system is composed of 12 static networks competing for access to a varied number of channels $M$. The networks are all within conflicting range, and therefore form a system with complete conflict graph topology. The networks dynamically form deference structures of variable sizes based on perceived spectrum contention risk level. A common control channel is reserved for message exchanges leading to the formation of deference structures.

The results, illustrated in figure 4.5, show that DS system derives more benefit than the NDS system. Performance of DS and NDS were evaluated based on system utility derived during the simulation period. Utility is measured in terms of number of time frames that
networks were able to operate without interference, including the period before and after the formation of deference structures. The results clearly show that the DS system generate more utility than NDS system, irrespective of the number of available channels, $M$. Based on these results, we say that the presence of deference structures leads to significant gains in system utility. The improvement in performance is accounted for by the reduction in the number of spectrum contentions encountered by insider networks, since they are no longer contending on channels of interest.

We also investigated the individual benefit derived by networks when they participate in deference structure formation. For this experiment, we specifically programmed the network models to initially compete for the spectrum access and then dynamically form deference structures as the risk in the system increases. An additional constraint was imposed on the system that disallows networks to belong to multiple deference structures with same deference channel. This implies that a network can belong to multiple deference structures but the channels chosen for those structures must be distinct.

In Figure 4.6, we have consisting of 5 CR nodes, with the edges between nodes indicating
the possible coalition that can be formed. Basically, members of a deference structure form a clique. The edges are labeled using the deference channel identity. For instance, deference structure formed the set \( \{N_1, N_2, N_3\} \) is valid. On the other hand, the deference structures \( \{N_1, N_5\} \) and \( \{N_4, N_5\} \) are invalid. The reason is that network \( N_5 \) would be benefiting after combining the transmission time slots obtained from both deference structures. This is malicious because \( N_1 \) and \( N_4 \) may not be aware of the \( N_5 \)'s actions. The situation can be normalized by setting up an additional edge between \( N_1 \) and \( N_5 \) to form a clique.

The experiments were conducted in two different modes - DS and NDS mode, with \( n = 10 \) networks. In the NDS mode, no network is willing to form a deference structure to access the channel of interest. However, in the DS mode, some networks are insiders while others are outsiders. The insider networks include \( \{N_5, N_6, N_7, N_8, N_9, N_{10}\} \) and the outsider consist of
networks $\{N_1, N_2, N_3, N_4\}$. Experimental results based on performance of the networks are illustrated in Figure 4.7.

Upon comparing the results from the two settings, we can clearly see that the average performance of the insider networks is far better than the outsider networks. The outsider networks’ average performance degraded compared to their performance in the NDS mode. Figure 4.8 shows the percentage increase with the implementation of the deference structure mechanism. The Jain’s fairness index for the insider gave a value of 0.99, highlighting the high degree of fairness in the DS coalitions.
4.5.2 Impact of Coalition Size on Average Network Utility and Contention

The number of networks that respond to the deference structure request message plays an important role on average utility derived from a DS coalition. This is because the formation of the DS coalition would subsequently lead to spectrum sharing, in a TDMA fashion, by the networks that responded to the request.

We investigated the impact of DS coalition size, denoted as $\kappa$, on average network utility per timeslot. For the sake of conciseness, we refer to average network utility per time slot as the network’s utility rate. Basically, average coalition size correlates with the number of insider networks willing to participate in DS coalition formation. On the other hand, the resulting size of a deference structure coalition depends on the risk levels on the contended channels. Since we are investigating a dynamic system of networks, we expect the DS coalition sizes to vary, given the scarce supply of spectrum resources. Results show the dependency of the utility rate on average coalition size of DS coalitions.

In our experimental setup, we emulated a system of networks with insufficient supply of spectrum resources by setting $N = 50$ and $M = 35$. For networks to derive any form of benefit, they would have to form DS coalitions and share the spectrum resources in TDMA manner. This implies that the time frames are partitioned into equal time slots for members of a given DS coalition.

Figure 4.9 illustrates the variation of network’s utility rate with $\kappa$. We can observe that the insider networks have higher utility rate than outsider networks. The trend suggests that as $\kappa$ increases, the average utility of the insiders gradually increases, while that of the outsiders decreases towards zero percent utility. The maximum utility for insider networks reaches a peak at $\kappa = 35$, which corresponds to the number of channels available for contention. The insider networks are not able to achieve 100% utility rate because they have to
Figure 4.9: Comparison of insider and outsider networks performance based on utility rate. Insiders share the available resources, which is insufficient given the number of networks present.

Figure 4.10 shows the variation of system utility and contention rates with $\kappa$. We can observe that an increase in $\kappa$ increases utility rate of spectrum resources. Likewise, we can observe that the amount of spectrum contention recorded in the system diminishes as $\kappa$ increases. The more networks are organized into DS coalitions, the more the reduced spectrum contention recorded in the system. The insider networks are able to minimize spectrum contention and boost spectrum utilization. However, the presence of the outsider networks poses considerable spectrum contention risk to their overall performance.

The formation of deference structures has been shown to be beneficial to the CR networks, but we observe a tipping point after which admission of an additional insider network triggers a decline in utility rate. An increase in $\kappa$ with fixed time slots on the deference channel leads to a reduction in the number of transmission slots that each member network gets. This impacts negatively on the system utility.
Figure 4.10 shows the variation of the utility rate with different DS coalition sizes for different values of $M$. With a fixed number of spectrum bands $M$, utility rate reaches a peak and starts to decay with further increase in $\kappa$. The peak utility rate is attained when $\kappa \approx M$. This can be interpreted as the limit beyond which the utility rate of the networks degrades. Intuitively, additional members to the coalition would increase coordination cost and average waiting time that delays network’s access to the spectrum. Therefore, it is might be important for the initiator network to estimate the optimal $\kappa$ prior to issuing a DS formation request. In the request, the initiator can put a cap on the required DS coalition size. Networks are then admitted into the DS coalition based on first-come, first-serve basis. This will help reduce the coordination and waiting costs to a minimum and maximize the utility derived by the insider networks.
Figure 4.11: Performance comparison of different DS coalition sizes with varying $M$, number of spectrum bands. The performance reaches a peak when $\kappa \approx M$.

4.6 Conclusions

In this work, we found out that the formation of deference structure coalitions helps to foster coexistence of cognitive radio networks. The presence of DS coalitions improves spectrum utility and minimizes spectrum contentions between spectrum contenders. Valuation of any DS coalition can be done based on either network utility rate or risk of spectrum contention. The risk-motivated channel selection scheme suggested guides networks in making decision regarding the formation of DS coalitions. We also discussed the DS coalition formation protocol. We identified that the main factors that spur the DS formation process include spectrum starvation as well as persistence spectrum contention on preferred channels.

We also demonstrated via simulation the relationship between size $\kappa$ of the deference structure community and the utility derived by the CR networks. We were able to show that the existence of DS coalitions is beneficial, as utility is observed to increase as $\kappa$ increases. The simulation results obtained also demonstrate the impact of size $\kappa$ of deference structure coalitions on the performance of the member networks and suggest the determination of an optimal $\kappa$ for the best network performance.
Chapter 5

Mitigating against Intelligent Sybil Attacks using a Dynamic Reputation System

In this chapter, we explore the dynamic behavior of the Sybil attacker that operates in a CR network where CR nodes collaborate to perform distributed spectrum sensing. The CR nodes then report the results to a centralized Fusion Center (FC), responsible for fusing the spectrum reports and taking decision on spectrum availability. Each node has a unique identity associated with every sensing report it makes to the FC about the spectrum state. The attacker is capable of generating multiple false sensing reports directed at the FC with the help of its multiple Sybil identities. We implement a number of identity sampling strategies that an attacker can use to select the number of identities $k$ to be used for false reporting. Based on feedback from the FC and with the help of reinforcement learning (RL), the Sybil dynamically adjusts $k$ for the next stage of attack.

We present an adaptive dynamic reputation system for spectrum decision making by the fusion center (FC). The dynamic reputation system relies on a non-linear reputation function
CHAPTER 5. SYBIL ATTACKS AND DYNAMIC REPUTATION SYSTEM

to compute the reputation of a cognitive radio node. Each node is assigned a separate reputation function that evaluates its reputation based on false and correct reporting rates. Based on attained reputation, nodes can be distinguished into honest and malicious nodes. However, the reputation system does not sideline the malicious nodes completely by ignoring their reports. Rather the system considers that maliciousness might sometimes be induced and creates an opportunity for nodes to recover from this kind of setback. The reactionary measures are implemented with the help of fuzzy logic control techniques. A fuzzy logic (FL) controller is designed to dynamically adjust the value of $\lambda$ which is an important component of the reputation function. With the support of the feedback control technology, the FL control based dynamic reputation system guarantees accurate spectrum decision-making by FC based on the reputation of nodes.

The key contributions of this chapter are as follows:

1. An overview of intelligent and context-aware Sybil attack in a Cognitive Radio Network. We model Sybil attacks as intelligence-based attacks that rely on the Reinforcement Learning technique, Q-learning, to dynamically select identities for attacks. The most important aspect of the model is capability of an attacker to learn its environment and use the knowledge obtained to carry out intelligent and sophisticated attacks.

2. A novel reputation system that tracks the reputations of spectrum state reporting cognitive radio nodes. We propose the Dynamic Reputation system, which provides the security framework to mitigate the impact of malicious Sybil nodes on spectrum decision. The Dynamic reputation system controlled by the Fusion Center relies on non-linear reputation functions to compute reputations. The reputation system was shown to be flexible but robust to the accuracy of spectrum reports.

3. Fuzzy logic controlled reputation function. We propose the use of fuzzy logic to control the reputation function parameter $\lambda$ that is considered very important in reputation
CHAPTER 5. SYBIL ATTACKS AND DYNAMIC REPUTATION SYSTEM

evaluation. This provides the reactionary mechanism that is needed to respond to changes in reporting behavior of nodes by dynamically adjusting the reputation growth rate $\lambda$.

4. Extensive experiments to highlight the following: effectiveness of Intelligence-based Sybil attacks, flexibility and robustness of the Dynamic Reputation System in countering malicious attacks and dynamic/responsive control of reputation functions using fuzzy logic controllers.

5.1 System Model

This section provides an insight into cognitive radio network model that is center to our study on Sybil attacks and reputation system mitigate the impact of the attacks. The cognitive radio network in perspective consists of $N$ cognitive radio (CR) nodes equipped with spectrum sensing capability. The cognitive radio nodes are allowed to sense $m \in M$ where $M$ is the total number of spectrum bands available. All nodes periodically sense the spectrum bands and report their results to the Fusion Center (FC). After reporting, all nodes wait for FC’s decision before commencing activity in the spectrum.

CR nodes can be compromised or become malicious and therefore could forward erroneous report to the FC. In a situation, where these erroneous reports are reported using multiple identities, we refer to the CR node as a Sybil attacker. The aim of the Sybil attacker is to maximally corrupt sensing result, thereby forcing the FC into wrong conclusions. Wrong conclusions drawn by the FC are costly because that could lead to either under-exploitation of the spectrum or conflicts with the primary user. The attacker derives its utility by successfully causing a disruption in the efficient use of the scarce spectrum resources.

In reporting, CR nodes send their bit reports together with their unique IDs to the FC. A channel with primary user present is reported as busy with a bit value 1 and one with primary
user absent is reported as free with a bit value 0. In the case of multiple channel report, the channel ID is included in the report; to specify which channel the report is intended for. Nodes are error-prone and can give false report about the state of channel(s). In this model, node behavior is measured per interval. An interval is comprised of a finite number of rounds, determined by the FC, during which nodes’ reporting accuracies are measured. FC is not aware of the false reporting rates of the nodes during in an interval. The false reporting rates of the nodes are modeled using the Poisson distribution. This implies that in a given interval, the average rate of false reporting of a node is defined by the parameter $\mu_{\text{avg}}$. The use of Poisson distribution to model the reporting behavior of nodes makes it possible to capture spontaneous change in false reporting rate, which is possible strategy that a malicious node can adopt to foment an attack. Also the strategy of malicious nodes being passive for some time to gain reputation before attacking the system is also captured by this distribution.

FC has the capability to verify the reports made by CR nodes with the help of policy nodes [67] or simply by “listening” on the channels to detect contentions or white spaces. The verification process allows the FC to extract important information about each node false reporting rate. However, there is an error associated with the verification process, which we refer to as verification error. False reporting rates of nodes are measured periodically and with the help of the reputation system, decisions about spectrum state are made. Decision is reached in such a way that the malicious nodes’ reports would have minimal or no impact on the final spectrum decision.

5.2 The Sybil Attacker

We assume that Sybil attacker can generate up to $M$ identities. For example, in our experimental test bed setup, Soekris Net-5501 boards enabled with Atheros chipsets based Wireless
NIC and programmable Madwifi device driver, we are able to support up to 64 identities for one physical device [98]. The attacker is aware of FC’s vigilance on relegating suspicious identities by assigning low reputation to those identities. At every stage of reporting, it uses $k \in [0 \cdots M]$ to report falsely and $M - k$ to report truly the spectrum state. Since the main objective of the attacker is to avoid detection which reduces its reputation but at the same time maximize impact on the FC’s decision, it should selectively choose the $k$ identities used for the attack. The selection is done such that the frequency of use of each identity in reporting to the FC is kept under control. Later on, we shall consider various identity sampling strategies including the identity hopping strategy used by the attacker.

5.2.1 Sybil Attacker Learning Strategy

The Sybil attacker’s goal is to maximize the effectiveness of its attacks (i.e. its performance) on the FC. The attacks have to be unpredictable and in such a manner that the Sybil identities are not compromised. In considering the optimality of $k$, the Sybil attacker has to consider its level of success in the previous stages of attacks. The knowledge of its previous attack strategies that were successful will enhance the decision making process of the attacker in ascertaining the right number of identities to use in embarking on an attack. It must be noted that since the cumulative number of successful attacks varies in each time slot, $k$ needs to be kept dynamic. Another reason why $k$ should be varied is to accommodate the mechanism that allow identities to recover their reputation after a period of intensive attacks. Keeping $k$ constant could reveal the periodicity or the distribution used in sampling the identities.

Given the complexity and dynamism of the wireless environment, reinforcement learning (RL) can provide the Sybil attacker the context awareness and intelligence to conduct its attack efficiently in the system. RL have been applied in many aspect of wireless network such as routing, resource management and dynamic channel selection. We adopt the Q-learning
algorithm in learning the Sybil attacker on the best $k$ to use at any level of performance measure.

When making false reports with $k$ of its identities, the goal of an attacker is to force the FC to accept whatever those identities reported. Let $Z(t) \in \{0, 1\}$ be an indicator function of time that shows whether FC concluded in favor of the attacker. The attacker risks exposing the $k$ identities if it decides to use all of them at once. The attacker associates a cost $K(t)/M$ with the exposure, where $K(t)$ is a function that returns the value of $k$ at time $t$. An attacker can have a variable belief $\theta \in [0, 1]$ which represents its level of conviction that the identities will be penalized by the FC for false reporting. So after $t_c$ stages of attacks, attacker’s perceived performance $P(t_c) \in [0, 1]$ is expressed as follows:

$$P(t_c) = \frac{1}{M \cdot t_c} \cdot \sum_{t=1}^{t_c} [M \cdot Z(t) - \theta \cdot K(t)]$$ (5.1)

In a case where $\theta = 0$, which indicates attacker’s utmost confidence that its identities would not be discovered by FC, equation 5.1 simplifies to

$$P(t_c) = \frac{1}{t_c} \cdot \sum_{t=1}^{t_c} Z(t)$$ (5.2)

With $\theta = 1$, which indicates that the attacker is certain of the risk of exposure, we can observe the dependency of $P(t_c)$ on the value of $k$ used at each stage of the attack. There is no gain for the attacker using $k = M$ in all the stages of the attack, even if all attacks were successful. So it is not in the best interest of the attacker to use all its identities but rather intelligently choose $k$ of best fit for an attack.

For the purpose of implementing RL based Sybil attack, we need to define the terms: state and action. We define a state $s_t$ of an attacker as an indicator of its performance level at time $t$. The attacker defines an arbitrary finite number of states $\eta$ solely to differentiate its performances level and learn the best action to take at each level. The range of $P(t_c) \in [0, 1]$ is partitioned into $\eta$
possible intervals and each interval is associated with a unique state. For an example, \( \eta = 4 \) and \( P(t_c) \) uniformly partitioned, the state \( s_t \) of an attacker can be given as:

\[
s_t = \begin{cases} 
1 & 0.0 \leq P(t) < 0.25 \\
2 & 0.25 \leq P(t) < 0.5 \\
3 & 0.5 \leq P(t) < 0.75 \\
4 & 0.75 \leq P(t) < 1.0 
\end{cases}
\]

Worst performance of attacker is therefore associated with state \( s_t = 1 \), and the best performance, with the state \( s_t = 4 \). For a uniformly partitioned interval, \( s_t \) can be expressed concisely as \( s_t = \lfloor P(t) \cdot \eta \rfloor, s_t \in \mathbb{Z}_{>0} \)

An action, however, is defined by the number of identities \( k \) that is used by attacker in making false report to FC. For example in state \( s_t = 3 \), an attacker can choose to use \( k = 4 \) identities, where \( k \in [1, M] \), to make false report. Using Q-learning, some other important parameters include learning rate denoted by \( \alpha \) and discount factor denoted by \( \gamma \). The reward \( r \) is dependent on the success of an attack and \( k \). In the case of success the reward assigned is inversely proportional to the \( k \) but in case of failure, the reward is negative and directly proportional to \( k \). The reward is designed in such a manner to discourage any tendency to “greedy attack” i.e. \( k \rightarrow M \). The Q-learning algorithm uses the function \( Q : \mathcal{S} \times \mathcal{A} \rightarrow \mathcal{R} \) to compute the quality of a state \( s \in \mathcal{S} \) after performing an action \( a \in \mathcal{A} \). \( \mathcal{S} \) is a set of possible states and \( \mathcal{A} \) is a set of possible actions. After carrying out an attack at time \( t \), the attacker updates the value of the state-action pair \((s_t, a_t)\) in its Q-table as follows:

\[
Q_{t+1}(s_t, a_t) = Q_t(s_t, a_t) + \alpha \cdot \left[ r(a_t) + \gamma \cdot \max_{a_{t+1}} Q_t(s_{t+1}, a_{t+1}) - Q_t(s_t, a_t) \right]
\]

where \( s_{t+1} \) and \( a_{t+1} \) are the new state (after performing action \( a_t \)) and the best action in the new state respectively. The iterative nature of the algorithm uncovers the best action to be taken given a certain state of performance. The best action \( a^* \), given the current state \( s_t \), is the action

\(^1\eta \) is a positive integer. \( \eta = 4 \) was chosen to demonstrate one of many possible ways an attacker can use to determine its state, based on performance level.
$a \in A$ with the maximum Q-value which is given by the equation

$$a^* = \max_{a \in A} Q(s_t, a) \quad (5.4)$$

### 5.2.2 Identity Ranking Algorithm

An identity $i$ used by the Sybil attacker is characterized by the number of successful attacks $z_i$ and the number of exposures $e_i$. To maintain a balance between the effectiveness of its attacks and its reputation with the FC, attackers select identities that have been less exposed with high success rate with respect to the number of exposures. So the first criterion ensures that the least exposed identities are used in attack. The second criterion further ensures that the least exposed identities have been effective in previous attacks.

The attacker can use the following algorithm to rank the identities, before selecting the best $k$ candidate identities for an attack. Let us assume that the attacker has a set of identities $I = \{(z_i, e_i) | i \in M\}$ to rank. We can decide to use a sorting algorithm (merge sort) with an optimal complexity of $O(n \log n)$ to rank the identities in ascending order. In that case the merge function is modified as follows. Two identities $i$ and $j$ are compared based on the ratios $z_i/e_i$ and $z_j/e_j$. The identity with the least ratio is appended first. If the ratios of the identities are equal, then $e_i$ and $e_j$ are compared. Since $e_i$ and $e_j$ are measures of exposure, the identity with the least exposure is appended first. It is obvious that the complexity algorithm is not affected by the modification. The outcome of the modified sorting algorithm is a set $I^*$ of ordered (ranked) identities.

### 5.2.3 Identity Sampling Strategies

The identity sampling strategy adopted by the Sybil attacker is targeted towards evading discovery by the FC. The attacker can choose to sample its identities in a particular order that reduces the frequency of their appearance in attacks. Some of the strategies that we considered are sliding window, best performing $k$, and identity hopping.
CHAPTER 5. SYBIL ATTACKS AND DYNAMIC REPUTATION SYSTEM

Sliding Window Strategy

The sliding window (SW) strategy selects identities based on specified window, whose size is controlled by $k$. The identities are arranged in such an order that they form a loop. In each round, the window slides fixed number of position(s) to the right. The identities that fall within the window are used to conduct the attack. The identities are arranged to form a loop such that the window simply wraps around. As we can see, the strategy ensures that in every round, one new identity is featured and one old identity is withdrawn. The sliding window strategy exhibits periodicity, which is dependent on the number of positions it slides across. As a result, the identities are periodically sampled for the attack. An illustration of the sliding window identity sampling strategy can be seen in Figure 5.1a.

![Figure 5.1a: Sliding Window Identity Sampling Strategy with $k = 3$.](image)

Best Performing-$k$ Strategy

In best performing $k$ (BP) strategy, the attacker samples those identities obtained from the identity ranking algorithm described. The algorithm is designed to favor the selection of identities with relatively better performance per exposure, and ensures that identities with high failure rate are
sampled less often. The best performing $k$ strategies leverages this approach to inject some sort of balance between success of an attack and the reputation of identities.

**Identity Hopping Strategy**

Inspired by the concept of frequency hopping mechanism [99], the identity hopping (IH) algorithm is targeted towards generating a pseudo-random sequence of identities. It involves ranking of the identities, which is carried out using the IR algorithm described. A pseudo-random sequence is generated using the ranks of the identities. The sequence allows some bias towards identities that are ranked high. Using a decreasing linear function, the number of occurrence $y_i$ of each identity in the sequence is determined using the expression: $y_i = M - r_i + 1$, where $r_i$ is the identity’s rank. A decreasing parabolic function can also be used instead, defined as $y_i = (M - r_i + 1)^2$. In this work, we assume that linear function is used in the pseudo-random sequence generation. Consider the following example of the pseudo-random sequence generation. Assuming that the identities are ranked in the following order: \{1, 4, 2, 5, 3\}, then identity 1 occurs 5 times in the sequence, 4 occurs 4 times etc.

The $k$ identities used in the attack are selected from the sequence with replacement. It is obvious that the probability of selecting the highest ranked identity is high given that the length of the sequence is $M(M+1)/2$. But we cannot ignore that it is still probable to pick an identity other than highest ranked identity. The randomness associated with this strategy makes it difficult for the FC to learn the sampling pattern of the Sybil attacker. The attacker achieves a dual goal here: increasing the chances of selecting the best performing $k$ identities and randomizing its choices.

### 5.3 Dynamic Reputation System

The Dynamic Reputation System we are about to discuss provides a flexible but robust framework to counteract the effect of malicious activities on spectrum decision making process, especially in the case of Sybil attacks [31], [36]. The reputation system is managed by the FC, which observes correct reporting of CR nodes and computes their reputation of the nodes using reputation functions. The
system is dynamic because the steepness of a reputation functions changes based on the perceived performance of node to which it was assigned. Hence reputation functions play a vital role in evaluating the likelihood of accurate reports made by nodes.

5.3.1 Reputation Function

The dynamic reputation system relies on reputation functions to assign reputation to nodes. Most reputation mechanisms are implemented using a linear reputation function that is dependent on nodes performance [7]. The problem with linear reputation system is that it penalizes every node equally, even the honest nodes. There is no mechanism to deal with each node separately based on its performance. Here, we introduce a reputation mechanism that relies on a non-linear reputation function to compute the reputation of nodes. The reputation function is a non-decreasing exponential function that converges to 1.0. We express a reputation function $R(k)$ in a continuous form as:

$$R(k) = e^{-\lambda} \int_{0}^{k} \frac{\lambda^x}{x!} dx$$

(5.5)

where $\lambda$ is the steepness parameter that determine the rate of reputation growth for a node and $k$ is the mean number of correct reporting made by a node. Equation 5.5 can be represented in a discrete form as,

$$R(k) = e^{-\lambda} \sum_{x=0}^{k} \frac{\lambda^x}{x!}$$

(5.6)

In making decision about channel state, the spectrum reports of nodes are combined in such a way that their reputation values serve as weights to their various reports. Each $i$-th CR node is assigned a reputation function $R_i(k)$ which is used to compute the reputation of the node. At the end of $t$-th observation interval, the number of correct reports made by node $i$ is $k = \bar{k}_i(t)$. The

---

2Reputation in this context can be interpreted as the trust FC has for a node to report correctly. In our model, the opinions of nodes about their peers are not required by the FC. FC only listens to policy nodes to confirm or verify spectrum state decisions.
value of $k$ can be estimated as a running average of correct reports,

$$\bar{k}_i = \frac{1}{T} \cdot \sum_{t=1}^{T} k_i(t)$$

(5.7)

where $k_i(t)$, in the case of multiple channel reporting, is given as

$$k_i(t) = \frac{1}{M} \cdot \sum_{\tau=T_s}^{T_f} \sum_{m=1}^{M} \sigma_j(\tau)$$

(5.8)

$\sigma_j(\tau) \in \{0, 1\}$ is an indicator function of accuracy for channel $j$ during the observation interval $[T_s, T_f]$.

The parameter $\lambda$ is of prime importance in measuring the reputation of a node. A small value of $\lambda$ is indicative of node’s good performance in terms of accurate reporting. With small $\lambda$ a node builds its reputation faster with fewer accurate reporting. On the other hand, a large $\lambda$ would keep the reputation of a node low and will require a longer period of accurate reporting for a node to prove itself with the FC.
In figure 5.2, reputation functions for varying $\lambda$ are illustrated. The observation interval $T = 20$ and we observe that reputation function tends to maximum reputation value $R_{max}(k) = 1.0$ as the number of correct reporting increases. The speed of attaining $R_{max}(k)$ can be seen to depend on $\lambda$, which determines the steepness of a function curve. For nodes with $\lambda = 3.75$, fewer correct reports $k$ are needed attain maximum reputation $R_{max}(k)$ than nodes with $\lambda = 9.25$. For instance, consider two nodes $A$ and $B$ $k_A = k_B = 7$ but different $\lambda$ values, $\lambda = 3.75$ and $\lambda = 9.25$ respectively. By equation 5.6, the reputation of the nodes are computed as $R_A = 0.97$ and $R_B = 0.29$. By virtue of the reputation values, the reports of $A$ would carry much more weight than those of $B$.

The update of $\lambda$ by the FC is done at end of every observation interval $[T_s, T_f]$. With the current $\lambda$ and the number of accurate reports $k_i(t)$ for the last observation interval, the FC computes the change in $\lambda$, denoted as $\Delta \lambda$. To determine the value of $\Delta \lambda \in [-1, 1]$, FC uses a Fuzzy Logic (FL) control which is based on fuzzy membership functions and linguistic rules. We will be discussing the FL controller for the reputation system in the next session.

5.3.2 Spectrum Decision Making

In dynamic system such as the cognitive radio networks, nodes operate on multiple spectrum bands or channels. It has been shown that cooperative spectrum sensing and decision-making improves efficiency of transmission and increases utility.

Consider a cooperative CR network with $N$ active nodes operating on $M$ channels implementing a cooperative spectrum sensing (centralized or distributed). A node can be actively sensing and reporting spectrum state for $m$ of $M$ available channels to the fusion center. CR nodes are allowed to tender reports on as many channels as they can sense. The number of channels allocated to a node might be depended on the number of channels that it reported and some other parameters. A lot of chapters have been published on efficient spectrum allocation mechanisms (cite as many chapter as possible), therefore no discussion on spectrum allocation will be done here.

At the end of every sensing phase, combined sensing reports of nodes produces a matrix $S$ of dimension $N \times M$. Each cell in $S$ corresponds to a node $i$ opinion about the state of the spectrum
In order to simplify the complex scenario which may arise and lead incomplete information because of nodes sensing only $m_i$ of the channels, we assume that $m_i = M$ for all nodes.

On the basis of the spectrum matrix $S$, a decision has to be reached on the actual state of the spectrum bands based on the speculation of the CR nodes. The decision reached after number of operations involving $S$ is represented as a matrix $A$ of dimension $1 \times M$. We introduce $R$ as reputation matrix that influences the validity of the reports given by nodes. $R$ is a diagonal matrix of $N \times N$ and $R = (R_{ij})$ where

$$R_{ij} = 0 \text{ if } i \neq j \forall i, j \in 1, \cdots, N$$

The elements of the diagonal matrix $R$ is correspond to the reputation of the nodes. We chose this matrix structure in representing reputation because it allows us to represent the spectrum decision-making process as a series of matrix operations. This also allows to utilize the tools of matrix operations in analyzing the decision making process.

In a case where $M = 1$ (one channel scenario), the decision about the channel state is taken with the consideration of nodes’ reputations as follows. First compute the decision using weighted arithmetic mean method, that is

$$\bar{x}_k = \frac{\sum_i R_{ij} \cdot x_{ik}}{\sum_i R_{ij}}$$

where $k = 1$ and $i = j$. Then, based on decision is reached based on the function $d(\bar{x})$ which is expressed as

$$d(\bar{x}_k) \begin{cases} 0, & \text{if } \bar{x}_k \leq 0.5 \\ 1, & \text{otherwise} \end{cases}$$

where 0 indicates that the spectrum is vacant and can be used for transmission purposes and 1 indicates busy (primary user’s presence). So generalizing the process of evaluating the spectrum
state we have an intermediate matrix $Y$ whose entries are defined as

$$(RS)_{ik} = \sum_{j=1}^{N} R_{ij} \cdot S_{jk} \quad (5.12)$$

and

$$X = \frac{1}{tr(R)} \cdot J_{1,N}Y \quad (5.13)$$

where $J_{1,N}$ is a matrix of ones and $tr(.)$ returns the trace of a matrix, and in our case $R$. Finally, the spectrum state matrix $A$ is obtained, each element $A_k$ is computed as

$$A_k = d(X_k) \quad (5.14)$$

The vector $A$ contains the final decision about the spectrum state. In a situation where all nodes are honest and their reports accurate, the actual spectrum state $A^*$ would be equivalent. But as a result of interference, poor sensing capability and activity of malicious agents, $A^*$ differs from $A$. The estimation error vector is given as $e = A^* - A$ and the mean squared error is given by the trace of the error covariance matrix

$$MSE = tr\{E\{(A^* - A)(A^* - A)^T\}\} \quad (5.15)$$

which simplifies to

$$MSE = \sum_{k}^{M} E\{e_k^2\} \quad (5.16)$$

The ability of nodes to report the spectrum might depend on some other factors such as the nature of their locality (sparse or dense), and known capability of the nodes etc. These factors are independent of the reputation of a node giving accurate report about the spectrum. For example a node in one location might sense transmission in some bands better than others. With the knowledge that the accuracy with which a node senses a channel clearly depends on its location, we can assign weights to the node. The channels that it can sense clearly from its location are assigned higher weights while other channels are assigned lower weights. This gives rise to a matrix
A close look at the reputation function (see Figure 5.2) will reveal the dependency of the reputation of a node on $\lambda$. With a large $\lambda$, the reputation grows slower. This implies that it will take a node a considerable number of accurate reporting to gain reputation with the fusion center. In contrast, a small $\lambda$ allows the reputation of a node to grow fast with fewer accurate reporting. The main question arising is how the parameter is controlled such that honest nodes are assigned low $\lambda$ values and malicious nodes receive high $\lambda$ values. Supposing that at end of a spectrum reporting observation interval each node has a certain $\lambda$ and a corresponding number of observed correct reports $\mu$. Based on these input parameters, the change $\delta \lambda$ to be made to $\lambda$ is computed as part of the update of the reputation parameter.

We consider spectrum reporting as a fuzzy process, where honest nodes can sometimes be delinquent and give inaccurate reports. Such behaviors among honest nodes are short-lived; otherwise
they would simply resemble malicious nodes. Using a fixed threshold to penalize nodes by increasing their $\lambda$ values does not accommodate such unintentional and short-lived false reporting and makes honest nodes vulnerable to be perceived as malicious. To prevent this kind of scenario, we propose the use of fuzzy logic controller to decide how nodes reputation parameters would be adjusted to control their reputation functions. Since the reporting behavior could be fuzzy, it is particularly reasonable to have fuzzy rules that decides how $\lambda$ should be adjusted. A fuzzy logic controller that provides a feedback control would be suitable to handle such spontaneous transition from being honest to being malicious and vice versa. The use of fuzzy logic control might not be the only approach to dynamically control the value $\lambda$ but one that is best suited and feasible for the dynamic process of spectrum reporting. Fuzzy logic control is known to be a non-linear adaptive control method based on artificial intelligence (AI) and provides the robust control that is much desired in dynamic systems [80]. It has proven to be a powerful technique for controlling processes that are quite difficult to model and linearize [76].

Figure 5.3: Architecture of a fuzzy logic controller for $\lambda$ control.
Figure 5.4: Membership functions of input variable $\lambda$.

An illustration of a typical fuzzy logic controller (FLC) architecture is presented in figure 5.3. FLC comprises of the fuzzification module, the inference module and the defuzzification module. The modules have specific roles they play in the control process. The fuzzification module is responsible for converting the crisp values of $\lambda$ and $\mu$ into fuzzy values with the help of fuzzy membership functions assigned to the fuzzy sets. For $\lambda$ we have three fuzzy sets LOW, MEDIUM, HIGH with membership functions as $f_L(\lambda_i)$, $f_M(\lambda_i)$ and $f_H(\lambda_i)$ respectively. Each measured value $\lambda_i$ has a degree of membership with each fuzzy set that lies in the interval $[0, 1]$. The membership functions of $\lambda$ fuzzy sets are illustrated in figure 5.4. Three fuzzy sets are defined for $\mu$, which include LOW, MEDIUM and HIGH with membership functions as $g_L(\mu_i)$, $g_M(\mu_i)$ and $g_H(\mu_i)$ respectively. The membership functions for the fuzzy sets of $\mu$ are illustrated in figure 5.5. Measured values of $\mu_i$ are first normalized and then mapped to values in the interval $[0, 1]$ by the membership functions to obtain their fuzzy equivalents.

The transformation of the measured crisp values of $\lambda$ and $\mu$ into fuzzy sets, makes them compatible with fuzzy set representation of the linguistic variables in fuzzy rules. We denote the set of fuzzy rules as $\Gamma = \{\Gamma_i \mid i \in [1, |\Gamma|]\}$.

The inference module computes for each fuzzy rule the overall control output derived from the individual components of the rule. The components of rules are outputs of the fuzzification module
that represent the original crisp values. The fuzzification outputs are matched to each fuzzy rule and the degree of match for each rule is computed. The degree of match is representative of the degree of satisfaction of a fuzzy rule and together they form a set of fuzzy control output for the inference module.

The fuzzy rules represent the control policy or strategy space of an experienced FC to tackle false reporting and make accurate decisions. A fuzzy rule consists of an antecedent or premise part and the consequence or conclusion part. The rule-antecedent comprises of the values of $\lambda$ and $\mu$ and the consequence of the rule denotes the type of action taken by the FC. An action is either to (slightly) increase or (slightly) decrease $\lambda$ by $\Delta \lambda$ or keep the value unchanged. The fuzzy rules\(^3\), generated for the FL control, are as follows:

1. if $\lambda$ is LOW & $\mu$ is LOW then $\Delta \lambda$ is NCHG
2. if $\lambda$ is LOW & $\mu$ is MEDIUM then $\Delta \lambda$ is SINC
3. if $\lambda$ is LOW & $\mu$ is HIGH then $\Delta \lambda$ is INC
4. if $\lambda$ is MEDIUM & $\mu$ is LOW then $\Delta \lambda$ is DEC

\(^3\)The number of fuzzy rules used for fuzzy inference is dependent on the number of fuzzy sets defined for the FLC and the overlaps between the fuzzy sets. We can recall that by definition, a fuzzy set is defined for a particular linguistic variable. In our case, we have 3 possible linguistic variables for the fuzzy input and 5 linguistic variables for the fuzzy output.
5. if $\lambda$ is MEDIUM & $\mu$ is MEDIUM then $\Delta\lambda$ is INC

6. if $\lambda$ is MEDIUM & $\mu$ is HIGH then $\Delta\lambda$ is INC

7. if $\lambda$ is HIGH & $\mu$ is LOW then $\Delta\lambda$ is DEC

8. if $\lambda$ is HIGH & $\mu$ is MEDIUM then $\Delta\lambda$ is SDEC

9. if $\lambda$ is HIGH & $\mu$ is HIGH then $\Delta\lambda$ is NCHG

INC, SINC, DEC, SDEC, NCHG are fuzzy sets of $\Delta\lambda$ that denote increment, slight increment, decrement, slight decrement and no change respectively. Henceforth, we shall denote each fuzzy set for $\Delta\lambda$ as $X$. It is important to note that the fuzzy rules can be condensed to obtain fewer rules or varied to achieve different goals.

The fuzzy rules are used to evaluate the fuzzy output of the inference module. The fuzzy rules contain the conjunction & and therefore are evaluated using the AND (intersection) operator as follows:

$$v(\Gamma_i \rightarrow X) = \min[f_A(\lambda), g_B(\mu)]$$ (5.18)

where $A$ and $B$ are representative of the fuzzy sets of $\lambda$ and $\mu$ respectively. It is easy to note that $v(\Gamma_i \rightarrow X) = h_X(\Delta\lambda_X)$ and constitute the output of the fuzzy inference rule $\Gamma_i$, such that $h_X(\Delta\lambda_X)$ is the value of the membership function $h_X(\cdot)$ returned for a certain anticipated change in $\lambda$ denoted as $\Delta\lambda_X$.

Defuzzification module takes the fuzzy output values of the inference module and converts them into crisp $\Delta\lambda$ value. For the defuzzification module there are six different fuzzy sets with membership function set $\{h_X(\cdot)\}$. We use the centroid principle, proposed by Sugeno(1985) for the defuzzification process. This principle is also referred to as center of gravity method in most literature on defuzzification. Each fuzzy set has a centroid $\Delta\lambda_X$ which coincides with the horizontal coordinate that corresponds with the center of mass of the area under its membership function. $\Delta\lambda$ is computed as

$$\Delta\lambda = \frac{\sum_{\Gamma_i \rightarrow X} h_X(\Delta\lambda_X) \cdot \Delta\lambda_X}{\sum_{\Gamma_i \rightarrow X} h_X(\Delta\lambda_X)}$$ (5.19)
where $\Delta \lambda \in \mathbb{R}$ and $-1 \leq \Delta \lambda \leq 1$. $\Gamma_i$ is the $i$-th fuzzy rule whose consequent belongs to the fuzzy set $X$. We denote the pair as $\Gamma_i \rightarrow X$. The values of $\{h_X(\Delta \lambda_X)\}$ are output values of the inference modules fired by each fuzzy rule $\Gamma_i$. At the end of defuzzification process, $\lambda$ is updated simply as follows:

$$\lambda = \lambda + \Delta \lambda$$  \hspace{1cm} (5.20)

It is the sole decision of the FC to define the fuzzy sets and their membership functions used in the FLC. The fuzzy membership functions come in different shapes such as triangular, trapezoidal, sigmoidal, bell-shaped. In this work, a combination of sigmoidal and bell-shaped membership functions were used for the fuzzy set of the input and output variables. This type of membership functions have been used successful in modeling controllers as stated in [80].

As we stated earlier, the main goal of the FC is keeping $\lambda$ low for the honest nodes and high for the malicious nodes. The fuzzy rules $\{\Gamma_i\}$ ensure that this goal is attained. The rules also make it possible for a node induced into malicious behavior to recover once its $\mu$ reduces. A node is capable of restoring its reputation, provided there is significant improvement in its reporting over a number of observational intervals. The speed of restoring its reputation with the FC largely

Figure 5.6: BellShape membership functions for output variable $\Delta \lambda$. 

![BellShape membership functions for output variable $\Delta \lambda$.](image)
depends on its current value of $\lambda$. With FLC, the restoration of the reputation is not drastic but follows smooth transition which is reflected in the rate of change of $\lambda$. Likewise, a malicious node that begins reporting by pretending to be an honest node is quickly identified. The persistence of malicious nodes to compromise FC’s decision eventually reflects in the reporting. With the help of the FLC, FC can detect the increased rate of false reporting and decide to increase $\lambda$, irrespective of the initial values.

5.5 Numerical and Experimental Results

We conducted simulation experiments to evaluate the performances of the reinforcement learning based Sybil attacker and the adaptive Fusion Center. In all experimental setups, we focused on scenarios where the number of Sybil identities exceeded or is equivalent to the number of honest identities ($M \geq N$). The main intent behind the experiments is to show the impact of Q-learning on the effectiveness of Sybil attacks and how the success of such intelligent attacks can be counteracted using dynamic reputation mechanism (DRM).

The RL based Sybil attack was implemented using the following settings for the learning rate...
and discount rate: $\gamma = 0.1$ and $\alpha = 0.8$. The learning rate indicates to what extent the newly acquired information should override the old information. We choose a relatively high learning rate $\alpha = 0.8$ for the attacker; this allows the attacker to quickly adapt to the sudden changes in the effectiveness of its attacks. We set the discount factor as $\gamma = 0.1$, which indicates that Sybil attacker is interested only in short-term positive outcome. The number of possible states $\eta = |\mathcal{S}| = 10$ and the number of possible actions $|\mathcal{A}| = M$, which is equivalent to the maximum number of Sybil identities that can be used in an attack.

For the dynamic reputation system, CR nodes in the simulation model were assigned different false reporting rates $\{\mu_i\}$, which correlated with the number of false reports that they can produce on average within a predefined observation interval. The FC is not aware of these rates and at the beginning assigns all nodes an arbitrary $\lambda_0$ as the initial value of $\lambda$ of their reputation functions. By observing and monitoring the reporting trends, FC is capable of adjusting $\lambda_i$ for each $i$-th node with the help of the FL controller. Experimental results shows that $\lambda$ converges and is independent of the initial value of $\lambda_0$. Performance in all experimental setups was measured as the number of times the attacker was successful in fooling the FC to decide the spectrum state in its favor.

In subsequent subsections we present the analysis of experimental results obtained from our simulation. First, we will show that the fuzzy logic based DRM is more effective in controlling the reputation of CR nodes than the static linear reputation mechanism (SRM) [67]. Then, a detailed comparison of the two mechanisms using the performance of the Sybil attacker during the stages of attacks will be presented. Finally, we will compare the performance of the Sybil attacker under the different identity sampling strategies discussed earlier.

### 5.5.1 Fuzzy Logic Control of $\lambda$

Our experimentation results revealed that the fuzzy based dynamic reputation system is effective in keeping the influence of malicious reporting on spectrum decision-making under control. The ability of FC to separate honest nodes from malicious nodes using the FL controller is dependent on the parameterization of the membership functions. FC alone decides the acceptable ranges for
\( \lambda^* \), hence establishing the threshold for poor performance normally associated high \( \lambda \) values (see section 5.4).

We also observed quick convergence in identifying and separating the nodes based on reporting patterns. Nodes with high false reporting rates emerge with higher \( \lambda^* \) values. As a result, their reports are assigned low importance, which have no significant impact on FC’s decision-making process.

### 5.5.2 Comparing Linear and Dynamic Reputation Systems

In a linear reputation mechanism, the reputation values of nodes are initialized to be 1 at the beginning and updated according to the following relations:

\[
\frac{r_i}{s} = \begin{cases} 
    r_i + \delta r & \text{spectrum report is correct} \\
    r_i & \text{spectrum report is wrong}
\end{cases} 
\]  
\[
(5.21)
\]

where \( r_i \) is the reputation of the \( i \)-th node and \( \delta r \) is the pre-determined quantum of increase in reputation for each correct report. The reputation values are used as weights after normalization, which is given as

\[
\tilde{r}_i = \frac{r_i}{\sum_j r_j} 
\]  
\[
(5.22)
\]

For the experimental setup, we set \( N = 7 \) and the corresponding \( \lambda \) values for the nodes \( \{ \lambda_i \} = \{4, 5, 6, 7, 8, 9, 10\} \). Reputation measurements are taken at the end of each observation interval which consists of 20 rounds of spectrum reporting. Experimental results for Linear and Dynamic Reputation Systems, collected over an observational period of 1000 time intervals, are illustrated in figures 5.8 and 5.9 respectively. In our dynamic reputation system, the nodes are assigned high \( \lambda \) value of 30 by the FC. This implies that spectrum reporting begins with FC assigning an approximate reputation of zero, compared to the linear mechanism where reputation values are initialized to 1 at the beginning.

In linear reputation approach, the reputations of nodes are not dynamically controlled; making
it possible a node maintains the same reputation over time. The approach does not take into consideration of induced malicious behavior of nodes, where nodes make false reports influenced by malicious activities. Also not considered is the malicious attack strategy, where malicious nodes are passive during certain intervals but become active during those periods where accurate spectrum reporting is critical. Tracking such malicious nodes using this approach is highly ineffective and inefficient and impacts negatively on spectrum utilization.

The approach we propose takes care of this scenario by being proactive about what nodes report.
Figure 5.10: Time series plot of $\lambda$ values for CR nodes as updated by FC using FL controller during the observation intervals.

in every interval. Based on node’s reporting history, which is embedded in $\lambda$ and its current false reporting rate, nodes are apportioned reputation that accurately reflects their reporting status. The absence of a fixed threshold for false reporting rate also benefits the system. The threshold in the dynamic reputation system is fuzzy, allowing FC to define a range of values (fuzzy sets) that is acceptable. The fuzzy rules are defined in a manner that enforces correct reporting and deals decisively with false reporting. An honest node with high false report is encouraged to restore its reputation by consistently reporting correctly over a period of time. With a $\lambda$ value that is high and low $\mu$, its $\lambda$ value is slightly decreased until there is a significant improvement in $\lambda$. It is difficult for a malicious node to exploit this mechanism because malicious node is persistent in its attack and would be easily identified. Also, a rule exists that ensure that sudden increment in $\mu$ is matched with a corresponding increment of the node’s $\lambda$. For honest nodes, such drastic change in $\mu$ is rarely observed and if it occurs, is treated as a malicious attempt.

5.5.3 Comparison of Output Membership Functions

Here nodes are assigned the following false reporting rates $\mu_{avg} = \{4, 5, 8, 11, 10, 15, 16\}$ respectively. Simulation results obtained under this setting are illustrated in figures 5.11, 5.12, 5.13, 5.14. Figures 5.11 and 5.12 illustrate the reputation and $\lambda$ series obtained with triangular membership
functions for the output variable. Figures 5.13 and 5.14 shows the results obtained in the case where ball-shaped membership functions were used for the output variable. Triangular and bell-shaped membership functions are illustrated in figure ???. In both scenarios, the input membership functions were composed of sigmoidal and bell-shaped functions. By mere observation of the plots for the reputation and $\lambda$ values, there is little or no difference in the result obtained.

One thing that is common in both cases is that the reputation of nodes that are reporting correctly most times are assign high reputation. For instance, in figure 5.11 the reputations of nodes $N_1$ and $N_2$ become equal to 1 within few observation intervals. These nodes are favored because they are reporting with false reporting rates that within the range that FC considers to be low. The membership function $f_L(\lambda)$ for the fuzzy set LOW (see figure ??) has the following properties:

- The centroid is positioned at $\lambda = 5$.
- Maximum degree of membership is attained at the value $\lambda = 0$.
- The degree of membership gradually phases out as $\lambda$ increases.

This explains the reason why nodes $N_1$ and $N_2$ were able to attain the maximum reputation faster than the rest of the nodes. Node $N_3$ falsely reporting at the rate of $\mu = 8$ maintains high reputation but fails short of attaining the maximum reputation. By shifting the centroid of the membership function of the fuzzy set LOW to the left, it will be observed that $N_3$ might eventually be unable to attain such high reputation. The others \{ $N_4, N_5, N_6, N_7$ \} have low reputations. Since the false reporting rates are high, the reports are assigned low importance. In a case where these nodes are mere Sybil identities, operated by a single malicious node, their impact on FC’s spectrum decision making will be quite insignificant. Compared to the linear reputation mechanism, our approach is more effective in counteracting this type of scenario. In the linear reputation system (see figure 5.8) the reputations of both the good nodes and the malicious nodes are very close and therefore if the Sybil nodes do not need to be majority to overcome the reputation system and corrupt FC’s spectrum decisions.
5.5.4 Performance of RL based Sybil Attack

To demonstrate how the use of RL can enhance the performance of the Sybil attacker, we considered two different methods employed by FC in making decision about spectrum availability: static reputation mechanism (SRM) and dynamic reputation mechanism (DRM). In order to demonstrate the benefit of employing RL in the attack, we further embark on comparing the performances of a RL based attack and a random attack. Random attack involves the attacker randomly selecting the number of identities $k$ to use for false reporting in each stage. It is comparable to an RL based
CHAPTER 5. SYBIL ATTACKS AND DYNAMIC REPUTATION SYSTEM

147

Figure 5.13: Time series plot of reputation value for output variable with Bell-shaped membership functions.

Figure 5.14: Time series plot of $\lambda$ for output variable with Bell-shaped membership functions.

attack with $\epsilon = 1$ i.e. 100% exploration.

Using the SRM mechanism, we consider the following cases where an attacker implements: random attack, RL based attack with $\epsilon = 0.3$ and RL based attack with $\epsilon = 0.8^4$. The results obtained for the cases just stated are illustrated in Figure 5.15. In general, we observe that the effectiveness of the Sybil attacks improves with increased verification error $\xi$ of the FC. This trend is expected as an increase in $\xi$ indicates that FC cannot correctly identify the false-reporting identities

---

4The choice of $\epsilon = 0.3$ and $\epsilon = 0.8$ is representative of low and high exploration of the Q-table, chosen to highlight performance at the two different exploration levels. Dependency of performance on the $\epsilon$, which varies between 0 and 1, would be considered in future works.
and penalize them. The figure further reveals the benefits of using an RL technique (Q-learning) in conducting Sybil attacks. It can be seen that it is more effective if RL technique is employed in the attacks with small $\epsilon$. In Figure 5.15, it is obvious that best performance was mostly attained with varying $\xi$ when $\epsilon = 0.3$. This implies that the attacker explores the possible actions less frequently and exploits the Q-table often to determine the best action to take in each stage, which eventually leads to a better performance.

The same experiment was repeated using the settings as described above but now with FC implementing our proposed DRM mechanism. Due to the effectiveness of the DRM method, the performance of the Sybil attacker remains very low. Despite Sybil attacker’s use of RL, it was not capable of “fooling” the FC into concluding in its favor. Irrespective of the attack strategy adopted by the attacker, the DRM mechanism was capable of isolating the Sybil identities and assigning them low reputations. The low reputations of the identities account for the very poor performance of the attacker which is shown in Figure 5.16. DRM, in comparison with SRM, is a better reputation mechanism to counteract the impact of Sybil attackers on spectrum decisions.
5.5.5 Comparison of Identity Sampling Strategies

In the next set of experiments, we compare the performances of the Sybil identity sampling strategies discussed earlier. To test their various performances we implement SRM decision-making mechanism for the FC. In the first simulation setting we kept $\epsilon = 0.3$. The result of the experiment is illustrated in Figure 5.17.

It can be seen vividly that BP outperforms other sampling strategies employed by the attacker. As seen in previous experiments, an attacker experiences performance improvement as $\xi$ increases which reflects FC’s increasing inability to accurately verify its decisions. Among the identity sampling strategies, BP shows the best performance. BP strategy, which involves selecting highly successfully but less frequently used identities, accounts for the improvement performance. The poor performance of the IH strategy can be attributed to the low $\epsilon$, which actually reduces the randomness associated with attacker’s exploration of possible actions with different $k$.

A different result was obtained in the second experiment (Figure 5.18), where exploration probability was increased to $\epsilon = 0.8$. BP still gives a better performance compared to other sampling
Figure 5.17: Comparison of the Sybil identity sampling strategies based on their Performance with varying $\xi$, with $\epsilon = 0.3$.

Figure 5.18: Comparison of the Sybil identity sampling strategies based on their Performance with varying $\xi$, with $\epsilon = 0.8$. 
strategies. However, an interesting trend is observed for IH at $\xi = 0.65$ in Figure 5.18, where its performance overtakes that of SW. This trend can be attributed to the increased exploration, which allows the attacker to explore more often. The increased exploratory activity of the attacker adds to the randomness that is already inherent in IH, thereby boosting its performance. We can also recall that IH is randomized equivalent of BP and that explains why BP always does better than it. It can also be observed in Figure 5.18 that the curves produced by IH and BP are congruent. The difference between the two strategies is induced by the random selection of identities that is biased towards the best candidate identities.

5.5.6 Comparison of Decision Making Mechanisms

The performance of FC is of paramount importance in controlling the effectiveness of Sybil attacks. The goal, therefore, would be to minimize the effectiveness of the Sybil attacks, despite the strategy used by the attacker. FC assigns reputation to identities of nodes used in sensing reports and the reputation of an identity reflect the importance of its report. Reputation values are used as weights to arrive at the right conclusion about the state of the spectrum.

Here we compare the performances of the static reputation mechanism (SRM) and our newly proposed dynamic reputation mechanism (DRM). The performance of a decision-making mechanism is computed from the perspective of Sybil attacker’s performance. Better performance of the attacker indicates inability of the mechanism to control Sybil attacks. Therefore we expect that a better mechanism would reduce the performance of the Sybil attacker by reducing the number of successful attacks. For experimental purpose, we kept $\xi$ between 0 and 0.45.

The result of the first experiment with $\epsilon = 0.3$ is illustrated in Figure 5.19.

In general, we can observe that the performance of the attacker increases as $\xi$ increases in Figure 5.20. But we can make clear distinction as to which reputation mechanism is best in maintaining control over Sybil identities. DRM mechanism presents a clear choice to control false reporting from the Sybil identities.

The results obtained with $\epsilon = 0.8$ (Figure 5.20) does not differ much from the results described
Figure 5.19: Comparison of the decision making mechanisms based on their performance with varying $\xi$, $\epsilon = 0.3$.

Figure 5.20: Comparison of the decision making mechanisms based on their performance with varying $\xi$, with $\epsilon = 0.8$. 
above. For the SRM mechanism, we observe a decrease in the performance rate as \( \xi \) increases but DRM mechanism is more effective in keeping this rate low. We also observe that the trend for the attacker’s performance using DRM mechanism is practically the same, proving the robustness of the DRM.

The better performance of DRM mechanism can be attributed to the approach used in computing reputation for identities. The non-linear reputation function assigned separately to each identity is dynamically adjusted based on an identity’s performance over the period of reporting. It is not as static and linear as implemented in the SRM mechanism. This gives the DRM mechanism an edge to control false-reporting highly effectively.

5.6 Conclusions

In this chapter, we present identity-sampling strategies that can be employed by the Sybil attacker in choosing identities used in false reporting. The main aim of the identity sampling strategies is to minimize exposure of the identities and enhance their reputation with the FC. We demonstrate also that an attacker can improve the effectiveness of its attacks by employing RL techniques. The attacker implements Q-learning algorithm and relies on the Q-table to determine the optimal action (\( k \) identities) to perform based on its performance state. In future, we intend to investigate how long it takes for the attacker, on the average, to learn the optimal action-selection policy.

We also present a novel dynamic reputation mechanism implemented by FC and used in keeping false reporting under control. The reputation function is robust and effective in assigning the appropriate reputation to nodes based on their performances. Our experimental findings reveal the effectiveness of the dynamic reputation mechanism making the proposed mechanism a clear defense choice against intelligent Sybil attacks.
Chapter 6

Conclusions

In this research, we studied the various challenges facing the application of cognitive radios in the current state-of-the-art wireless technologies. We addressed issues relating to spectrum scarcity, network starvation, self-coexistence and security.

To address the problem of self-coexistence of CR networks in a decentralized, we study and propose multiple channel acquisition heuristics. We show that under limited communication constraints, these heuristics enable CR networks to satisfy their channel size requirements. One of the proposed channel acquisition heuristics, the FAK algorithm, converges faster than the CFL algorithm in a multiple channel acquisition scenario.

We show that under constrained supply of spectrum resources, the formation of risk-motivated deference structure coalitions can be beneficial to the CR networks. We propose a risk-motivated channel selection scheme that helps CR networks to access channel viability for transmission based on the risk of spectrum contention. We also demonstrated that minimizing the risk of spectrum contention could serve as an incentive for networks to merge and form deference coalitions.

As far as spectrum contention is concerned, we devised a modified version of the On-Demand Spectrum Contention protocol that is distributed and cheat-proof with enhancement to promote fairness and efficient spectrum utilization. Our proposed spectrum contention protocol MODSC, eliminates monopoly and CPN manipulation that is common with the ODSC. We also highlight
that the topology of the network can impact on the level of fairness in spectrum contention.

We present the dynamic reputation system, which provides the efficient and effective mechanism to control the impact of Sybil attacks on CR networks. We present a concise mathematical framework for spectrum decision making by the fusion center. This framework allows the fusion center to combine spectrum reports (busy or idle) in a way that suppresses malicious reports by taking into consideration the reputation of the reporting CR nodes. We also demonstrate the dynamic reputation system is robust and effective in mitigating intelligent Sybil attacks fomented using learning techniques.


