INFORMED COGNITIVE RADIOS

A Dissertation in
Electrical Engineering
by
Khashayar Kotobi

© 2017 Khashayar Kotobi

Submitted in Partial Fulfillment
of the Requirements
for the Degree of

Doctor of Philosophy

December 2017
The dissertation of Khashayar Kotobi was reviewed and approved* by the following:

Sven G. Bilén  
Professor of Engineering Design, Electrical Engineering,  
and Aerospace Engineering  
Dissertation Advisor, Chair of Committee

W. Kenneth Jenkins  
Professor Emeritus of Electrical Engineering

Julio V. Urbina  
Associate Professor of Electrical Engineering

Kyusun Choi  
Associate Professor of Computer Science and Engineering

Kultegin Aydin  
Professor of Electrical Engineering  
Department Head

*Signatures are on file in the Graduate School.
Abstract

We introduce an “informed cognitive radio” that data mines new information to improve the understanding of its environment and novel mathematical algorithms to react to that environment. We propose the data mining–informed cognitive radio, which uses non-traditional data sources and data-mining techniques for decision making and improving the performance of a wireless network.

We consider a cognitive wireless network in which users adopt a spectrum-sharing strategy based on cooperation constraints. The majority of cognitive radio schemes bifurcate the role of players as either cooperative or non-cooperative. In this work, however, we modify this strategy to one in which players are hybrid, i.e., both cooperative and non-cooperative. Using a Stackelberg game strategy, we evaluate the improvement in performance of a cognitive radio network with these hybrid cognitive players using an M/D/1 queuing model. We use a novel game strategy (which we call altruism) to “police” a wireless network by monitoring the network and finding the non-cooperative players. Upon introduction of this new player, we present and test a series of predictive algorithms that show improvements in wireless channel utilization over traditional collision-detection algorithms. Our results demonstrate the viability of using this strategy to inform and create more efficient cognitive radio networks. Next, we study a Stackelberg competition with the primary license holder as the leader, and investigate the impact of multiple leaders by modeling the wireless channel as an M/D/1 queue. We find that, in the Stackelberg game, the leader can improve its utility by influencing the followers’ decisions using its advertised cost function and the number of followers accepted in the network. The gain in utility monotonically increases until the network is saturated. The Stackelberg game formulation shows the existence of a unique Nash equilibrium using an appropriate cost function. The equilibrium maximizes the total utility of the network and allows spectrum sharing between primary and secondary cognitive users.
We propose a novel medium access protocol. We investigate an auction mechanism for sharing available wireless bandwidth among competing cognitive radios. The bandwidth under consideration may be either in an unlicensed spectrum or in an unused licensed band. Spectrum sharing is achieved via a mechanism in which a cognitive radio acting as the auctioneer advertises spectrum availability to bidding cognitive radios and defines a puzzle to solve as a method to access it. The cognitive radios act as bidders by computing the solution to the problem (i.e., the “puzzle”). The winner is the bidder who submits the first correct bid and thus gains access to the spectrum for the next time interval. We consider two different variations of our scheme based on parallelizable and non-parallelizable problems and demonstrate that the latter provides a fair auction in contrast to the former. We propose a verification database to counter malicious “greedy” players. Our algorithm provides a centralized, easy-to-implement, and computationally fast multiple-access scheme that is verifiable by all participating cognitive radios.

To ensure a secure cognitive radio network, we propose a blockchain verification protocol as a method for enabling and securing spectrum sharing in cognitive radio networks. The spectrum-sharing mechanism is used as a medium access protocol for accessing wireless bandwidth among competing cognitive radios. We introduce a virtual currency, called “Specoins”, for payment to access the spectrum. An auction mechanism based on a first-come-first-served queue is used, with the price for the spectrum advertised by each primary user in a decentralized fashion. The blockchain protocol facilitates the transactions between primary and secondary users and is used to validate and save each user’s virtual wallet. Also important for mobile networks, the blockchain serves as a distributed database that is visible by all participating parties, and any node can volunteer to update the blockchain. The volunteer nodes are called miners and are awarded with Specoins. We propose diverse methods to exchange the Specoins in order to make leasing possible even by cognitive radios that are not miners. We show the improvement of the proposed algorithm compared to the conventional ALOHA medium access protocol in terms of spectrum usage. This difference is investigated using small-scale fading variation in the wireless channel to compare the performance of our secure method with the conventional medium access used in communications. The blockchain verification protocol is not only secure but also outperforms conventional systems in moderate cases of small-scale fading. In the case of severe small-scale fading the blockchain protocol will outperform the conventional system if multipath diversity is not used.
# Table of Contents

List of Figures .................................................................................................................. viii

List of Tables ..................................................................................................................... x

List of Symbols .................................................................................................................. xi

Glossary ................................................................................................................................ xiii

Acknowledgments ............................................................................................................... xiv

1 Introduction ..................................................................................................................... 1

1.1 Wireless Technology ................................................................................................. 1

1.1.1 Motivation ............................................................................................................. 1

1.1.2 Cognitive Radios and Software-Defined Radio ................................................. 2

1.2 Software-Defined Radios .......................................................................................... 3

1.3 Cognitive Radios ....................................................................................................... 3

1.3.1 Definition .............................................................................................................. 4

1.4 Motivation .................................................................................................................. 5

1.5 Contributions ............................................................................................................. 7

1.6 Outline of the Dissertation ....................................................................................... 8

2 Background ................................................................................................................... 11

2.1 Scarce Spectrum Problem ......................................................................................... 11

2.2 Cognitive Radio Background ................................................................................... 13

2.3 Game-Theoretic Background .................................................................................... 15

2.4 Multiple-Access Scheme Background ..................................................................... 17

2.5 Blockchain Background ........................................................................................... 18

2.5.1 Distributed Database ......................................................................................... 18
## 3 Data-Throughput Enhancement Using Data Mining–Informed Cognitive Radio

### 3.1 Chapter Introduction
- 3.1.1 Big Data Framework
- 3.1.2 Proposed Cognitive Radio
- 3.1.3 Chapter Organization

### 3.2 Problem Definition
- 3.2.1 Big Data Framework for Wireless Communication
- 3.2.2 Problem Definition
- 3.2.3 Wireless Channel Modeling

### 3.3 Proposed Algorithms
- 3.3.1 Data Transmission Algorithms
- 3.3.2 Incorporating Network Burstiness

### 3.4 Results and Discussion
- 3.4.1 Simulation Setup
- 3.4.2 Throughput

### 3.5 Simulation Methods
- 3.5.1 Programming
- 3.5.2 Simulation Supplementary Materials

### 3.6 Chapter Summary and Conclusions

## 4 Spectrum Sharing via Hybrid Cognitive Players Evaluated by an M/D/1 Queuing Modeled

### 4.1 Chapter Introduction

### 4.2 Game-Theoretic Study

### 4.3 Spectrum Sharing Algorithm
- 4.3.1 Vigilante Player
- 4.3.2 M/D/1 Queueing Model

### 4.4 System Model
- 4.4.1 Game with Three Players
- 4.4.2 Stackelberg Game in an M/D/1 Queue

### 4.5 Numerical Analysis
- 4.5.1 Cyclic Behavior for Vigilante Player
- 4.5.2 Spectrum Sharing Performance Analysis of a Stackelberg Game using an M/D/1 Queueing Model

### 4.6 Chapter Summary and Conclusion
5 Non-parallelizable Auction for Spectrum Sharing in Cognitive Radio Networks with a Security Verification

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>60</td>
</tr>
<tr>
<td>5.2</td>
<td>61</td>
</tr>
<tr>
<td>5.3</td>
<td>62</td>
</tr>
<tr>
<td>5.3.1</td>
<td>64</td>
</tr>
<tr>
<td>5.3.2</td>
<td>65</td>
</tr>
<tr>
<td>5.4</td>
<td>66</td>
</tr>
<tr>
<td>5.4.1</td>
<td>66</td>
</tr>
<tr>
<td>5.4.2</td>
<td>69</td>
</tr>
<tr>
<td>5.5</td>
<td>70</td>
</tr>
</tbody>
</table>

6 Blockchain Verification as a Spectrum Access Protocol in Cognitive Radio Networks

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>74</td>
</tr>
<tr>
<td>6.2</td>
<td>75</td>
</tr>
<tr>
<td>6.3</td>
<td>76</td>
</tr>
<tr>
<td>6.3.1</td>
<td>76</td>
</tr>
<tr>
<td>6.3.2</td>
<td>77</td>
</tr>
<tr>
<td>6.4</td>
<td>79</td>
</tr>
<tr>
<td>6.4.1</td>
<td>79</td>
</tr>
<tr>
<td>6.4.2</td>
<td>82</td>
</tr>
<tr>
<td>6.4.3</td>
<td>85</td>
</tr>
<tr>
<td>6.5</td>
<td>85</td>
</tr>
</tbody>
</table>

7 Conclusions and Future Work

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>87</td>
</tr>
<tr>
<td>7.1.1</td>
<td>87</td>
</tr>
<tr>
<td>7.1.2</td>
<td>88</td>
</tr>
<tr>
<td>7.2</td>
<td>89</td>
</tr>
<tr>
<td>7.3</td>
<td>89</td>
</tr>
</tbody>
</table>

Bibliography

91
# List of Figures

1.1 The concept map used in this dissertation, this figure will be modified soon .................................................. 10

2.1 United States Frequency Allocations ................................................................. 12

2.2 The perception–action cycle of a cognitive system .............................................. 14

3.1 Proposed data mining-informed cognitive radio (DMICR) system
    utilizes other data sources .................................................................................. 26

3.2 Variation in calculated point-to-point communication Shannon capacity .................. 27

3.3 Comparison between a given demand for data transmission as a function
    of the number of the Tweets ............................................................................. 28

3.4 Comparison between normalized channel usage with the dropping of
    data packets ........................................................................................................ 29

3.5 Comparison between normalized channel usage with using the dropping
    of non-real-time data packets ........................................................................... 30

3.6 Comparison between the normalized channel usage with channel capacity prediction
    by Method 3 ........................................................................................................ 31

3.7 Comparison between normalized channel usage with channel capacity prediction
    during burst traffic ............................................................................................. 35

3.8 Comparison between normalized channel usage with channel capacity prediction
    during steady traffic ........................................................................................... 36

3.9 The channel throughput by Method 3 .................................................................. 37

4.1 Queuing model of primary user as leader and secondary user as a follower in Stackelberg game. ........................................................................................................ 43

4.2 Cognitive network with $M$ players can be divided into $m$ cells each
    with $N$ players ................................................................................................... 45

4.3 The cyclic behavior of a moving greedy player’s throughput ................................ 53

4.4 Effect of a vigilante player’s aggression coefficient ............................................. 54
4.5 The two players normalized utilities versus the number of secondary users ........................................ 55
4.6 The two players normalized utilities versus the number of primary users ........................................ 56
4.7 The two players normalized utilities with different cost functions ........................................ 57
4.8 The two players normalized utilities versus the number of secondary users with different cost functions ........................................ 58
4.9 Greedy player in a queue ........................................ 59

5.1 Network model of competing secondary user ........................................ 63
5.2 Comparison of histogram of the winning bidders for two different auctions ........................................ 69
5.3 Comparison of histogram of the winning bidders for an auction using Newton–Raphson method ........................................ 70
5.4 Comparison of the bidders computational time for an auction using Newton–Raphson method ........................................ 71
5.5 Comparison of the two multiple threaded bidders in terms of number of iterations ........................................ 72

6.1 Time frame for CR to access the available spectrum. ........................................ 78
6.2 Performance comparison of data transmitted versus the Number of CRs ........................................ 82
6.3 Performance comparison of data transmitted versus the fading coefficient ........................................ 83
List of Tables

4.1 Summary of variables used in Chapter 4. . . . . . . . . . . . . . . . . . . . 44
6.1 Summary of variables used in Chapter 6. . . . . . . . . . . . . . . . . 80
List of Symbols

$A_i$ Total number of normal players in $i$th cell

$B_i$ Total number of players that are not vigilante in $i$th cell

$C$ Cost function

$C_k$ Cost function to update blockchain for iteration $k$

$e_g$ The aggressiveness of the greedy player

$e_v$ The aggressiveness of the vigilante player

$i$ Cell indicator

$M$ Total number of players in network

$m$ Total number of cells in network

$N_i$ Total number of players in $i$th cell

$n_p$ Number of primary players

$n_s$ Number of secondary players

$P_g$ Transmitting probability of greedy player

$P_n$ Transmitting probability of normal player

$P_V$ Transmitting probability of vigilante player

$Q_g$ Throughput of greedy player

$Q_n$ Throughput of normal player
\( Q_V \) Throughput of vigilante player

\( R \) Total number of orthogonal channels in network

\( S_i \) \( i \)th secondary user or miner

\( T \) Total number of time slots in network

\( T_i^p \) Transmitted packets by \( i \)th primary user

\( T_i^s \) Transmitted packets by \( i \)th secondary user

\( u_g \) Greedy utility function

\( u_p \) Primary utility function

\( u_s \) Secondary utility function

\( u_v \) Vigilante utility function

\( W_p \) Primary waiting time

\( W_s \) Secondary waiting time

\( \alpha_p \) Share of bandwidth used by primary user

\( \alpha_s \) Share of bandwidth used by secondary user

\( \lambda_p \) Packet rate for the primary user

\( \lambda_s \) Packet rate for the secondary user

\( \mu \) Server rate or bandwidth
Glossary

APSK  Asymmetric Phase-Shift Keying
CDMA  Code-Division Multiple Access
CR    Cognitive Radio
CRN   Cognitive Radio Network
GSM   Global System for Mobile Communications
MAC   Medium Access Control
ML    Machine-Learning
OFDM  Orthogonal Frequency-Division Multiplexing
OFDMA Orthogonal Frequency-Division Multiple Access
QAM   Quadrature Amplitude Modulation
QPSK  Quadrature Phase Shift Keying
RF    Radio Frequency
SDR   Software-Defined Radio
SNR   Signal-to-Noise Ratio
TDMA  Time-Division Multiple Access
USRP  Universal Software Radio Peripheral
Acknowledgments

First and foremost, I would like to express my sincerest gratitude to my advisor, Prof. Sven Bilén, who has greatly supported me during my Ph.D. studies. Without his guidance and persistent help, this dissertation would not have been possible. Sven’s thorough insight in research and his brilliance in connecting deep mathematical notions with practical engineering ideas have always amazed me. He was not only my advisor, but also a great example of an academic researcher with very positive attitude towards life. I truly appreciate that he let me explore a variety of problems across different areas. One simply could not wish for a better or friendlier advisor. I have been very fortunate to collaborate with Robert Capuro. I truly appreciate his guidance during my Ph.D. studies, and his amazing ability to come up with simple solutions for complicated problems I faced in my research. My best friend Mohammad Mirhosseini has been very helpful to me with his knowledge and patience. I would next like to thank my thesis committee members, Prof. Jenkins, Prof. Urbina and Prof. Choi provided great feedback and insight during my research, such as when we discussed my research problem, or when I attended their talks. I would also like to thank Tim Hackett, with whom I collaborated as a researcher in the Systems Design Laboratory. I had great fun doing research with him, and learned many things during my time in the lab with him. Special thanks goes to Ramtin Pedarsani and Kayvan Samimi, with whom I had many hours of fruitful discussion. Thanks to all my friends and colleagues in the Systems Design Lab: Aaron Fleishman, Peng Liu, Hanxiong Hu, Jesse McTernan, and Mike Conway. Thanks to my friends Mostafa Khoshnevisan, Navid Nakhjiri, and Ashkan Pourkand who greatly supported me in the past six years. Last, but not least, I devote my special thanks to my family. There are no words that can fully express my gratitude to my parents. This thesis is dedicated to them with love.

Khashayar Kotobi

_University Park, PA_

_2017_
To my beloved parents Mahshid and Mostafa.
Chapter 1

Introduction

1.1 Wireless Technology

1.1.1 Motivation

In a world of increasing mobility and applications that require much higher data rates than those of conventional voice communications, there is a growing need for users to access networks regardless of their locations and at much higher data rates than currently available. For example, a mobile user in a bus streaming high-definition video. Given the scarcity of available spectrum and the growing demand for wireless communication, researchers and engineers face significant challenges in designing efficient spectrum-sharing systems. Thus, it is essential to pursue a multifaceted approach to develop viable solutions.

While mobile phones and tablets are well-known communication devices with a networking performance dependent on available wireless spectrum, the impact of wireless technology growth into medical systems, home automation systems, smart-grid systems, and sensor networks must be considered in future wireless system spectrum-sharing solutions. Cellular and WiFi systems are the most well-known of the wireless standards; however, wireless systems and standards are significantly more varied. The various wireless systems can be categorized using their coverage area, transmission power, and rate of transmission:

1. cellular systems with high power and wide coverage areas;
2. cordless voice systems with low power and small coverage areas;
3. paging systems with wide coverage areas and low data rates; and
4. wireless LANs with small coverage areas and high data rates.

The first two are voice-based and the second two are data-based systems. Standardization is one of the most important features of these systems. For example, in cellular systems a user may move from city to city and, thus, for the cellular system to provide continuous access, there must be mutually compatible systems. There are currently three major incompatible digital cellular medium access protocols used in cellular standards:

1. TDMA: time-division multiple access protocol;
2. CDMA: code-division multiple access protocol; and
3. OFDMA: orthogonal frequency-division multiple access protocol.

Therefore, a system that can seamlessly switch between these protocols depending on spectrum availability would be highly desirable.

Wireless technology is changing our lives in ways that we can only begin to comprehend; for example, researchers are proposing various protocols for the Internet of Things, which means that not only laptops and smart phones need wireless connections, but also ordinary objects in the home like appliances or climate control systems. The new automated home systems will also require advanced sensors to share the limited spectrum to transfer their data. Spectrum sharing is one of the methods available to use the limited wireless spectrum more efficiently. But, the current wireless frequency spectrum is heavily regulated; as a result, it is imperative that new methods are found to facilitate spectrum sharing.

1.1.2 Cognitive Radios and Software-Defined Radio

Cognitive radios (CRs) employing software-defined radio (SDR) technologies to perform spectrum sharing are widely studied in literature and beginning to be fielded. SDR technology has advanced to the point that commercially available systems are now advanced enough for use in CRs. These advances are essential
for CRs to gain higher throughput (data rate per energy and spectrum used) in a
limited and congested wireless spectrum. In the following sections, SDRs and CRs
are introduced.

1.2 Software-Defined Radios

In 2002, the IEEE P1900.1 group provided a definition for SDRs to facilitate the
understanding of the technology, for consistency among researchers, and to further
its advancement:

**Definition 1.1.** *SDR is a radio in which some or all of the physical-layer functions
are software-defined.*

In contrast to a hardware radio, an SDR can dynamically change multiple
modulation parameters and techniques including waveform, narrow- or wide-band
operation, modulation adaptation strategy, communication security functions, and
other transmission qualities or strategies. This feature gives SDRs the ability to
dynamically adapt to a varying wireless environment. Current SDRs can change
their modulation type entirely. For example, they can move from quadrature
phase-shift keying (QPSK) to asymmetric phase-shift keying (APSK). Researchers
have also defined an ultimate software radio (USR), which is a theoretical limit for
SDR. USR is capable of supporting a wide range of frequencies, modulation type,
and so on, without RF front-end or even an antenna.

As introduced above, SDR platforms make an excellent implementation system
for CRs. Researchers and industry are working to develop SDRs with capabilities
more closely equivalent to the USR. Ultimately, as research and development efforts
enable SDR capabilities to approach those of a USR, the contributions of this
dissertation will be of even greater relevance and value.

1.3 Cognitive Radios

Using techniques including control theory and adaptive processes, signal process-
ing, and game-theoretic approaches, Haykin [2005] introduced the detailed concept
of CR in 2005. With cognitive-radio network (CRN) technology, wireless devices
have the capability to dynamically adapt their performance and spectrum access strategies, based on feedback regarding the dynamic wireless channel. The feedback information creates a perception–action cycle. Haykin introduced four major tasks for the operation of CRs based on the perception–action cycle:

1. receiver performs a radio analysis of the environment;
2. receiver provides the transmitter with necessary feedback;
3. transmitter adjusts the transmission scheme based on the information provided by the receiver; and
4. transmitter performs power control and spectrum management.

1.3.1 Definition

A radio can be regarded as a CR if it has the following features in order to communicate effectively and more efficiently in terms of bandwidth used to send a fixed amount of data:

1. ability to understand the physical environment;
2. capable of autonomous operation, meaning a CR can use machine-learning techniques to perform its goals;
3. ability to calculate the trade-offs associated with its decisions and consider them in its decision making; and
4. ability to use past strategies to better understand the impact of its new strategies (e.g., using game-theoretic techniques).

These features will allow CRs to overcome the current problems facing wireless communications such as increasing demand and requirements for security. Based on the features that a radio device needs to possess to become “cognitive”, we can define a CR as [Haykin, 2005]:

**Definition 1.2.** An intelligent and reactive wireless communication system that is aware of its surrounding environment (i.e., outside world), and uses the methodology of understanding-by-building to learn from the environment and adapt its
internal states to statistical variations in the incoming RF stimuli by making corresponding changes in certain operating parameters (e.g., transmit power, carrier frequency, and modulation strategy) in real time, with two primary objectives in mind:

• **highly reliable communications whenever and wherever needed**, and

• **efficient utilization of the radio spectrum**.

Definitions of CRs vary among researchers as there is not yet a well established standard. As presented in Section 1.2, the goal is to move in the direction of a perfect “cognitive” transceiver. Every wireless communication system with cognitive features can be considered as a CR. However, one can summarize the most common aspects of CR definitions as the following:

• **Observation**: a CR can access feedback information whether it is sent by another CR or is collected by itself (using novel feedback information is presented in Chapter 3);

• **Intelligence**: a CR can use its observation to develop a “better” transmission strategy (we use this feature extensively in Chapter 4); and

• **Adaptability**: a CR can perform consistently in dynamically changing environments.

Using these features allows us to develop a strategy to gather information regarding a dynamic environment in Chapter 3. By employing game-theoretic techniques, we introduce a novel transmission strategy in Chapter 4 to maximize the available spectrum usage. Combining the feedback gathering and dynamic transmission strategy make a novel spectrum access algorithm possible, which is presented in Chapter 5.

### 1.4 Motivation

In this dissertation, we propose several techniques that make CRs more “informed”. This goal is achieved by enhancing the observation, intelligence, and adaptability aspects of the CRs.
We study the use of information obtained via data mining of datasets that are correlated or uncorrelated with wireless channel information, as opposed to only the use of wireless channel information itself [Qiu and Wicks, 2014]. This step will improve CR observation. For example, in Chapter 3 we investigate additional information that can lead to better data traffic prediction, which can be used to enhance the performance of CRNs. Currently, an extensive understanding of the wireless channel capacity based on the wireless channel information is the only source of information used for determining the best transmission plan, modulation, and data rate. We argue there are other sources of data/information available that can help predict the near and far future environment of the network. Using this information helps inform the decisions that the CR will need to make.

Traditional game strategy for CRNs generally only include static non-cooperative players. To improve the CR intelligence and adaptability, we propose in Chapter 4 that more efficient CRNs can be constructed by modeling more realistic dynamic CR players with various goals that lead to different strategies. Our assessment shows that CRs using our proposed algorithms will perform differently than a regular (non-CR) wireless radio. This study is crucial for designing a medium access control (MAC) protocol for competing CRs.

After studying the competition between CRs, we introduce a novel MAC protocol, addressing adaptability in Chapter 5. Using a dynamic auction, we force the CRs to cooperatively share a limited resource in a dynamic environment. This dynamic auction is decentralized and can be managed by any CR. One of the main advantages of this approach is the self-organizing capability for a CRN.

We are concerned about the security of the CRN and the overhead cost associated with it. In Chapter 6, we propose a novel security protocol to address the vulnerability associated with CRNs. These vulnerabilities are due to the fact that each CR can access and receive the signals associated with other CRs. We use the concept of a distributed blockchain the best known example of which is Bitcoin, to manage and secure the MAC protocol introduced in previous chapters.
1.5 Contributions

In this dissertation, the concept of an “informed cognitive radio” is introduced to improve the performance of CRs by improving their understanding of their environment beyond the dynamic wireless environment. These improvements are made possible by employing various techniques, including data mining and game theory. This CR is informed because it is aware of its environment to a degree that outperforms the CRs introduced in literature in terms of wireless communication metrics. This CR also uses dynamic algorithms and protocols to react faster and more efficiently to changes in the wireless environment. This informed CR uses feedback data regarding the environment that is not limited to the wireless channel information.

In Chapter 3, we enhance the informed CR’s understanding of the environment through the utilization of crowd-sourced social media information. That is, we extract relevant information about the wireless channel condition and current and future user demands through sources of information that are not currently considered for this purpose. This informed CR is assumed to be self-driven to use a cooperative or non-cooperative strategy to access and share a limited resource. As a result, we propose a hybrid game-theoretic strategy to study this informed CRs use of an M/D/1 queue to assess their performance (Chapter 4).

With the improved feedback gathering and strategy, we build a new spectrum access auction mechanism in Chapter 5 to fully utilize wireless spectrum by the proposed informed CR. This auction uses those two improved features fully and makes the spectrum sharing more efficient and robust against most intruders. In the simulation, we use spectrum as a limited resource under investigation, but the same approach can be used for other important resources in CRNs, such as power consumption.

Security is also a huge issue in CRNs. In this work, we propose using a distributed blockchain database to make spectrum sharing robust and provide a necessary virtual currency we call “Specoins” for the proposed auction algorithm. The CRs use a blockchain verification protocol as a method for enabling and securing spectrum sharing in CRNs. The spectrum-sharing mechanism is used as a MAC protocol for accessing wireless bandwidth among competing CRs. We introduce a
virtual currency for payment to access the spectrum. The blockchain protocol facilitates the transactions between primary and secondary CR users. We show that the blockchain serves as a distributed database that is visible by all participating parties and any node can volunteer to update the blockchain.

For validating the result, we show the improvement of the proposed algorithms compared to the conventional ALOHA medium access protocol in terms of spectrum usage. This difference is investigated using small-scale fading variation in the wireless channel to compare the performance of our secure method with the conventional medium access used in wireless communications. The secure blockchain verification protocol is not only secure but also outperforms the conventional system in moderate cases of small-scale fading. In case of severe small-scale fading the blockchain protocol will outperform the conventional system if multipath diversity is not used.

The concept map for this dissertation is shown in Figure 1.1. First, we consider frequency spectrum as a limited and underutilized resource that needs to be shared between competitive CRs. Then, using SDR as a solution candidate, we introduce and investigate two algorithms. First by categorizing CRs without spectrum rights (secondary users) as cooperative and non-cooperative (normal and greedy, respectively), we propose a hybrid player (vigilante) to stop non-cooperative CRs. Second, using the primary user as leader in Stackelberg game, we propose a novel game strategy to share a limited spectrum. The security of spectrum sharing is ensured by a distributed blockchain database.

1.6 Outline of the Dissertation

In Chapter 2, we introduce and summarize the system model for this dissertation. We also present the main results of some related work, identify the gaps in the literature, and overview their methods.

Chapter 3 introduces and provides analysis of additional relevant data sources (among them, social media, like Twitter) used as feedback for CRNs. We build predictive algorithms for the network load of the wireless network that increase the network throughput.

In Chapter 4, we introduce the spectrum sharing cooperation strategy for CRN
and then evaluate it by modeling the spectrum and users as an M/D/1 queue. Our goal is to encourage the CR players to cooperate. We have focused on the strategy that, despite the desire to maximize their individual utilities, the CR players find it beneficial to cooperate. We have formulated a Stackelberg game in which the primary license holder and secondary user are leader and follower, respectively, and studied how the leader can influence the follower’s decision of participating in the game by varying the cost function.

Chapter 5 combines the novel feedback algorithm with the spectrum sharing strategy by a new auction mechanism to address the spectrum underutilization. We proposed a decentralized auction algorithm as a multiple access method for CRs to share available unused spectrum. One of the main advantages of this algorithm is that it can be used to access a free licensed band without the need for constant spectrum sensing.

Chapter 6 presents our secure proposal for CRNs. We proposed using blockchain as a decentralized database to verify spectrum sharing between CRs. We show that this secure and decentralized medium access control protocol (MAC) can outperform the current conventional system in both moderate and severe fading conditions to share available unused spectrum.

Chapter 7 presents our conclusions and outlines some directions for future work on this project.
Figure 1.1. The concept map used in this work to make a secure and informed CRNs using learning and game-theoretic techniques
2 Background

2.1 Scarce Spectrum Problem

Demand is growing rapidly for wireless communication technologies, such as wireless data links, mobile telephones, and wireless medical devices. This demand places a significant burden on the limited wireless spectrum. One method to mitigate this lack of spectrum is to employ CR techniques in these wireless technologies. Prior research has explored CR aspects, such as spectrum access [Jana et al., 2013], truthful spectrum auctions [Sodagari et al., 2010a;b], and dynamic spectrum rental [Fatemieh et al., 2010].

The frequency allocation in the United States is shown in Figure 2.1. The process of regulating the use of these frequency bands is called spectrum management. Radio spectrum that can be used for wireless communications ranges from 3 kHz to 300 GHz. As a result of signal interference, exclusive licensing has been imposed to protect the spectrum licenser holders. As can be seen from Figure 2.1, there are four major spectrum users:

- wireless broadcasting for TV and radio;
- public government and services such as defense, police, and transportation;
- scientific and medical services; and
- public usage such as data and phone services.
Spectral and temporal analysis of the radio spectrum reveals three broad categories of frequency band usage [Haykin, 2005]:

- frequency bands that are predominantly unoccupied;
- frequency bands that are moderately occupied; and
- frequency bands that are heavily occupied.

Note that a channel may be heavily occupied at one period in time, but not at another. CR offers opportunistic usage of the frequency spectrum if permitted by primary users who currently “own” that slice of spectrum [Yucek and Arslan, 2009]. This process is called dynamic spectrum access, which may rely on algorithms and concepts found in game theory and network information theory.
2.2 Cognitive Radio Background

The inefficient usage of the limited frequency spectrum makes it difficult to meet the increasing demand for wireless communication capacity [Akyildiz et al., 2004; Giannoulis et al., 2013; Wang et al., 2010]. CR has been introduced as a solution to this problem. CR is defined as “a radio that can change its transmitter parameters based on interaction with the environment in which it operates” [FCC 2003]. The term “cognitive radio” was first introduced by Mitola in 1999 [Mitola and Maguire, 1999]. CR is an evolved version of software-defined radio that can reconfigure itself such that it can adapt its waveform parameters to the environment to meet higher-layer user demands for quality of service (e.g., voice over IP, voice over ZigBee [Zhang et al., 2015], video). CR implementations fall between two extremes. At one end is the “Mitola radio”, a radio that collects information about all observable wireless information. As such, it is a theoretical construct that cannot be implemented in practice, but provides an ideal to aim for in CR research. At the other end is what can be practically implemented, which may be a spectrum-sensing CR with information about only the frequency spectrum [Akyildiz et al., 2006]. In our work, we seek to move towards the Mitola radio ideal by employing more and varied information in our control loop, such that the CR can make more informed decisions. This concept is explored in Chapter 3.

One can define the cognitive ability of a radio as capturing and gathering information regarding the state of the environment, processing this information, and then determining corrective action based on its findings. This cognitive process is not limited to monitoring the power level in a specific frequency band, but can also include the spatial and temporal variations in the radio environment due to the mobility and time dependency of most wireless devices. Based on the users’ demands, these devices need to access a free and/or unused spectrum band at different times and/or locations [Ferreira et al., 2014]. Reconfigurability empowers the radio to dynamically adapt to a changing radio environment [Akyildiz et al., 2006]. This means that the CR will adjust to communicate in an appropriate frequency band and with a suitable waveform (i.e., modulation type).

A dynamic system is defined to be cognitive if it employs the perception–action cycle and has memory, attention, and intelligence [Haykin, 2012]. In the
perception–action cycle depicted in Figure 2.2, a perceptor gathers measurements and sends them as feedback information to an actuator that uses this to control the perceptor via the environment. Memory is needed since the environment is nonstationary. The actuator prioritizes the allocation of limited resources, and feedback enables the presence of intelligence in this system by providing the perception of the environment to the actuator.

Three fundamental CR tasks based on the perception–action cycle are introduced in Haykin [2005]. For the receiver, information gathering and analysis must be performed to determine the condition of the dynamic radio environment [Ferreira et al., 2017]. For the transmitter, power budgeting and dynamic spectrum access based on information regarding the presence of the primary users must be calculated and executed. Finally, there must be a feedback channel between the transmitter and receiver regarding information about the radio environment. A CR can more effectively adapt to the radio environment if it can cooperate with other CRs as introduced in Jondral [2005].

A CRN seeks to serve the individual communication requirements of multiple primary and secondary users. In doing so, three practical challenges arise introduced in Haykin [2012]. First, the vacancies in spectrum come and go due to temporary usage of the spectrum by a licensed primary user. Finding these vacan-
cies can be accomplished more efficiently in a cooperative manner by the secondary users in a CRN. Second, for each CR, information gathered by the receiver components must be processed and sent to the transmitter side. This will induce a delay in the feedback channel. Third, the security of the CRN can be compromised by malicious users in different locations and time frames. These practical issues need to be solved; in addition, solutions that use game theory to promote a cooperative strategy between the secondary users are also necessary.

### 2.3 Game-Theoretic Background

Game theory has played an important role in developing efficient algorithms for sharing a common spectrum between secondary users [Del Re et al., 2012]. Game theory is the study of cooperation and conflict between cognitive decision-makers, which, in our context, are represented by CRs. Spectrum sharing via game theory occurs in both licensed and unlicensed bands [Baldini et al., 2013; Forde and Doyle, 2013]. CRNs can be used for spectrum sharing both in unlicensed and licensed bands by using methods that can combine unused frequency bands and share them dynamically [Kurve et al., 2013a; Tootaghaj et al., 2015; Farhat et al., 2016]. Heterogeneous wireless systems are an example of unlicensed-band devices that rely on games for spectrum sharing [Felegyhazi and Hubaux, 2006]. Cellular operators that use WAN-WiFi are prime candidates for using games to share spectrum in licensed bands. In Chapter 4, we focus on spectrum sharing in licensed frequency bands with primary users as license holders.

Game theory also plays an important role in deciding how a user must react to an event played by other users in order to maximize its utility (a measure of preferences over some set of strategies) [Attar et al., 2009; Suris et al., 2007]. This decision is made by measuring the user’s throughput (packets successfully sent over some specified time frame) and waiting time as metrics for each player’s measured cost and gain.

Secondary users can be classified into cooperative and greedy players [Kotobi and Bilén, 2015]. Greedy players are not cooperative in the sense that their only objective is to maximize their throughput. In Kotobi and Bilén [2015], we proposed an “altruistic” user that is cooperative until it senses the presence of a
greedy player via observation (for instance, channel usage) similar to Sani and Vosoughi [2015a]. In this situation, the altruistic player will turn into a non-cooperative player to punish the greedy players by jamming the wireless channel. This new altruistic player would subsequently back off when the greedy players act cooperatively with the other players. Adaptive greedy and altruistic players in spectrum-sharing games require an iterative method to study and predict their response. In Chapter 4, we propose a new equilibrium concept, beyond that of Nash theory, that includes the strategy of a dynamically-changing greedy player.

In the literature, spectrum allocation has been modeled with various pricing schemes as a non-cooperative game, with each CR acting as a player. Wang et al. [2008] and Kotobi et al. [2016] propose price-based spectrum management systems using a water-filling algorithm. Their algorithms employ a distributed pricing procedure that lead to improved Nash equilibrium solutions compared to iterative water filling [Yu, 2002]. However, in Chapter 4, our proposed pricing scheme to be used in the utility function, based on primary users only, is intuitively more realistic since the primary users are the license holders. A game-theoretic model is presented in Niyato and Hossain [2008] that achieves the optimal pricing for spectrum sharing based on competition between multiple primary users to give spectrum access to secondary users. However, in Chapter 4, we assume a generalized distributed system that uses a single pricing model for each primary user. Yet, to address the secondary users’ competition to maximize their spectrum access, we offer different pricing functions based on the traffic on the network and other variables such as available spectrum.

An extensive survey presented in Gavrilovska et al. [2014] reviews the state-of-the-art and advances in CR medium-access-control protocols. A stochastic geometry framework that captures the performance of an asynchronous ALOHA network in which a subset of nodes operates in full-duplex mode is presented in Munari and Petri [2015]. Compared to [Kotobi, 2011; Lo and Akyildiz, 2012], in which an altruistic player can regain access to shared spectrum in an asynchronous ALOHA network, Munari and Petri [2015] only allow licensed primary users to access the network.
2.4 Multiple-Access Scheme Background

As mentioned, frequency bands that are suitable for wireless communication can be bifurcated into licensed and unlicensed bands. In both cases, if secondary users could access unused spectrum, this would lead to higher overall usage and higher overall throughput. Various multiple spectrum-access schemes have been proposed for use in unlicensed frequency bands. These schemes often require better knowledge of the wireless channel when compared to operating as license holders in licensed bands. For example, sensing the wireless channel to avoid collision with other primary and/or secondary users is an important difference compared to conventional multiple access schemes. Such sensing schemes impose computational delay and power limitations on secondary users. To address these limitations, multiple access schemes based on reduced-sensing functions may be employed. For example, in Li et al. [2010] restricted- and minimum-sensing schemes are proposed and modeled by combining a multichannel carrier-sense multiple-access algorithm and a distributed-learning algorithm. The sensing considerably increases delay and power usage of the CRs, which are usually sensitive to those properties.

Addressing these power and bandwidth restrictions, in Chapter 5 we introduce a scheme for a self-organizing auction to access the spectrum by defining the secondary users as auctioneer and bidders, and then assess our method. The significance of our scheme is that it is an orthogonal medium access method that does not require a continuous sensing scheme (only an initial sense to determine the presence of primary users) and, hence, reduces delay and decreases power usage.

In a licensed spectrum band, a primary license holder can lease any unused portions to secondary users via, for instance, a dynamic spectrum-sharing scenario. By omitting the role of the primary user as a leaser, one can assume the algorithms used for spectrum assignment in a licensed band can be also applied to an unlicensed band with some modifications. One method to perform this allocation is via an auction, in which a spectrum manager is responsible for assigning spectrum access among secondary users. For example, a sequential auction for sharing wireless bandwidth is discussed in Bae et al. [2008]. The proposed auctions are usually time-consuming and they require extensive processing time. These auctions may not guarantee “fair” access for all secondary users. Additionally, because CRs
generally do not possess significant processing capabilities, we show our auction only requires a basic processing capability, which will also provide more equal access time for all bidders. The other important improvement in our algorithm is the processing time required to access the spectrum. To better utilize spectrum, CRs need to access allocated spectrum quickly before the primary user is online again. Our auction scheme can assign spectrum in a time frame on the order of microseconds.

2.5 Blockchain Background

2.5.1 Distributed Database

Blockchains are distributed databases that can be securely and iteratively updated. Although the concept has been around since the early 1990s [Haber and Stornetta, 1991], only recently have applications employing blockchain been developed, primarily to facilitate secure, private financial transactions and, specifically, as Bitcoin, which has made it a well-known technology. In Chapter 6 we propose to use blockchain technology to improve the medium access protocol and security of CRs desiring access to unused licensed spectrum.

Blockchains are used to improve the recording and sharing of financial transaction information, which can be seen in terms of increased transaction speed, decreased procedural cost, fewer transaction errors, and increased general security, as well as having a decentralized approach [Ron and Shamir, 2013]. This decentralized method removes a central point of system failure and cyber attack. For example, Bitcoin is defined by the transactions that are recorded in a blockchain, which acts as a universal spreadsheet. Using the power of peer-to-peer calculations, a network can verify and approve each transaction and save them in this distributed database. The main idea behind blockchain usage in virtual financial transactions is that the wallet of each user is not saved centrally, rather, it is secured by storing the record of transactions between users in a blockchain.
2.5.2 Security for VANETs

Security in vehicular ad hoc networks (VANETs) is a major concern since malicious users may try to attack the network. Infrastructure-based VANETs provide new private keys in real time to ensure security; however, this approach requires infrastructure and provides a central point of attack for malicious users. One proposal is to introduce certification authorities (CAs) for the VANET, with a CA responsible for each cell. The CAs provide certificates for CRs inside each cell and “foreigner” certificates for CRs associated with another cell when they enter its cell [Lee et al., 2009]. This approach not only requires infrastructure to be implemented for each cell, but also requires a protocol for defense against a central-point attacks. Other drawbacks associated with this protocol are greater calculation complexity and longer packet lengths, which increases overhead in VANETs.

In contemporary advanced vehicles, there are multiple sensors, control units, and actuators that generate data that need to be sent to the cloud over wireless links, either directly or through a vehicle’s network gateway. If these elements are considered to be CRs, they may access shared spectrum to exchange their vital information. The shared spectrum is easy to access by a malicious attacker and a secure medium access communication protocol is needed to prevent attacks. To analyze VANET security protocols, we use the following metrics: signature methods, security and complexity of hash functions, transfer mechanisms, and secure multiparty functions [Lee et al., 2009]. In addition, VANETs are vulnerable to intruders in the network who may attack and take control of CAs. In this work, the trust between the cognitive radios in a VANET is obtained using a trusted and distributed database.

2.5.3 Secure Auctions

Auction mechanisms have been proposed as multiple access protocols for secondary users to access unused spectrum resources. These auctions can be separated into two categories. In a single-round auction, the available spectrum is awarded to the “best” bid provided by a secondary user [Kotobi et al., 2016; Li et al., 2010]. In a repeated auction, secondary users learn about the environment as well as their competitors’ strategies in each round, which makes the medium access protocol
There are a number of major drawbacks to the repeated-auction approach. First, a bidder must find an optimal strategy to maximize its long-term utility function and, as such, its complexity can grow exponentially \cite{Bae et al., 2008; Kurve et al., 2013b}. Some auctions will require a lot of computational power to converge to an optimal solution or a Nash equilibrium, but the required computational power is generally not feasible for ordinary CRs. Second, the computational delay is usually longer than the timescale of small-scale fading assumed for a typical wireless channel \cite{Zhao et al., 2008; Kotobi, 2011}. This drawback is due to the fact that a CR starts calculating its bid under a specific wireless channel condition and uses that condition as its feedback information, but when the repeated auction concludes, the wireless channel has changed to a new state that may no longer reflect an optimal solution.

As mentioned, security is another major concern for medium access protocols. Nearly all proposed medium access protocols for CRs lack the verification and validation scheme necessary to ensure the security of the network, \cite{Kotobi and Bilén, 2015; Kotobi et al., 2016}. Generally, proposed mechanisms have not included authentication methods for validating transactions, and those that have, have proposed centralized validation mechanisms. However, having a decentralized validation algorithm enables a medium access protocol to be more accessible, and the implementation will be easier since there is no need for a central-authority node. Lacking a centralized node for validating a transaction and monitoring the spectrum access makes the overall system robust against single-point failures.
Chapter 3

Data-Throughput Enhancement Using Data Mining–Informed Cognitive Radio

3.1 Chapter Introduction

In this chapter, we propose the data mining–informed cognitive radio, which uses non-traditional data sources and data-mining techniques for decision making and improving the performance of a wireless network. To date, the application of information other than wireless channel data in CRs has not been significantly studied. We use a novel dataset (Twitter traffic) as an indicator of network load in a wireless channel. Using this dataset, we present and test a series of predictive algorithms that show an improvement in wireless channel utilization over traditional collision-detection algorithms. Our results demonstrate the viability of using these novel datasets to inform and create more efficient CRNs.

3.1.1 Big Data Framework

As introduced in Chapter 2, cognitive radio is being explored to address the problem of spectrum scarcity. The medium access control (MAC) protocol for any realizable system allows wireless users to use the frequency channels based on the

1The research presented in this chapter has been published in Kotobi et al. [2015].
current state of the network. For example, in *Hu et al.* [2014], various MAC protocols are investigated for use in CR based on different methods for users to start communication. In this chapter, the usage of data-mining techniques in MAC protocols for CR is studied.

The term “big data”, often used when referring to data mining, extends beyond the *volume* of data acquired to include also the *velocity* (how fast the data are being transmitted), the *variety* (the different data types included), *veracity* (the accuracy or truthfulness of the data), and *value* (the tangible benefits that the data provide). Researchers have demonstrated that large-scale social media networks exhibit the five Vs of “big data” and can serve as a viable source of real-time knowledge extraction though data mining [*Bodnar et al.*, 2014; *Yin et al.*, 2014].

Using techniques, such as data mining, and including them in the perception–action cycle (Figure 2.2) of a CR is an emerging concept. Recently, a vision was presented for the use of “big data” techniques to enhance the performance of a CRN [*Qiu and Wicks*, 2014]. The big data vision is foundational for illustrating cognitive networked sensing, cognitive radar, smart grid, and CRNs. The data employed in *Qiu and Wicks* [2014], however, are only those concerning the wireless channel, which are then employed to enhance the decision-making process regarding the usage of available wireless channels. Hence, the application of data sources other than wireless channel data in CR has not been significantly studied. These new information sets can be used to predict the traffic, channel condition, and other conditions of a wireless network. As an example, we demonstrate herein that data extracted from a social media network by means of data mining can inform a CR.

As discussed before, CRs work by collecting information about a statistically varying environment and then applying methods and algorithms that react to this collected information to maximize certain performance goals. In this work, we employ data mining and game-theoretic techniques that employ new environmental data. Specifically, we investigate a new CR scheme that uses crowd-sourced social media information obtained through data mining of a large-scale social media network. We employ game-theoretic algorithms for adaptation and reaction to a varying radio environment. The performance improvements from these adaptations help demonstrate the merit of what we call the “data mining–informed cognitive radio”.
3.1.2 Proposed Cognitive Radio

The research framework that we employ to develop more informed CRNs consists of two thrusts. First, we use sources of information other than wireless channel information and collect relevant information using data-mining techniques to inform CRNs. The main goal of this thrust is to understand these novel sources of information and to find new methods to collect and analyze data that are not directly correlated to the wireless channel information, but which are relevant to channel usage. The second thrust employs appropriate game-theoretic techniques to better utilize the spectrum and to perform resource sharing between the secondary wireless users in a wireless network. In this chapter, we introduce smarter CR nodes and networks by way of improved algorithms and it is shown that, based on crowd-sourced information, one can increase data transmission throughput.

Wireless channel information is currently the primary feedback information source used in CR. This information helps the various radio network nodes to adapt their waveforms, e.g., frequency, data transmission rate, modulation, etc. If the channel is used by other primary or secondary users, the user can detect the channel load and back off. However, there are other sources of information that may be helpful in predicting the near-term or future conditions of a wireless channel. For example, information about nearby weather conditions or forecasting a rainy day will help the coordinator and/or secondary users to use more robust modulations compared to more data-rate-efficient modulations, which could be used when a sunny day is predicted. Another example is the acquisition of information about an emergency situation, such as a fire at a school, by data mining of social media and other sources. In this case, the moderator or secondary users must prioritize data transmission related to the emergency event over their own data. Gathering these new data will add additional information for better decision making and, thus, improve the performance of a wireless network.

3.1.3 Chapter Organization

The reminder of this chapter is organized as follows. In Section 3.2, we consider general CR concepts, investigate their current limitations and introduce methods for improvement in performance regarding spectrum usage. In Section 3.3, the
proposed algorithms to improve channel traffic allocation are introduced. Simulation results are presented in Section 3.4. In Section 3.6, we summarize our results and present conclusions.

3.2 Problem Definition

3.2.1 Big Data Framework for Wireless Communication

As mentioned in Section 3.1.1, wireless channel information is not the only relevant information that can be considered for a CR or by a CRN administrator. In this section, an example of a data source that is not directly related to the wireless channel information is presented, and several algorithms to use these data are presented with the goal of improving the throughput of current CRNs.

3.2.2 Problem Definition

With the goal of enhancing the performance of a CRN, there has been limited study of the use of information obtained via data mining of datasets that are correlated or uncorrelated with wireless channel information, only the use of wireless channel information itself [Qiu and Wicks, 2014]. We posit, however, that additional information can lead to data traffic prediction, which can be used to enhance the performance of a CR. Better understanding of the wireless channel capacity based on the wireless channel information is critical for finding the best transmission plan, modulation, and rate, although one can argue there are other sources of data available that can help predict the near or far future environment of the network. For example, one can predict data traffic by using information gathered on the daily schedule of events in a restaurant. A popular concert in a city center can cause collision and denial of service in wireless mobile phone communication. Using this information and allocating more frequency spectrum to use in those cells in which the event is taking place will help avoid congestion in the network.

The emergence of low-cost mobile communication devices and digital storage technologies is enabling the rapid creation and dissemination of information on a global scale. Digital information, ranging from user-generated data (e.g., captured through social media, such as Twitter, Facebook, Google +, etc.), to data
generated through industry and government efforts, is establishing a new dimension of social-driven knowledge discovery. These data, fed through the appropriate cognitive engines, might inform CR beyond what radio parameters alone can do and, in the process, expand bandwidth. The challenge facing us is not the lack of digital information, but rather the synthesis of large-scale, multi-domain data and their transformation into actionable information by CR systems. Figure 3.1 shows how data may come from CRs and/or other sources. Some of the CRs may be collocated in a geographical region (e.g., coffee shop, mall, concert venue, etc.) that also have data associated with them, as well as data generated by the CRs in that region, all of which may be mined [Bilén et al., 2014].

3.2.3 Wireless Channel Modeling

Knowledge of wireless channel traffic is one of the parameters that can be used to improve the performance of the CRN. Conventionally, this might be modeled by channel signal-to-noise ratio (SNR). If the SNR in the receiver is higher than a specific threshold, one can assume that the wireless channel is occupied. However, channel occupying level might also be modeled by the number of Tweets or Facebook posts per unit time in a specific location (a more nuanced analysis might also include other aspects of the social media data obtained through the five Vs discussed in Section 3.1.1). We demonstrate here a collision-free data transmission scheme that mimics the channel capacity by using the current and past channel traffic and the channel information, which will result in a close-to-optimum throughput. For this demonstration, we use the dataset of received signal strength (RSS) measurements for WiFi signals collected at the University of Colorado as our wireless channel information (obtained from CRAWDAD: Community Resource for Archiving Wireless Data At Dartmouth at http://crawdad.cs.dartmouth.edu/). We use the number of Tweets (actual data for a specific location in New York City) as an indicator of demand for data transmission over the wireless network. The Tweets used in the simulations have geolocation tags, which are used to extract the data traffic for a specific location.

To simulate a wireless network environment, our algorithm uses wireless channel characteristics measured for a particular channel (measured at the University of
Figure 3.1. The proposed data mining–informed cognitive radio (DMICR) system utilizes other data sources in addition to the usual parameters employed in cognitive radio networks [Bilén et al., 2014].

Colorado). We use Rayleigh fading to model the multipath fading of the wireless channels. We then impose a set of unrelated network loads (here, in the form of Twitter data from the New York City area) to measure the effectiveness of the algorithm. By employing uncorrelated data, we avoid the scenario in which network traffic for a wireless network strongly matches its signal strength, i.e., a poor-quality wireless signal discourages its use. In this simulation setup, we use Twitter traffic (more specifically, the publication of Tweets as opposed to reading of Twitter feeds) as an indicator of the actual network load. Various studies (e.g., [Li et al., 2014] and [Das et al., 2014]) show that a certain fraction of a wireless network load is Twitter traffic. Although that fraction may depend on the time and location, for this study, we assume that it is a fixed fraction.

The actual wireless channel capacity depends on many factors, including the coding scheme used in the physical layer, but here, we use the Shannon capacity to correlate the RSS measurements and the channel’s available capacity. Based on
Figure 3.2. Variation in calculated point-to-point communication Shannon capacity of a WiFi network based on the received signal strength measurements as function of the signal-to-noise ratio with respect to time.

RSS measurements, the channel Shannon capacity can be seen in Figure 3.2 for 4,000 min with one-minute resolution. For the demonstration of the algorithms proposed, we plot only the first 120 min, such that the channel variations can be observed. The channel usage and capacity are normalized by the maximum channel capacity, and their variations over time are plotted in Figure 3.3. As shown, the demand for usage can be higher than the channel capacity during some time periods, which results in collisions in the current medium-access algorithms. During other time slots, the wireless channel is underutilized. In order to achieve a closer-to-optimum throughput, the radio network should delay transmitting data packets in an over-utilized channel until the wireless channel is underutilized. This requires that the layers higher than the physical layer need to have understanding of the physical layer for wireless communication.
Figure 3.3. Comparison between a given demand for data transmission as a function of the number of the Tweets and calculated point-to-point communication Shannon capacity of a WiFi network based on the received signal strength measurements as function of the signal-to-noise ratio with respect to time.

\[
\text{for each } t \in \{1, 2, ..., M\} \text{ Find all capacity in } \{1, 2, ..., t\} \text{ do}
\]

\[
\text{if } \text{Capacity}(t) < \text{Demand}(t) \text{ then}
\]

\[
\text{Data}(t) = 0
\]

\[
\text{end}
\]

\[
\text{end}
\]

Algorithm 1: Algorithm for data throughput with collisions.

3.3 Proposed Algorithms

3.3.1 Data Transmission Algorithms

In the conventional implementation of channel access, data packets are dropped in the case of a collision, which results in a throughput far from the channel capacity, as shown in Figure 3.4. This process is presented in Algorithm 1.

If we categorize data packets into two data types, one for real-time applications, like voice over IP or video broadcasting, and the other as non-real-time data, like
Figure 3.4. Comparison between normalized channel usage with the dropping of data packets in the event of collision and the calculated point-to-point communication Shannon capacity of a wireless channel with respect to time.

downloading an email file attachment, then we can choose to transmit only the real-time data types when we predict that the collisions will occur, which is based on the current change in the data usage and the current channel capacity. The algorithm for this is presented in Algorithm 2. The implementation of this method is depicted in Figure 3.5, wherein it can be seen that the throughput is increased compared to that of the former method. The throughput is the integral of usage over time.
Figure 3.5. Comparison between normalized channel usage with using the dropping of non-real-time data packets in the event of collision method and calculated point-to-point communication Shannon capacity with respect to time.

For each $t$ in $\{1, 2, ..., M\}$ do

Find all capacity in $\{1, 2, ..., t\}$

if $\text{Capacity}(t) < \text{Demand}(t)$ then

Data$(t) = \text{Data}_{\text{Real}}$

end

if $\text{Capacity}(t) < \text{Data}(t)$ then

Data$(t) = \text{Data}_{\text{Real}}$

end

end

Algorithm 2: Algorithm for prioritizing real-time data.

To improve the throughput of the CRN, we can shape the transmission of the non-real-time packets based on the prediction of the channel capacity. Our prediction method uses the assumption that the channel capacity will change at the rate at which it was changing one or more time slots previously. In the case
that the prediction is not true, the non-real-time data will be lost due to a collision according to Algorithm 3. The results of this proposed method are shown in Figure 3.6 when using the last three time slots, i.e., $N = 3$. The throughput is significantly higher than that with Algorithm 2, shown in Figure 3.5.

### 3.3.2 Incorporating Network Burstiness

Traditional Ethernet traffic exhibits a long-tailed probability distribution rather than a Poisson distribution, because of its self-similarity. Wireless networks have similarly shown this property [Basgeet et al., 2002]. This means that predicting Ethernet or wireless traffic is difficult: the self-similar nature of the traffic indicates that there is no defining length characteristic of network traffic bursts. This self-similarity increases as the number of network traffic sources increases [Leland et al., 1993].

Incorporating a linear weighting element of “burstiness” to our traffic predic-
tion algorithm can help ameliorate issues with the Poisson distribution model. Based on the time fidelity of the data, an interval of prior traffic can be analyzed for a proportional burst factor. This factor can then be used to linearly weight the prediction of available capacity. There exists a wide variety of traffic prediction techniques that incorporate the self-similar behavior of network traffic: neural networks, auto-regressive integrated moving average models, and alpha-stable models \cite{Zhou et al., 2005; Sang and Li, 2002; Xiaohu et al., 2004}. These models are a trade off between traffic prediction accuracy and the complexity of implementation, as well as the cost of performing such analysis. We choose a simple linear weighting to demonstrate the utility of incorporating self-similarity in network traffic prediction for many-user systems.

To analyze the burst factor, the number, size, and length of bursts are computed by the method of \textit{Krzanowski} \cite{2006} and given in a form modified for $N = 3$ in Algorithm 4. A burst is defined as a period during which the traffic exceeds the average traffic of the network (over some tolerance factor of time). Once these burst characteristics are calculated, the network traffic can be characterized as either bursty or non-bursty (i.e., steady). The analysis of these network traffic data show them to be primarily bursty with a low average load.

Having determined periods of network traffic that lie within bursts, the algorithm can either (1) send additional traffic during burst periods or (2) send additional traffic during steady, non-burst periods. We now develop a modified version of Algorithm 3 with $N = 3$ to include a weighting factor proportionate to
burst or steady periods.

for each $t$ in \{1, 2, ..., $M$\} do

Find all capacity in \{1, 2, ..., $t$\} if Capacity($t$) < Demand($t$) then

Data($t$) = Data$_{\text{Real}}$ + Capacity($t - 1$) − Demand($t - 1$)
+ Capacity($t - 2$) − Demand($t - 2$) + ... +
Capacity($t - N$) − Demand($t - N$)

end

if Capacity($t$) < Data($t$) then

Data($t$) = Data$_{\text{Real}}$

end

end

Algorithm 3: Algorithm for predicting channel condition and demand for $N^*$ previous time slots.

* One can use $N$ time intervals to find the largest capacity for data transmission.

for each $t$ in \{1, 2, ..., $M$\} do

Find all capacity in \{1, 2, ..., $t$\} if Data($t$) > AverageData then

burstStart = $t$ burstData = Data($t$)

end

for each $tPrime$ in \{$t$, $t + 1$, $t + 2$, ..., $M$\} do

if Data($tPrime$) < AverageData then

if Data($tPrime - t$) > ToleranceFactor then

burstEnd = $tPrime - 1$

burstsPerTime[$t$] = Burst(burstStart, burstEnd, burstData)

else

burstData = burstData + Data($tPrime$) continue

end

end

end

Algorithm 4: Finding bursts* in a time period.

* One can find the number of bursts in a data transmission.
for each $t$ in $\{1, 2, ..., M\}$ do
  Find all capacity in $\{1, 2, ..., t\}$
  if $\text{Capacity}(t) < \text{Demand}(t)$ then
    \[
    \text{PredictiveCapacity} = \\
    \text{DataReal} + \text{Capacity}(t - 1) - \text{Demand}(t - 1) + \text{Capacity}(t - 2) \\
    - \text{Demand}(t - 2) + \text{Capacity}(t - 3) - \text{Demand}(t - 3)
    \]
    \[
    \text{BurstProportionCapacity} = \\
    \text{DataReal} + (\text{BurstLength}(t)/\text{TimePeriod}) \times \text{Demand}(t)
    \]
    \[
    \text{NonBurstProportionCapacity} = \\
    \text{DataReal} + (\text{TimePeriod} - (\text{BurstLength}(t)/\text{TimePeriod})) \times \text{Demand}(t)
    \]
  end
end

$\text{MaximumPrediction} = \text{DataReal}$ for Prediction in
  PredictiveCapacity, BurstProportionCapacity, NonBurstProportionCapacity
  do
  if Prediction $> \text{MaximumPrediction}$ and Prediction $< \text{Capacity}(t)$ then
    MaximumPrediction = Prediction
  end
  Data($t$) = MaximumPrediction
end

Algorithm 5: Algorithm for predicting channel condition and demand incorporating* traffic bursts.

* One can use the number of burst to improve the transmission algorithm.

This revised algorithm (presented in Algorithm 5) incorporates burst characteristics to find an improved data transmission rate. It considers three factors: the network load steadiness (as a proportion of time), the network load burstiness (as a proportion of time), and the prediction for the network load (i.e., Algorithm 3 with $N = 3$). Using the time proportions for burst traffic and steady traffic, the algorithm generates a weighted data rate for both scenarios. It compares the three possible data rates and uses the method that results in the maximum usage of the channel without exceeding the capacity. We show here the results for both ap-
Figure 3.7. Comparison between normalized channel usage with channel capacity prediction based on a three-point prediction algorithm incorporating data transmission during burst traffic.

These results show that the inclusion of burstiness results in slight throughput enhancement, but the additional computational complexity may not warrant its use.

3.4 Results and Discussion

3.4.1 Simulation Setup

In this section, we present the simulation setup and the datasets used to investigate the proposed algorithms for improving the throughput of the wireless network. Here, we implement our methods to improve the throughput of the MAC protocol used for different network loads.
Figure 3.8. Comparison between normalized channel usage with channel capacity prediction based on a three-point prediction algorithm incorporating data transmission during non-bursty (steady) traffic period.

3.4.2 Throughput

One can compare the throughput when using Algorithm 3 for different values of $N$. For the simulation environment we have developed, we have determined that the optimal throughput is achieved when $N = 3$; however, in actuality, minimal throughput gain is found beyond $N = 2$. To visualize this, the results for three different network loads are shown in Figure 3.9, which shows throughput with $N = 1$ to be much higher than with $N = 0$, and $N = 2$ and $N = 3$ achieving some small increase over $N = 1$. Given the extra computational complexity for higher values of $N$, we suggest using $N = 2$. Other network environments may find a different optimal value.

In order to assess the performance of our network protocol, we compare it against a standard protocol, such as slotted ALOHA, which is equivalent to $N = 0$ in our protocol. Figure 3.9 shows the throughput of our protocol under three different network loads for increasing values of $N$. We see that the throughput of
Figure 3.9. The channel throughput versus the number of time slots $N$ used by Algorithm 3 for three different network load levels.

our network is similar to that of slotted ALOHA for $N = 0$, but much larger when $N \geq 1$. Throughput improvements for $N \geq 1$ are due to predicting the network traffic and shaping the data traffic. As similar patterns of improvement are seen under all three network loads, this demonstrates the generality of our proposed algorithms.

This work employed a dataset built from several sources, as discussed in Section 3.2.3. The correlation between the number of Tweets sampled in a time slot and the network traffic needs can be used to further fine tune the throughput achieved and needs to be investigated in future work.
3.5 Simulation Methods

3.5.1 Programming

We used MATLAB 2013 to implement the algorithms. C# and Visual Studio 2012 were used to compute the list of bursts for network traffic for a given time period, while the predictive algorithms were implemented using MATLAB.

Data existing in large-scale social networks, such as Twitter, can be acquired through application programming interfaces (APIs) provided by these systems. In the case of Twitter, their API can be accessed by visiting https://dev.twitter.com/. The API handles queries made about users of the social network, such as: (i) time of a post, (ii) location (if available), (iii) message content, etc. [Russell, 2013]. Using a vector of keywords (e.g., find all Tweets containing the words [restaurant, friends, pictures]), messages pertaining to a given query are returned and subsequently can be stored in a database. Data-mining techniques can then be employed on these data.

3.5.2 Simulation Supplementary Materials

The dataset of received signal strength (RSS) measurements for WiFi signals used in Chapter 3 was collected at the University of Colorado and obtained from CRAWDAD, which can be found at: http://crawdad.cs.dartmouth.edu/.

The number of Tweets (actual data for a specific location in New York City) with geolocation tags was obtained from dataset available to Conrad S. Tucker’s research group.

3.6 Chapter Summary and Conclusions

For our simulations, we constructed a test dataset using Twitter traffic as a model of network load in a measured wireless channel. We developed new algorithms that employ both predictive techniques, as well as network traffic analysis. By measuring their performance against traditional collision detection algorithms, we have shown that these algorithms improve the utilization (i.e., data throughput) of the wireless channel.
In next chapter, additional improvements to CRNs can be made through the introduction of game-theoretic techniques. Altruistic cognitive players can be introduced to monitor and police the network. The combination of further data mining and game theory will increase the performance of CRNs.
Chapter 4

Spectrum Sharing via Hybrid Cognitive Players Evaluated by an M/D/1 Queuing Modeled

4.1 Chapter Introduction

In this chapter,\textsuperscript{1} we consider a CRN in which users adopt a spectrum-sharing strategy based on cooperation constraints. The majority of CR schemes bifurcate the role of players as either cooperative or non-cooperative. In this chapter, however, we modify this strategy to one in which players are hybrid, i.e., both cooperative and non-cooperative. Using a Stackelberg game strategy, we evaluate the improvement in performance of a CRN with these hybrid cognitive players using an M/D/1 queuing model. We use a novel game strategy (which we call altruism) to “police” a wireless network by monitoring the network and finding the non-cooperative players. Upon introduction of this new player, we present and test a series of predictive algorithms that shows improvements in wireless channel utilization over traditional collision-detection algorithms. Our results demonstrate the viability of using this strategy to inform and create more efficient CRNs. Next, we study a Stackelberg competition with the primary license holder as the leader, and investigate the impact of multiple leaders by modeling the wireless channel as

\textsuperscript{1}The research presented in this chapter has been published in Kotobi and Bilén [2017a].
an M/D/1 queue. We find that, in the Stackelberg game, the leader can improve its utility by influencing the followers’ decisions using its advertised cost function and the number of followers accepted in the network. The gain in utility monotonically increases until the network is saturated. The Stackelberg game formulation shows the existence of a unique Nash equilibrium using an appropriate cost function. The equilibrium maximizes the total utility of the network and allows spectrum sharing between primary and secondary cognitive users.

In order to evaluate our game-theory modeling approach, we used a queuing analysis that is used in Suliman and Lehtomaki [2009]. The opportunistic access used for the performance analysis in Suliman and Lehtomaki [2009] does not consider different cost functions or pricing schemes; number of primary or secondary cognitive users; or congestion. An M/G/1 queuing system (a queue model in which arrivals are Markovian and service times have a general distribution with a single server) containing one primary and multiple secondary users is presented in Zhang et al. [2009]. Here we use an M/D/1 queuing system, merely to be used for analysis. Secondary users can gain access to the spectrum through an amplify-and-forward time-division-multiple-access protocol. Our method is more generalized in that it supports multiple primary users, as well as supports general cost functions that are not imposing any performance requirement for secondary users such as amplify and forward.

### 4.2 Game-Theoretic Study

The dominant spectrum allocation method (i.e., fixed allocations) does not maximize channel efficiency since the license holders (primary users) generally do not utilize their allocated spectrum at all times. A primary approach for increasing the efficiency of spectrum allocation is to allow a second group of unlicensed users to use it when the spectrum is idle. The users who wish to use the spectrum but do not have the primary license are called secondary users, and they can opportunistically access the channel when the primary user is idle [Lal and Mishra, 2003]. To facilitate this, we introduce a self-organizing mechanism and assess it by modeling the network as a queue that allows both classes of user to wait in a queue to access the channel modeled as a server.
In this chapter, we investigate a Stackelberg competition with the primary user as leader and find that, in the Stackelberg game, the leader can improve its utility by influencing the follower’s decision using its advertised cost function and the number of followers accepted into the network. For a given stable system and for feasible transmission-rate sets, based on the number of primary and secondary users, we find a Nash equilibrium for primary and secondary users. We study a network of CRs competing to access the spectrum that are either cooperative or non-cooperative. We introduce a hybrid player, i.e., one which is both cooperative and non-cooperative. Using Stackelberg game strategy, we evaluate the improvement in performance of the cognitive players using an M/D/1 queuing model. We use altruism to monitor the spectrum usage and find the non-cooperative players. We also study a Stackelberg competition with primary users as leaders, and investigate the impact of multiple leaders by modeling the wireless channel as an M/D/1 queue.

The remainder of this chapter is organized as follows. In Section 4.3, we describe the game with a greedy and normal player, and demonstrate that a vigilante player mitigates the impact of a greedy player. We then describe the M/D/1 queuing modeling and the proposed cooperation scheme. In Section 4.4, we formulate and solve a Stackelberg game with the primary user as the leader and employ a Vickrey auction between secondary users. In Section 4.5, we provide the numerical results for several communication scenarios, and observe the impact of the network parameters in each case. In Section 4.6, we discuss our results and conclusions.

### 4.3 Spectrum Sharing Algorithm

We study various generalizations of fundamental communication models for CRs, using new equilibrium concepts beyond Nash theory that can capture the realistic aspects of spectrum sharing. We consider two CR player types in which only the primary user has access rights to radio resources as shown in Figure 4.1. Both primary and secondary cognitive users have data to transmit using the spectrum, which is modeled as a server in our queuing model presented in Figure 4.1. Cognitive users participating in a Stackelberg game are selfish in the sense that they will act to maximize their respective utilities, i.e., minimizing the time in the queue.
Figure 4.1. Queuing model of primary user as leader and secondary user as a follower in Stackelberg game.

The primary and secondary users are leader and follower, respectively, in a Stackelberg game, and the follower will control the game by advertising its strategy to the follower. As it can be seen in Figure 4.1, both players are competing to access the server (spectrum) to transmit their data, but the leader can influence the strategy that the follower chooses by advertising its parameters.

Below, we first introduce a vigilante player to cope with a greedy player that maximizes its utility function by transmitting more than its allocation. Second, we focus on a queuing analysis of opportunistic access in CRs. All variables used in this chapter are defined in Table 4.1.

### 4.3.1 Vigilante Player

All players in this setup are considered secondary cognitive players. We desire a wireless network with only one visible greedy player for any specific cell. We assume that a cognitive network with $M$ players can be divided into $m$ cells each with $N_i$ players in the $i$th cell as shown in Figure 4.2. Without loss of generality, we assume that there are the same number of CRs on average in each cell, i.e., the $N_i$ terms are equal. This simplifies our study of movement of a greedy player and its impact on our proposal because only $N_i$ players will be affected by the greedy player. The greedy player is defined as one that is not transmitting with probability $1/N_i$ in
Table 4.1. Summary of variables used in Chapter 4.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_i$</td>
<td>Total number of normal players in $i$th cell</td>
</tr>
<tr>
<td>$B_i$</td>
<td>Total number of players that are not vigilante in $i$th cell</td>
</tr>
<tr>
<td>$C$</td>
<td>Cost function</td>
</tr>
<tr>
<td>$e_g$</td>
<td>The aggressiveness of the greedy player</td>
</tr>
<tr>
<td>$e_v$</td>
<td>The aggressiveness of the vigilante player</td>
</tr>
<tr>
<td>$i$</td>
<td>Cell indicator</td>
</tr>
<tr>
<td>$M$</td>
<td>Total number of players in network</td>
</tr>
<tr>
<td>$m$</td>
<td>Total number of cells in network</td>
</tr>
<tr>
<td>$N_i$</td>
<td>Total number of players in $i$th cell</td>
</tr>
<tr>
<td>$n_p$</td>
<td>Number of primary players</td>
</tr>
<tr>
<td>$n_s$</td>
<td>Number of secondary players</td>
</tr>
<tr>
<td>$P_g$</td>
<td>Transmitting probability of greedy player</td>
</tr>
<tr>
<td>$P_n$</td>
<td>Transmitting probability of normal player</td>
</tr>
<tr>
<td>$P_V$</td>
<td>Transmitting probability of vigilante player</td>
</tr>
<tr>
<td>$Q_g$</td>
<td>Throughput of greedy player</td>
</tr>
<tr>
<td>$Q_n$</td>
<td>Throughput of normal player</td>
</tr>
<tr>
<td>$Q_V$</td>
<td>Throughput of vigilante player</td>
</tr>
<tr>
<td>$u_g$</td>
<td>Greedy utility function</td>
</tr>
<tr>
<td>$u_p$</td>
<td>Primary utility function</td>
</tr>
<tr>
<td>$u_s$</td>
<td>Secondary utility function</td>
</tr>
<tr>
<td>$u_v$</td>
<td>Vigilante utility function</td>
</tr>
<tr>
<td>$W_p$</td>
<td>Primary waiting time</td>
</tr>
<tr>
<td>$W_s$</td>
<td>Secondary waiting time</td>
</tr>
<tr>
<td>$\alpha_p$</td>
<td>Share of bandwidth used by primary</td>
</tr>
<tr>
<td>$\alpha_s$</td>
<td>Share of bandwidth used by secondary</td>
</tr>
<tr>
<td>$\lambda_p$</td>
<td>Packet rate for the primary</td>
</tr>
<tr>
<td>$\lambda_s$</td>
<td>Packet rate for the secondary</td>
</tr>
<tr>
<td>$\mu$</td>
<td>Server rate or bandwidth</td>
</tr>
</tbody>
</table>

its current cell and uses the following for updating its transmitting probability in a slotted ALOHA accessing scheme:

$$P_g(t + 1) = e_g P_g(t) : (P_g(t + 1) < 1),$$  \hspace{1cm} (4.1)

where $e_g$ is used to model the aggressiveness of the greedy player and the : condition denotes that probability cannot exceed 1. $P_g$ and $t$ denote transmitting probability of greedy player and time respectively. Other models are possible, but Equation 4.1 adequately models a greedy player that aggressively updates its transmission.
Figure 4.2. Cognitive network with $M$ players can be divided into $m$ cells each with $N$ players.

probability. By using the throughput

$$Q_g = P_g \prod_{A} (1 - P_a),$$

(4.2)

where $A$ is all players except the greedy player and $P_a$ is the transmission probability for those players, one can define a basic utility function for the greedy player that needs to be minimized, i.e.,

$$U_g = 1 - Q_g.$$  

(4.3)
A vigilante player can be defined with an altruistic approach to jam the shared resource causing the greedy player to lower its transmission probability with a similar transmission probability to Equation 4.1. Assume, if

\[ Q_v = P_v \prod_B (1 - P_b) < Q_n, \]

where \( Q_n \) is the throughput of a normal player in the absence of a greedy or vigilante player [Kesidis et al., 2013], \( B \) is all players except the vigilante player, and \( P_b \) is the transmission probability of those players, then the vigilante player uses the following to update its transmission probability:

\[ P_v(t + 1) = e_v P_v(t) : \left( P_v(t + 1) < 1 \right), \]

where \( e_v \) is an aggressiveness factor used to cope with the greedy player. Define \( Q_v = P_v \prod_B (1 - P_b) \) as the throughput of the vigilante player, where \( B \) represents other players in the same cell as the vigilante player. The vigilante player acts greedy to make the nodes cooperate rather than maximizing its throughput, so the vigilante player’s utility function is defined as

\[ U_v = \left| Q_v - Q_n \right|, \]

where \( Q_n \) represents a throughput for a cooperative player without any greedy or vigilante players. Assuming an approximation of a throughput, we can find the following equation for the choice of \( e_g \) for the greedy player to minimize its utility function based on full knowledge of the game played by the vigilante player:

\[ \frac{dU_g}{de_g} = 0 \rightarrow e_g = e_v \frac{N}{N - 1}, \]

where the vigilante player is aware of \( e_g \) because of the nature of Stackelberg games and \( N \) is total number of CRs in the corresponding cell.

In our model, one must assume that a greedy player is able to move between the geographical cells, in which case it can move from a cell with an active vigilante player to a cell in which the presence of a vigilante player is unknown. Once moved, then a cooperative player will turn into a vigilante player and the same
cyclic behavior occurs. If the greedy player is static, i.e., not able to move between cells, then it cannot achieve more than its share because of the presence of an active vigilante player. We investigate these behaviors and show that the same cyclic behavior happens in the new cell.

4.3.2 M/D/1 Queueing Model

Here we show that the problem of spectrum sharing between multiple primary and secondary users can be analyzed by a queuing model. We assume a channel with accessible bandwidth of $\mu$ and two virtual queues for primary (leader) and secondary (follower) users, as shown in Figure 4.1. A Poisson process is assumed for packet arrival times with a uniform packet size and we use a modified M/D/1 (i.e., a queue in which arrivals are governed by a Markovian process, service rate is fixed, and it has a single server) queuing system to analyze the network performance. We use the waiting time to correlate our game theory approach with the M/D/1 queuing model. The expected waiting time for a stable queue is positive and finite. Waiting time is one of the parameters used to define the utility function in our Stackelberg game. In a Stackelberg game, the follower chooses its game strategy to maximize its utility based on the leader’s advertised strategy. That means the leader and follower play a sequential game in which the follower must react optimally to a strategy imposed by the leader. Furthermore, the leader is capable of calculating the follower’s best response to any imposed plan. As a result, the leader chooses a strategy to maximize its utility knowing the follower’s reaction [Osborne, Martin J, 1994]. For the M/D/1 queuing system and a primary user, we know that [Jansson, 1966] (for our model we employ a Poisson distribution as this is simpler, yet can be shown to be equivalent to Markovian):

$$W_p = \frac{1}{2(\mu - \lambda_p)} \frac{1}{2\mu},$$  \hspace{1cm} (4.8)

where $W_p$ is the expected delay in the queue for the primary user, $\lambda_p$ is packet rate for the primary, and $\mu$ is server rate, or, in this model, the spectrum bandwidth. By assuming that the primary user is going to auction the spectrum access to a
secondary user, we can define
\[ n_p \alpha_p + n_s \alpha_s = 1, \]  
(4.9)
where \( \alpha_p \) is the share of bandwidth used by a primary user, \( \alpha_s \) is the share of bandwidth used by a secondary user, \( n_p \) is the number of primary users, and \( n_s \) is the number of secondary users. These coefficients must add up to one in order to fully utilize the spectrum bandwidth available to the CRs. We define the utility function of the leader to share the spectrum as
\[ u_p(\alpha_p, \lambda_p, \mu, n_s, n_p) = -\ln(W_p) - \ln(\alpha_p/n_t)C(n_s, n_p, \mu), \]  
(4.10)
where \( C(n_s, n_p, \mu) \) is the cost function used by the primary user to advertise the excess bandwidth available to the followers. We can define a simple cost function to capture the impact of \( n_s \) on the cost by a logarithmic function as
\[ C_1(n_s) = \ln(1 + n_s). \]  
(4.11)

In Section 4.5, a comprehensive discussion for the choice of cost functions and their impact on the Stackelberg game is presented. The follower, or the secondary user, in the Stackelberg game uses the following as its utility function (since waiting time in the queue has a negative impact on the utility):
\[ u_s(W_s, n_s) = n_s - \ln(W_s). \]  
(4.12)
where \( W_s \) is secondary user’s waiting time.

To find the Nash equilibrium, both primary and secondary users will gain no additional access to bandwidth (server) by moving from the point defined by \((\alpha_p, \alpha_s)\). As a result we have:
\[ \frac{\partial u_p(\alpha_p, \lambda_p, \mu, n_s, n_p)}{\partial \alpha_p} = 0 \]  
(4.13)
and
\[ \frac{\partial u_s(W_s, n_s)}{\partial \alpha_s} = 0. \]  
(4.14)
To ensure the M/D/1 queue is stable, the pair of points found in Equations 4.13 and 4.14 must mutually lie in the set:

\[ 0 \leq \alpha_p, \alpha_s \leq 1, \quad (4.15) \]

\[ \alpha_p \mu \leq \lambda_p, \text{ and} \quad (4.16) \]

\[ \alpha_s \mu \leq \lambda_s. \quad (4.17) \]

\section*{4.4 System Model}

Below, we first study a game with three players who desire to maximize their utility functions, each using a unique strategy. Then, we formulate and solve a Stackelberg game for the communication scenario described in Section 4.3.2 with the primary license holder and secondary users as leader and followers of the Stackelberg game, respectively.

\subsection*{4.4.1 Game with Three Players}

Without loss of generality, the utility functions defined in Section 4.3.1 are simplified versions of the utility functions defined in Kesidis et al. [2013]. Based on different pairs of \((e_v, e_g)\), one can see either a cyclic behavior for the throughput of the players [Kesidis et al., 2013] or a Nash equilibrium [Griffin and Kesidis, 2014]. For the case of reaching an equilibrium, the vigilante player uses most of the shared bandwidth, which keeps the greedy player from increasing its transmission probability and, as a result, there is no fair resource sharing for cooperative players to use.

By moving from a cell that has an active vigilante player, the greedy player can minimize its utility function. In a distributed cognitive network, a predefined radio node in each cell can be considered/assigned as a vigilante player. For a dynamic greedy player, the measured throughput that is an indicator of \(e_v\) is used to calculate the best \(e_g\) and/or the best time to move to a new cell.

By introducing a vigilante player and using non-traditional game strategy for decision making, we hope to improve the performance of a CRN. To date, the appli-
cation to CRNs of a hybrid player, which is both cooperative and non-cooperative, has not been studied significantly. We propose a play strategy (i.e., altruism) to police a wireless network. Using this new player, we will test a series of predictive algorithms to investigate a potential improvement in wireless channel utilization by punishing the non-cooperative players. Then, we will use this strategy to demonstrate the application of a vigilante player in an M/D/1 queue.

The mean value of a received signal in a certain frequency range is an indicator of the presence of a primary user. Since malicious users are more effective in acting in a cooperative manner with other malicious users to change the mean and make a false pretense that a primary user is active, one can suggest finding these users in an iterative manner [Kotobi et al., 2015]. With this method, one can find their intention for changing the mean by averaging their advertised signal power and treating them as a separate group inside each cell, which is plausible since one can argue that, by introducing a fusion center, the algorithm will be capable of disregarding the malicious users as a group. If a user is falsely accused of being malicious due to multipath fading and/or shadowing, it can be reclassified as a normal user if the weight-assignment method is implemented [Griffin and Kesidis, 2014].

### 4.4.2 Stackelberg Game in an M/D/1 Queue

In our Stackelberg game in order to have a stable queue, the validity and stability of spectrum sharing assessed via the M/D/1 queuing system needs to be investigated in terms of the number of primary and secondary users as leaders and followers, respectively. By having more than one primary user it is intuitive to show that the M/D/1 queue with a constant $\mu$ will be unstable for a larger set of $\lambda_p$. A similar argument applies for followers with $\lambda_s$. This will lead to a feasible set tighter than Equations 4.15, 4.16, and 4.17 redefined using Equation 4.9, i.e.,

\[
0 \leq n_p \alpha_p, n_s \alpha_s \leq 1, \quad (4.18)
\]

\[
\alpha_p \mu \leq n_p \lambda_p, \text{ and} \quad (4.19)
\]

\[
\alpha_s \mu \leq n_s \lambda_s. \quad (4.20)
\]
This tighter feasible set requires a careful consideration for the number of followers admitted to the queue to ensure that it remains stable. A network can estimate the number of secondary users it can accept based on multiple variables such as the number of primary users, service rate, and request rates by primary and secondary users. Cost functions used in Equations 4.13 and 4.14 can be chosen to prioritize one or more variables mentioned above and/or, by using a Vickrey auction, the highest bidder will win and then the leader’s strategy will adapt to that. The existence of Nash equilibrium in this tighter feasible set will allow the network to share unused spectrum with the followers with a gain in spectrum usage advertised by the cost function to the leaders by transmitting that cost function. By defining the set of pairs \((\alpha_p, \alpha_s)\) satisfying Equations 4.15, 4.16, and 4.17 as set \(A\), it is easy to show that the Nash equilibrium point for the leader of the Stackelberg game can be found from:

\[
\alpha_p = \begin{cases} 
\frac{\lambda_p(C-1)}{\mu(C-2)} & \text{if } \alpha_p \in A \\
1/n_p & \text{if } \alpha_p \notin A
\end{cases}
\]  

where \(C\) is the cost function for that pair, for example the simple cost function defined in Equation 4.11. If there is no answer for \(\alpha_p\), then the primary user has no motive to share the spectrum because it makes the network unstable.

The Stackelberg game using three types of secondary users introduced in Section 4.4.1 and a primary user as follower will result in a cyclic behavior. The leader cannot stop a greedy player, instead it will not share the spectrum when the network is saturated, according to Equation 4.21. In this scenario, the vigilante player will force the greedy player to move to another cell.

### 4.5 Numerical Analysis

Here, we present the simulation results of cyclic behavior of the three players’ utility functions introduced in Section 4.3.1. Then, we introduce the numerical analysis of a Stackelberg game introduced in Section 4.3.2 with parameters inside the feasible set defined in Section 4.4.2.
4.5.1 Cyclic Behavior for Vigilante Player

Via numerical analysis, we study the movement of a greedy player and the correlation between $e_v$ and the average throughput of a greedy player based on the number of cooperative players in a cell. First, without loss of generality in our numerical simulation, we specify 10 cells with $N = 5$ players in each cell, assuming one will turn vigilant if its throughput is less than $Q_n$. The vigilante player always assumes that this decrease in its utility function is due to the presence of a greedy player. If this assumption is wrong due to transmission error, the vigilante player will turn to a normal player in the next iteration according to the algorithm. The turned node will then follow Equation 4.5 as its transmission probability. In order to clearly see the changes in throughput we use $e_g = 1.1$ and $e_v = 1.3$ (assuming $e_v \geq e_g > 1$). The sudden decrease in throughput for the greedy player leads the dynamic greedy player to change cells to minimize its utility function as seen in Figure 4.3. Each cycle represents a migration from a cell.

To study the effect of $e_v$, we assumed a greedy player with $e_g = 1.2$ (to show a smaller aggression) for updating its transmission probability (Equation 4.1) in a cell of $N$ nodes from 5 to 45. After sensing the presence of a vigilante player, the greedy player will move to a neighboring cell. Different values for $e_v$ that do not cause a desired Nash equilibrium are shown in Figure 4.4. As it can be seen from Figure 4.4, less aggressive vigilante players ($e_g = 1.2, e_v = 1.2$) will cause the greedy player to stay in a cell and, as a result, its utility function will be minimized allowing greater throughput. More aggressive vigilante players ($e_g = 1.2, e_v = 1.5$) cause the greedy players to switch cells and in a new cell it takes time for the greedy player to minimize its utility function, which when minimized leads to less throughput for others. If a greedy player were static, the behavior would not be cyclic, and would be represented by the first “hump” only (i.e., time slots 0–17 in Figure 4.3).

4.5.2 Spectrum Sharing Performance Analysis of a Stackelberg Game using an M/D/1 Queueing Model

For the Stackelberg game’s Nash equilibrium analysis, we first present the simulation results analyzed via an M/D/1 queue, with one primary user as the leader
and then extend the results with multiple leaders. We evaluate the utilities of the leader and follower at the equilibria found in Sections 4.3.2 and 4.4.2. We omit the equilibria found in the feasible set defined by Equations 4.15, 4.16, and 4.17 when the utility function for both leaders and followers yields zero. As shown later in this section, this happens when the network is close to saturation. The available bandwidth is between 40 to 160 kbps (we use actual numbers to compare the results for different scenarios). We vary the remaining parameters, such as the number of primary and secondary users \( (n_p, n_s) \), cost function, and accessible spectrum \( \mu \), in order to assess their impact on the utilities.

Figure 4.5 shows the utilities resulting from the Stackelberg game’s Nash equilibrium, defined in Section 4.4.2 and with the scenario presented in Section 4.3.2, with the simple cost function of Equation 4.11. For this set of analyses there is only one primary user as a leader and the number of secondary users varies from 1
Figure 4.4. Effect of a vigilante player’s aggression coefficient, $e_v$, on the throughput of a moving greedy player.

In this Stackelberg game, as the number of secondary users increases, their utility decreases while the leader’s utility increases until the cognitive network is saturated. It is intuitive to show that the followers’ utility functions decrease because of competition with the fellow followers to access the limited spectrum, and it gets increasingly critical when $\mu$ decreases for the constants $\lambda_p = 10$ kbps, $\lambda_s = 1$ kbps. In this scenario, the best approach by the leader is to admit as many secondary cognitive nodes in the cell based on the available $\mu$, until its normalized utility function reaches an optimum. For $n_s = 5, 7, \text{ and } 9$ this happens for $\mu = 40, 70, \text{ and } 100$ kbps, respectively.

Figure 4.6 shows how the utility function reacts by varying the number of primary users, in order to observe the impact of the number of leaders in the Stackelberg game. To satisfy the feasible set defined by Equations 4.15, 4.16, and 4.17, the server rate $\mu$ varies from 100 to 160 kbps. This range will delay the saturation and will let us understand the impact of the number of leaders in the game. As before, $\lambda_p = 10$ kbps and $\lambda_s = 1$ kbps, but the number of secondary users is constant, $n_s = 3$. In this case, the main reason for the decrease in the
Figure 4.5. The two players normalized utilities versus the number of secondary users with $n_p = 1$, $\lambda_p = 10$ kbps, $\lambda_s = 1$ kbps and different $\mu$ ranging from 40 to 100 kbps for the Stackelberg games in Section 4.4.2 and cost function defined with Equation 4.11.

normalized utility is the competition to access the network between the primary users; when the cognitive network is saturated there will be no utility for the secondary users. The saturation for $\mu = 100$, 130, and 160 kbps happens at $n_p = 7$, 8, and 9, respectively.

Figures 4.7 and 4.8 demonstrate the impact of different cost functions on the utility function and the saturation of the cognitive network. In the following cost functions, we include $\mu$ and $n_p$ as additional inputs to determine the cost of spectrum access. First, the cost is monotonically increasing with the number of primary users in the cognitive network and with the available spectrum, i.e.,

$$C_2(n_s, n_p, \mu) = \ln (1 + n_s) + \ln (n_p \mu).$$

(4.22)

In the second cost function, we assume that an increase in $\mu$ reduces the cost of sharing the available spectrum, i.e.,

$$C_3(n_s, n_p, \mu) = \ln (1 + n_s) + (n_p \mu).$$

(4.23)
Figure 4.6. The two players normalized utilities versus the number of primary users with $n_s = 3$, $\lambda_p = 10$ kbps, $\lambda_s = 1$ kbps and different $\mu$ ranging from 100 to 160 kbps for the Stackelberg games in Section 4.4.2 and cost function defined with Equation 4.11. Figure 4.7 shows the relationship between the cost function and varying normalized utility of both players versus the number of primary users. Here, the parameters for our game are $n_s = 3$, $\lambda_p = 10$ kbps, $\lambda_s = 1$ kbps, and $\mu = 100$ kbps. It can be concluded that, via a Vickrey auction, we can have different saturation points for the number of secondary users. For Equations 4.11, 4.22, and 4.23, we have a saturated network for $n_p = 5, 6, \text{and } 6$, respectively.

Figure 4.8 provides a comparison of the utility functions of both players versus the number of secondary users, where $n_p = 2$, $\lambda_p = 10$ kbps, $\lambda_s = 1$ kbps, $\mu = 100$ kbps. Here, for Equations 4.11, 4.22, and 4.23, we have saturation for $n_s = 8, 9, \text{and } 9$, respectively. As can be seen in Figure 4.8, there will be a cutoff point for the number of secondary users. This means that, no matter what cost function we use, there is a point beyond which the queue will be saturated. By choosing an appropriate cost function, one can modify the maximum number of secondary users admitted in to the network.

In a queue with $n_s = 2$, $n_p = 2$, $\lambda_p = 10$ kbps, $\lambda_s = 1$ kbps, and $\mu = 100$ kbps, we assume that one of the secondary users is a greedy player defined in Section 4.4.1 with $e_g = 1.05$. As mentioned before, the other secondary users will sense the extensive spectrum usage and turn into a vigilante player with $e_v = 1.2$. The
Figure 4.7. The two players normalized utilities versus the number of primary users with $n_s = 3$, $\lambda_p = 10$ kbps, $\lambda_s = 1$ kbps, and $\mu = 100$ kbps, and three cost functions with $C_1$, $C_2$, and $C_3$ defined by Equations 4.11, 4.22, and 4.23, respectively.

cyclic behavior of the greedy player in each cell can be seen in Figure 4.9. This cyclic behavior has been predicted by the analysis presented in Section 4.3.1. A normal player turned to a vigilante player will force a greedy player to act normal in our queue.

4.6 Chapter Summary and Conclusion

In this chapter, we investigated the spectrum sharing cooperation by modeling the spectrum and users as a queue, with the goal of encouraging the CRs to cooperate. We have focused on the system model that, despite the desire to maximize their individual utilities, the CRs find it beneficial to cooperate. We have formulated a Stackelberg game in which the primary license holder and secondary user are leader and follower, respectively, and studied how the leader can influence the follower’s decision of participating in the game by varying the cost function. Additionally, we observed that a pricing algorithm can be employed to improve all utilities to
the social optimality of an M/D/1 queue. In this scenario, CRs can employ the cost function to decide how much of the spectrum is used by primary users and secondary users.

Figure 4.8. The two players normalized utilities versus the number of secondary users with $n_p = 2$, $\lambda_p = 10$ kbps, $\lambda_s = 1$ kbps, and $\mu = 100$ kbps, and three cost functions with $C_1$, $C_2$, and $C_3$ defined by Equations 4.11, 4.22, and 4.23, respectively.
Figure 4.9. Greedy player in a queue with $n_s = 2$, $n_p = 2$, $\lambda_p = 10$ kbps, $\lambda_s = 1$ kbps, $\mu = 100$ kbps, and $e_q = 1.05$, $e_v = 1.2$ for the Stackelberg games in Section 4.4.2 and cost function defined in Equation 4.11.
Chapter 5

Non-parallelizable Auction for Spectrum Sharing in Cognitive Radio Networks with a Security Verification

5.1 Chapter Introduction

In this chapter,\(^1\) we investigate an auction mechanism for sharing available wireless bandwidth among competing CRs. The bandwidth under consideration may be either in an unlicensed spectrum or in an unused licensed band. Spectrum sharing is achieved via a mechanism in which a CR acting as the auctioneer advertises spectrum availability to bidding CRs and defines a puzzle to solve as a method to access it. The CRs act as bidders by computing the solution to the problem (i.e., the puzzle). The winner is the bidder who submits the first correct bid and thus gains access to the spectrum for the next time interval. We consider two different variances of our scheme based on parallelizable and non-parallelizable problems and demonstrate that the latter provides a fair auction in contrast to the former. We propose a verification database to counter malicious greedy players. Our algorithm provides a centralized, easy-to-implement, and computationally fast

\(^1\)The research presented in this chapter has been published in \textit{Kotobi et al.} [2016].
multiple-access scheme that is verifiable by all participating CRs.

5.2 Multiple Access Scheme

Spectrum usage efficiency can be increased if secondary users that are not primary license holders can access the spectrum when idle. For instance, currently assigned spectrum can be monitored in real time to allow usage of any unutilized spectral opportunities [Lal and Mishra, 2003]. Proposals regarding power- and bandwidth-constrained distribution have been investigated [Sani and Vosoughi, 2015b; 2016] in order to minimize the probability that secondary users cause a blockage for primary users.

In our scheme we assume that a primary user charges an entrance fee for any interested CR to enter the auction. The main idea of our scheme is that secondary users are required to solve a problem in order to submit a request to access the available spectrum (e.g., Dwork and Naor [1992]). Our auction concept is based on past proposals in which network administrators suggested solving a puzzle in order to access a resource in order to deny access to those with malicious intentions or who are resource hogs. Such schemes require that the user spend resources to access resources. For example, an email spammer, who must pay a little for each email sent, may gain a reward when a user clicks on an emailed offer, but they need to pay for all the email spam they sent, which reduces or even removes the incentive to spam.

As mentioned, we propose an auction mechanism to access the spectrum in which the winner is determined by solving a problem and submitting the solution. To make this auction fair for all bidders, we need to provide a problem with the property of non-parallelizability. Current smartphone processing powers are on the order of 10–100 GFLOPS. For example, Apple’s A9 chip is 115 GFLOPS and Samsung’s Exynos 7420 is 35 GFLOPS. Because of the communication delay and the simplicity of our auction problems in terms of processing time (less than 100 microseconds), the difference in these processing powers is negligible. But some CRs may have more parallel processing units than others and, as such, they can solve a parallelizable problem faster compared to their competitor bidders by using multi-threaded computation. We demonstrate that multi-threaded processing
units will create an unfair auction compared to simple units with a better processing power, which will not. Allocating multi-threaded processing makes the outcome of an auction predetermined, thus forfeiting the advantages of spectrum sharing. To demonstrate this, we compare auctions based on parallelizable problems with their non-parallelizable counterparts and investigate the results with respect to bandwidth access.

The problems used in this auction must be easy to solve (to reduce the delay to access the spectrum) and to verify the solution. However, easy problems may result in malicious attempts by greedy players [Kotobi and Bilén, 2015] to guess the answer such that their bids are placed before other players who are calculating the answer. To combat this, we propose a distributed database to blacklist greedy players, i.e., those submitting many incorrect solutions, to ensure that our scheme is robust against any malicious attacks by greedy CRs.

The remainder of this chapter is organized as follows. In Section 5.3, we demonstrate how the CRs can access the spectrum as bidders. We then define our multiple spectrum-access method. In Section 5.4, we describe the auction and a class of non-parallelizable problems, provide the numerical results for several communication scenarios, and observe the impact on spectrum access for the proposed auctions in each case. In Section 5.5, we discuss our results and present conclusions.

5.3 Auction Model

We assume that multiple secondary users must compete for transmission over an available wireless spectrum, which may result in issues of fairness and efficiency should the mechanism not be properly formulated. In light of transmission delay, it is desired that secondary users are able to access the spectrum with high availability. Competing with other secondaries will decrease the effective achievable rate of access for a secondary user, which will result in reduced spectrum utilization efficiency (throughput) of the wireless network. For a given frequency band, diversifying spectrum access that refrains from continuous transmission attempts (similar to what occurs in an ALOHA system) will result in fairer multiple access.

With reference to Figure 5.1, we consider a CRN involving \( N \) secondary users. For simplicity, we assume that all secondary users know the presence of primary
Figure 5.1. Network model of competing secondary users trying to access a shared spectrum with an auctioneer

users and other secondary users for initiation and the time interval that spectrum is free. By using collaborative sensing among all CRs, the sensing errors for initial sensing can be significantly decreased [Zhao et al., 2008]. We propose a distributed auction that can be verified by all bidders. An auctioneer signals all CRs about the availability of spectrum for a given time interval by an auction signal. Then, the secondary users willing to participate in the auction will respond with a delegate signal. The auctioneer sends a problem to all bidders and each bidder starts a thread to solve the problem. The first bidder to submit a correct solution from a set of solutions (for instance a polynomial equation that may have several roots) will gain access to the spectrum.

We present a set of problem constructions that are simple and resource-light to construct and verify by competing bidders to evaluate efficiency of our multiple-access scheme. Since the auctioneer can be any secondary user that is not on a blacklist and has no data to transfer in that time interval, this algorithm establishes a distributed method for the secondary users to access available spectrum.
5.3.1 Non-parallelizable Auction

By forcing the secondary user to solve a computational problem before attempting to transmit a signal, the auctioneer ensures that the secondary user spends sufficient resources before committing spectrum. In particular, a greedy player (a scenario presented in Kotobi and Bilén [2015] shows jamming of a wireless spectrum by a greedy CR) who wishes to monopolize available spectrum, will have to solve a huge number of problems.

We define a problem to be solved by a secondary user as non-parallelizable if the solution to the problem cannot be computed via a parallel process. If the problem introduced by the auctioneer is parallelizable, the wireless network can face two major problems. First, a secondary user with more computational power can submit correct bids faster than its less-capable counterparts and win in most time slots. This can be done via a multi-threading method or by dynamic programming (as demonstrated in, for instance, Kurve et al. [2013b]). This will jeopardize the fairness of our multiple-access algorithm. Second, a greedy player can jam a network and other mechanisms need to be used to combat this [Kotobi and Bilén, 2015].

In this work we assume that the auctioneer and bidders have similar resources regarding both their computational ability and their memory capacity. This will allow the possibility of assigning one of the CRs as the auctioneer in the time slots it has no data to transmit, thus decentralizing this algorithm. Properties defined by Tritilanunt et al. [2007] for evaluating client puzzles used to mitigate denial-of-service attacks can similarly be used within our scheme. The auctioneer’s cost is defined by the computational cost for it to do pre-computing, problem construction, and verification of the bidders’ solutions. The computational processing power of the CRs for preparing and submitting their bids may be restricted, so the problems must be solvable using limited processing power and within a time constraint. If the auctioneer’s problem can be solved via parallel computation, then it leads to a multiple-access scheme that is biased for CRs with more computational power. Also, a non-parallelizable scheme can stop greedy and/or malicious users from gaining access or jamming the spectrum by costing them processing time.

We assume that the CRs may have a single thread or multiple threads to perform the necessary computation needed to solve the auctioneer’s advertised
problem. In this scheme, to ensure that the bidders follow our requirement, we have to design the problem’s difficulty in a manner such that the suggested algorithm is more efficient (in terms of computational time for a single-thread secondary user) than brute-force searching, even if solving the problem can be done by parallel-computing methods.

5.3.2 Malicious Attacks

The problem-set properties defined in Section 5.3.1 should be simple and inexpensive to construct and verify for the auctioneer and for the bidders to solve, but there must be an effort to stop greedy bidders who attempt to flood the auctioneer with a large number of bogus solutions. We propose a blacklist database to combat this. Since the individual bids are visible by the rest of the network (ignoring the hidden node problem for simplicity), then by utilizing a majority vote the MAC address of the greedy node will be added to the blacklist database to ensure a decentralized algorithm. Since the database may grow large over time, there will be a time frame to expire the entries of the list (for example using a first-in-first-out process).

In our multiple-access algorithm, a malicious user may want to submit multiple bogus bids to avoid the computational time and/or processing power required. If a malicious user guesses a correct answer, this will result in unfair spectrum access that can be avoided by making a blacklist of those users (i.e., those who have submitted multiple wrong answers before a correct one) by the auctioneer and/or other bidders. All bidders can agree on a threshold number of incorrect bids that makes a bidder malicious to prevent an error in judgment. Then, once a malicious bidder is added to the database, this will prevent it from having new bids accepted for a period of time. This database is accessible by all bidders, which is a necessity for a decentralized algorithm. This also makes it possible to designate any CR as the auctioneer.
5.4 Auction Performance

In this section, we compare the performance of an auction with non-parallelizable problems with that of an auction with parallelizable problems. With the optimal channel-sensing method defined in Section 5.3.1, the channel usage achieved by the non-parallelizable auction defines the performance limit of a wireless channel-access system.

Here, we investigate the performance of the proposed schemes by programming our scheme in C# and using threads as the bidders, since this programming language supports multi-threaded computations. We construct a wireless network with an auctioneer and a number of secondary users as bidders. All secondary users are assumed to have a communication channel to the auctioneer to receive the auction problem and other necessary information to submit their bids.

5.4.1 Parallelizable vs. Non-parallelizable Auctions

To demonstrate the advantage of an auction with non-parallelizable problems over parallelizable ones, we define two sets of problems. The first problem is to calculate the $n$th iteration of Fibonacci series with random initial values recursively and the second is to find any root of a random function advertised by the auctioneer. Solving the Fibonacci series recursively is a problem that cannot be solved using any parallelizable method and, as a result, a secondary user with multi-threaded processing power does not have an advantage over a single-threaded one. On the other hand, solving for the roots of a function is parallelizable using the Newton–Raphson method (as shown in Kurve et al. [2013b]).

Another example of a recursive problem is computing $\pi$ using a recursive method [Offner, 2015]. For initial values we select $a_0 = 4\sqrt{3}$ and $b_0 = 6$. Then we have,

$$a_{n+1} = \frac{2a_nb_n}{a_n + b_n}, \quad (5.1)$$

and,

$$b_{n+1} = \sqrt{b_na_{n+1}}, \quad (5.2)$$

where $n$ defines the iteration step. Using this recursion, both $a_n$ and $b_n$ will
converge to $2\pi$. If one wants to use this problem, the auctioneer can set other initial values for $a_0$ and $b_0$, which avoids the situation in which a bidder can look up the answer. We used Fibonacci series in our simulation scenario.

To compare our non-parallelizable method with a parallelizable one via simulation, we use the Newton–Raphson method to solve a random function generated by the auctioneer. In this auction, the bidder will compute the derivative of a function advertised by the auctioneer and use the following equation to calculate the feed for the next iteration:

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)},$$

(5.3)

where the initial value $x_0$ is chosen randomly. The bidder will continue the iteration until the $\Delta$ defined by

$$\Delta = |f(x_n) - 0|$$

(5.4)

for a given iteration step is less than the one advertised and acceptable by the auctioneer. $\Delta$ gives us a degree of freedom to match the complexity of this method to the non-parallelizable problem by choosing smaller values for $\Delta$ and comparing the processing time of a bidder to solve both problems. For both methods, a bidder who submits the correct answer before all the others will gain access to the spectrum for the next time interval.

Using the Newton–Raphson method, the time complexity of calculating a root with accuracy of $n$ (that is correlated with $\Delta$) is $\mathcal{O}(F(n) \log n)$, where $F(n)$ is the complexity of calculating $f(x)/f'(x)$. For a single-threaded bidder, $x_0$ is a random number in an initial interval. To compare the single- and multi-threaded bidders, we divide the initial interval and choose a random number ($x_0$) from each smaller interval for each thread. The reason for the performance improvement in terms of iterations comes from picking a random number close to the solution. Against a wide enough bidding field, the chances of one multi-threaded bidder picking a number closer to the solution than all the other single-threaded bidders combined is quite small (for example, they have three threads, i.e., three chances, to pick a close value). So, it can be concluded that multi-threaded bidders do not win all the time, they only have a greater chance of winning than an average bidder.

For the recursive method (that can be $n$th digit of $\pi$ or Fibonacci series with a
random initial value) the complexity of calculation is $O\left(\frac{10^n - 1}{2}\right)$. One can suggest that bidders may look up the correct answer or bidders can record the result of previous auctions to avoid the calculation. One solution to these concerns is to use Fibonacci sequences with different initial values or other recursive problems. Another suggestion is to use the Ackermann function, which can be computed using iterative constructs, but may require unlimited memory.

Via numerical analysis, first we study a wireless network with $N = 21$ CRs as secondary users who wish to access spectrum. One CR will act as the auctioneer and the other 20 will be the bidders (Figure 5.1). In this simulation, we assume all CRs have a single thread for their processing unit. We use the methods above for the auction and for each method the simulation runs for 1000 auctions. For the Newton–Raphson method, a function is chosen randomly for each auction and $\Delta$ is set to 0.0001. The comparison for the winning-bidder histograms can be seen in Figure 5.2. As it can be seen, the winner is chosen uniformly for both methods since all the bidders have a single thread for the processing. For the recursive method (Fibonacci sequences with different initial values), the average number of wins is 50 and the standard deviation is 8.8. For Newton–Raphson method, the average is 50 and the standard deviation is 8.5.

For the second setup, we assume two wireless CRNs. In the first network, one of the 20 bidders has 10 separate threads (Bidder 5). For this multi-threaded bidder, we divide the initial domain of random numbers for the Newton–Raphson method by choosing a $x_0$ for each thread from different intervals. The second network contains all single-threaded CRs. We use the two networks for the auction and for each network the simulation runs for 1000 auctions. For the Newton–Raphson method, a function is chosen randomly for each iteration and $\Delta$ is 0.0001. The winning-bidder histograms can be compared in Figure 5.3. As it can be seen from the figure, Bidder 5 not only wins approximately three times more than its competitors, it also lowers the average spectrum access time for the other CRs. With the multi-threaded network, the average number of wins without considering Bidder 5 is 45 and the standard deviation is 5.6. Bidder 5 wins 133 times. For the second network without a multi-threaded bidder, the mean is 50 and the standard deviation is 7.9.

In the third setup, we use the average computational time to compare methods
using a bidder with a processor with 10 threads. The simulation runs for 1000 auctions and the average computational time for each bidder is measured. As before, Bidder 5 has 10 threads. As it can be seen from Figure 5.4, Bidder 5 has an advantage in terms of computational time in the parallelizable versus the non-parallelizable problem. The average time for the recursive problem is in order of 1000 microseconds and the standard deviation is 30. For the Newton–Raphson method the average time for a winning bidder is in order of 100 microseconds and the standard deviation is 72, and Bidder 5 finds the solution on average faster.

### 5.4.2 Thread Starvation

In this simulation setup, we investigate the impact of the number of threads for a multi-threaded bidder for both methods in terms of average number of iterations. We want to investigate if an auction with all multi-threaded bidders is fair using a parallelizable problem. For 1000 auctions, we measured the average number of

**Figure 5.2.** Comparison of histogram of the winning bidders for two auctions, calculating the $n$th number in Fibonacci series and Newton–Raphson method to solve a random function for 20 bidders.
Figure 5.3. Comparison of histogram of the winning bidders for an auction using Newton–Raphson method to solve a random function for 20 bidders for two sets of CRs, one including a bidder (bidder 5) with 10 threads and the other network with all single threaded CRs iterations for both methods to find a correct solution. As it can be seen in Figure 5.5, for the recursive method the number of iterations does not depend on the number of threads used since that problem is non-parallelizable. A bidder with multiple threads can find a correct solution using the Newton–Raphson method in fewer iterations using 2 to 8 threads. This performance is saturated for 9 threads because of thread starvation. Starvation happens when a thread cannot access the processing unit because other threads are using it. These threads have the same priority and, because of this, they are in contention. That means the bidder is using all of its processing power and we have a resource contention.

5.5 Chapter Summary and Conclusions

In this chapter, we proposed a decentralized auction scheme as a MAC protocol for CRs. This protocol can be applied for a free licensed band without the need for
Figure 5.4. Comparison of the bidders computational time for an auction using Newton–Raphson method to solve a random function and calculating the $n$th number in Fibonacci series for 20 bidders for two sets of CRs, one including a bidder (Bidder 5) with 10 threads and the other network with all single threaded bidders.

constant spectrum sensing. The auctioneer signals the beginning of an auction to the other parties. The bidders or CRs then try to solve a problem that has been set and announced by the auctioneer and the winner is granted the spectrum access. We showed how choosing a non-parallelizable problem is essential for ensuring that the proposed multiple-access algorithm is robust against malicious attacks and also fair for all users. This has been done by comparing the performance of a parallelizable problem to a non-parallelizable one.

The next chapter includes improving security policies and usage of improved database to combat malicious attempt to obtain spectrum access. The overload in terms of time and processing power imposed by using a database implementation needs to be evaluated. The processing delay caused by database calculation and verification must be considered to estimate the time delay needed for a CR to access the wireless channel.
Figure 5.5. Comparison of the two multiple threaded bidders in terms of number of iterations to complete an auction using Newton–Raphson method to solve a random function and calculating the $n$th number in Fibonacci series.
Chapter 6

Blockchain Verification as a Spectrum Access Protocol in Cognitive Radio Networks

In this chapter,\(^1\) we propose a blockchain verification protocol as a method for enabling and securing spectrum sharing in moving cognitive radio networks. The spectrum-sharing mechanism is used as a medium access protocol for accessing wireless bandwidth among competing cognitive radios. We introduce a virtual currency, called “Specoins”, for payment to access the spectrum. An auction mechanism based on a first-come-first-served queue is used, with the price for the spectrum advertised by each primary user in a decentralized fashion. The blockchain protocol facilitates the transactions between primary and secondary users and is used to validate and save each user’s virtual wallet. Also important for mobile networks, the blockchain serves as a distributed database that is visible by all participating parties and any node can volunteer to update the blockchain. The volunteer nodes are called miners and they are awarded with Specoins. We propose diverse methods to exchange the Specoins in order to make leasing possible even by cognitive radios that are not miners. We show the improvement of the proposed algorithm compared with the conventional Aloha medium access protocol in terms of spectrum usage. This difference is investigated using small-scale

\(^1\)The research presented in this chapter has been published in Kotobi and Bílén [2017b, 2018].
fading variation in the wireless channel to compare the performance of our secure method with the conventional medium access used in vehicular communications. The secure blockchain verification protocol is not only secure but also outperforms the conventional system in moderate cases of small-scale fading. In the case of severe small-scale fading, the blockchain protocol will outperform the conventional system if multipath diversity is not used.

6.1 Chapter Introduction

The current paradigm of fixed wireless spectrum assignments is a major challenge facing the ever-growing demand for mobile wireless communications. To address the desire of mobile device users to be connected everywhere, at all times, and for any application, more spectrum bandwidth and/or more efficient usage of that bandwidth is needed. Many studies have shown that fixed spectrum allocations are wasteful because the license holders (which we call primary users) do not utilize their full spectrum allocation continuously (see references within Kotobi et al. [2015]). One method for addressing the spectrum scarcity problem, for instance in a wireless sensor network [Sani and Vosoughi, 2015b; Kotobi and Bilén, 2017b], is to introduce secondary users that opportunistically monitor the spectrum and then transmit their data whenever the spectrum is idle [Lal and Mishra, 2003]. Security concerns in such sharing schemes and their corresponding medium access protocols are current thrusts of particular research interest [Shukla et al., 2006].

The remainder of this chapter is organized as follows. In Section 6.2, we investigate the concept of a blockchain as a distributed database used to facilitate the use of a virtual currency and as a security measure to validate transactions. In Section 6.3, we then define our system model and blockchain protocol to validate our multiple access protocol. In Section 6.4, we describe simulations and compare our findings with current medium access protocols found in the literature. In Section 6.5, we discuss our results and present conclusions.


6.2 Background

Blockchains are decentralized databases that are inherently resistant to modification of the data contained within them. Recently, they have been proposed as a way to secure online transactions, with the most significant usage to date being Bitcoin virtual currency. The database is authenticated through the collaboration of self-interested parties. The initial use of this technology has been to share and send virtual currency safely and anonymously between users without the use of a third party like a credit card company or bank.

Let us examine how blockchains work via an example. Assume that Alice wants a service from Bob in exchange for virtual currency. After agreeing on the details of the transaction, Alice’s virtual wallet initiates the change in the blockchain. This results in a reduction in virtual currency in Alice’s virtual wallet and an increase in Bob’s virtual wallet. To validate this, other users check if Alice’s virtual wallet has enough funds. Then, after validation, miners will start to make a new block to be added to the chain. This will lead to an updated blockchain.

To update the blockchain, the hash value of each transaction that occurred during a specific interval must be added into a Merkle tree. This combined hash value, with the hash value of the previous block’s header and a timestamp, make up the new block’s header. Then, the header become part of a puzzle that can be solved only by trial and error. A miner who finds the answer sooner is awarded with virtual currency and creates the new blockchain [Nakamoto, 2008].

In this chapter, we take advantage of the open-source nature of blockchains to propose a secure distributed medium access protocol for CRs to lease and access available wireless channels. In our proposed scheme, every spectrum leasing transaction is verified and cleared, then stored within a block. The new block is linked to the previous block, forming a chain. Each block records the transactions of potentially thousands of users in a manner that the records cannot be altered by a malicious user or users.

The main features of blockchains are as follows:

1. Distributed: Having a distributed database makes the system robust against hacking attacks. Hacking a central database is one of the main vulnerabilities of current online systems. With blockchains, there is no official centralized
copy, and no user is trusted more than others.

2. Public: There is no central authority to validate or record the data and transactions, which results in a more transparent system without loss of security.

3. Secure: The distributed database is encrypted via a two-key system, i.e., private and public keys. The difficulty of the encryption process is rewarded via virtual currency.

4. Permissionless: Since there is no single trusted user as the central authority, applications can be added to the overall system without seeking the approval of other users.

In this chapter we employ all of these features. First, we propose a distributed medium access protocol that is open to any secondary user. Second, the protocol has no central authority. Third, the protocol employs a secure algorithm that stops malicious users from gaining access to spectrum without payment. Fourth, we use the permissionless property to address the security of the protocol. We propose a virtual currency, which we call “Specoins”, for use in transactions and as a reward for mining to update the blockchain. These Specoins can be used by secondary users to lease available spectrum owned by a primary user.

6.3 System Model and Blockchain Definition

Secondary users, which have no spectrum allocation, must access the spectrum opportunistically. Hence, the spectrum allocation and monitoring problem is defined as finding an optimal collision-free method to access the unused spectrum. Policing the CRs so that they follow the protocol and act cooperatively is an important element of any proposed algorithm.

6.3.1 System Model

We present a network consisting of primary and secondary users. In our wireless system, primary users are spectrum license holders and can lease their allocated
spectrum to increase spectrum efficiency as well as generate additional revenue. Primary users are CRs 1, 2, ..., P with half-duplex transceivers, meaning they can either transmit or receive at any instant of time on a specific wireless channel. The frequency spectrum is divided into R orthogonal channels 1, 2, ..., R that are symmetric and assumed to be error-free. In our simulation, time is divided into $T_2, ..., T_n$ equal-length slots for simplicity and $T_1 \neq T_i$ represents overhead. Further, we assume that a common control channel is available for exchanging control messages between primary and secondary users. This channel is used to advertise the available channels and the auction information needed to access it. The control channel is also used to synchronize the timebases of the CRs. When the control channel is busy, e.g., when auction availability and information regarding it is being advertised, time synchronization can be achieved via other methods, such as a local GPS receiver. Our medium access control frame (Figure 6.1) consists of information exchange and an allocation period as opposed to conventional overhead with an extra sensing period.

A CR that uses its processing power to update the blockchain will be rewarded in Specoins, which can then be used to lease available spectrum from a primary user. The protocol also provides a mechanism for converting between a real currency and Specoins, and vice versa. This allows a cognitive secondary user with limited processing power to obtain Specoins in lieu of updating the blockchain. The currency conversion mechanism helps CRs in two major scenarios that occur in simulations and in practical applications. In the first scenario, if a CR has a large amount of data to transmit and does not have enough Specoins to lease the spectrum it needs (i.e., it has not earned enough by updating the blockchain), it loses the opportunity to transmit. In the second scenario, a CR does not have sufficient processing power, battery, and/or time to update the blockchain and, as a result, also cannot transmit its data.

### 6.3.2 Blockchain Usage in Spectrum Access

In the previous section we defined two methods for secondary users to obtain Specoins: exchanging real currency for them and/or preparing and updating the blockchain. The main purpose of the blockchain is to record all transactions be-
Auc
Proc
Auc
Alloc
Data Transmission Time

Figure 6.1. Time frame for CR to access the available spectrum.

tween secondary users, such as exchanging currency; mining and updating the blockchain; and leasing available spectrum through an auction.

To compare our proposed blockchain scheme with existing multiple access techniques for accessing wireless channels, we first need to develop metrics used to evaluate their performance. We use an approach similar to Pawelczak et al. [2005] to define a metric to evaluate and compare our scheme with existing protocols. The system requirements that need to be addressed for our spectrum access scheme using a Specoin blockchain include:

1. Scalability: Adding additional secondary users should not decrease the quality of service of the network significantly. More primary users means more available channels for spectrum sharing and, thus, improved quality of service. In general, it means that our spectrum access method is able to support a large number of primary and secondary users without impacting the quality of service.

2. Power Efficiency: Our scheme supports power efficiency by allowing the CRs to buy Specoins rather than participating in blockchain building or verification. Buying the Specoins also significantly reduces the data transmission between CRs that are sensitive to power constraints.

3. Security: Secondary users' permission to access the spectrum must be verified. Malicious users cannot access the network without participating in an auction or paying fees. Other forms of security concerning encrypting the transmitted messages are addressed in a network layer.

4. Distributed Topology: By allocating the security verification and authentication to individual users as miners, the need for a central-authority node is
removed. This results in no firewall requirement to protect single-entry-point attacks such as denials of service.

5. Accessibility: By introducing direct exchanges and mining as methods to earn Specoins, the network can accommodate any type of CR as a secondary user competing to access the unused spectrum. Blockchain accessibility by all users allows users to validate bids.

6. Multicasting: A primary user does not need to advertise its available spectrum to a single entity. The need for a middle man is removed by introducing a blockchain registry. The auction advertisement is available to any interested secondary user.

In the next section, we compare our proposed medium access protocol to conventional systems via simulation. Each simulation happens for 1000 iterations and the average of the results are presented in the figures. For moving vehicles, small-scale fading results in rapid variations in the received signal. In the next section, we investigate this effect on our secure spectrum sharing scheme.

6.4 Simulation Results

In this section, we first introduce the simulation setup. Then, we overview the simulation results and highlight the proposed protocol’s advantages and drawbacks. All variables used in this section are provided in Table 6.1.

6.4.1 Method for Spectrum Allocation

Assume that a secondary user $S_1$’s wallet, $W_s^1$, has enough Specoins to lease spectrum, $A_1$, advertised by a primary user $P_1$. First, a puzzle mechanism similar to the one introduced in Kotobi et al. [2016] is advertised by the primary user, and if the secondary user wins the auction, then the spectrum $A_1$ is leased by the primary user $P_1$ to the secondary user $S_1$ and the transaction is approved. Then, in a process similar to how the Bitcoin blockchain works, $P_1$ will generate the new block and broadcast it to all available miners (which could include $S_1$). The first miner, $M_1$, that makes the hash will be granted the ability to update the blockchain. $M_1$
Table 6.1. Summary of variables used in Chapter 6.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_i$</td>
<td>Available bandwidth from the $i$th primary user</td>
</tr>
<tr>
<td>$B_i$</td>
<td>Blockchain built in $i$th iteration</td>
</tr>
<tr>
<td>$C$</td>
<td>Cost function</td>
</tr>
<tr>
<td>$C_k$</td>
<td>Cost function to update blockchain for iteration $k$</td>
</tr>
<tr>
<td>$M_i$</td>
<td>$i$th iteration of updated blockchain</td>
</tr>
<tr>
<td>$n_p$</td>
<td>Number of primary players</td>
</tr>
<tr>
<td>$n_s$</td>
<td>Number of secondary players</td>
</tr>
<tr>
<td>$P$</td>
<td>Total number of players in network</td>
</tr>
<tr>
<td>$P_i$</td>
<td>$i$th primary user with available spectrum to share</td>
</tr>
<tr>
<td>$Q^p_i$</td>
<td>Power consumption by $i$th primary user</td>
</tr>
<tr>
<td>$Q^s_i$</td>
<td>Power consumption by $i$th secondary user</td>
</tr>
<tr>
<td>$R$</td>
<td>Total number of orthogonal channels in network</td>
</tr>
<tr>
<td>$S_i$</td>
<td>$i$th secondary user or miner</td>
</tr>
<tr>
<td>$T$</td>
<td>Total number of time slots in network</td>
</tr>
<tr>
<td>$T^p_i$</td>
<td>Transmitted packets by $i$th primary user</td>
</tr>
<tr>
<td>$T^s_i$</td>
<td>Transmitted packets by $i$th secondary user</td>
</tr>
<tr>
<td>$W^p_i$</td>
<td>Wallet of $i$th primary user</td>
</tr>
<tr>
<td>$W^s_i$</td>
<td>Wallet of $i$th secondary user</td>
</tr>
</tbody>
</table>

will encrypt the transaction with its private key and update the blockchain $B_1$. For its effort, it will be rewarded in Specoins according to a cost function $C$. The cost function here is a function of time because, as time passes, the updating of the blockchain will require more and more processing power and time. Here, we define a simple cost function:

$$C_i = C_{i-1} + C_0,$$

where $C_0$ is set according to the number of participating secondary and primary users and $i$ represents the number of transactions so far.

Specoins also can be exchanged between users by updating the blockchain. The party that receives the Specoins will advertise the update of blockchain, $B_i$, and the winning miner $M_i$ will gain $C_i$ according to Equation 6.1. Before any exchange or leasing, a cognitive user decrypts the blockchain using its private key and confirms the availability of funds claimed by the CR that desires spectrum access.

In our simulation, we assume that there are $n_p$ available primary users to
provide enough available spectrum that comparison between two systems is fair. For each step we increase \( n_s \) by 1 with \( n_s = 10 \) initially and satisfy \( P = n_s + n_p \), ensuring \( n_p \) provides enough primary users that statistically there is not a lack of available spectrum. For each simulation campaign, the number of time slots, \( T \), and orthogonal wireless channels, \( R \), are the same for the conventional system and our proposed system.

In the simulations, we assume an Aloha medium access protocol as our conventional scheme. The fading coefficients change based on a Rayleigh distribution and in a setup similar to Kotobi [2011]. According to the system model defined in Section 6.3.1, we calculated the transmitted packets for all CRs and their power consumption to make the blockchain and perform the wireless transmission. In a wireless environment with a poor fading condition, our results show that, although consuming more power, our proposed system transmits more packets compared to a conventional system using Aloha medium access (Figure 6.2). In more severe fading conditions, our system performs almost as well as the conventional system when there are few participating secondary users, but it outperforms as more users join the network, as shown in Figure 6.2, where the beginning and ending points are shown with format: (Number of CRs, Packets Transmitted, Power Consumed).

To more broadly investigate the impact of fading and secure spectrum sharing, we altered the fading parameters drastically in Figure 6.3. In this simulation setup, similar to one introduced in Kotobi [2011], the small-scale fading is varied with the normalized multipath fading coefficient changing from 0.2 to 1. In the first setup, the conventional multiple access method does not use multipath fading diversity gain and, as result, our secure proposed system outperforms the conventional system both in terms of power consumption and packets transmitted (Figure 6.3). Using multipath fading to provide diversity gain (similar to Kotobi [2011]), will result in improved performance for the conventional system in terms of both power consumption and packets transmitted. In Fig. 6.3 we see that the conventional system can transmit more packets with lower power consumption for the case of severe fading when the normalized fading coefficient is more than 0.7. As expected, since we are using orthogonal channels in our system, we do not obtain a diversity gain in our proposed system due to multipath fading. In Figure 6.3 the beginning and ending points are shown with format: (Fading Coefficient,
Figure 6.2. Performance comparison of data transmitted versus power consumption and the number of cognitive radios for conventional and proposed wireless systems in severe and moderate fading condition.

Packets Transmitted, Power Consumed).

6.4.2 Algorithms

In our simulations, we assume that CRs are following three main algorithms for securing their spectrum access. First, a secondary and primary user agree on a price for an available spectrum resource. Then, the availability of funds from the secondary user will be checked. If the secondary user has sufficient funds it will be granted the available spectrum resource; otherwise, it will be flagged as a malicious user. After approval of the transaction, then $A_j$, which is the spectrum band to be leased, is removed from the available spectrum pool. This eliminates the probability of collision in our proposed algorithm. This procedure is documented in Algorithm 6.

Second, after verifying the transaction can proceed between primary and sec-
Figure 6.3. Performance comparison of data transmitted versus power consumption and the fading coefficient for conventional and proposed wireless systems with only five cognitive radios in both systems and with random number of available orthogonal wireless channels (seven for this simulation) with and without using multipath fading for diversity.
and more computationally expensive mining, here we reset the blockchain after a certain amount of time (e.g., daily). With Bitcoin, the total available virtual currency is limited and, as more miners participate, the increasing complexity of the hash generation acts as a natural moderator to the Bitcoin value. However, we do not require that feature, rather we prefer to limit overall complexity in hash generation, so we elect to periodically reset the blockchain. The blockchain reset procedure is shown in Algorithm 8. In performing a reset, a miner will put the current balances of all CRs into a new block $B_{t+1}$.

Algorithms used in this chapter can be found in the following:

For assigning a new spectrum, we use Algorithm 6.

**Result:** How a secondary user $S_i$ accesses an unused spectrum $A_j$ owned by a primary user $P_k$.

**Initialization**

```
while $A_j$ is not used do
    Advertise $A_j$ as one of the available spectrum
    if $W_i^s > C_i(A_j)$ then
        $S_i \leftarrow A_j$ Request to update $B_t \leftarrow B_{t+1}$
        Remove $A_j$ from the available spectrum pool
    else
        Remove $S_i$ from the bidding pool
    end
end
```

**Algorithm 6:** Secure spectrum allocation.

For mining a new blockchain, we use Algorithm 7.

**Data:** Block $M_t$

**Result:** How a miner, $S_k$, updates the $t + 1$th iteration of blockchain, $B_{t+1}$.

**Initialization**

```
while hash of $M_{t+1}$ is not verified do
    Advertise new transaction $S_i \leftarrow A_j$
    with $C(A_j)$
    if hash of $M_{t+1}$ is correct then
        $S_t \leftarrow C(B_{t+1})$
    else
        Remove $S_t$ from the bidding pool
    end
end
```

**Algorithm 7:** Updating the blockchain.
For updating the blockchain and making a new one, we use Algorithm 8.

**Data:** Blockchain \( B_t \)

**Result:** How a miner, \( S_m \), removes the unused transaction of \( B_t \)

**Initialization**

\[
\text{while hash of } B_{t+1} \text{ is not verified do}
\]

Advertise compressing \( B_t \)

\[
\text{if hash of } B_{t+1} \text{ is correct then}
\]

\[ S_m \leftarrow C(B_{t+1}) \]

\[
\text{else}
\]

\[ \text{Remove } S_m \text{ from the bidding pool} \]

\[
\text{end}
\]

\[
\text{end}
\]

**Algorithm 8:** New compressed blockchain.

### 6.4.3 Comparing the Results

As can be seen in Figure 6.2, for any number of secondary users our proposed algorithm outperforms the conventional system in terms of data transmitted. This increase in throughput comes at a cost of higher power consumption, which can be critical for a CR. Here, we can see a tradeoff between the expensive spectrum and the ability of wireless devices to store power. The same points are valid for the worse fading condition in Figure 6.2. Here, the improvement in terms of throughput does not start as more CRs join the network. It can be viewed as a free market in the sense that, with more secondary users participating, the new system can outperform the random access and opportunistic nature of a conventional multiple access system, which performs well under good wireless conditions and limited number of users.

### 6.5 Chapter Summary and Conclusions

In this chapter, we proposed using blockchain as a decentralized database to verify and secure spectrum sharing between mobile cognitive radios. This medium access protocol can outperform current conventional systems in sharing available unused spectrum under both moderate and severe fading conditions. This method can be used to access available licensed spectrum without the need for constant spectrum
sensing. Here, we focused on fading as a single parameter to distinguish different wireless channels. We have also investigated the impact of multipath small-scale fading and, by using diversity to improve the performance of the conventional system, we showed that conventional system may be able to outperform our secure system in terms of power consumption.

In our scheme, the primary user signals the beginning of an auction to the other parties. The winning bidder(s) use Specoins to buy that spectrum. Secondary users can earn Specoins by making the blockchain or through direct exchange. All transactions are recorded in the blockchain and updated by miners. This blockchain is then used to validate any transactions. We have shown how our proposed multiple access scheme can improve and secure leasing of spectrum provided by a license holder. Our scheme is public and, because it has a permissionless property, it is secure against single-point attacks. Studying the impact of other parameters of a wireless channel is a future research direction. Another future research direction is mitigating the issues related to higher power consumption rates when there is a limitation in resources (e.g., battery, memory, processing power, etc.).
Conclusions and Future Work

7.1 Conclusion

7.1.1 Informed CRs

Data sources for CRNs have generally only included the properties of the wireless channel. In this dissertation, we introduced an informed CR that used additional relevant data sources (among them, social media, like Twitter) as indicators of a dynamically changing environment. By applying these new data sources, we can build predictive algorithms for the network load of the wireless network that increase the network throughput. We call such a radio a data mining-informed cognitive radio.

Traditional game strategies for CRNs generally only include static non-cooperative players. To improve the perceptor of the informed CR, we showed that more efficient CRNs can be constructed by modeling more realistic dynamic players with various goals that lead to different strategies. First to model realistic CRs, we introduced an altruistic cognitive player to monitor and police the network. A dynamic greedy player and vigilante player in each cell are used to study the cyclic behavior of a game to maximize the throughput of greedy and cooperative (non-vigilante) players, respectively. In our simulations, without loss of generality we assumed that the network is divided into cells containing the same number of nodes. We assumed a static vigilante player because any cooperative player can sense its throughput and follow an altruistic strategy. Second to im-
prove the CR’s strategy, we studied the correlation between the number of players in a cell and the aggression factor of a vigilante player with the greedy player’s throughput. The result is used in our proposal of perceptor for the informed CR using a Stackelberg game. We assessed the algorithm using an M/D/1 queue.

We provided new and improved algorithms for CRNs using the following features:

- **Observation**: if the CR can access feedback information whether it is sent by another CR or is collected by itself;
- **Intelligence**: if the CR can use its observation to develop a “better” transmission strategy; and
- **Adaptability**: if the CR can perform consistently in dynamically changing environments.

To evaluate the perceptor of the informed CR, we studied the spectrum sharing cooperation by modeling the spectrum and users as an M/D/1 queue, with the goal of encouraging the cognitive players to cooperate. We have focused on the system model that, despite the desire to maximize their individual utilities, the cognitive players find it beneficial to cooperate. We have formulated a Stackelberg game in which the primary license holder and secondary user are leader and follower, respectively, and studied how the leader can influence the follower’s decision of participating in the game by varying the cost function. Additionally, we observed that a pricing scheme can be employed to improve all utilities to the social optimality of an M/D/1 queue. In this scenario, cognitive users can employ the cost function to decide how much of the spectrum is used by primary users and secondary users.

### 7.1.2 Fair MAC

To improve the MAC used by informed CRs, we proposed a decentralized auction scheme for CRs to share available unused spectrum. This method can be used to access a free licensed band without the need for constant spectrum sensing. The auctioneer signals the beginning of an auction to the other parties. The bidders then try to solve a problem that has been set and announced by the auctioneer
and the winner is granted the spectrum access. We showed how choosing a non-
parallelizable problem is essential for ensuring that the proposed multiple-access
algorithm is robust against malicious attacks and also fair for all users. This has
been done by comparing the performance of a parallelizable problem to a non-
parallelizable one. The proposed MAC guarantees fairness among the CRs. This
will lead the informed CRs that can be cooperative or non-cooperative to use it.

7.2 Security

Security is one of the primary issues in wireless communications and needs to be
addressed. We introduced using blockchain as a decentralized database to ver-
ify spectrum sharing between cognitive radios. The secured MAC outperforms
the current conventional system in both moderate and severe fading conditions
to share available unused spectrum. This method can be used to access available
licensed spectrum without the need for constant spectrum sensing. Here, we fo-
cused on fading as a single parameter to distinguish different wireless channels.
We have also investigated the impact of multipath small-scale fading, and by us-
ing diversity to improve the performance of the conventional system we showed
that conventional system may be able to outperform our secure system in terms
of power consumption.

In our proposed MAC, the primary user signals the beginning of an auction
to the other parties. The winning bidders use Specoins to buy that spectrum.
Secondary users can earn Specoins by making the blockchain or through direct
exchange. All transactions are recorded in the blockchain and updated by miners.
This blockchain is then used to validate any transactions. We have shown how our
proposed multiple access scheme can improve and secure leasing of spectrum pro-
vided by a license holder. Our scheme is public and, because it has a permissionless
property, it is secure against single-point attacks.

7.3 Future Research

A future direction is to study the impact on performance of full and partial knowl-
dge of the game strategies for all players. The partial knowledge is a more realistic
study of cognitive radio to be used for wireless transmission. The throughput used by a vigilante player to make the greedy player migrate or cooperate needs to be studied to assess the performance accurately. The complexity of our network can be investigated by modeling it with an embedded Markov chain using an approach similar to that in de Boer [2000], which investigated consecutive loss in a simple queue. By introducing cells into their scheme, one can use an approach similar to the one presented in that work to study large networks. Naturally, computational complexity will increase significantly if cognitive radios act in a strategy that is between greedy and hybrid. Investigating these tradeoffs is left as future work.

While our methods for medium access guarantees fair access, there is still need for investigating the role of overload imposed by a distributed database [Tootaghaj et al., 2015; Farhat et al., 2016]. Future directions include improving security policies and usage of an improved distributed database in terms of accessibility to combat malicious attempts to obtain spectrum access. The overload in terms of time and processing power imposed by using a database implementation needs to be evaluated. The processing delay caused by database calculation and verification must be considered to estimate the time delay needed for a cognitive radio to access the wireless channel.

For the secure auction, studying the impact of other parameters of a wireless channel, for example the number of CRs supported in the network, is another future research direction. Combining all proposed MAC and security algorithms and evaluating the performance of the system will require simulation campaigns to investigate the power and packet requirements for these new systems. These additional power and data transmission requirements will decrease the efficiency of the new system and need to be accounted for the system design. Comparing them to conventional systems is another future research direction.
Bibliography


de Boer, P. (2000), *Analysis and Efficient Simulation of Queueing Models of Telecommunication Systems*, Centre for Telematics and Information Technology University of Twente.


Dwork, C., and M. Naor (1992), Pricing via processing or combatting junk mail, *Advances in Cryptology (CRYPTO92 Springer Berlin Heidelberg)*, pp. 139–147.


Krzanowski, R. (2006), Burst (of packets) and burstiness, Montreal, July, in **66th IETF Meeting**.


Zhang, C., X. Wang, and J. Li (2009), Cooperative cognitive radio with priority queueing analysis, in *2009 IEEE International Conference on Communications*, pp. 1–5, IEEE, doi:10.1109/ICC.2009.5198858.


Vita
Khashayar Kotobi

KHASHAYAR KOTOBI received his B.Sc. in Electrical Engineering from University of Tehran and his M.Sc. in Telecommunication from Delft University of Technology. His research interests include machine learning, deep learning, data science, cognitive radios, and wireless communications.