

Investigation of Security and Spectrum Management Issues in Cognitive Radio Aided by Machine Learning

Thesis by

Shaher Suleman Mousa Slehat

In Partial Fulfillment of the Requirements of the Requirements for the Degree of
Doctor of Philosophy

University of Technology Sydney
Faculty of Engineering and Information Technology

Supervisor

Zenon Chaczko

Autumn, 2020

CERTIFICATE OF ORIGINAL AUTHORSHIP

I, Shaher Slehat declare that this thesis, is submitted in fulfilment of the requirements for the award of Phd, in the School of Electrical and Data Engineering/ Engineering and Information Technology at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise reference or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis. This document has not been submitted for qualifications at any other academic institution. This research is supported by the Australian Government Research Training Program.

Production Note:

Signature: Signature removed prior to publication.

Date: 10/01/2020

Acknowledgments

First and foremost, i would like to thank Allah the Al-Mighty for blessing me with the will, dream, and the resource to complete my PhD work.

My appreciation and special thanks are also due to my supervisor Dr. Zenon Chaczko for his invaluable support and guidance. He has indeed been an enthusiastic supporter of me work, providing a nearly unending stream of ideas. And providing me the independence to pursue my interests, and lending me the moral support, to clear the final hurdle. I am forever indebted to him for all his moral support and encouragement. And he always made me go this additional mile to resolve the different issues that lead to this work. i cherish the opportunity to see and learn from his experience and knowledge. His continual insights and patience with me are constantly appreciated.

I would also like to his opportunity to express my appreciations to my co-supervisor, Professor Robin Braun for supporting me throughout this work. Through this research, my grateful thanks are also due to the librarians of UTS main librarians who helped me in one way or

other both efficiently and courteously.

I also wish to thank all my friends and fellow participants who have supported and helped me over the last few years: Dr. Pakawat Papatwibul and Dr. Anup Kale for their help in difference ways and from time to time.

Last but no the least, I wish to give special thanks to my family, Mr. Suleman Mousa Slehat, Ms. Seeta Helal , my brothers, and my sisters, for their massive support and all of the sacrifices that the have made on my behalf. My parents constantly gave me continual support and tried to provide me with the best education they can tolerate. They have been an important leading force to promote me behind this PhD research

Abstract

Cognitive Radio (CR) is an intelligent and adaptive radio and network technology that allows transceivers to sense available frequency spectrum and change its parameters, to switch to available channels(frequency bands) without interruption to other connected transceivers.

It is primarily a technology to resolve spectrum scarcity problems using Dynamic Spectrum Access (DSA). The potential aspects and applications of Cognitive radio are far superior to DSA alone. CR abilities and CR reconfiguration abilities are essential components for electronic warfare (communications). It provides capabilities for developing and deploying advanced anti-jamming methods, by assisting in the development of advanced intelligent, self-reconfiguration methods to alleviate the effects of jamming.

This thesis examines the effects of jamming and other attacks on Cognitive Radio Networks and provides methods and processes to overcome those effects. Cognitive Radio architecture simulation was applied so that policies and their application correlate to Cognitive Radio jamming and anti-jamming issues. Simulation is employed for test-

ing Multi-Armed Bandit and machine learning strategies/solutions as shown by this thesis. The central part of the thesis is the mitigation of jamming outcomes on Cognitive Radio Networks by using proactive steps to increase communication robustness and contentiousness. The thesis utilizes game theory (i.e. the Multi-Armed Bandit problem) and protection using Machine Learning (ProML) design for analyzing jamming behavior on Cognitive Radio systems. MAB experiment show MAB approach is effective against random attack, whereas, the proposed machine learning has its own merits to overcome constant and reactive jamming.

Contents

Acknowledgments	iv
Abstract	vi
Nomenclature	xvii
1 Introduction	3
1.1 Research Gap in Anti-Jamming Strategies	8
1.2 Motivations and Research Problem	9
1.3 Research Significance	9
1.4 Objective and Aims of Research	10
1.5 Research Hypothesis	10
1.6 Research Question	11
1.7 Research Contribution	11
1.8 Structure of Thesis	11
2 Literature Review	17
2.1 Background of Cognitive Radio	17
2.2 How Does Cognitive Radio Work?	20
2.3 Advantages of Cognitive Radio	21
2.4 Cognition Capability of a Cognitive Radio	21
2.4.1 Spectrum Sensing	22
2.4.2 Spectrum Analysis	23
2.4.3 Spectrum Decisions	25
2.4.4 Reconfigurability of Cognitive Radio	26
2.4.5 Spectrum Mobility	27
2.5 Cognitive Radio Spectrum Sensing	29
2.5.1 Cognitive Radio Spectrum Sensing Basics	29
2.5.2 Kinds of Cognitive Radio Spectrum Sensing	30

2.6	Definition of Cooperative Spectrum Sensing	31
2.7	Application of Cognitive Radio	32
2.8	Architecture of the Cognitive Radio Network	32
2.8.1	Primary Network	34
2.8.2	Cognitive Radio base station	35
2.8.3	Cognitive Radio user	35
2.8.4	Spectrum broken	35
2.8.5	Infrastructure Based Network (Centralized Cognitive Radio Networks)	37
2.8.6	Ad-hoc Network (Distributed Cognitive Radio)	39
2.8.7	Mesh Architecture	40
2.9	The Application of Cognitive Radio Networks	41
2.9.1	Mesh Cognitive Radio Networks	41
2.9.2	Public Safety Networks	42
2.9.3	Catastrophe Relief and Emergency Networks	43
2.9.4	Battleground Military Networks	45
2.9.5	Leased Network	46
2.10	Security of Cognitive Radio	47
2.10.1	Traditional Threats	49
2.10.2	New Types of Threats in Cognitive Radio	51
2.10.3	Layers Attacks on Cognitive Radio Networks	55
2.10.3.1	Physical Layer Attacks	56
2.10.3.2	Link Layer Attacks	58
2.10.3.3	Network Layer Attacks	60
2.10.3.4	Transport Layer Attacks	61
2.10.4	Related Work and History of Multi-Armed-Bandit Problem	61
2.10.5	Related Work for Jamming Attack in Cognitive Radio	62
2.10.5.1	Work in Jamming Attacks	62
2.10.5.2	The Theoretical Participation	63
2.10.5.3	The Experimental Participation	64
2.10.5.4	The Game-theoretical participation	65
2.11	Multi-Armed Bandit Strategies	68
2.11.1	Upper Confidence Bound (UCB)	68

2.11.2	KL-Confidence Bound (KLUCB)	69
2.11.3	Thompson Sampling	71
3	Theoretical Apparatus	73
3.1	Game Theory	73
3.2	Multi Armed Bandit	73
3.2.1	Stochastic Bandit Problem	76
3.2.2	Adversarial Bandit Problem	88
3.2.3	Markov Bandits	91
3.3	Investigation Strategies	91
3.3.1	Random Selection	95
3.3.2	Greedy Selection	95
3.3.3	ϵ -Greedy Selection	97
3.3.4	Boltzmann Exploration	99
3.3.5	Upper-Confidence-Bound Arm Selection	100
3.3.6	Thompson Sampling Strategy	102
4	Methodology	107
4.1	Introduction	107
4.2	The Communication model in Cognitive Radio	107
4.3	The Multi-Armed Bandit Model in Cognitive Radio	108
4.4	Proposed method	110
4.4.1	Multi-Armed Bandit	110
4.5	Multi Armed Bandit Policies	111
4.5.1	Adaption Upper Confidence Bound (UCB)	115
4.5.2	Adaption KL-UCB (Kullback-Leibler Upper Con- fidence Bound)	116
4.5.3	Adaption Thompson Sampling	118
5	Experimental Work	119
5.1	Design of Experiment	120
5.2	Multi- Armed Bandit (MAB) Strategies	121
5.3	Result and Discussion	123
5.4	Upper Confident Bound	127
5.5	Kullback-Leibler Upper Confidence Bound (KLUCB)	135
5.6	Thompson Sampling (TS)	144

5.7	ProML: A Method for Cognitive Radio Jamming Attack Simulation and Protection Using Machine Learning Approach	155
5.7.1	Background	156
5.7.2	ProML Approach	158
5.7.3	Experimental Simulation	165
6	Action Research	171
6.1	The Design for Competing Cognitive Radio Networks . .	174
6.1.1	Multi-armed Bandit Model for Competing Cognitive Radio Network	175
6.2	Algorithm 1 (Lai and Robbins Algorithm)	177
6.3	Algorithm 2 (Upper Confidence Bound Algorithm)	182
6.4	Algorithm 3 (Thompson Sampling Algorithm)	187
6.5	Main Challenges of WiFi Communication	192
6.5.1	Channel Interference	192
6.5.2	Channel Congestion	193
6.5.3	Jamming the Network	194
6.6	Wi-Fi Analysis Tools	195
6.7	Analysis of Wi-Fi Challenges With The Tools	196
7	Conclusion and Future work	205
7.1	Outline of Contributions and Main Findings	206
7.2	Future Work	209
	Bibliography	211

List of Figures

2.1	Cycle of Cognitive Radio, Adapted from (Khattab et al., 2013)	22
2.2	Spectrum Holes, adapted from (Yücek and Arslan, 2009)	24
2.3	Cognitive Radio Network Architecture	33
2.4	Centralized based Cognitive Radio, adapted from (Khattab et al, 2013)	39
2.5	Distribution of Ad hoc Cognitive Radio, adapted from (Khattab et al., 2013)	40
2.6	Mesh Cognitive Radio Architecture adapted from (Chen et al., 2008)	41
2.7	Mesh Cognitive Radio Network	42
2.8	Public Safety Network	44
2.9	Catastrophe Relief and Emergency Network , adapted from (Oliveira et al., 2011)	45
2.10	Battleground Military Network	46
2.11	Leased Cognitive Radio Networks	47
3.1	Testing Resulting of Strategies (Raja, 2016)	105
4.1	Transmission of Opportunity in Slotted Multi-channels Spectrum	108
4.2	Centralized and Distribution Multi-Player Multi Armed Bandit, adapted from (Gwon et al., 2013)	110
4.3	Different Ways to Minimize Fuel Consumption	114
5.1	Design of experiment, adapted from (Bahrak et al., 2012)	121
5.2	Results for scenario 1 MatLab Environment	124
5.3	Results for scenario 2 MatLab environment	125
5.4	Results for scenario 3 MatLab environment	126

5.5	Environment with Jamming Level Zero Using Python Environment (Jupyter Notebook)	128
5.6	Environment with Jamming Level One Using Python Environment (Jupyter Notebook)	130
5.7	Environment with Jamming Level Two Using Python Environment (Jupyter Notebook)	132
5.8	Environment with jamming Level Three Using Python Environment (Jupyter Notebook)	134
5.9	Environment with Jamming Level Zero Using Python Environment (Jupyter Notebook)	137
5.10	Environment with Jamming Level One Using Python Environment (Jupyter Notebook)	139
5.11	Environment with Jamming Level Two Using Python Environment (Jupyter Notebook)	141
5.12	Environment with Jamming Level Three Using Python Environment (Jupyter Notebook)	143
5.13	Flowchart of the Thompson Sampling Process	146
5.14	Environment with Jamming Level Zero Using Python Environment (Jupyter Program)	147
5.15	Environment with Jamming Level One Using Python Environment (Jupyter Notebook)	149
5.16	Environment with Jamming Level Two Using Python Environment (Jupyter Notebook)	151
5.17	Environment with Jamming Level Three Using Python Environment (Jupyter Notebook)	153
5.18	ProML Schematic Diagram	159
5.19	Features Channel Selection	162
5.20	Random Forests	163
5.21	Classification Process	165
5.22	Average Performance and Accuracy Comparison Between Three most Common Classification Algorithms (Random Forests, Support Vector Machines and Artificial Neural Networks)	167

5.23	Average Performance and Accuracy Comparison Between Three most Common Classification Algorithms (Random Forests, Support Vector Machines and Artificial Neural Networks)	168
6.1	Transmission Prospects in Multi-Channel Band Process	174
6.2	Centralized Control Cognitive Radio Network	176
6.3	Distributed Control Cognitive Radio Network	177
6.4	Algorithm 1 Running before the Simulation Using OMNET++	180
6.5	Algorithm 1 Simulation Running Using OMNET++	180
6.6	Access Point after Applying Algorithm 1 Using OMNET++	181
6.7	Access Point Simulation Showing Packets Dropped Using OMNET++	181
6.8	Performance in Centralized Scenario for 1 Host Using OMNET++	182
6.9	Performance in Centralized Scenario for 4 Hosts Using OMNET++	182
6.10	Upper Confidence Bound Simulation before Running Using OMNET++	184
6.11	Algorithm UCB Simulation Running Using OMNET++	184
6.12	Access Point Simulation Using OMNET++	185
6.13	Access Point Simulation Showing Packets Dropped Using MONET++	185
6.14	Performance in Centralized Scenario for 1 Host Using MONET++	186
6.15	Performance in Distributed Scenario for 4 Hosts Using MONET++	186
6.16	Performance in Centralized Scenario for 4 Hosts Using MONET++	187
6.17	Access Point Simulation Showing Packets Dropped Using MONET++	188
6.18	Performance in Distributed Scenario for 4 Hosts Using OMNET++	189

6.19 Performance in Centralized Scenario for 4 Hosts Using OMNET++	189
6.20 Wi-Fi Channel Allocation in 204 GHz, adapted from (Miucic, 2018)	194
6.21 Wi-Fi Channels using Analysis WiFi Tool	197
6.22 Wi-Fi Channels using Analysis WiFi Tool	197
6.23 Noises on Channel 1 using the Chanalyzer and Acrylic Tools	198
6.24 Noise on Channel 12 using the Chanalyzer and Acrylic Tools	199
6.25 Heatmap of RSSI using the Acrylic Wi-Fi Heatmaps Tool	199
6.26 Heat Map 3D using the Acrylic Wi-Fi Heatmaps Tool .	200
6.27 Heat Map of SNR using the Acrylic Wi-Fi Heatmaps Tool	200
6.28 Heat map of SNR in 3D Using the Acrylic Wi-Fi Heatmaps Tool	201
6.29 Jamming at Channel One using the Chanalyzer Tool .	201
6.30 Jamming in all Channels using the Chanalyzer Tool . .	202

List of Tables

- 1.1 Structure of Thesis Part 1 14
- 1.2 Structure of Thesis Part 2 15

- 5.1 Typical Data-Set Example 160
- 5.2 Expected Outcome 162
- 5.3 Percentage Improvement 169

Nomenclature

16-QAM	16-Quaternary Amplitude Modulation
BPSK	Binary Phase Shift Keying
BSSI	Basic Service Set Identifiers
CPU	Central Processing Unit
CR	Cognitive Radio
DoS	Denial-of-Service
DSL	Digital Subscriber Lines
FPGA	Field Programmable Gate Array
HRRSS	High Relative Received Signal Strength
HWP	Hardware Platform
MAC	Media Access Control
MIMO	Multiple-Input Multiple-Output
MTS	Mobile Telecommunication Services
NCR	Network Cognitive Radio
NIICT	National Institute of Information and Communication and Technology
OA	Optimal Algorithm
OSA	Opportunistic Spectrum Access

ProML	Protection using Machine Learning
PU	Primary Users
PUE	Primary User Emulation
QoS	Quality of Service,
QP-SK	Quaternary Phase-Shift Keying
QPAM	Quaternary Phase Amplitude Modification
RF	Radio Frequency
RFU	Radio Ferquency Uint
RSSI	Received Signal Strength Indication
SDR	Software Defined Radio
SIP	Softwaer Infrastructure Platform
SNR	Signal-to-Noise Ratio
SPU	Signal Processing Unit
SUs	Secondary Users
TCP	Transmission Control Protocol
WLAN	Wireless Local Area Network
WNAN	Wireless Network After Next

