SECURITY ISSUES IN COGNITIVE RADIOS

Shivanshu Shrivastava

TH-1605_10610214

SECURITY ISSUES IN COGNITIVE RADIOS

A

Thesis submitted

for the award of the degree of

DOCTOR OF PHILOSOPHY

By

SHIVANSHU SHRIVASTAVA

DEPARTMENT OF ELECTRONICS AND ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI

GUWAHATI - 781 039, ASSAM, INDIA

APRIL 2017

TH-1605_10610214

TH-1605_10610214

Certificate

This is to certify that the thesis entitled "**SECURITY ISSUES IN COGNITIVE RADIOS**", submitted by **Shivanshu Shrivastava** (10610214), a research scholar in the *Department of Electronics and Electrical Engineering, Indian Institute of Technology Guwahati*, for the award of the degree of **Doctor of Philosophy**, is a record of an original research work carried out by him under our supervision and guidance. The thesis has fulfilled all requirements as per the regulations of the institute and in my opinion has reached the standard needed for submission. The results embodied in this thesis have not been submitted to any other University or Institute for the award of any degree or diploma.

Dated:
Guwahati.

Dr. A. Rajesh
Associate Professor
Dept. of Electronics and Electrical Engg.
Indian Institute of Technology Guwahati
Guwahati - 781 039, Assam, India.

Dated:
Guwahati.

Prof. P. K. Bora
Professor
Dept. of Electronics and Electrical Engg.
Indian Institute of Technology Guwahati
Guwahati - 781 039, Assam, India.

TH-1605_10610214

TH-1605_10610214

To my parents

TH-1605_10610214

TH-1605_10610214

Acknowledgements

First of all, my heartiest gratitude to my supervisors Dr. A. Rajesh and Prof. P. K. Bora. From learning the most initial steps in research to learning critical and analytical reasoning, I learnt everything which led to this thesis from them. They taught me introspection, unbiased assessment, questioning, and criticizing my work. My biggest strength was their confidence in me. One of my major motivations for working hard was that I feared losing that confidence. Their world is externally simple and internally easy, providing an ideal environment for a research student. Their belief in free thinking gives the best opportunities for a student to evolve. They found time and took pain to correct my manuscripts from the busiest of their schedules, incomparable workload, and severely distressed family conditions. Apart from these, they instilled in me an exceptional level of patience and an extreme level of relaxation. Expressing my gratitude to them in words seems impossible to me.

I would like to mention my sincere thanks to my doctoral committee members: Dr. Tony Jacob, Dr. Smarajit Das, and Dr. Benny George for evaluating the progress of my work. Their suggestions were always valuable. I would also thank Dr. P. R. Sahu who was previously associated with my doctoral committee for his significant suggestions. I am specially thankful to Dr. Tony Jacob for one of his random statements during a presentation that motivated me throughout my PhD that "PhD is the beginning of your research life, not the end of your research life." I would like to express my heartiest gratitude to Prof. S. K. Bose for his help and support when I needed it the most. He is one of the most wonderful persons I have met in my life and I have the deepest regards for him. My sincere thanks to the Prof. Ratnajit Bhattacharjee for his valuable guidance on many occasions. I thank Dr. Praveen Kumar for his valuable suggestions at various occasions. My sincere thanks to Dr. B. K. Rai for being a constant support during my PhD period. He helped me during many difficult times in my PhD and I will remain obliged to him. My sincere thanks to Dr. Ribhu Chopra for his help and insightful suggestions on various occasions. I thank all the other faculty members of the department of EEE for their support whenever I needed.

I thank Shri. Sanjib Das for providing excellent computational facilities and helping me in software related issues on many occasions. My thanks to Shri. Utpal Sharma, Shri. M. P. Das, Shri. Pranab Jyoti Goswami, and Shri. Sidananda Sonowal for offering a helping hand whenever I needed and being such jovial people. Special thanks to Shri. Utpal Sharma for educating me about the politics, society,

TH-1605_10610214

and culture of Assam during our casual discussions.

During my PhD, I found really wonderful research mates. I had never expected such sensitive and helping people existing in highly professional research institutes like IITs. My sincere thanks to Dr. S. Padam Priyal for some of the extremely important discussions in my initial days of research. She finished her defense and left during the period I was beginning my research work. In the short period of time, she helped me in some very significant aspects. My sincere thanks to Kuntal bhaiya, Samdarshi bhaiya, Gaurav bhaiya, Rahul bhaiya, Samar bhaiya and Sayantan bhaiya. I had very fruitful discussions with them during my research work. I have no words to thank my friends Murli bhaiya, Vinay Rao, Mridul, Pavan, Karteek, Atul, Vinay Pandey, Brijesh, Parveen, Joshi (Deepak), Sandeep (P) bhaiya, Shashank Sir, Kukil, Sikandar, Anand, Somen, Arijit Sir and Sumantra Sir. Special thanks to Karteek for being my badminton buddy throughout. These guys made my stay at IIT Guwahati memorable. I will cherish the time spent with them. I thank them all for their friendship.

I thank the scenic beauty of IIT Guwahati. I thank the IIT administration for providing excellent sports facilities. I thank the race track, the badminton halls and everyone responsible for their maintenance and making life so enjoyable here. I would like to thank singers and musicians like Mukesh, M. Rafi, Linkin Park, A. R. Rahman and many others. They have a very significant contribution in my PhD. I could not have been able to complete my work without their music.

I extend my thanks to the EEE office and the Academic section for all sorts of administrative helps. Special thanks to Shri. Pradeep Sinha of the Academic section for being so helpful and student friendly. I would like to thank the Ministry of Human Resources and Development (MHRD) for all the supports it provides to the researchers.

My deepest thanks to my parents for their patience. Words cannot describe their sacrifices for me and I cannot put in words my gratitude for them. To my best I can only say that a single word found useful in this thesis belongs to them. My deepest thanks to my other family members for their constant love and support. They are the motivation of my life. Whatever I have done or accomplished is all because of them.

Shivanshu Shrivastava

TH-1605_10610214

Abstract

Cognitive Radio (CR) based spectrum sensing has been identified as an effective measure to combat spectrum scarcity. Individual CR sensing may suffer performance deterioration due to deep fading. Cooperative spectrum sensing (CSS) has been realized as an effective means to counter this problem. CSS is severely affected if some secondary users (SUs) become malicious for their selfish intentions. These SUs are called malicious users (MUs). The objective of this research is suppressing the MUs. We aim at suppressing two types of malicious attacks, namely the spectrum sensing data falsification (SSDF) attacks and the primary user emulation attacks (PUEAs). The first part of the thesis investigates the SSDF attacks. The SSDF attacks are caused when the MUs report malicious data to mislead the CSS system. We propose two schemes to enhance the applicability of the Dixon's statistical outlier detection test in discarding single and multiple malicious data. Simulations reveal that the proposed schemes enhance the performance of the Dixon's test significantly. The proposed schemes are also successful in enhancing its applicability to multiple MU detection. These improvements are obtained without a significant compromise on the complexity of the system. The second part of the thesis investigates SSDF attacks launched in collusion. We design a comprehensive categorization of the collusion attack scenarios. The PU is considered to impose a collision penalty on the SUs on suffering any interference. We derive bounds on the collision penalty to prevent attacks in each scenario. It is verified that the bounds on the collision penalty successfully suppress each of the attacks. The derived bounds are also successful in suppressing the reluctance of the PU in sharing its spectrum for the fear of interference. The Nash equilibrium showing the best strategy for the SUs to obtain the maximum gain from the PU spectrum is also derived. The third part of the thesis investigates the PUEAs in CSS. We aim at suppressing its effects on the SU throughput. We maximize the SU throughput in the presence of PUEAs. Maximizing the SU throughput results to increased interference to

TH-1605_10610214

the PU. We formulate an optimization problem to maximize the SU throughput with a constraint on the interference to the PU. We propose an algorithm based on the Nelder Mead simplex method to solve this problem. Simulations reveal that the throughput of the SU in a CSS system facing PUEAs is maximized. The proposed algorithm is successful in bringing the performance of the PUEA affected CSS system close to an unaffected system in terms of the SU throughput.

TH-1605_10610214

Contents

List of Figures **xix**

List of Tables **xxiii**

List of Acronyms **xxv**

List of Symbols **xxvii**

1 Introduction **1**

1.1 Background . . . 2

1.2 Areas of Research in CRs . . . 4

1.2.1 Signal Propagation . . . 4

1.2.2 Signal Processing . . . 5

1.2.3 Cooperative Spectrum Sensing . . . 6

1.2.4 Security Issues in CSS . . . 8

1.3 Motivations and Problem Statements . . . 11

1.3.1 Problem 1 . . . 11

1.3.2 Problem 2 . . . 12

1.3.3 Problem 3 . . . 12

1.4 Contributions of the Thesis . . . 13

1.4.1 Individual SSDF Attacks: . . . 13

1.4.2 Collusion SSDF Attacks: . . . 13

1.4.3 PUEAs: . . . 13

1.5 Organization of the Thesis . . . 13

1.5.1 Chapter 2 . . . 14

1.5.2 Chapter 3 . . . 14

1.5.3 Chapter 4 . . . 14

TH-1605_10610214

1.5.4 Chapter 5 . . . 14
1.5.5 Chapter 6 . . . 15

2 Security Issues in Cognitive Radios - A Review 17

2.1 Introduction . . . 18
2.2 Basic SS Concepts . . . 18
2.2.1 Energy Detection . . . 18
2.2.2 Cyclostationary Feature based Detection . . . 19
2.2.3 Matched Filter and Waveform based Detection . . . 20
2.2.3.1 Matched Filter based Sensing . . . 20
2.2.3.2 Waveform based Sensing . . . 20
2.2.4 Covariance based Sensing Methods . . . 21
2.2.4.1 Covariance Matrix based Sensing . . . 21
2.2.4.2 Autocorrelation based Sensing . . . 22
2.2.4.3 Eigen Value based Sensing . . . 23
2.3 Security Issues in SS . . . 24
2.4 SSDF Attacks in CR Communications . . . 25
2.4.1 Active Methods . . . 25
2.4.2 Passive Methods . . . 30
2.5 PUEAs in CR Communications . . . 36
2.5.1 Active Methods . . . 36
2.5.2 Passive Methods . . . 39

3 Suppression of SSDF Attacks by Multiple Malicious Users 43

3.1 Objective . . . 44
3.2 System Model . . . 46
3.2.1 Hypothesis Testing for PU Detection . . . 46
3.2.2 Performance Parameters . . . 48
3.2.3 The Uncertainty in SS and the Attack Process . . . 49
3.3 Detection of MUs as an Outlier Detection Problem . . . 51
3.3.1 Grubbs' Test . . . 52
3.3.2 Boxplot Test . . . 54

TH-1605_10610214

3.4 Dixon's Test for Outlier Detection . . . 55
3.4.1 Outlier Factor in the Dixon's Test . . . 56
3.4.2 Calculation of the Critical Value (C_v) . . . 57
3.5 Proposed Method . . . 59
3.5.1 Scheme 1: Three-Point Dixon's Test over Non-Overlapping Blocks . . . 60
3.5.2 Scheme 2: Three-Point Sliding Window Dixon's Test . . . 60
3.6 A Note on the Complexity of the Proposed Schemes . . . 62
3.7 Simulation Results and Performance Assessment . . . 63
3.7.1 Evaluating the Robustness of the Dixon's Test over Small Data Samples . . . 65
3.7.2 Performance Evaluation in Suppressing a Single MU . . . 65
3.7.3 Performance Evaluation in Suppressing Multiple MUs . . . 71
3.8 Conclusion . . . 75

4 Collision Penalty based Mechanism for Countering Smart SSDF Attacks 77

4.1 Introduction . . . 78
4.2 System Model . . . 83
4.2.1 System Model and Assumptions . . . 83
4.2.2 Decision Fusion Rule . . . 84
4.2.3 Evaluation Parameters and Conditions . . . 84
4.2.4 Assumptions . . . 84
4.3 Proposed Scheme . . . 85
4.3.1 Bound on C_P for Sharing the Spectrum by the PU . . . 85
4.3.2 Optimal Decision Fusion Rule . . . 85
4.4 Bounds on C_P for Attack Prevention . . . 90
4.4.1 Avoiding Malicious Strategies when the FC declares H_1 . . . 95
4.4.1.1 Avoiding (H, M) . . . 95
4.4.1.2 Avoiding (M,M) . . . 96
4.4.2 Avoiding Malicious Strategies when the FC declares H_0 . . . 98
4.4.2.1 Avoiding (M,H) . . . 98
4.5 The Best Strategy for the SUs . . . 102
4.6 Conclusion . . . 104

TH-1605_10610214

5 Countering the Primary User Emulation Attacks **105**

5.1 PUEAs . . . 106

5.2 Approaches to Combat PUEAs . . . 107

5.3 System Model, Sensing Mechanism and Parameters . . . 110

5.3.1 System Model . . . 110

5.3.2 Characterization of the Parameters . . . 112

5.3.2.1 Probabilities of False Alarm and Miss Detection . . . 112

5.3.2.2 Throughput of an SU ($G_i(\mathbf{w}, \lambda)$) . . . 113

5.3.2.3 Effective Interference to the PU ($I_{eff}(\mathbf{w}, \lambda)$) . . . 114

5.4 Maximization of the SU Throughput under PUEAs . . . 114

5.5 Obtaining Optimal Weights for Performing CSS . . . 117

5.5.1 Calculation of $\mathbf{w}_0$ . . . 118

5.5.2 Obtaining $\mathbf{w}*$ . . . 120

5.5.3 Average Throughput and Interference . . . 123

5.5.3.1 Average Throughput . . . 123

5.5.3.2 Average Interference . . . 124

5.6 Experimental Results and Performance Evaluation . . . 125

5.6.1 Static Transmitters and Receivers . . . 125

5.6.2 Transmitters and Receivers in Motion . . . 135

5.7 The Reason for using the NMA . . . 136

5.8 Conclusion . . . 137

6 Conclusions **139**

6.1 Summary of Contributions and Discussions . . . 140

6.2 Suggestions for Future Research . . . 142

6.2.1 Suppression of Multiple Malicious Users . . . 142

6.2.2 Suppressing Collusion Attacks . . . 143

6.2.3 Suppressing PUEAs . . . 143

6.2.4 Security issues in frequency selective fading channels . . . 143

6.2.5 Research on military applications . . . 144

TH-1605_10610214

A Table for Critical Values for Dixon's Test **147**

A.1 Table for Critical Values 148

B Evaluation Parameters for PUEA Model **149**

B.1 Probability of False Alarm 150

B.2 Probability of Miss Detection 151

Bibliography **153**

List of Publications **165**

TH-1605_10610214

TH-1605_10610214

List of Figures

1.1 The ever increasing annualized cost of frequency spectrum in India [1] 3
1.2 Centralized CSS 7
1.3 Decentralized CSS 8
1.4 Spectrum Sensing Data Falsification Attack 10
1.5 Primary User Emulation Attack Model 11

3.1 Periodic Sensing by SUs 46
3.2 Unreliability in Spectrum Sensing 50
3.3 Box Plot method for outlier detection 54
3.4 Comparison of MU detection performance of the N-point Dixon's tests with Grubbs tests and Boxplot test in a single high reporting MU case. 64
3.5 Comparison of MU detection performance of the N-point Dixon's tests with Grubbs tests and Boxplot test in a single low reporting MU case. 64
3.6 Comparison of MU detection performance of the N-point Dixon's tests for $N = 3, 5, 7$ and 20 in the single high reporting MU case. 65
3.7 Comparison of MU detection performance of the N-point Dixon's tests for $N = 3, 5, 7$ and 20 in the single low reporting MU case. 66
3.8 Comparison of MU detection performance of the N-point Dixon's tests for $N = 3, 5, 7$ and 20 in the two high reporting MUs case. 66
3.9 Comparison of MU detection performance of the N-point Dixon's tests for $N = 3, 5, 7$ and 20 in the two low reporting MUs case. 67
3.10 MU detection of the proposed schemes and the scheme in [2] for a single high reporting MU 68

TH-1605_10610214

3.11 MU detection of the proposed schemes and the scheme in [2] for a single low reporting MU . . . 68
3.12 P_{fa} vs λ plot for a single MU reporting high value among 20 SUs showing the shift in P_{fa} reduced with the proposed schemes. . . . 69
3.13 P_d vs λ plot for a single MU reporting high value among 20 SUs showing the shift in P_d reduced with the proposed schemes. . . . 69
3.14 P_{fa} vs λ plot for a single MU reporting low value among 20 SUs showing the shift in P_{fa} reduced with the proposed schemes. . . . 70
3.15 P_d vs λ plot for a single MU reporting low value among 20 SUs showing the shift in P_d reduced with the proposed schemes. . . . 70
3.16 P_{fa} vs λ plot for MUs reporting low Values among $N = 40$ SUs when the PU signal is present, showing the shift in P_{fa} reduced with scheme 1. . . . 71
3.17 P_d vs λ plot for MUs reporting low values among $N = 40$ SUs when the PU signal is present showing the shift in P_d reduced with scheme 1. . . . 72
3.18 P_{fa} vs λ plot for MUs reporting high values among $N = 40$ SUs when the PU signal is absent showing the shift in P_{fa} reduced with scheme 1. . . . 72
3.19 P_d vs λ plot for MUs reporting high values among $N = 40$ SUs when the PU signal is absent showing the shift in P_d reduced with scheme 1. . . . 73
3.20 P_{fa} vs λ plot for MUs reporting low Values among $N = 40$ SUs showing the shift in P_{fa} reduced with scheme 2. . . . 73
3.21 P_d vs λ plot for MUs reporting low values among $N = 40$ SUs showing the shift in P_{fa} reduced with scheme 2. . . . 74
3.22 P_{fa} vs λ plot for MUs reporting high values among $N = 40$ SUs showing the shift in P_{fa} reduced with scheme 2. . . . 74
3.23 P_d vs λ plot for MUs reporting high values among $N = 40$ SUs showing the shift in P_{fa} reduced with scheme 2. . . . 75

4.1 Periodic Sensing . . . 83
4.2 Variation of $A(n)$ vs n for N=10 . . . 88
4.3 Variation of $A(n)$ vs n for N=18 . . . 88
4.4 Variation of $A(n)$ vs n for N=20 . . . 89

TH-1605_10610214

4.5 Variation of $A(n)$ vs n for N=22 . . . 89
4.6 Variation of $A(n)$ vs n for N=28 . . . 90
4.7 Variation of $G_{Ui}(m,n)$ vs n for N=10 . . . 92
4.8 Variation of $G_{Ui}(m,n)$ vs n for N=15 . . . 92
4.9 Variation of $G_{Ui}(m,n)$ vs n for N=18 . . . 93
4.10 Variation of $G_{Ui}(m,n)$ vs n for N=20 . . . 93
4.11 Variation of $G_{Ui}(m,n)$ vs n for N=22 . . . 94
4.12 Variation of $G_{Ui}(m,n)$ vs n for N=28 . . . 94
4.13 Variation of $G_{Ui}(m,n)$ vs n after using additional bounds on C_P for N=10 . . . 99
4.14 Variation of $G_{Ui}(m,n)$ vs n after using additional bounds on C_P for N=15 . . . 99
4.15 Variation of $G_{Ui}(m,n)$ vs n after using additional bounds on C_P for N=18 . . . 100
4.16 Variation of $G_{Ui}(m,n)$ vs n after using additional bounds on C_P for N=20 . . . 100
4.17 Variation of $G_{Ui}(m,n)$ vs n after using additional bounds on C_P for N=22 . . . 101
4.18 Variation of $G_{Ui}(m,n)$ vs n after using additional bounds on C_P for N=28 . . . 101

5.1 Primary User Emulation Attack Model . . . 111
5.2 Periodic Sensing . . . 111
5.3 Plot of the $G_i(\mathbf{w},\lambda)$ vs $I_{eff}(\mathbf{w},\lambda)$ . . . 120
5.4 Plot of the $G_i(\mathbf{w},\lambda)$ vs PU SNR (at $I_{eff} = 0.0695W$) . . . 121
5.5 Plot of the $G_i(\mathbf{w},\lambda)$ vs N ($I_{eff} = 0.0758$) . . . 122
5.6 Working simplex with reflection, contraction and expansion points . . . 123
5.7 Plot of $G_i(\mathbf{w},\lambda)$ vs $I_{eff}(\mathbf{w},\lambda)$ when both PU-SU and PUE-SU channels are Rayleigh faded . . . 126
5.8 Plot of $G_i(\mathbf{w},\lambda)$ vs $I_{eff}(\mathbf{w},\lambda)$ when PU-SU and PUE-SU channels are Rayleigh and Rician faded respectively . . . 126
5.9 Plot of $G_i(\mathbf{w},\lambda)$ vs $I_{eff}(\mathbf{w},\lambda)$ when PU-SU and PUE-SU channels are Rician and Rayleigh faded respectively . . . 127
5.10 Plot of $G_i(\mathbf{w},\lambda)$ vs $I_{eff}(\mathbf{w},\lambda)$ when both PU-SU and PUE-SU channels are Rician faded 127
5.11 Plot of $G_i(\mathbf{w},\lambda)$ vs PUE SNR at fixed interference ($P_{md} = 0.1$) . . . 129
5.12 Plot of $G_i(\mathbf{w},\lambda)$ vs PUE SNR at fixed interference ($P_{md} = 0.2$) . . . 129
5.13 Plot of $G_i(\mathbf{w},\lambda)$ vs PU SNR ($P_{md} = 0.1$) . . . 130

TH-1605_10610214

5.14 Plot of $G_i(\mathbf{w}, \lambda)$ vs PU SNR ($P_{md} = 0.2$) 130
5.15 Plot of $G_i(\mathbf{w}, \lambda)$ vs SU SNR ($P_{md} = 0.1$) 131
5.16 Plot of $G_i(\mathbf{w}, \lambda)$ vs SU SNR ($P_{md} = 0.2$) 131
5.17 Plot of $G_i(\mathbf{w}, \lambda)$ vs PU SNR and PUE SNR moving away from each other 132
5.18 Plot of $G_i(\mathbf{w}, \lambda)$ vs PU SNR and PUE SNR moving towards each other 132
5.19 Plot of $G_i(\mathbf{w}, \lambda)$ vs PUE SNR for only PUE moving 133
5.20 Plot of $G_i(\mathbf{w}, \lambda)$ vs SU SNR vs $I_{eff}(\mathbf{w}, \lambda)$ 133

TH-1605_10610214

List of Tables

2.1 Attacks and categorization of their countering strategies 26

4.1 $E_{U_i}(n)$ at $n = N/2 - 3$ to $n = N/2 + 1$ for $P_{f_i} = 0.1$ and $P_{d_i} = 0.9$ 90

4.2 $E_{U_i}(n)$ at $n = N/2 - 3$ to $n = N/2 + 1$ for $P_{f_i} = 0.2$ and $P_{d_i} = 0.8$ 91

4.3 $E_{U_i}(n)$ at $n = N/2 - 3$ to $n = N/2 + 1$ for $P_{f_i} = 0.3$ and $P_{d_i} = 0.7$ 91

4.4 Checking $\frac{1}{2}R_1$ for different P_{f_i} and P_{d_i} 97

4.5 Values for $L(n)$ for $n \in [1, 3]$ 102

4.6 $G_{U_i}(m, n)$ for various n and m with $C_P = U_{PU}$ 103

4.7 $G_{U_i}(m, n)$ for various n and m with $C_P = 722$ 103

4.8 Payoff matrix when the FC declares H_1 103

A.1 Critical values for different confidence limits (CLs) 148

TH-1605_10610214

TH-1605_10610214

List of Acronyms

AWGN	Additive White Gaussian Noise
BPSK	Binary Phase Shift Key
BS	Base Station
BER	Bit Error Rate
CRN	Cognitive Radio Network
CSS	Cooperative Spectrum Sensing
CR	Cognitive Radio
COI	Combinatorial Optimization Identification
DOA	Direction of Arrival
DSA	Dynamic Spectrum Access
EWSPRT	Enhanced Weighted Sequential Probability Ratio Test
EWZOT	Enhanced Weighted sequential Zero/One Test
EWSZT	Enhanced Weighted Sequential Zero Test
FC	Fusion Center
FFT	Fast Fourier Transform
FCC	Federal Communications Commission
GNSS	Global Navigation Satellite System
HMM	Hidden Markov Models
IRIS	cooperatIve sensing via iteRatIve State estimation
LRMI	Location Reliability and Malicious Intention
MATLAB	Matrix Laboratory
MLM	Multilevel Median
MANET	Mobile Adhoc Network
MAC	Medium Access Control

TH-1605_10610214

MU	Malicious User
NE	Nash Equilibrium
NMA	Nelder Mead Algorithm
OWDFR	Optimal Weighted Decision Fusion Rule
PU	Primary User
PUE	Primary User Emulator
PUEA	Primary User Emulation Attacks
RSS	Received Signal Strength
ROC	Receiver Operating Characteristics
RF	Radio Frequency
RKRL	Radio Knowledge Representation Language
SPRT	Sequential Probability Ratio Test
SP	Service Provider
SR	Software Radio
SS	Spectrum Sensing
SDR	Software Defined Radio
SU	Secondary User
SSDF	Spectrum Sensing Data Falsification
SNR	Signal to Noise Ratio
SUN	Secondary User Network
STF	Special Task Force
TLD	Thin Line Details
WDFR	Optimal Weighted Decision Fusion Rule
WSPRT	Weighted Sequential Probability Ratio Test

TH-1605_10610214

List of Symbols

N	Number of SUs performing CSS
M	Number of samples sensing duration is divided
C_P	Collision Penalty
$E_{U_i}(t)$	Expected Utility of ith SU
$G_{U_i}(t)$	Malicious Utility of ith SU
P_{d_i}	Probability of detection of ith SU
P_{f_i}	Probability of false alarm of ith SU
P_d	Global probability of detection at the FC
P_{fa}	Global probability of false alarm at the FC
P_{md}	Global Probability of miss detection at the FC
P_e	Probability of error
T_1	Transmission time
T	Sensing Time
H_1	Hypothesis representing the presence of the PU
H_0	Hypothesis representing the absence of the PU
$y_i(t)$	Received Signal from the PU by the ith SU
$s(t)$	Signal transmitted by the PU
$u_i(t)$	AWGN at ith SU receiver
$h_i(t)$	Fading coefficient of the ith SU with the PU
S_λ	Set of λ values
e_i	Energy calculated by the ith SU
$\bar{e}$	Mean of e_i values
E	Total energy at the FC (weighted or non-weighted)
λ	Threshold for forming decision regarding the spectrum occupancy at the FC

TH-1605_10610214

$o_{[n]}$	Outlier factor for nth value
$o_{[N]}$	Outlier factor for suspected high malicious values
$o_{[1]}$	Outlier factor for suspected low malicious values
C_v	Critical value for outlier detection
D_i	Decision formed by ith SU
D	Global decision at the FC
U_{PU}	Utility obtained by the Primary User
U_{SU}	Utility obtained by the SU
$\gamma(n)$	Probability of collision in the phase 2
$P_{e_{\overline{PU}}}$	Probability of error in the SU transmission when the PU is absent
$P_{e_{PU}}$	Probability of error in the SU transmission when the PU is present
w_i	Weights assigned to the SUs
$\mathbf{w}$	Weight vector $[w_1, w_2, \ldots, w_N]$
S_P	1-$P_{e_{\overline{PU}}}$
$x_p(m)$	Signal from the PU at an SU
$x_e(m)$	Signal from the PUE at an SU
$\mathrm{h}_{p_i}(\mathrm{m})$	Channel gain of the ith SU with the PU
$h_{e_i}(m)$	Channel gain of the ith SU with the PUE
G_i	Throughput of the ith SU
I_t	Total interference suffered by the PU
I_{SU}	Interference to the PU caused by the SU
I_{PUE}	Interference to the PU caused by the PUE
I_{eff}	Effective interference to the PU
γ_P	Transmit SNR of the PU
γ_e	Transmit SNR of the PUE
c	Centroid for NMA
$\widetilde{\mathrm{h}_{p_i}}(m)$	Normalized channel gain of the ith SU with the PU
$\widetilde{\mathrm{h}_{p_i}}(m)$	Normalized channel gain of the ith SU with the PUE

TH-1605_10610214

1

Introduction

Contents

1.1 Background 2
1.2 Areas of Research in CRs 4
1.3 Motivations and Problem Statements 11
1.4 Contributions of the Thesis 13
1.5 Organization of the Thesis 13

TH-1605_10610214

1.1 Background

Wireless communication devices need the electromagnetic spectrum to transmit information. The use of the spectrum is authorized by the government of a state or a territory [3]. Different parts of the spectrum are suitable for different types of communications. However, the available suitable spectrum is scarce for the number of wireless network operators present and there is a strong competition for it [4]. Consequently, the spectrum is auctioned by the government [3]. Each winner of the auction is granted the full use of a particular part of the spectrum and is called the *primary user (PU)*. Henceforth, the PUs hold the legitimate right over the part of the spectrum granted to them.

In the year 2002, the special task force (STF) appointed by the Federal Communications Commission (FCC) reported inefficient usage of the spectrum [5]. It was found that in a given space and time span, most of the spectrum licensed by the government to the auction winners remains unused. This brought the need for revising the spectrum allocation strategy. A significant idea in this regard came from the PhD dissertation of Joseph Mitola III [6]. It proposed the design of a software radio (SR) capable of sensing its environment. Mitola termed such an SR as a *cognitive radio (CR)*. A CR is an extension of an SR to learning about the RF bands, air interfaces, protocols, spatial and temporal patterns that moderate the use of the radio spectrum. Mitola's work mainly proposed a Radio Knowledge Representation Language (RKRL) to obtain the equalizer taps so that, the use of equalizers can be limited to the places with less multipath fading or a good signal to noise ratio (SNR). It was suggested that CR can also be used to increase the spectrum efficiency. Based on this idea, the annual report of the FCC in 2003 [7] proposed to apply the learning capabilities of a CR to allow *dynamic spectrum allocation (DSA)* among the wireless operators based on its availability. Subsequently, extensive researches started on DSA. The most significant work was by Simon Haykin [8] in 2005, which quantified Mitola's work for DSA. Haykin suggested to accomplish DSA by using CR technology for the unlicensed users. An unlicensed user was termed as a *secondary user (SU)*. It was realized that a CR can be installed in an SU to sense the presence of the PU signal on its spectrum. This function was termed as *spectrum sensing (SS)*. If the PU signal was found to be absent, its spectrum can be used by the SU. However, there should be no interference to the PU. If the PU signal is present, the SU should refrain from any kind of transmission.

Since Haykin's work has been published, SS has emerged as a significant area of research [9, 10]. It was found that the most important objective of SS is accuracy, so that the PU should not suffer

TH-1605_10610214

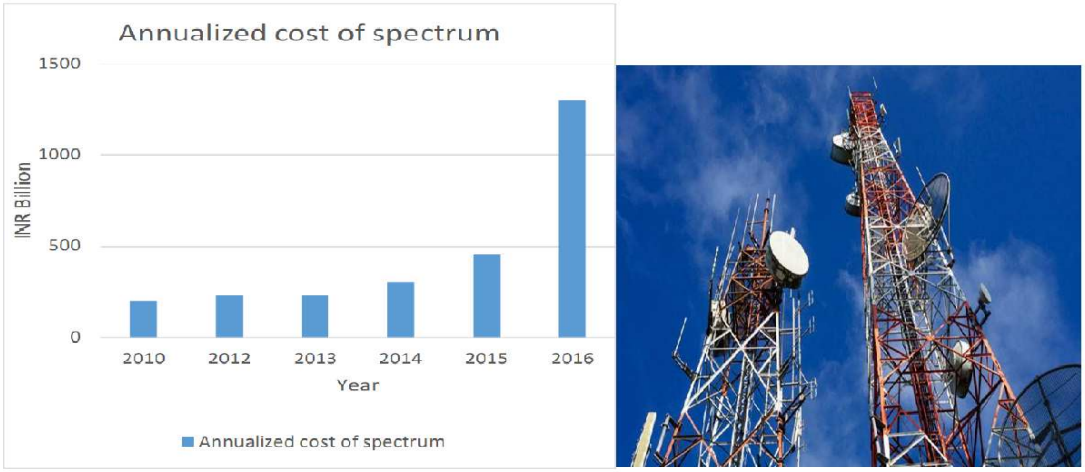

Figure 1.1: The ever increasing annualized cost of frequency spectrum in India [1]

interference [1]. However, the SS performed by an individual SU can be highly inaccurate in deep fading environments. To overcome this problem, a cooperation between more than one SU to sense the spectrum has been proposed [12–14]. This scheme is known as *cooperative spectrum sensing* (CSS). CSS is classified as centralized and decentralized [15]. In centralized CSS, the cooperating SUs report their data or decisions to a central body known as a fusion center (FC) or a base station (BS). Based on these data or decisions, the FC forms its decision about the presence or the absence of the PU and broadcasts it to all the SUs. On the other hand, decentralized CSS is based on the sharing of data or decisions among all the cooperating SUs to arrive at a final decision. In this thesis, we focus on centralized CSS. Henceforth, unless mentioned otherwise, any mention of CSS will mean centralized CSS.

CSS significantly improves the SS performance in deep fading environments. However, its performance depends on the data or decision of an individual SU. Any flaw in an individual SU's data or decision can cause a significant error at the FC [16]. The flaws can be caused by many reasons, like hardware malfunction, deep fading etc. It can also be caused if an SU deliberately reports wrongly to the FC for selfish reasons. Such an SU is termed as a *malicious user (MU)* [14]. Subsequently, there

[1] In the meanwhile, underlay CR systems [11] which allow some predefined interference to the PU and overlay CR systems where the SUs assist the PU in exchange of its spectrum were proposed. However, this thesis is based on interweave CRs where no or negligible interference is allowed to the PU.

TH-1605_10610214

were researches on the possible malicious attacks [17–21].

Two attacks launched by the MUs have mainly been classified as *spectrum sensing data falsification* (SSDF) attacks and the *primary user emulation attacks* (PUEAs). In SSDF attacks, the MUs misdirect the FC regarding the spectrum status by reporting to it wrongly. These attacks may cause the FC to declare the vacant spectrum as occupied and force the honest SUs to cease their transmissions. The MUs may take the advantage of this situation by using the band for their own purpose. In the other scenario, the MUs may misdirect the FC to declare an occupied spectrum as unoccupied. Following this decision, the honest SUs may start transmitting which would cause severe interferences to the PU. The PU may impose penalty on the honest SUs and can also restrict them from further using its spectrum [22]. The MUs may take the advantage of this situation by getting the honest SUs punished.

The PUEAs are launched when an MU transmits the emulated PU signal to misdirect other SUs [23]. An MU causing PUEA is termed as a *primary user emulator (PUE)*. PUEs are classified as *always-on* and *smart* [24]. Always-on PUEs do not know about the status of the licensed spectrum. They attack with emulated PU signals seamlessly. Smart PUEs are capable of knowing the PU spectrum status by individual decision making or listening to other SUs. They plan and attack depending on the presence of the PU. As a result of the PUEAs, the honest SUs may get misdirected in deciding the spectrum status and report wrong decisions to the FC. If the PU is absent, the SUs mistake the PUE's signal to be coming from the PU and cease their transmissions. The PUE takes the advantage of this situation by transmitting on the vacant band. On the other hand when the PU is present, the PUEs cause interference to it (intentionally by smart PUEs while always on PUEs do it anyways). As a result, the PU may penalize the honest SUs and the PUE may take advantage of the situation.

In the next section, we explain the different approaches of researches in CRs.

1.2 Areas of Research in CRs

1.2.1 Signal Propagation

The fundamental operation of a CR is to identify the PU on the frequency band allocated to it, and design a transmission strategy that causes minimum interference to it. For the identification of a PU, and the design and the implementation of the transmission strategies, understanding the propagation channel is imperative. Signal propagation domain is mainly concerned with the propagation environ-

ment [25] of the CR systems. The transmission strategies of an SU, the pathloss and the multipath fading suffered by the PU signals to reach the SU, the interference caused to the PU, the fraction of the transmitted PU signal reaching the SU receiver etc are the main focus here [26–29]. The operation of an SU depends on the presence of the PU. The SUs need to design their transmission strategies according to the arrival and the departure of the PU. For the dynamic spectrum access, the CRs adapt to the present state of the environment, which includes the center frequency, bandwidth and transmission time [30]. The strategy design depends upon the range of the frequency band of interest. If the band of interest can support only one SU signal, the SU may have to stop transmitting upon the arrival of the PU. If the band of interest is wide, the SU may have to switch to another vacant band by changing its transmission signal frequency for uninterrupted communications [31].

Another propagation issue is the attenuation caused by shadowing and multipath fading to the PU signals in reaching the SUs [32]. Shadowing is caused by large objects such as buildings, hills, big trees etc. These large objects attenuate the signal by blocking it from reaching the receiver. Multipath fading is caused because of the reflections of the signals from the various obstacles in the wireless environment. Multipath signal propagation results into several copies of the transmitted signal reaching the receiver from different directions and at different time instants. The SU senses the licensed spectrum by detecting the PU signals on it. The fraction of the transmitted signal that reaches the receiver indicates the path loss and fading in its propagation environment. If the path between the PU transmitter and the SU receiver is under deep fading, the incoming PU signals get highly attenuated. This affects the robustness of the sensing system. As a result of this, the SUs may miss to detect the presence of the PU and cause interference to it.

The PU signal suffers multipath propagation and splits into multiple components. We will discuss later that these components can be exploited by employing more than one receive antennas or SUs to bring improvement in sensing the spectrum.

1.2.2 Signal Processing

After the signal propagates through the wireless environment, it is used to form the decision about the spectrum occupancy. This part comes under the signal processing domain. The efficient implementation of CR technology is highly dependent on this area of research. The major challenge here is to detect the licensed spectrum status with the incoming signal samples [33]. The SU has to differentiate between the spectrum with and without the PU signal. This differentiation can be done

TH-1605_10610214

by detecting the difference created in the spectrum by the presence of the PU. This is done in terms of a *statistic* which is obtained from the incoming signal samples [34]. The larger the sensing time, the more will be the number of signal samples and hence the more accurate will be the sensing. However, there are constraints on the sensing time. Consequently, robust SS with a limited number of samples is needed to evaluate the statistic. The major signal processing goal is adaptability of the SU according to the presence of the PU [16]. The arrival and departure make the CR network (CRN) fluctuating in nature. The available bandwidth for the SU varies accordingly. The SS process should also be able to adapt to such a fluctuating nature of the CRN and the variation in the available bandwidth of the SU. In multi-carrier sensing, the SU needs to sense the bands of different frequencies continuously. Hence, the SS system must be adaptable to different frequencies also.

Another significant signal processing challenge is the robustness of the sensing system to the attenuation induced in the signals because of the propagation environment [35]. The effective SNR between the PU transmitter and the SU receiver may be low because of the obstacles present. If an identifying feature of the PU signal gets sufficiently distorted, SS will be inaccurate and interference can be caused to the PU. As a result, the PU can impose penalty on the SUs. Hence, the sensing system must be able to detect the signals in a deep faded environment.

1.2.3 Cooperative Spectrum Sensing

The pathloss and multipath fading caused to the PU signal result into inaccurate sensing. Consequently, the SU can make a wrong decision about spectrum occupancy. This can cause a severe interference to the PU. As a countermeasure, a cooperation among multiple SUs for sensing the spectrum has been proposed [36]. The process is called *cooperative spectrum sensing* (CSS). The idea of CSS is to exploit the spatial diversity of the propagation environment. Exploiting spatial diversity was first proposed in $1938 - 1939$ in [37] and [38]. In CRs, diversity is obtained when different copies of the same signal due to multipath diversity are received by multiple antennas or multiple SUs [15]. The gain obtained by exploiting multipath diversity is called *diversity gain*. The idea of CSS is that out of the various copies of the PU signal received by different SUs, some copies would have suffered more attenuation while some copies would have suffered lesser attenuation. The SU receiving a highly attenuated signal is likely to make a wrong decision regarding spectrum occupancy. In this regard, if a decision is made by combining the individual decisions of the SUs, the bad decisions will be compensated by the decisions from the good paths, and the effects of attenuation can be mitigated. CSS

TH-1605_10610214

significantly reduces the inaccuracy in SS by a single user. It is mainly categorized as centralized and decentralized CSS. They are described below:

(i) Centralized CSS: In this scheme, the SUs fuse their individual parameters to a central body known as the *fusion center* (FC) as shown in Figure 1.2 [14]. The FC combines the individual parameters and makes the decision regarding spectrum occupancy. The decision made at the FC is called global decision. The centralized CSS systems are further divided into two categories:

(a) Data Fusion: In data fusion systems, the SUs donot form their own decisions. All individual SUs report their recorded data to the FC. The FC combines them to form the global decision. The FC broadcasts the global decision to all the SUs. This scheme gives a high sensing accuracy but requires a large bandwidth for reporting the data to the FC. Hence, data overhead is the major issue in this scheme.

(b) Decision Fusion: In decision fusion systems, each SU can form its individual decision and then report it to the FC. The FC combines the decisions to form a global decision. The advantage with this scheme is that it requires low bandwidth. Its disadvantage is that it is lesser accurate as compared to the data fusion scheme.

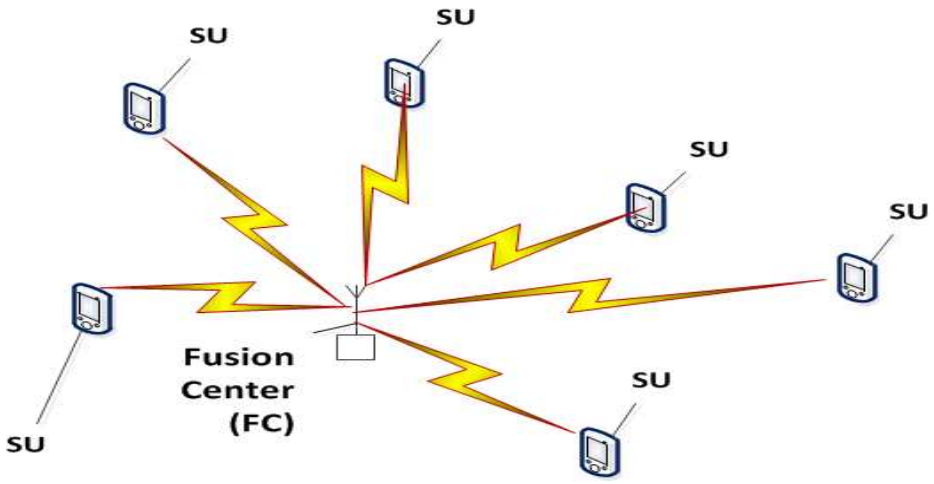

Figure 1.2: Centralized CSS

(ii) Decentralized CSS: In this scheme, there is no FC [39]. It is based on sharing of data or decisions

TH-1605_10610214

among the SUs as shown in Figure 1.3. Each SU shares its data or decisions with other SUs and forms its decision about the spectrum occupancy.

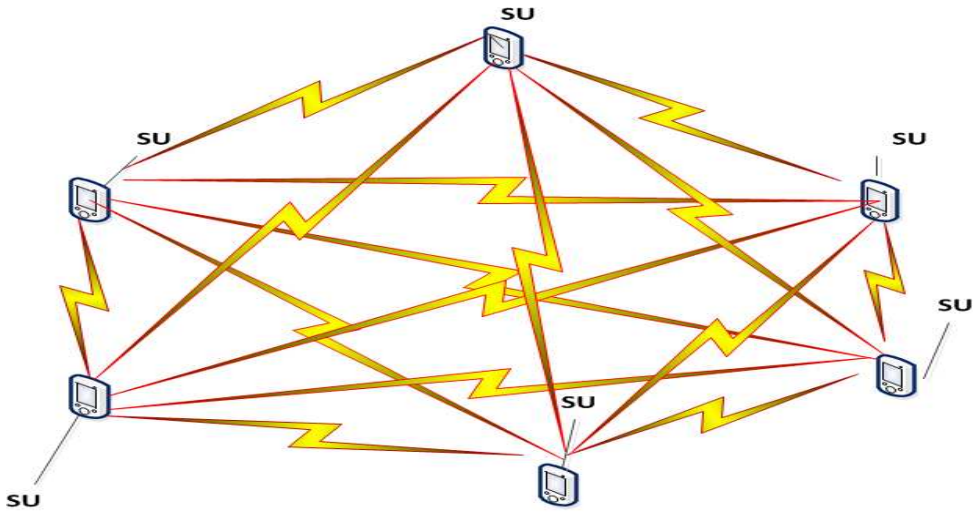

Figure 1.3: Decentralized CSS

In this thesis, all the studies have been conducted on centralized CSS systems.

1.2.4 Security Issues in CSS

The belief of an SU about the spectrum occupancy depends on the data or decisions of the other SUs. The belief may be formed with the help of the FC or by the sharing of the data or decisions among the SUs. In either case, it depends on the other SUs. As mentioned before, it may be possible that some SU in the network, termed as an MU [40], indulges in malpractices to misguide the SS system for its selfish interests. The MUs severely affect the signal processing and propagation characteristics of the sensing system. Their presence necessitates the redesigning of the transmission strategy and sensing process of the SUs. As a result, the throughput of the SUs is degraded and the interference on the PU increases severely. There are different ways in which the MUs can launch attacks. The most significant attacks are as follows:

(i) Spectrum Sensing Data Falsification (SSDF) Attacks: These attacks are caused in centralized CSS systems. They are the outcome of the *Byzantine failure problem* which is caused when a cooperating SU reports wrongly to the FC [41]. This false reporting may be due a hardware

TH-1605_10610214

fault or a selfish intention of an MU. The false reporting due to selfish intentions of the MUs is known as the *SSDF* attack [41–46]. The MUs report falsely to misguide the FC regarding the spectrum status. On getting misdirected, the FC broadcasts wrong decisions to the cooperating SUs. Hence, the entire network is misdirected regarding the spectrum status. If the FC gets misguided regarding the presence of the PU and broadcasts it as 'absent' to the cooperating SUs, the SUs will start transmitting resulting into a strong interference to the PU. As a consequence, the PU may impose penalty on all the SUs. On the other hand, if the FC gets misdirected about the absence of the PU and broadcasts it as 'present', the SUs will cease their transmissions. Hence, their throughput will be severely affected. These attacks can be launched individually by one or more MUs or the MUs can collude and cooperatively launch attacks [22,47,48]. Another consequence of these attacks is that the PU becomes reluctant to share its spectrum with the SUs.

There are mainly two approaches to counter individual SSDF attacks in literature: Active approaches and Passive approaches [17,18,49–54]. The major active approaches in literature are location identification based and Statistical approaches. The major passive approaches are Reputation based mechanisms, game theoretic, and damage suppression based approaches. Location based approaches counter the SSDF attacks by identifying the locations of the PU, the SU, or the MU. Statistical approaches differentiate the statistical properties of the MUs' data with the honest SUs' data. The statistical tests are based on outlier rejection from a sample of data. An outlier is a value in a data-set having different statistical properties. The incoming data to the FC from the cooperating SUs follow a specific statistical distribution. A random low or high value transmitted by an MU belongs to a different distribution. Using statistical tests, these outliers can be identified and discarded. Different statistical tests have been reported in the literature [2,44]. Reputation based mechanisms depend on the previous history of the SU node. The reporting of the SUs is compared with a trusted SU. Based on the previous history of the reported decisions, the SU nodes are assigned weight values. The SU nodes repeatedly giving values similar with the trusted node are weighed high. The main challenge in these mechanisms is to identify the trusted SU. In game theoretic approaches, the SUs, the PU, and the FC are regarded as players. Their actions are termed as strategies and the outcome of their actions are termed as utilities or pay offs. To counter the security threats with game theoretic approaches,

TH-1605_10610214

the benefits obtained by an SU in reporting honestly or maliciously are termed as honest and malicious utilities. The objective in these approaches is to maximize the honest utilities and minimize the malicious utilities, so that the SUs do not turn malicious. In damage suppression, instead of detecting the MUs, a particular damage of the SSDF attacks is identified and is minimized. The damage can be caused on the PU or the SUs.

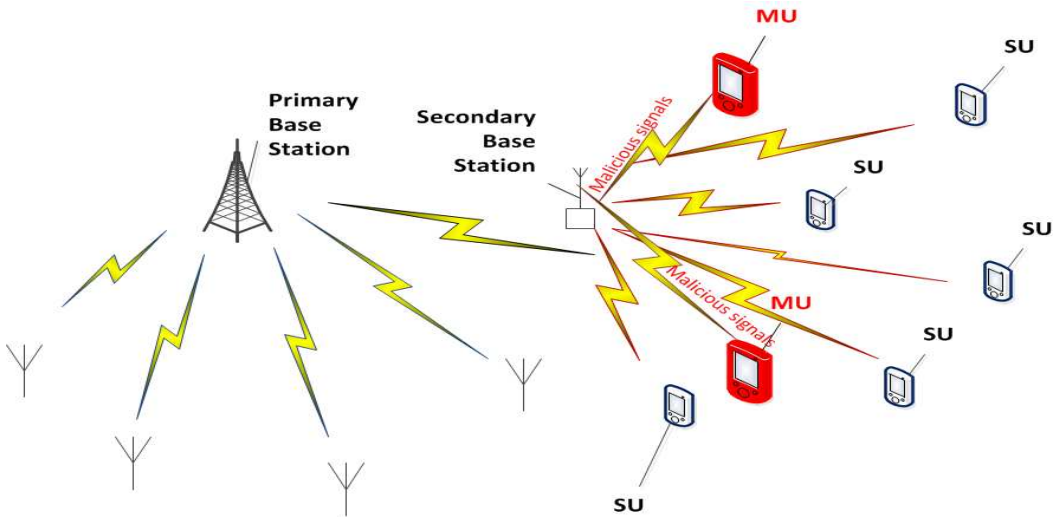

Figure 1.4: Spectrum Sensing Data Falsification Attack

(ii) Primary User Emulation Attacks (PUEAs): These attacks are caused when an MU deliberately transmits emulated PU signals [55]. As a result of this, the honest SUs sense the PU to be present and cease their transmission. The MU takes advantage of this situation and starts transmitting on the licensed band. Such attacks are known as *PUEAs* and the MUs causing them are called primary user emulators (PUEs). These attacks severely affect the throughput of the SUs. They also increase interference to the PU.

We categorize the counter mechanisms to PUEAs also as Active and Passive mechanisms. Active mechanisms aim at canceling or suppressing the PUE signal by differentiating it from the PU signal. This differentiation is facilitated by differentiating the RSS, some features, location of the PU and the PUE [55–57]. The second approach is Passive approach where instead of detecting the PUE, a specific damage done by the PUE on the SUs is suppressed [24, 58–60].

TH-1605_10610214

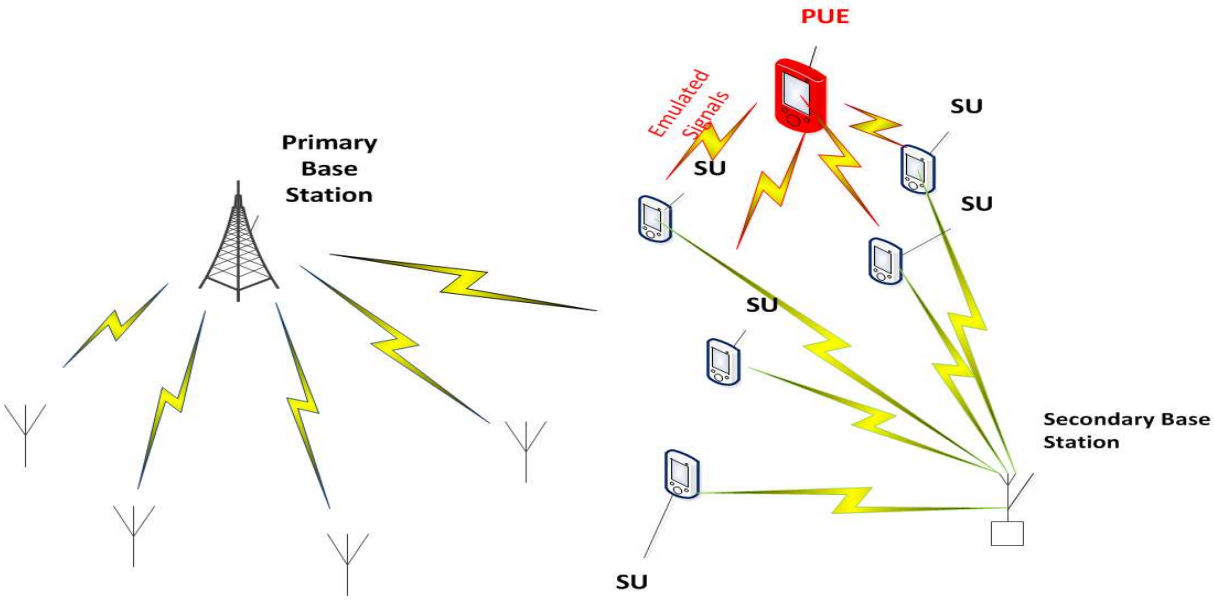

Figure 1.5: Primary User Emulation Attack Model

A detailed literature review of the existing approaches has been presented in chapter 2. The above security issues affect the CR systems in all the domains described above. This main focus of this thesis is on their effects in the signal processing domain.

1.3 Motivations and Problem Statements

1.3.1 Problem 1

Motivation: Since there are no strict protocols on the physical layer air interfaces, keeping in check the transmission of every SU transmitter is not feasible. Hence, launching individual SSDF attacks is not difficult in CRNs. Considering the gain SUs get in turning malicious, there is a high possibility of SSDF attacks. The FC cannot identify the honesty of the sensing reports because of the unpredictability in the wireless signal propagation model. Therefore, designing efficient schemes to counter these attacks is a problem of practical significance. An efficient class of active approaches to counter SSDF attacks are the statistical tests based mechanisms. In [44], the authors have studied various statistical tests for detecting the MUs. The limitation of the proposed scheme in [44] was its dependence on the estimation of the statistical parameters of the data. Further in [2], the authors proposed Dixon's test for the detection of the MUs. Though

TH-1605_10610214

independent of the statistical parameters of the data, the proposed algorithms in [2] suffered low efficiency and inability to detect multiple MUs. In the first part of the thesis, we aim to overcome these limitations of the schemes proposed in [2].

Problem Statement: Design an efficient statistical mechanism to counter multiple SSDF attacks.

1.3.2 Problem 2

Motivation: The SSDF attacks can become more disastrous if the MUs have learning capabilities to collude among themselves. With such a capability, the MUs can manipulate their reports more intelligently. The schemes for independent SSDF attacks are likely to fail on such attacks. In the second part of the thesis, we propose a scheme to counter the collusion SSDF attacks. There have been various works for countering collusion SSDF attacks [47, 48, 61–66]. The existing works on countering collusion attacks are based on collision penalty based mechanisms. The limitation of the existing mechanisms is that they fail to provide a comprehensive categorization of the different collusion attack scenarios. In the second part of the thesis, we design a collision penalty mechanism for countering the collusion attacks subject to different attack scenarios. We propose to first categorize different attacks and then derive different attack prevention strategies based on these categorizations.

Problem: Designing an efficient mechanism for countering collusion SSDF attacks in different scenarios.

1.3.3 Problem 3

Motivation: PUEAs cause severe degradation to the throughput of the SUs. However, this problem has not received sufficient focus in research. This motivated us to devise a scheme to combat the degradation in the SU throughput due to PUEAs. The passive methods study the damages caused by the PUEAs on different parameters like the probability of detection and the probability of error [24, 58–60, 67]. However, none of the existing researches study the damage of PUEA on the throughput of the SU. In the third part of the thesis, we study the damages caused by the PUEA on the throughput of the SUs.

Problem: Maximization of the SU throughput with a constraint on the interference to the PU in a CSS system facing PUEAs.

TH-1605_10610214

1.4 Contributions of the Thesis

Following are the contributions of the thesis:

1.4.1 Individual SSDF Attacks:

Following are the contributions in combating the individual SSDF attacks:

(i) Enhancing the applicability of the Dixon's test to multiple outlier detection.

(ii) Enhancing the efficiency of the Dixon's test based MU detection schemes.

(iii) Achieving these improvements without a significant increase in the computational complexity.

(iv) Suggesting optimum group size division of the incoming data for the application of Dixon's test.

1.4.2 Collusion SSDF Attacks:

Following are contributions in combating the collusion SSDF attacks:

(i) Providing a comprehensive categorization of the different collusion attack scenarios.

(ii) Deriving different attack prevention strategies based on these categorizations.

(iii) Obtaining optimal strategy for all the SUs for attaining Nash Equilibrium.

1.4.3 PUEAs:

Following are the contributions of the thesis in combating PUEAs:

(i) Redesigning of the SU throughput maximization scheme for the presence of the PUEAs.

(ii) Schemes independent of the location, the direction of arrival (DOA), the features, the power of the PUE signal.

(iii) Defense to the PUEAs focussed in the interest of the SUs at the physical layer.

1.5 Organization of the Thesis

The rest of the thesis is organized into five chapters. They are outlined below:

TH-1605_10610214

1.5.1 Chapter 2

This chapter is dedicated to a detailed literature review on the security issues in CRs. First, the major SS techniques have been explained briefly. Then, we discuss the existing and the ongoing works on various attacks possible in CRNs.

1.5.2 Chapter 3

In this chapter, we study individual SSDF attacks and propose a method to counter them. A brief review on the existing countering techniques has been presented. We adopt the statistical approach in our work. We first study the Dixon's test for outlier rejection. We suggest the optimal size of the data set to maximize the outlier rejection capacity of the Dixon's test. The Dixon's test is applicable only to a Gaussian distributed data sample. However, it is found that when the data set is of size 3, it performs well for any underlying distribution. The data set reported by the SUs to the FC follows a Chi-Square distribution. This data set is divided into groups of three. Then, the Dixon's test is applied on on the minimally to maximally overlapping groups. Applying the test on separate groups enhances the capability of Dixon's test to multiple MUs detection. Simulation results show that applying the test on maximally overlapping groups gives highest possible efficiency.

1.5.3 Chapter 4

This chapter studies the collusion SSDF attacks. Countering collusion attacks is difficult because the attackers collude intelligently and attack. The procedures for individual SSDF attacks may fail to counter them. We first formulate a condition on C_P which provides sufficient incentives to the PU for sharing its spectrum even in hostile environments. Then, we define "expected utility" for the SUs and "malicious utility" for the MUs which they gain while transmitting honestly or maliciously. The MUs attack when they see a positive malicious utility. The different collusion attack scenarios are categorized. Then, we formulate additional conditions on C_P which prevent the malicious utility from going positive in each of these scenarios. Finally the best strategy for the SUs is obtained which brings the CSS system to Nash equilibrium.

1.5.4 Chapter 5

This chapter studies PUEAs. First, the weighted CSS model in the presence of PUEs is considered. We aim to optimize the weights to suppress the effects of PUEAs on the CRN. The expressions for

TH-1605_10610214

the SU throughout and the interference to the PU are formulated. We maximize the SU throughout keeping a constraint on the interference to the PU to obtain the optimal weights. This is done by applying the Nelder Mead algorithm (NMA). The obtained optimal weights are then used to combine the SUs data at the FC. Simulation results endorse the effectiveness of the proposed scheme in preventing the damages caused to the SU throughput by the PUEs.

1.5.5 Chapter 6

This chapter summarizes the contributions made by the thesis. It also points at some interesting extensions of the proposed methods.

TH-1605_10610214

TH-1605_10610214

2

Security Issues in Cognitive Radios - A Review

Contents

2.1 Introduction 18
2.2 Basic SS Concepts 18
2.3 Security Issues in SS 24
2.4 SSDF Attacks in CR Communications 25
2.5 PUEAs in CR Communications 36

TH-1605_10610214

2.1 Introduction

This thesis mainly studies the effects of the SSDF attacks and PUEAs on CSS. CSS is achieved through collaboration among SUs performing SS individually. In this chapter, some basic SS mechanisms have been explained in detail. Then, a detailed literature review on both the attacks has been carried out. The various countering strategies in the literature have been elaborated for both these attacks.

In the next section, we explain some basic SS mechanisms.

2.2 Basic SS Concepts

The first and the most important function carried out in CRs is SS [8]. SS is mainly a binary hypothesis test with hypothesis H_0 denoting the absence while H_1 denoting the presence of the PU. The CRs make their decisions in favor of H_0 or H_1 based on the signal they receive from the PU.

Let there be an SU in the vicinity of the PU and let $y(k)$ denote the signal it receives from the PU at the kth instant of time. The presence of the PU can be expressed in the binary hypothesis form as

$$y(k) = \begin{cases} h(k)s(k) + w(k) & : H_1 \\ w(k) & : H_0 \end{cases} \tag{2.1}$$

where $s(k)$ denotes the PU signal, $h(k)$ denotes the multipath channel fading component and $w(k)$ is the additive white Gaussian noise (AWGN) at the SU. Now the CR installed in the SU uses an SS mechanism to perform the binary hypothesis testing. There are many SS techniques used for this purpose. We brief about a few important SS techniques as follows:

2.2.1 Energy Detection

Energy Detection is a blind signal detection technique proposed in [68]. It does not need any knowledge of the characteristics of the signal. The CRs compute the energy of the incoming signal. Then, the computed energy is compared to a predefined threshold. If it is higher than the threshold, the decision is made in favor of H_1 otherwise H_0 is concluded. The calculation of the threshold is done using the Neyman-Pearson method [34]. The decision statistic in energy detection systems is the energy of $y(k)$ given as

$$T_E = \frac{1}{K} \sum_{k=1}^{K} |y(k)|^2 \tag{2.2}$$

TH-1605_10610214

The SU compares T_E in (2.2) to a predefined threshold λ_E and decides H_1 or H_0 as follows

$$T_E \underset{H_0}{\overset{H_1}{\gtrless}} \lambda_E \tag{2.3}$$

This method is very simple and has low computational complexity. However, it does not perform well under low SNR conditions.

2.2.2 Cyclostationary Feature based Detection

In this detection, the cyclostaionary feature exhibited in $y(k)$ is the factor for deciding about the spectrum occupancy [69]. The cyclostationary feature is in-built in the PU signals because of the periodicity in their carrier signals like sine wave carriers, pulse trains, etc or in the hopping sequences, spreading codes, training sequences or the cyclic prefixes used in coding schemes. Consider a slow fading channel with $h(k)$ constant for one sensing duration. When the stationary noise $w(k)$ is added to the $h(k)s(k)$ in (2.1), $y(k)$ exhibits cyclostationarity under H_1. On the other hand, under H_0, $y(k)$ does not exhibit cyclostationarity. The exhibition of cyclostationarity is devised as the deciding factor between H_1 and H_0. Because of the cyclostationary feature, the mean and auto-correlation of the PU signals exhibit periodicity in time. When a signal is cyclostationary, its cyclic aotocorrelation function (CAF) for a set of cyclic frequencies (α) is non-zero [69]. Let $\widehat{R}^{\alpha}_{yy}$ be the estimated CAF of $y(k)$ given as

$$\widehat{R}^{\alpha}_{yy} = \frac{1}{K}\sum_{k=1}^{K} y(k)y^*(k-\tau)e^{-j2\pi\alpha k/K} \tag{2.4}$$

$\widehat{R}^{\alpha}_{yy}$ in (2.4) comes out to be a zero mean complex random variable (RV) and is represented as

$$\widehat{R}^{\alpha}_{yy} = X(\alpha) + jY(\alpha) \tag{2.5}$$

where $X(\alpha)$ and $Y(\alpha)$ are normal distributed zero mean RVs.

The statistic T_{Cy} for cyclostaionary feature based detectors is expressed as

$$T_{Cy} = \widehat{\mathbf{r}}^{\alpha}_{yy}\widehat{\Sigma}^{-1}_{2c}\left(\widehat{\mathbf{r}}^{\alpha}_{yy}\right)^T \tag{2.6}$$

where $\widehat{\Sigma}_{2c}$ is an estimate of covariance matrix of $y(k)$ given as

$$\widehat{\Sigma}_{2c} = \begin{bmatrix} E(X^2) & E(XY) \\ E(XY) & E(Y^2) \end{bmatrix} \tag{2.7}$$

TH-1605_10610214

and

$$\widehat{\mathbf{r}}_{yy}^{\alpha} = [X(\alpha)\ Y(\alpha)] \tag{2.8}$$

The decision about H_0 or H_1 is made by comparing T_{Cy} to a predefined threshold λ_{Cy} as

$$T_{Cy} \underset{H_0}{\overset{H_1}{\gtrless}} \lambda_{Cy} \tag{2.9}$$

This method is more robust than the energy detection method, particularly in low SNR conditions. However, it is computationally highly complex.

2.2.3 Matched Filter and Waveform based Detection

2.2.3.1 Matched Filter based Sensing

The matched filter is a coherent detector which maximizes the receive SNR [70]. The PU signal needs to be known at the SU receivers. The detection statistic T_{MF} for matched filter detection is expressed as

$$T_{MF} = \sum_{k_1=-\infty}^{\infty} g(k-k_1)y(k_1) \tag{2.10}$$

where $y(k_1)$ is the unknown received signal given by (2.1) and $g(k)$ is the impulse response of the matched filter. $g(k)$ is matched to the reference PU signal as

$$g(k) = s(T-k) \tag{2.11}$$

T_{MF} is compared to a predefined threshold λ_{MF} to decide between H_0 and H_1 as

$$T_{MF} \underset{H_0}{\overset{H_1}{\gtrless}} \lambda_{MF} \tag{2.12}$$

Matched filtering is optimal only when the PU signal is perfectly known.

2.2.3.2 Waveform based Sensing

In wireless communication systems, known patterns are transmitted with the transmitted information to facilitate synchronization or to estimate channel conditions. Few examples of such patterns are preambles, midambles, pilot symbols, spreading sequences etc. Waveform based sensing is performed by correlating the received signal with a known copy of itself. This method is only applicable to systems with known signal patterns, and hence is a coherent sensing technique. We explain the

TH-1605_10610214

formulation of the decision statistic is done in [71]. In (2.1), $s(n)$ is expressed as

$$s(k) = s_t(k) + s_d(k) \tag{2.13}$$

where $s_t(k)$ is the pilot and $s_d(k)$ is the data of the signal. Now, a new hypothesis problem is formulated as

$$\begin{aligned} H_0 &: x(k) = w(k) \\ H_1 &: x(k) = s_t(k) + w(k) \end{aligned} \tag{2.14}$$

The decision statistic in waveform based sensing T_{pr} is the projection of $x(k)$ on $s_t(k)$ given as

$$\begin{aligned} H_0 &: T_{WF} = \mathrm{Re}[\sum_k s_t^*(k)w(k)] \\ H_1 &: T_{WF} = \mathrm{Re}[\sum_k |s_t(k)|^2 + \sum_k s_t^*(k)w(k)] \end{aligned} \tag{2.15}$$

The decision regarding the spectrum occupancy is taken as

$$T_{WF} \underset{H_0}{\overset{H_1}{\gtrless}} \lambda_{WF} \tag{2.16}$$

where λ_{WF} is the decision threshold for waveform based SS.

Waveform based sensing method is applicable only when the PU signal can be generated at the receiver side.

2.2.4 Covariance based Sensing Methods

2.2.4.1 Covariance Matrix based Sensing

Covariance based sensing exploits the difference in the covariance of the received signal when the PU signal is present and when it is absent [72]. Let there be L samples received in the model shown in (2.1) as

$$\begin{aligned} \mathbf{y(k)} &= [y(k)\ y(k-1)...y(k-L+1)]^H \\ x(k) &= h(k)s(k) \\ \mathbf{x(k)} &= [x(k)\ x(k-1)...x(k-L+1)]^H \\ \mathbf{w(k)} &= [w(k)\ w(k-1)...w(k-L+1)]^H \end{aligned} \tag{2.17}$$

The covariance matrices of $\mathbf{y(k)}$ and $\mathbf{x(k)}$ are defined as

$$\begin{aligned} \mathbf{R_y} &= E[\mathbf{y(k)y^H(k)}] \\ \mathbf{R_x} &= E[\mathbf{x(k)x^H(k)}] \end{aligned} \tag{2.18}$$

TH-1605_10610214

Since under H_0, $\mathbf{R_x} = 0$, the binary hypothesis testing problem is expressed as

$$\begin{aligned} H_0 &: \mathbf{R_y} = \sigma_k^2 \mathbf{I}_L \\ H_1 &: \mathbf{R_y} = \mathbf{R_x} + \sigma_k^2 \mathbf{I}_L \end{aligned} \tag{2.19}$$

where $\mathbf{I}_L$ is the $L \times L$ identity matrix. Since under H_0, $\mathbf{R_x} = \mathbf{0}$, the off-diagonal elements of $\mathbf{R_y}$ will be zero. Because of the spatial correlation in $s(n)$, the off-diagonal elements of $\mathbf{R_y}$ will not be zero, under H_1. This difference is used for the formulation of the decision statistic in covariance based mechanisms. Let $T_{1_{\text{cov}}} = \sum_{p \neq q, p=1, q=1}^{M} \mathbf{R_y}(p,q)$ and $T_{2\,\text{cov}} = \sum_{p=1}^{M} \mathbf{R_y}(p,p)$, where p and q represent the lags of $\mathbf{R_y}$, then the decision statistic T_{COV} for covariance based detectors is expressed as

$$T_{COV} = \frac{T_{1_{\text{cov}}}}{T_{2_{\text{cov}}}} \tag{2.20}$$

T_{COV} is compared to a predefined threshold λ_{COV} to decide between H_0 and H_1 as

$$T_{COV} \underset{H_0}{\overset{H_1}{\gtrless}} \lambda_{COV} \tag{2.21}$$

Covariance matrix based detection mechanism overcomes the limitations posed by noise uncertainty. It also performs excellently for detection with a limited number of PU signal samples.

2.2.4.2 Autocorrelation based Sensing

This technique exploits the difference between the signal and noise spectrums [73]. Consequently, this difference arises because of higher autocorrelation in the signal components arising by the use of modulation schemes as well as the presence of RF channel guard bands [73]. The principle of the method is to first calculate the autocorrelation of the signal under H_0, which in-turn gives only the autocorrelation of the noise. Then, the autocorrelation of the signal under H_1 is calculated which gives the autocorrelation of the signal also. These two autocorrelations are differentiated to decide about H_1 or H_0. The autocorrelation of $y(n)$, $R_{yy}(\tau)$ is given as

$$R_{yy}(k,\tau) = E[y(k)y^*(k+\tau)] \tag{2.22}$$

and the autocorrelation of $w(k)$, $R_{ww}(\tau)$ is given as

$$R_{ww}(k,\tau) = E[w(k)w^*(k+\tau)] \tag{2.23}$$

TH-1605_10610214

The decision statistic is given as

$$T_{AC} = \frac{1}{K}\sum_{k=1}^{N} |R_{yy}(k,\tau)| \tag{2.24}$$

The decision about the spectrum occupancy is taken as

$$T_{AC} \underset{H_0}{\overset{H_1}{\gtrless}} \lambda_{AC} \tag{2.25}$$

where λ_{AC} is the decision threshold for autocorrelation based SS. Note that the statistic for covariance based sensing T_{COV} is derived from the off-diagonal elements of the incoming signal covariance matrix. Whereas, the statistic for autocorrelation based sensing T_{AC} is derived from the autocorrelation functions of the incoming signal.

Further, in [74], both energy and correlation parameters have been exploited by proposing a simple correlation sum (CorrSum) detector for the improved sensing performance. Subsequently in [75], a Constant False Alarm Rate (CFAR) detection algorithm has been proposed using the estimated autocorrelation of the received signal.

2.2.4.3 Eigen Value based Sensing

Eigen value based detection has been popular in diversity exploiting techniques like multi-antenna sensing and CSS systems. The eigen values of the received signal's covariance matrix show some specific properties depending on the presence of the PU signal. Eigen value based detection is based on exploiting these properties. Let $\mathbf{R_s}$ represent the covariance matrix of $s(k)$ in (2.1), $\lambda_{y_1}, \lambda_{y_2}, \ldots, \lambda_{y_{Mr}}$ represent the eigen values of $\mathbf{R_y}$, and $\lambda_{s_1}, \lambda_{s_2}, \ldots, \lambda_{s_{Mr}}$ represent the eigen values of $\mathbf{HR_sH^H}$ for M_r number of receiving antennas. Here $\mathbf{H}$ is the channel gain matrix of $h(k)$ given as $\mathbf{H} = [\mathbf{hh}^H]$ where $\mathbf{h} = [h_1(k)\ h_2(k) \ldots\ h_{M_r}(k)]^H$, then for the ith SU,

$$\begin{aligned} H_0 &: \lambda_{y_i} = \sigma_w^2 \\ H_1 &: \lambda_{y_i} = \lambda_{s_i} + \sigma_w^2 \end{aligned} \tag{2.26}$$

There have been various methods for formulating the decision statistic for eigen value based detection T_{EV} [76, 77]. In general $T_{EV} = f(\lambda_{y_i})$ and

$$T_{EV} \underset{H_0}{\overset{H_1}{\gtrless}} \lambda_{EV} \tag{2.27}$$

where λ_{EV} is the decision threshold for Eigen value based detection. Eigen value based detectors are particularly found helpful for multi-antenna communication systems.

TH-1605_10610214

Throughout this thesis, we use energy detection method for performing SS. The reason for using this detection method is its wide popularity in researches [78]. It gains popularity because in a general situation, it is the most appropriate detection mechanism. The choice of an SS mechanism depends on the knowledge of the signal at the receiver and the channel and the SNR conditions. Some detection mechanisms illustrated above give a high performance given the signal knowledge is available with the receiver (examples are the matched filter detectors, the cyclostationary feature detectors, and the waveform based detectors). Other detectors which require a complex hardware are the covariance based detectors, the autocorrelation based detectors, the Eigen value based detectors. However, the detector which demands minimum resources for its implementation is the Energy detector. It has only one requirement that the signal SNR should satisfy a minimum SNR wall obtained in [9] as

$$SNR_{wall} = \frac{\rho^2 - 1}{\rho}, \tag{2.28}$$

where ρ signifies noise uncertainty N_u given as $N_u = 10\log_{10}\rho$. N_u signifies the uncertainty in the noise power. This makes energy detectors the most widely used sensing mechanism for SS. Throughout the thesis, we will assume that our SS environment satisfies the condition in (2.28).

The above explanation was intended to provide an insight to the principles of various detection techniques. In the following section, we present a detailed literature review of the security issues in Cognitive Radio systems.

2.3 Security Issues in SS

Security issues are one of the most significant concerns in CR systems [16]. In CR communications, the SUs sense the PU spectrum with the help of the CR technology. The sensing capability enabled by the CRs gives way to them to cause severe attacks. To launch attacks, the MUs can misdirect the SUs merely by manipulating their air interfaces and transmitting fake signals. The openness of the lower layers adds advantage to the MUs. The MUs can sense the spectrum and transmit fake signals according to the spectrum status. If the honest SUs are misdirected and cease their transmissions, the MUs easily take the advantage and start using the spectrum. Hence, security threat in CR communications is a serious obstacle in the successful operation of the CRs.

As mentioned in the previous chapter, the focus of this thesis is to counter the two major attacks namely SSDF attacks and PUEAs. The SSDF attacks have been further explored under individual

TH-1605_10610214

and collusion attacks. The SSDF attacks are caused in CSS systems while the PUEAs can be caused in individual and CSS systems both. In this thesis, both the SSDF attacks and the PUEAs have been studied for a CSS system. There are various counter mechanisms in the existing literature for these attacks [17–21]. We categorize the existing counter mechanisms as *active* and *passive* approaches. The active approach involves directly detecting the MUs with the help of some actions by the SU network towards the MUs. These actions involve detecting the location of the MUs by transmitting training signals, or installing hardware to detect the honesty and maliciousness of the incoming signals from the SUs by differentiating their strength, features or statistical properties. The passive approaches resist the MUs with some underlying actions. These actions may involve specially designing their SS mechanism to mitigate the effects of the MUs on a particular parameter like the probability of false alarm (P_{fa}) or the probability of detection (P_d). The passive approaches do not counter the MUs head-on. In the following sections, we explain the various studies carried out on these attacks and the mechanisms to counter them.

2.4 SSDF Attacks in CR Communications

As discussed earlier, the SSDF attacks are caused when one or more MUs transmit fake signals to misdirect the SUs performing CSS [14, 50]. The MU can be an external or an internal unlicensed user. An external MU is not a part of the CSS network while an internal MU is a user within the CSS network. These attacks can be caused by a single MU, multiple MUs independently, or multiple MUs in collusion. In the existing literature, various counter mechanisms for these attacks have been proposed. These mechanisms have been categorized as active and passive mechanisms and explained in the following sections.

2.4.1 Active Methods

Active methods aim at directly eliminating the malicious readings or detecting the MUs. The prominent active methods are location identification based approaches and statistical approaches. We brief about the existing works in each of these approaches as follows:

Location Identification based Approaches: Location identification based mechanisms counter the SSDF attacks by identifying the locations of the PU, the SU or the MU. The idea of using localization based approaches for countering MUs can be attributed to the Ma et al. in [17], where the localization of PUs has been carried out. They have aimed to locate the PU which

TH-1605_10610214

Table 2.1: Attacks and categorization of their countering strategies

Attack/ Strategy	Active	Passive
SSDF	Directly eliminate the malicious readings or point out the MUs	The SUs or the FC change their own detection strategies to minimize the damages caused by the MUs
PUEA	Active schemes are based on the cancelation of the PUE signal	Avoid the PUE signal or its interference by making appropriate changes in its own sensing mechanism.

helps in reducing interference to it and to detect it. The authors use the knowledge of the P_ds of all the SUs to detect the distances of each SU with the PU and formulate a weighted least squares mechanism and an iterative mechanism to improve the algorithm. The Cramer Rao Lower Bound (CRLB) of the mean square error (MSE) for the proposed algorithms has also been derived. Further this method is modified for detecting MUs. Ma et al. also design location aware mechanism access control protocol and show significant throughput gains. There are two kinds of algorithms for localization: range based algorithms and range free algorithms. The range free algorithms are less accurate but simple to implement, whereas Range based algorithms are accurate but complicated to implement. Ma et al. have obtained a simple to implement and accurate algorithm and term it as semi-range algorithm. They have mainly focussed on how the MUs are affecting the localization of the PU.

In [18], the MUs first geo-locate the position of the SUs from their sensing reports. This leakage of the location of the SUs is considered as the *privacy leakage* of the SUs. The authors in [18] carry out two steps, namely the privacy preserving sensing report aggregation (PPSRA) and the distributed dummy report injection (DDRI) protocols to prevent the privacy leakage. These two steps are together named as privacy preserving CSS. The PPSRA uses cryptographic techniques with which the FC can get the final result from each SU without needing its calculated individual value. Subsequently, the DDRI algorithm provides differential location privacy for SUs. In [18], a single service provider (SP) has been considered as a central entity serving a group of SUs. The authors in [79] consider the issue addressed in [18] for the multiple SPs case. In [79], each SP has a perfect knowledge of the group of SUs being served by it and CSS has been performed through the SPs. The attacks can be launched by the SUs, by the SPs, and by both. In the CSS model followed in [79], the information of SUs is shared with every entity in the network.

TH-1605_10610214

Hence, if some of the SPs or SUs are malicious, they can misuse the information to geo-locate the SUs by their sensing data. This causes compromises in localization privacy and hence the SUs are unwilling to share their spectrum. The proposed mechanism gives the SUs sufficient protection for privacy to incentivize them to share their data.

The authors in [80] aim at locating the mobile PUs under SSDF attacks. The accuracy in the localization of PU is severely affected under the attacks. The objective is to suppress the attacks from the MUs by tracking the mobile PUs. However, it becomes challenging when the MUs manipulate the data, because localization largely depends on the sensing results of the SUs. To face this challenge, the authors propose Sequential mOnte carLo combIned with shadow faDing estimation (SOLID) for attack/fault tolerant mobile PUs. This mechanism integrates sequentially Monte Carlo estimation based target tracking with shadow fading estimation. The sequential Monte Carlo estimation based tracking uses the sensing reports of the SUs iteratively to track the location of the PU. The shadow fading estimation part of the mechanisms refers to estimating the shadow fading correlation in the sensing reports induced by the PU's mobility. When the shadow fading estimation is integrated with sequential Monte Carlo estimation based tracking, the effects of the MUs on localizing the PU is significantly reduced.

In [81], the authors aim to detect the honest SUs in a CSS rather than the MUs. The authors aim to form a cluster with no MUs with a fast searching algorithm and propose a scheme based on clustering the honest SUs with a fast sensing algorithm. The proposed fast sensing algorithm groups the SUs into different clusters. The clusters transmit their decisions about the presence of the PU to the FC. From the decisions of various clusters, their distances from the PU is estimated. This estimated distance is compared to the actual distance and the corresponding error is calculated. If the error associated with a cluster is below a predefined threshold, it is regarded as honest with no malicious sensor. Such a cluster is categorized as a trusted cluster. Next, the FC decides the status of the PU channel only with the information shared by the trusted clusters.

Statistical Test based Approaches : In statistical approaches, the difference in the statistical properties of the honest SUs and the MUs is observed [49, 50]. The MUs transmit fake data to the FC which can be a constant or any other random value. Hence, the data from the MUs is likely to follow a distribution different from the SUs' data. One statistical approach is the outlier

TH-1605_10610214

detection approach where the data from the MUs are treated as outliers [44]. These outliers are aimed to be detected with various outlier detection methods.

One of the significant works in this regard have been done in [49] where the authors consider distributed detection in the presence of cooperative Byzantine attacks. These attacks are launched by Byzantine sensors which have been reprogrammed deliberately to send fictitious observations to the FC. To counter these attacks, the authors propose to obtain the optimal attacking distributions for the Byzantine sensors that minimizes the *detection error exponent*. Subsequently the smallest error exponent is obtained that signifies the power of the attack. The smallest error exponent is further used to obtain the minimum fraction of Byzantine attackers that are capable of damaging successful PU detection at the FC.

In [82], the authors propose an algorithm based on the Kruskal-Wallis test to detect the MUs without any a priori knowledge. This test is a non-parametric method for testing whether samples originate from the same distribution. The proposed algorithm uses the statistical differences between the cooperative decision and the individual SU decisions.

In [42], a Baysian approach is followed to detect the MUs. The authors assume some knowledge about the strategy of the MUs data to be available with the FC. Since it is assumed that the MUs' strategy is known, the a posteriori probability of their attacks can be known with reverse engineering on some captured MUs and hence all the MUs are detected subsequently. However, there is a limitation of having a priori information about the MUs' strategies.

The limitation of [42] has been overcome in [19]. Here, the authors consider that the knowledge about the strategy of the MUs is not available. They show that when the MU attacks individually, it can always be detected. Attacking individually means that the MUs are not aware about the responses of the other SUs. When the MUs know or can hear the other SUs, a strategy has been formulated such that the SUs are never detected by them. The authors formulate a strategy for the MUs that are never detected. The condition for this strategy is to have the knowledge P_{fa} and P_d. The authors point that practically the strategies of the MUs' cannot be known a priori, particularly for a system when the MUs can hear the other SUs and modify their attacks accordingly. Hence, the mechanisms proposed will fail to detect the MUs. To overcome the challenge of the unknown strategies of the MUs, a data mining technique to detect abnormalities has been proposed in [19]. This technique is essentially an outlier detection method and does

TH-1605_10610214

not require any a priori information regarding the MUs. The idea of this work is to place the sensing reports of the SUs in a high dimension space and detect possible abnormalities.

In [83], Srinu et al. study wideband sensing under SSDF attacks. The wideband is divided into multiple bands. They propose to predict the PU signal status on the multiple bands by integrating the entropy and cyclic properties of the received signal. The presence of MUs complicates accomplishing this proposal. The authors aim to eliminate the MUs by designing the generalized extreme statistical deviate and adjust boxplot methods by using uncertainty and autocorrelation properties of the signals. It is found that the proposed mechanism is efficient in eliminating the MUs.

Tang et al. in [84] have aimed to save the CR-mobile adhoc networks (MANETs) from security risks. The proposed scheme is a bio-inspired consensus algorithm. It takes the inspiration from self organizing behavior of the birds, fishes, ants, honeybees or other animals in groups. Engineering algorithms have been formulated on the basis of the behavior of animals in groups in the existing researches [85–87]. Studying the difference between the communication at the higher level and the animals at the lower level, the authors generate fundamental insights at the group decision at the higher level and individual communication. The algorithm makes the use of the local communication between the SUs. The major advantage of the algorithm is its low cost. Also the failure of a local SU node does not lead to the failure of the complete system. The basic requirement of this algorithm is to use the local communication and the group level communication model to strike out the unwanted signals inserted by the SSDF attacks and then make the correct decision about the presence of the PU which can be viewed as the multi agent coordination system. The summary of [84] is that it is local communication added to the global decision.

He et al. in [88] propose a statistical approach based on identifying the abnormal statistical spectrum sensing behaviors to suppress the malicious activities. Two hidden Markov models (HMM) have been adopted for the behaviors of the honest SUs and the MUs. The detection of the MUs is achieved by differentiating between the models. Due to the abnormal statistical characteristics, the HMM of attackers will be different from that of the honest SUs. Some features of the HMM will depict the difference. The algorithm is about inferring those different features regarded as the HMM parameters to fecilitate the detection of the MUs.

TH-1605_10610214

2.4.2 Passive Methods

In passive methods, the SUs or the FC make changes in their own detection strategies which minimize the damages caused by the MUs [51–54]. Passive methods include reputation based approaches, game theoretic approaches, and damage suppression. We briefly describe the major works done in each of these approaches below:

Reputation based Mechanisms: The reputation based mechanisms are mainly followed in centralized CSS systems [89, 90]. In these approaches, instead of directly adding the data from the cooperating SUs at the FC, a weighted decision rule is followed to implement CSS. The data from each SU is multiplied by a weight value. The weight value for an SU depends on the reputation of that SU which is formed by the *honesty* or *trust* in its data. The honesty is decided after observing its consistency with the FC over a period of time.

The authors in [51] consider reputation based sequential CSS for detecting MUs. They have investigated the existing data fusion techniques for their resistance towards the Byzantine Failure problem. Then, they propose a new algorithm which uses a variable number of samples rather than using a fixed number of samples. The *sequential probability ratio test* (SPRT) [91] has been extended by introducing a reputation based mechanism to develop the *weighted sequentially probability ratio test* (WSPRT). The SPRT supports sampling a variable number of observations. If a sensing terminal has low spectrum sensing accuracy, the SPRT can collect more local spectrum sensing reports. The reputation mechanism is introduced by associating weights with the likelihood function of each SU. The weights depend on the consistency of the sensing terminals with decision of the FC. At a time instant, if a sensing terminal is consistent with the FC, its reputation is incremented by 1. If it is not consistent, it is decremented by 1. A weight associated with an SU is a non-decreasing function of its reputation. It is seen that the proposed WSPRT is highly efficient in detecting the MUs.

The authors in [52] aim to restrict the damage caused by the MUs by considering more samples. They proposed the enhanced WSPRT (EWSPRT) and the enhanced weighted sequential zero/one test (EWZOT) which are robust against SSDF attacks. The EWSPRT and the EWZOT reduce the sample requirements for suppressing the effects of the MUs. However, the large number of samples causes high data overhead.

TH-1605_10610214

In [53], a reputation based approach is followed to detect the MUs. The system model contains multiple MUs and it is assumed that the number of MUs are known. An onion peeling approach, where the suspicious levels are calculated for each SU, is applied to detect the MUs. If the suspicious level is less than a threshold then the SU is regarded as honest. If the suspicious level crosses the threshold, its report is eliminated from decision making. The test is applied till there are no MUs left in the network.

The authors in [54] study the effects of MUs on CSS. The performance limits of CSS under these attacks have been analyzed. The authors show that above certain fraction of MUs, it is impossible for any reputation based attack strategy to counter them. The authors propose a new reputation based scheme. It is assumed that the attackers do not have the knowledge the other SUs in the network and are dependent only on their own decisions. The attack prevention strategies also aim at countering collaborative attacks. The proposed schemes are basically reputation based countering schemes designed by counting the mismatches between an SU's decisions and the FC's decision. After performing this operation for a period of time, the Byzantines are removed from the data.

In [89] and [90], the mobile CRNs under attacks have been considered. The existing researches to mitigate the attacks were proposed for static CRNs. These algorithms for static CRNs cannot be applied for mobile CRNs, because they need the localization information. If those algorithms are applied to mobile CRNs, the honest SUs having bad path-loss would be charged. For mobile CRNs, the authors propose to use two trust parameters *location reliability* and *malicious intention* (LRMI). A high LR signifies the location of an SU having less path-loss whereas MI signifies to the intention of the SUs. It is observed that the proposed scheme improves both the MU detection rate and the PU detection.

In [92], the effect of multiple MUs on the energy efficiency along with the detection accuracy of the CR has been studied. A low overhead symmetric cryptographic mechanism based protocol to address SSDF attacks under a trade-off between the energy efficiency and the security of the CRN is given. An optimal number of security bits needed to maximize the energy efficiency has been derived. The authors show that the effects of MUs on energy efficiency depend on the fusion rule, which is used to form the global decision.

The authors in [93] rely on the consistency of the system states estimated by each SU. The

TH-1605_10610214

proposed scheme removes the abnormalities in the data of the various sensors irrespective of the cause of the deviations in the abnormal reports. System states refers to the path loss exponent [94] and the PU signal power. The MUs do not have control over these parameters. The authors propose iteRatIve State estimation (IRIS) scheme to detect the abnormalities in the data. The IRIS scheme does two examinations: the received signal power and the path loss exponent of the path. By examining each sensor's result, the scheme finds the measurement residual, which indicates the deviation of the PU signal power and the path loss from their normal values.

In [95], the authors use *combinatorial optimization identification* (COI) [96] to counter the SSDF attacks. The proposed technique is a complement to the previously proposed IRIS technique. The authors have studied the attack scenario where IRIS does not work. The IRIS may also remove a good data sample having a large residual while keeping a compromised data sample. As a prevention mechanism, the authors propose COI to complement the IRIS.

The authors in [97] mainly design a reputation based classifier to classify the SUs and the MUs. The classification is based on more than the traditional two divisions of honest and malicious. Such classification helps to handle the case when different honest SUs have different individual P_{f_i}s and P_{d_i}s and there are multiple types of MUs. An iterative expectation maximization algorithm is used to make this classification, calculate global P_{fa} and P_d, and reliably detect the PU for the sensing system under the attacks. Their assumption is that the MUs are less in number than the SUs. Except this assumption, no prior knowledge at the FC has been assumed. The MUs can be classified on various grounds like having bad signal and channel characteristics. The MUs have been divided on causing more than one types of attacks. This is done with only few divisions from the CRs while in traditional reputation based classifiers large number of SUs cannot classify the SUs perfectly. The proposed mechanism outperforms other reputation based mechanisms particularly for large number of SUs.

Game Theoretic Approach: In the game theoretic approaches, the CR communication systems are analyzed with game theory [98–100]. In a general game theoretic set up, the SUs, the PU, and the FC are regarded as *players*. Their actions are termed as strategies and the outcome of their actions are termed as *utilities* or *pay offs*. The benefits obtained by an SU in reporting honestly and maliciously are termed as honest and malicious utilities respectively. A general

TH-1605_10610214

objective in this approach is to maximize the honest utility and minimize the malicious utility, so that the SUs do not turn malicious. Some of the major works following this approach are described as follows:

In [98], the following colluded denial of service (DoS) attacks has been studied: This paper performs the security study from the perspective of the MUs. The colluded malicious activity has been studied in single and multiple stages. These attacks are performed with a game theoretic approach. The attackers maximize their utility in a group rather than maximizing their individual utilities. In a single stage scenario, a cooperative game is formulated where the malicious nodes aim to attack as many secondary networks as possible while putting a minimum constraint on the cost or penalty they have to pay. The theoretical expression for the net pay off has been formulated for the MUs and the optimal strategy is derived for them. In a multistage discrete time scenario, the Markov chain model for the dynamic behavior of MUs has been formulated. The Markov chain models the change of the states. It is proved that as the system reaches the steady state, the net pay off becomes independent of the switching probability and becomes dependent on the number of SUs. Finally the authors obtain the optimal number of malicious users to carry out attacks successfully.

The colluded DoS attacks have been countered in [101], where the effects of coordinated DoS on identity management (IdM) systems have been minimized. A brief description of this paper will be given in Damage suppression approaches.

In [99], the authors have investigated an attack scenario where the SUs can access a single frequency band at a time and they hop among the different channels. They study the communication between the SUs and the MUs to find the optimum hopping strategy for the SUs using the Markov decision process. The hopping strategy is aimed towards countering the jamming attacks. Initially, the analysis is done for a perfect knowledge of the channels. Subsequently, two schemes have been proposed for the SUs to gain the knowledge of the adversaries. This knowledge enables them to handle attacks. The authors have also considered the case when the SUs can use all the channels simultaneously. The anti-jamming game is redefined for this case and the problem is modeled as Colonel Blotto game where random power allocation is the defense strategy. These games are zero sum games where players are tasked to distribute limited resources over several objects. The Nash Equilibrium has been established for this game which

TH-1605_10610214

minimizes the worst-case damage.

In [100], the authors have modeled the jamming and anti-jamming processes as Markov decision processes. Following this approach, the SUs are able to counter the attacks from the MUs and maximize their pay-off function. First the authors use *first policy iteration* [102] method. However, the method is computationally expensive. Hence, the authors use Q function method to solve the problem.

Damage Suppression Approach: In this approach, a particular damage caused by the MU to a specific entity of the SU network is detected and reduced [103–107]. Unlike the above approaches, it does not depend on detection, localization or down weighing of the MU. The affected entity can be the PU, the energy harvesting scheme, the channel coordination, the secrecy of the data etc. Some of the major existing works and their mechanisms have been briefly explained as follows:

In [103], the SUs get the favor from the PU to use its spectrum only when the SUs secure the PU communication from the MUs present in the system. Hence, the SUs behave as a jammer for the MUs. The mechanism has been carried out in two hops: In the first hop the SU transmitter sends the information to the relay set and the SU receiver acts as a friendly jammer to disturb the overhearing of the MUs. In the second hop the relay transmits the information to the SU receiver and the SU transmitter acts as a friendly jammer to disturb the overhearing of the MUs. In this process, the time duration of each hop, the power of the signals transmitted, and the relay selection at the second hop are allocated in a manner to maximize the secrecy rate of the SU subject to the minimum required secrecy rate of the PU. The possibly disturbing SU service from the perspective of the PU is brought into a rather beneficial service. The main objective of the work is that the secrecy of the SU should not be compromised. The authors design optimal relay selection, time allocation, and power allocation for these issues. The schemes are efficient in protecting the secrecy rate of the SU while at the same time protecting the secrecy rate of the PU.

In [106], the secrecy performance is investigated in terms of an outage probability. A relay scheme is proposed to prevent eavesdropping and assist transmission from the CR transmitter to CR receiver. It is shown that the physical layer secrecy is significantly improved by increasing the number of relays. An additional security issue is that a CR has the capability to sense the

TH-1605_10610214

environment. This capability can be used to launch attacks. This increases the chances of a CRN to have more attacks than a normal communication system. The broadcast system also increases the chances to overhear secure communications.

In [104], the energy harvesting systems have been considered. The issue addressed is that MUs can also harvest energy for their operations like the honest SUs. In this paper, the authors have formulated the throughput optimization problem under MU attacks as a Markov Decision process. Then a new solution based on deception tactics to stop smart MUs has been presented. Further, a learning algorithm for multiple SUs to find an optimal transmission policy has been designed. It is shown that these learning algorithms are effective in stopping smart MUs.

The authors in [105] focus on the coordination of channels in spectrum sharing systems in the presence of MUs. Reliable coordination of the channels is very important in CRNs. This coordination may be smooth until all the CRs in the SU network are honest. However, if the SUs start behaving contrary to their channel assignment, then such benefits associated with the channel coordination are negated. The authors in [105] focus on the dilemmas that occur in the coordination because of the attacks. The first dilemma is with the PU when it thinks that the SU is honest. On the other hand, if it thinks that the SU is malicious then it has to chose a band from a larger set of bands which invites more interferences. Similarly, there are dilemmas associated with the SUs about what the PU thinks about it. If the PU has a positive opinion about the SU, then the SU is allowed to transmit on the PU band. However, if the SU has a malicious image, then it will transmit on the SU band only. Corresponding to these beliefs, a game has been formulated and a game theoretic approach has been followed to solve the problem accordingly. The players are the PU, the SU, and the SP. The authors consider an example of two secondary service providers (SPs) with their own set of SUs. Suppose, each SP has been allotted a channel. The SPs will be benefitted in protecting its SUs from any possible interference. Similarly, they will get other benefits in harming the other channels. So, there are a set of strategies which the SUs can play. This reference also comes in the category of game theoretic approaches. However, since the authors aim to suppress the damage of SSDF attacks on the channel coordination, we have explained it in the damage suppression approaches category.

In [101], the damage caused by the coordinated DoS attacks designed with the mechanism in [98]

TH-1605_10610214

on the identity management (IdM) systems has been minimized. Identity management systems provide authentication authorities critical data. Through IdM systems, the SUs can authenticate at the single and multiple domains without providing additional information. IdM systems also help in reducing the complexity in the management of the data. They benefit many large systems like cyber-physical systems, smart grids, and vehicular ad-hoc networks. However, coordinated DoS attacks can severely affect IdM systems. The authors in [101] present Scheme for DoS Attacks Mitigation by the reOrganization and optimization of the IdM System (SAMOS). This scheme is based on adaptive reorganizations and optimization of the IdM systems' components to thwart DoS attacks. The coordinated DoS attack strategy has been considered from [98] and SAMOS aims at thwarting it. It is found that SAMOS is efficient in this purpose.

In [107], an attack aware CSS scheme has been proposed for detecting the MUs. An n out of N decision fusion CSS system has been studied. The proposed method obtains the optimal value of n by obtaining and applying the attack strength to it. The attack strength has been defined here as the ratio of the MUs to the total number of SUs in the system. This ratio comes out to be the probability of an SU of being malicious. The optimal value of n minimizes the Bayes risk.

2.5 PUEAs in CR Communications

As mentioned in the previous chapter, PUEAs are launched when the MUs attack by transmitting the emulated PU signal. The PUEAs severely compromise the functioning of the SU network. There are many existing and ongoing researches to defend the SU network from PUEAs. We categorize the the major proposed mechanisms as Active and Passive approaches.

2.5.1 Active Methods

The active methods aim at canceling or suppressing the PUE signal by differentiating the power or a feature of the PUE signal from the PU signal. There are many existing researches based on the active approaches. We describe some of the major researches here.

The most significant work on detecting a PUE is in [55]. Here the authors have focussed on the vacant TV bands, since the FCC has recognized the TV bands suitable for the initial application for CR technology. These TV bands experience lower dynamic traffic compared to the cellular networks. In this paper, a transmitter verification scheme termed as *LocDef (localization based defense)* has

TH-1605_10610214

been proposed. In this scheme, the source of the signal is verified for being the PU by observing the signal characteristics. The location information of the PU has been used to differentiate between the PU and the PUE signal characteristics. The authors assume a stationary and known PU location. To implement this scheme, LocDef uses a *non-iterative localization* scheme. This method primarily depends on the modeling of the received signal from the PUE.

In [20] , a tag authentication method has been proposed where a tag, dependent of the PU signal, is added in it. The tag acts as an authentication information of the PU and is transmitted concurrently with its data. It is added in the PU signal by superimposing a secret modulation in the transmitted PU signal without requiring additional bandwidth. The main contribution of this work is the designing of an authentication system in the physical layer. The problem with authentication at the higher layers is that the PU and the SU need the same protocol. However, it is not possible that the SU and the PU may always use the same protocol or even have the same layer or network architecture. Hence, the authors fulfill the need of authentication at the lowest layer so that the higher layers are neither disturbed by it nor depend on it. In [108], the authors further improve the tagging system of [20] by making it independent of the PU signal. In the first stage, a tag is developed and in the second, the developed tag is embedded with the PU signal. At the receiver, the PUE signals are checked for the tag and if they do not posses it, they are canceled out.

In [21], a mechanism based on finger print detection has been proposed, where some device specific features like device ID, MAC address, radio-metrics such as amplitude, frequency, and bandwidth etc are used as finger prints of the PUs. These features are used to determine the number of transmitting devices in the PU spectrum with a non-parametric classification method. The proposed method is also non-parametric since the number of devices needs not be known a priori. After forming the finger prints, the authors adopt the infinite Gaussian mixture model (IGMM) and propose a modified collapsed Gibbs sampling method to classify the extracted finger prints based on Baysian classification. In the first module, the authors first check the phase of the signal and the carrier frequency of the signal because those properties are unique for the transmitter. Then they check the MAC address and from the MAC ID database, they differentiate it. The second module checks the signal ID. If the PUE transmits from the same ID but a different finger print, it is detected. It is found that the proposed classification efficiently detects the PUEs. The proposed mechanism is independent of the number of transmitters, hence it needs not to be estimated.

TH-1605_10610214

In [57], the PUEs are assumed to have the capability to detect channels which are going to be used by the SUs and attack accordingly. The authors propose a cooperative mechanism based on sharing the messages among all the SUs. Each SU calculates a local function, a compatibility function, and exchanges the information with the neighboring SUs. It calculates its own belief with the help of the information from all the other SUs. The distribution of the RSS from the PU and the suspect are used to perform these operations. The belief calculation is performed iteratively until the SUs converge to a common belief about the PUE. Then, the PUE is detected and its signal characteristics are broadcast to the CRs in the network. Finally, the SUs are able to avoid the PUE's signal.

In [109], a game theoretic framework has been proposed to discard the PUEAs. The authors formulate a non-cooperative multistage game between the SUs and PUEs. The strategy of the SUs and PUEs are different. The SUs leave the spectrum on the arrival of the PU. But the PUE tries to interfere with it while also trying to keep the SUs away. A novel belief updating system for updating the SUs belief about the PUs has been proposed as the game evolves. It is shown that the proposed belief updating system achieves satisfactory performance for the SUs in terms of recognizing the true PUs and canceling out the signals from the PUEs.

The authors in [110] consider the two PUs: TV towers and microphones. The transmitters like the microphones or the mobile transmitters which are moving and have low transmission power. The relation between the RF signal energy level and the acoustic information of the TV signal which the PUE is not able to mimic has been exploited to differentiate the PUE from the PU.

In [111], RF finger-printing has been suggested to detect the PUE attackers. Low cost CRs have been considered for detecting the RF finger-prints in the PUEs. This is mainly an experimental work which investigates the distortions made by low-end CR receivers in the RF finger prints. The final conclusion is that RF finger-printing can successfully detect the PUEs only when the CRs have high end receivers.

In [112], the authors propose a mechanism which does not need any a-priori knowledge of the PU. The detection of PUE is done by the acquisition and the reconstruction of the signal activity pattern This technique acquires the activity pattern of the signal through SS. For example the ON and OFF periods of the signal may be acquired as the activity pattern. Then, it reconstructs the signal with a signal reconstruction model and checks it for any error. By examining a reconstruction error, the signals from a PU or a PUE are differentiated. The paper aims to overcome the limitations of location

TH-1605_10610214

based identification and finger-print methods which need knowledge about the signal characteristics or the location of the PUE.

Pu et el. in [113] detect the motion-related feature vectors of PUs in the FFT of its signal to differentiate PUE from it. A database where the signal from the PU is given is referred. The authors record the data from the incoming signal and compare it to the data from the database. For further classification, they feed this data to a covariance descriptor with the help of a neural algorithm. The covariance descriptor classifies the incoming signal database with the existing signal database to detect the PUEs.

In [114], two strategies have been proposed for the detection of the PUEs. The first strategy is a channel surveillance process to check for the presence of the PUEs. The second strategy is aimed at detecting new transmission opportunities for the PUEs. An extra sensing process has been implemented to carry out the second strategy. The PUEs have been categorized as *selfish*, *malicious*, and *mixed*. The selfish PUEs aim for transmitting whereas malicious PUEs only aim to cause problem for the SUs, like obstructing the operation of the CR network. The mixed PUEs launch attacks in both the forms. In this process, the channel has been sensed and if an SU signal is found on the channel, it indicates that it is being used by a selfish PUE. If the FC senses a channel declared busy as free after the sensing time, that means it was attacked by a PUE. It is found that it is possible to retrieve the opportunity of using the attacked channel by sensing it again after the sensing time finishes. Hence, an extra sensing process has been proposed. Essentially, the selfish PUE keeps transmitting throughout the sensing and the transmission periods of the SU whereas the malicious PUEs transmit only for the sensing time. The authors have studied this problem with a game theoretic approach. The PUEs and the defenders are considered players and the Nash equilibrium has been derived for all the three attackers (malicious, selfish, and mixed PUEs).

Many more existing and ongoing active researches can be found in the literature. However, the primary limitation of the active mechanisms is the need of at-least one characteristic of the PU or the PUE signal. This limitation is overcome in the passive mechanisms, which we will explain in the following section.

2.5.2 Passive Methods

The passive approaches have been applied in two ways:

(i) Suppressing one or more harmful effects of PUEAs on the SU network rather than directly

TH-1605_10610214

canceling its signal with the help of the channel state information (CSI) of the PUE with the PU or the SU with the PU.

(ii) Avoiding the signals from the PUE using the CSI of the PU or the PUE.

The difference between the passive approaches and the active approaches is that the passive approaches are independent of the features, the RSS, the external tagging, or the classification of the PU or the PUE. Secondly, the active approaches may have to make some modifications in their sensing strategies after detecting the PUE, like canceling its signals. However, the passive approach follow the normal sensing integrated with a mechanism for the suppression of a particular damage caused by the PUE signal or its avoidance with the help of CSI. Following are some of the major works with passive approaches with the above applications:

Suppressing the harmful effects of the PUEAs: The authors in [24] use the channel information to minimize the damage caused by the PUEAs to the robustness of a CSS system. The paper considers a basic cooperative model with an always-on PUE. The expressions for P_d and P_{fa} are obtained for a CSS system where a PUE is present. Then, P_d is maximized with a bound on P_{fa} to obtain the optimal weights for performing CSS. The optimal weights are functions of the channel gains of the PU and the PUE with the SU. Hence, in this paper, the damages of PUEAs on the PU detection performance of the SUs has been minimized.

The authors in [58] and [60] investigate the harmful effects of smart PUEAs on the CSS network. Smart PUEs attack only when the PU is absent. The degradation caused by the PUEAs is accounted as *probability of error* P_e, which is defined as the sum of P_{fa} and $1 - P_d$. In both these papers, decision fusion CSS has been considered and both aim at minimization of P_e. The parameter optimized for achieving the minimum P_e is the transmission time. The difference between the works is that the authors in [58] investigate for n out of N decision fusion systems whereas, the authors in [60] investigate for OR and AND rule based decision fusion systems.

Alahmadi et al. in [115] aim at countering the damages caused by PUEAs on energy harvesting in an OFDM modulation based CR system. A DTV signal has been considered and the P2 pilot symbols are generated using an advance algorithm for encryption. The main aim of this research is sum-rate-maximization of the energy harvesting based SU system facing PUEAs. The sum-rate is the sum of the downlink transmission and the uplink transmission of the SUs.

TH-1605_10610214

Alahmadi et al. minimize the interference of the PUEAs which affect the sum rate for the SUs.

Avoiding the PUE signal: The authors in [116] and [117] combat PUEAs with a game theoretic approach. It is assumed that the channel statistics like channel availability probability are known a priori. The proposed idea is that the SUs will escape the PUEAs by randomly hopping on the available channels. Such random hopping is unlikely to be detected by the PUEs, and hence they will fail to harm the SUs. However, this creates a dogfight between the PUEs and the SUs. The work is aimed at studying the dogfight in accessing the spectrum, which refers to random hopping over the frequency bands to get access to them for their transmission.

The authors in [118] and [119] address the similar objective of [116] and [117] but for an unknown channel. In [118] and [119], the channel availability probability is unknown, and a blind dogfight algorithm has been proposed. To solve this issue, the algorithm of the *adversarial bandit* problem is adapted. The proposed works are passive defense based on the assumption that there are multiple channels available. The objective here is to intelligently use those multiple channels to avoid the PUEAs.

In [120], the PUEs have been viewed as attackers which can behave as a PU or an SU. The authors assume that the other SUs do not know about their fellow SUs or the PU. To check their knowledge about the PU or their fellow SUs, a Bayesian game has been formulated which depends on the SUs' belief about a fraction of PUs. A policy maker can control the gains and costs associated with performing or checking for PUEAs. The authors derive conditions for the Nash equilibrium, the conditions which throw light of some important facts such as whether the honest SUs will exist with PUEAs, with what probability PUEAs launch attacks, under what conditions the PUEAs are discouraged, with what probability the radios will challenge the license of other radios etc. These results can be used to determine appropriate policies to keep the rate of PUEAs low.

It can be concluded from the literature review above, both the active and passive mechanisms are being followed to counter the SSDF and PUE attacks. Both these mechanisms have certain advantages and disadvantages in countering SSDF and PUE attacks respectively. With this background on the existing works, we proceed to the next chapter which presents our work on individual SSDF attacks.

TH-1605_10610214

TH-1605_10610214

3

Suppression of SSDF Attacks by Multiple Malicious Users

Contents

3.1 Objective 44
3.2 System Model 46
3.3 Detection of MUs as an Outlier Detection Problem 51
3.4 Dixon's Test for Outlier Detection 55
3.5 Proposed Method 59
3.6 A Note on the Complexity of the Proposed Schemes 62
3.7 Simulation Results and Performance Assessment 63
3.8 Conclusion 75

TH-1605_10610214

3.1 Objective

The SSDF attacks are caused when an MU reports false data or decisions to the FC in a CSS system. As mentioned in Chapter 2, there are various active and passive approaches to counter the SSDF attacks. An efficient active approach is based on statistical outlier detection tests. These tests remove the malicious data by determining their oddness with the rest of the data. One such statistical test known as Dixon's test, has been used for the detection of a single MU [121]. In this chapter, we propose to enhance the efficiency of the Dixon's test and make it applicable for detecting multiple MUs. In statistics, an outlier is a data sample inconsistent with the assumed distribution or the model of the data. The Dixon's test is a statistical tool to detect an outlier. It was proposed in the year 1950 by Wilfrid J. Dixon [121]. Later in 1951, it was found suitable for chemists in detecting outliers in small data sets [122]. Statistical tests have been used in Chemistry to detect the outliers in qualitative and quantitative observations [123]. The authors in [122] found Dixon's test computationally easier and accurate for detecting outlying observations in small data sets for chemists. Prior to the proposal of [122], the statistical tests for large number of data sets were used for smaller data sets also. However, such an application was found inaccurate, like the student's t test showing a Gaussian distributed error for small number of observations [124]. Dixon's test gained popularity for its use in small data samples in [122].

Other than applications in Chemistry, Dixon's test has also been applied in several research works in communication networks and signal processing. The main advantage of Dixon's test is its calculational simplicity. In [125], the authors have proposed a routing scheme based on Dixon's test named as *Priority-based Hybrid Routing (PHR)*. PHR assigns different priorities to the deployed nodes based on their environment. The nodes reporting sudden changes of high magnitude are given higher priorities. This is because such nodes are possibly subjected to hostile conditions like fire or cyclone. To detect these nodes, the authors apply Dixon's test for its simplicity and robustness. The work in [126] is based on global navigation satellite system (GNSS) positioning of nodes in an indoor environment. This is done with the help of carrier phase measurements of the transmitting node. These carrier phase measurements are interrupted by cycle slips. The cycle slips are outliers to the rest of the carrier phase measurements. The authors aim for a computationally simple mechanism to detect these cyclic slips. They use several statistical methods but find Dixon's test to be effective yet simple for detecting the cycle slips. The efficiency of Dixon's test over other statistical tests has also been proved in [2].

TH-1605_10610214

In [127], Dixon's test has been used to design a filter for image soothing and restoration. The paper uses multilevel median (MLM) filters to overcome the limitations of median filter in preserving thin line details (TLD). However, the proposed mechanism is not robust to the outliers arising as a result of the edges. To bring robustness towards these outliers, Dixon's test has been used for its simplicity and efficiency. In addition to the MLM filter, one module performs Dixon's test to find the different regions of the image. In [2], Dixon's test has been used to detect an MU in CSS. The limitation of the scheme in [2] are:

- Inefficient usage of Dixon's test.
- Inapplicability to the detection of multiple MUs

In this chapter, we propose to overcome the limitations of [2]. We propose two schemes that improve the outlier detection efficiency of the Dixon's test and make it applicable to detecting multiple MUs. The schemes are based on applying the test in multiple overlapping smaller blocks of the cooperating CR users' data. Applying the test on multiple blocks enhances the scope of the Dixon's test to multiple outlier detection.

The contributions of this chapter are as follows:

- Suggesting optimum group size division of the incoming data for efficient MU elimination.
- Making Dixon's test applicable to detecting multiple MUs.
- Bringing improvement in the performance of the Dixon's test without a significant increase in the complexity.

The rest of the chapter is organized as follows: In Section 3.2, we present the system model where the hypothesis testing problem, the parameters for the evaluation of the schemes, and the attack process have been explained in detail. In Section 3.3, we first illustrate the analogy between the detection of the MUs and the detection of the outliers. Then, we explain the outlier detection tests that have been used in the literature for detecting the MUs. Section 3.4 gives a detailed explanation of the Dixon's test for outlier detection. Then in Section 3.5, we illustrate the proposed schemes. Here, we discuss the application of Dixon's test in our work and the algorithms based on it. In Section 3.6, the complexity of the proposed mechanisms has been analyzed. In Section 3.7, we present the simulation results and discuss the outcome of the work in detail. Finally, in Section 3.8, the conclusions for the work in this chapter have been drawn.

TH-1605_10610214

3.2 System Model

In this section, the binary hypothesis testing problem for the detection of the PU, the performance evaluating parameters, and the attack process have been explained in detail.

3.2.1 Hypothesis Testing for PU Detection

Consider N SUs located arbitrarily in a region around the PU. The PU spectrum is to be sensed by the SUs for their usage. There are mainly two types of SS: continuous SS and periodic SS [128]. We consider periodic SS, where the cooperating SUs are allotted with time frames. Each time frame consists of a sensing period T and a transmission period T_1 as shown in Figure 3.1. The spectrum is

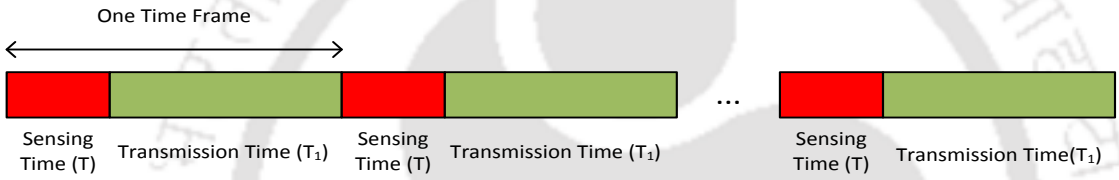

Figure 3.1: Periodic Sensing by SUs

sensed by the SUs during the sensing period T. This is done with the help of the received signal at the SUs from the PU band. The decision about the spectrum occupancy can be made by deciding one of the following two hypotheses [68],

Hypothesis H_1: The PU signal is present.

Hypothesis H_0: The PU signal is absent.

The received signal $y_i(t)$ by the ith SU from the PU can be expressed using the above mentioned hypotheses as

$$y_i(t) = \begin{cases} h_i(t)s(t) + w_i(t) & : H_1 \\ w_i(t), & : H_0 \end{cases} \tag{3.1}$$

where $s(t)$ denotes the PU signal, $h_i(t)$ denotes the multipath channel fading component and $w_i(t)$ is the additive white Gaussian noise (AWGN) at the ith SU.

Since, the sensors of the SUs are assumed to be energy detectors, (3.1) has to be recast with the decision statistic as the energy of the received signal. The energy $e_i(m)$ of the signal received by the

TH-1605_10610214

ith SU for the mth sensing interval is given by,

$$e_i(m) = \int_{(m-1)(T+T_1)}^{(m-1)(T+T_1)+T} |y_i(t)|^2 dt \tag{3.2}$$

Let the mth sensing interval of duration T be divided into M samples each of duration T_s, such that $MT_s = T$. The integration in (3.2) can be approximated by the sum of the squared signal samples. Thus,

$$e_i(m) \approx \sum_{j=0}^{M-1} |y_i((m-1)(T+T_1) + jT_s)|^2 \tag{3.3}$$

Since, $w_i(t)$ is assumed to be AWGN, $e_i(m)$ in (3.3) will follow a central chi-square distribution under H_0 and under H_1, it will follow a non-central chi-square distribution with M degrees of freedom [68] as

$$e_i(m) \sim \begin{cases} \chi^2_{2M}(\gamma_i) & : H_1 \\ \chi^2_{2M} & : H_0 \end{cases} \tag{3.4}$$

where γ_i is the non-centrality parameter and is the sum of the mean values of the $y_i(m)$ samples. Each SU sends its calculated energy value $e_i(m)$ to the FC through an error free reporting channel. The energies of the N cooperating SUs are fused at the FC as [2]

$$E_N(m) = \frac{1}{N} \sum\nolimits_{i=1}^{N} e_i(m) \tag{3.5}$$

At the FC, the calculated $E_N(m)$ is compared to a pre-determined threshold λ [34]. The decision rule at the FC is given by,

$$E_N(m) \underset{H_0}{\overset{H_1}{\gtrless}} \lambda \tag{3.6}$$

It can be seen that $E_N(m)$ in (3.5) will also follow a chi-square distribution as

$$E_N(m) \sim \begin{cases} \chi^2_{2MN}(\gamma) : H_1 \\ \chi^2_{2MN} \quad : H_0 \end{cases} \tag{3.7}$$

where χ^2_{2MN} is the chi-square distribution with $2MN$ degrees of freedom and γ is the non- centrality parameter given as $\gamma = \sum_{i=1}^{N} \gamma_i$. The probability density function (pdf) of $E_N(m)$ under H_0 will be,

$$f_{2MN}(E_N) = \frac{E_N^{MN-1} e^{-E_N/2}}{2^{N/2}\Gamma(N/2)}$$

TH-1605_10610214

while under H_1, its pdf will be given as

$$f(E_N, \gamma, 2MN) = \sum_{j=0}^{\infty} \frac{e^{-\gamma/2}\left(\frac{\gamma}{2}\right)^j f_{2LK+2j}(E_K)}{j}$$

The distribution of $E_N(m)$ under H_1 is the Poisson-weighted sum of $E_N(m)$s under H_0.

3.2.2 Performance Parameters

The performance evaluation of a SS scheme is based on two parameters, the probability of detection P_d and the probability of false alarm P_{fa} [34]. P_d is defined as

$$P_d = \Pr(E_N(m) > \lambda | H_1) \tag{3.8}$$

and P_{fa} is defined as

$$P_{fa} = \Pr(E_N(m) > \lambda | H_0) \tag{3.9}$$

An SS system is considered efficient if P_d is high and P_{fa} is low. The result of a higher P_d is a low SU interference to the PU, whereas a low P_{fa} results in a higher throughput of the SU system [129].

Note that P_d and P_{fa} depend on the choice of λ. The optimal value of λ is chosen using the Neyman Pearson method [34]. In this method, a value is fixed for P_{fa} and the corresponding λ are calculated. This calculation can be performed with the closed form expression of P_{fa}. However, when evaluating a closed form expression for P_{fa} is not possible or difficult, λ is calculated by Monte-Carlo simulations which have been extensively used in Communications and Signal Processing [130]. In our CSS model, the $e_n(m)$ values reported by the MUs follow a different distribution from the rest of the data. As a result, random shifts are caused in the $E_N(m)$ values and hence in the P_{fa} and P_d values. This makes obtaining their closed form expressions difficult. Hence, all the evaluations in this chapter have been done by Monte-Carlo simulations. We implement Monte-Carlo simulations in the following steps:

(i) Form a set S_λ of λ values. The values in S_λ should cover the entire range of the possible magnitude of $E_N(m)$ under H_0 and H_1 with a high resolution.

(ii) Assume H_0 true and calculate a sufficiently large number of $E_N(m)$ values, say N_E, over H_0.

(iii) Choose each λ iteratively from S_λ, and denote the number of $E_N(m)$ exceeding it by $N_{E_{H_0}}$.

(iv) Evaluating $N_{E_{H_0}}/N_E$ gives P_{fa} for that λ. Perform this step iteratively until the desired P_{fa} is

TH-1605_10610214

obtained.

(v) After obtaining the desired P_{fa}, save the corresponding λ as λ_o.

(vi) Now, calculate N_E number of $E_N(m)$ values over H_1.

(vii) If the number of $E_N(m)$ values crossing λ_o is $N_{E_{H_1}}$, evaluating $N_{E_{H_1}}/N_E$ gives P_d.

The evaluation of an SS system is done by plotting region of convergence (ROC) curves. These curves show the variation of P_d with P_{fa}. For plotting the ROC curves in Section 3.7, we perform Monte-Carlo simulations with the above mentioned steps over a set of distinct P_{fa} values covering the range $0 \leq P_{fa} \leq 1$ and obtain the corresponding P_d values. However, in order to show the shifts inserted by the MU data in the P_{fa} and P_d curves separately, we have modified the conventional ROC curves by plotting each of them separately with λ.

In the next section, we discuss the SSDF attack process followed in this chapter.

3.2.3 The Uncertainty in SS and the Attack Process

The unreliability in SS can be caused due to two causes: the system uncertainty and the maliciousness of some SUs. Figure 3.2 shows the factors responsible for these causes. The system uncertainty is caused by the receiver noise and the attenuation in the signal from the environmental obstacles. The environmental obstacles cause small scale fading, large scale pathloss, and shadowing to attenuate the PU signal. Small scale fading refers to the rapid fluctuations caused in the transmitted signal due to smaller obstacles like trees, small buildings, etc. These obstacles attenuate the signal by scattering, dispersing or reflecting it. Large scale pathloss refers to the effects of the transmitter-receiver distance on the signal. The power of the transmitted signal attenuates with the distance it travels. This attenuation depends on the path loss exponent. Shadowing refers to the attenuation caused in the transmitted signal by large environmental obstacles like hills, tall buildings etc. These obstacles attenuate the transmitted signal by absorbing it. The above mentioned natural causes of attenuation, if present between the PU and the SUs, prevent the PU signal from reaching the SU receivers in its original form and power. Hence, they bring uncertainty in SS. As mentioned before, CSS has been proposed to minimize these natural causes of uncertainty. The idea of CSS is to exploit the spatial diversity of the environment. An SU may be present in a more faded area while another SU may be present in a less faded area. When all the SUs fuse their data or decisions to the FC, it can benefit from

TH-1605_10610214

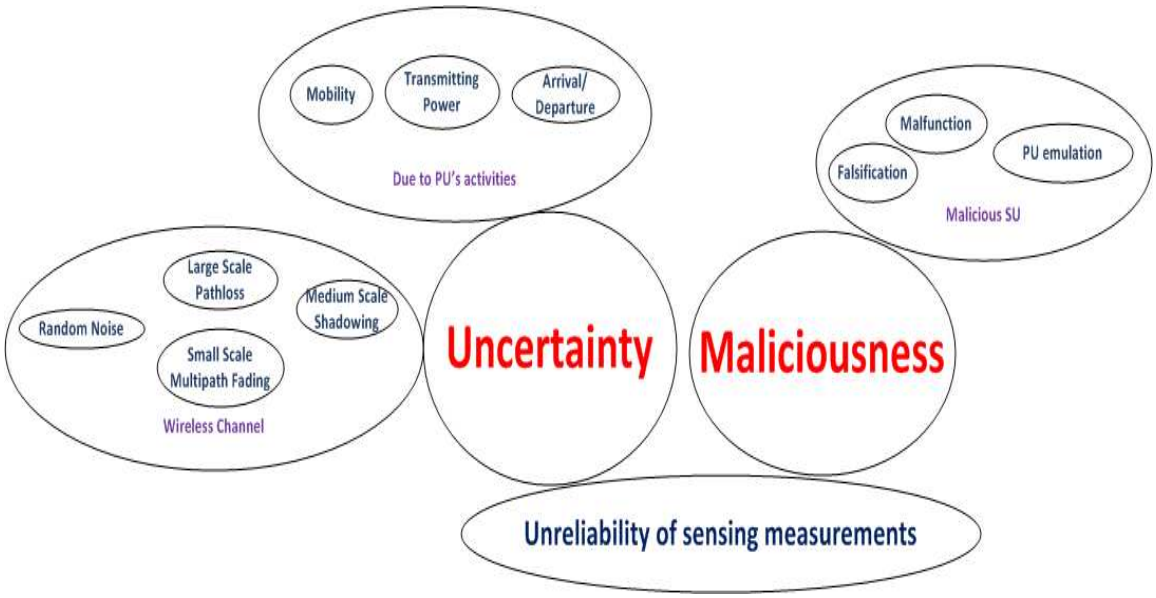

Figure 3.2: Unreliability in Spectrum Sensing

TH-1605_10610214

the SUs present in the less faded areas. This is known as *diversity gain*. CSS can be performed with data fusion and decision fusion. Both these CSS mechanisms have their advantages and disadvantages. Data fusion CSS outperforms decision fusion CSS in terms of accuracy in sensing [36]. Decision fusion CSS outperforms data fusion CSS in terms of the bandwidth requirements. However, the sole idea of CSS can fail if some SUs start malfunctioning because of the Byzantine failure problem. When the Byzantine failure problem is intentional, it means that the SSDF attacks have been caused.

SSDF attacks can be caused by external or internal MUs. External MUs are the SUs not participating in CSS. Internal MUs are some of the SUs participating in CSS. The MUs can cause SSDF attacks in both the data fusion and the decision fusion CSS systems. In data fusion CSS, the MUs attack by reporting false data. On the other hand, in decision fusion CSS, the MUs attack by reporting false decisions. In this chapter, we study the attacks by the internal MUs in data fusion CSS.

Consider a frequency band allotted to a PU. Suppose at a given sensing interval n, the band is not occupied by the PU signal. Evidently, $e_i(m)$ in (3.3) calculated by the ith SU will be low. We assume that the MUs can individually make their decisions based on their calculated energies [131]. The cooperating SUs sensing the band will send their calculated energies to the FC. The MUs, after detecting the low incoming energy $e_i(m)$ values, intentionally send higher values to the FC. Hence, the value of $E_N(m)$ in (3.5) will be higher than its true value. This increases the chances of the FC making a wrong decision regarding the absence of the PU signal in (3.6), thus increasing the P_{fa} in (3.9). This in turn decreases the throughput of the SUs. Similar attack is made by the MUs by sending low energy values when the spectrum is occupied. This will result into the decrement of the P_d value of the SS system, thereby increasing the interference caused to the PU by the SUs.

3.3 Detection of MUs as an Outlier Detection Problem

The data set reported by the honest SUs to the FC follows a particular distribution. Since, the MUs are deliberately reporting manipulated data, it likely follows either a distribution different from honest SUs' data or the same distribution with different statistical parameters [44]. Hence, the false data from the MUs appear as outliers in the data-set reported by the SUs. A conventional FC is not intelligent enough to detect these outliers. Hence, it needs an outlier detection mechanism to detect them. There are various outlier detection schemes available in literature [126, 132–154]. Among these tests, Grubbs' tests [126, 132–136] and Boxplot test [149–154] have been found suitable and have been

TH-1605_10610214

investigated for the detection of MUs in [44] and [2]. These two tests have been outlined below:

3.3.1 Grubbs' Test

The Grubbs' test for outlier detection has mainly two parts: Grubbs' test 1 and Grubbs' test 2. For a data set denoted as $e_1, e_2, \ldots, e_N$, Grubbs' tests are based on the calculation of the outlier factor o_n given as

$$o_n = \frac{e_n - \bar{e}}{\sigma} \tag{3.10}$$

where e_n is the nth data value, $\bar{e}$ and σ are the mean and the standard deviation of e_n values. The outlier factor in (3.10) represents the limit up to which an e_n value is not considered as an outlier. It essentially represents the distance of e_n from the mean of $e_1, e_2, \ldots, e_N$. If $e_n > o_n$, e_n is considered as an outlier and the nth SU is identified as an MU.

The major issue in (3.10) is to estimate $\bar{e}$ and σ. In [44], the Grubbs' test 1 has been demonstrated to estimate $\bar{e}$ and σ. The estimate of $\bar{e}$ has been given by the bi-weight scale (BWS) estimate as

$$\bar{e}^* = \frac{\sum w_n e_n}{\sum w_n}$$

where

$$w_n = \begin{cases} \left\{\left(1 - \left(\frac{e_n - \bar{e}^*}{c_1 S}\right)^2\right)\right\}, \left\{\left(1 - \left(\frac{e_n - \bar{e}^*}{c_1 S}\right)^2\right)\right\} < 1 \\ 0, \text{otherwise} \end{cases}$$

and

$$S = \text{median}\{|e_n - \bar{e}^*|\}$$

And a robust estimate of σ, $\hat{\sigma}$ is given by,

$$\hat{\sigma} = \sqrt{\frac{N \sum\limits_{u_n^2 < 1} (e_n - \bar{e}^*)^2 (1 - u_n^2)^4}{s(-1 + s)}}$$

where

$$s = \sum_{u_n^2} (1 - u_n^2)(1 - 5u_n^2)$$

and

$$u_n = \frac{e_n - \bar{e}^*}{c_2 \underset{n}{\text{median}}\{|e_n - \bar{e}|\}}$$

c_1 and c_2 are tuning constants whose values have been considered as 6 and 9 [43].

The Grubbs test 2 brings more robustness to the Grubbs test 1 by making use of a time span.

TH-1605_10610214

A new parameter m denoting the time iteration is introduced in Grubb's test 2. Since our objective is detecting the MUs, we confine its explanation to the context of CRs. The iteration m represents the mth sensing iteration in the Figure 3.1. In [44], the authors use this method by noting that if the PU status alters frequently, detecting the malicious data can be further improved. This is because, significant increments observed in the reports of the SUs would suggest that the PU has begun transmission at the specific iteration. Likewise, when the reports of the SUs exhibit a noteworthy decline, it suggests that the PU has ceased transmission. The change in the estimations of the SUs, as the status of the PU changes, can be utilized to identify those MUs which do not show comparative conduct as the rest of the SUs. However, it is crucial to recognize the iterations showing change in the data because of the alteration in the PU occupancy, rather than because of the variations in noise and fading. At each iteration, the e_n values having high anomaly are discarded and new $\bar{e}^*$ and $\hat{\sigma}$ are evaluated utilizing remaining e_n values. Let $\hat{\bar{e}}$ be the new $\bar{e}^*$ value. Then, the difference between the $\hat{\bar{e}}$ at the mth and $m-1$th instants will be given as

$$\Delta\hat{\bar{e}}_\alpha[m] = \hat{\bar{e}}_\alpha[m] - \hat{\bar{e}}_\alpha[m-1] \tag{3.11}$$

A positive $\Delta\hat{\bar{e}}_\alpha[m]$ means that the PU has arrived. At every detecting cycle, $\Delta\hat{\bar{e}}_\alpha[m]$ from the past L iterations is evaluated. From these L iterations, all the iterations where the PU occupancy has altered are identified. Out of these changes, $L_m/2$ highest positive magnitude changes and $L_m/2$ highest negative magnitude changes are identified. Let L_m^+ denote the iterations where $\Delta\hat{\bar{e}}_\alpha[m]$ is positive with $L_m/2$ largest magnitudes. Similarly, let L_m^- denote the iterations where $\Delta\hat{\bar{e}}_\alpha[m]$ is negative with $L_m/2$ largest magnitudes.

The following penalty factors are assigned to each of the SUs as

$$P_n = \sum_{m' \in L_m^+} (o_n^+[m'-1] + o_n^-[m']) + \sum_{m' \in L_m^-} (o_n^-[m'-1] + o_n^+[m']) \tag{3.12}$$

where

$$o_n^-[m] = \begin{cases} \frac{-e_n[m'] - \hat{\bar{e}}_\alpha[m']}{\sigma_\alpha^*[m']} & e_n[m'] < \hat{\bar{e}}_\alpha[m'] \\ 0 & \text{otherwise} \end{cases} \tag{3.13}$$

and

$$o_n^+[m] = \begin{cases} \frac{e_n[m'] - \hat{\bar{e}}_\alpha[m']}{\sigma_\alpha^*[m']} & e_n[m'] > \hat{\bar{e}}_\alpha[m'] \\ 0 & \text{otherwise} \end{cases} \tag{3.14}$$

The disadvantage of the Grubbs' test is the complication involved in the calculations of the mean

TH-1605_10610214

and the standard deviation. Particularly, its usage in SS process can prove to be risky, where a slightest delay in sensing the spectrum can cause interference to the PU.

3.3.2 Boxplot Test

The second test for outlier rejection investigated in [44] and [2] is the Boxplot test. A box plot is a quartile grouping of numerical data on the real line as shown in Figure 3.3.

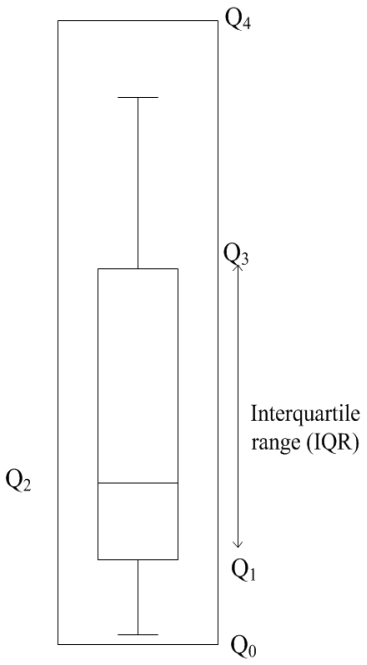

Figure 3.3: Box Plot method for outlier detection

In this method, the data set of the SUs $e_1, e_2, \ldots, e_N$ is first arranged in ascending order as $e_{[1]}, e_{[2]}, \ldots, e_{[N]}$. Then, these values are divided into quartiles. Each of the quartiles mark the 25th, the 50th, and the 75th percentiles of $e_{[1]}, e_{[2]}, \ldots, e_{[N]}$. Suppose, Q_0, Q_1, Q_2, Q_3, and Q_4 denote the minimum, first quartile, the median, the third quartile, and the maximum of the data. On a vertical real line, let us mark Q_0, Q_1, Q_2, Q_3, and Q_4. Then, draw a rectangular box between Q_1 and Q_3 divided into two parts at Q_2. Dividing the data in this manner reveals the skewness in it. The vertical lines extending from the boxes are called whiskers. If the data has positive outliers then its distribution will show a longer whisker in the positive direction. Similarly, for the data having negative outliers, the whiskers are in negative direction. The Boxplot test has two thresholds for discarding high value

TH-1605_10610214

and low value outliers. The lower and upper thresholds Q_l and Q_u are formulated as

$$Q_l = Q_1 - 1.5IQR \tag{3.15}$$

and

$$Q_u = Q_3 + 1.5IQR \tag{3.16}$$

where IQR represents the inter-quartile range. The factor 1.5 has been taken as considered in [155].

The Boxplot test is efficient in representing the skewness in $e_1, e_2, \ldots, e_N$ and the outliers present. However, its disadvantage is that it presents a very gross analysis of these data values. It only shows the summary of the groups where the data values are lying while it fails to show the exact data values and obtain a precise idea about the distance of the outliers with respect to the honest data values.

3.4 Dixon's Test for Outlier Detection

In [121], Dixon's test has been introduced for removing outliers in a data sample. This test investigates the outlier factor associated with each data value. The main advantage of this test is that the calculation of its outlier factor does not depend on the mean or variance of the data and that it is considerably simpler than Grubbs and Boxplot tests specially for datasets of small sizes. The idea of Dixon's test originates from the testing of the null and the alternate hypothesis (H_0 and H_1) where the null hypothesis H_0 represents that all the data points in the data set belong to the same distribution while the alternate hypothesis H_1 suggests that at least 1 data point comes from some other distribution. According to H_0, the data set $e_1, e_2, \ldots, e_N$ belongs to some distribution F. Suppose e_N is quite different from the remaining data samples so that it is suspected to be coming from a different distribution G. The hypothesis testing problem is formulated as

$$\begin{aligned} &\mathrm{H}_0 : e_1, e_2, ..., e_N \quad \text{belong to } F \\ &H_1 : e_1, e_2, ..., e_{N-1} \text{ belong to } F \text{ and } e_N \text{ belongs to } G \end{aligned} \tag{3.17}$$

Note that Dixon's test is only applicable to the data sets following the normal distribution. Here, $F \sim \mathcal{N}(\mu, \sigma^2)$ and G follows a distribution different from that of F or it is normally distributed with its mean or variance different from F. To check whether e_N belongs to G or not, the strength of the evidence for H_0 or H_1 is determined by evaluating the log likelihood ratio (LLR) of the data samples over both the hypothesis [156]. The LLR obtained gives the statistic representing the outlying element

TH-1605_10610214

in the data sample as

$$T_N = \frac{e_N}{\bar{e}}. \tag{3.18}$$

where $\bar{e}$ represents the mean of the data sample $e_1, e_2, ..., e_N$. Suppose $e_1, e_2, \ldots, e_N$ are ordered as $e_{[1]}, e_{[2]}, \ldots, e_{[N]}$, then it is found that the statistic

$$T_N = \frac{e_{[N]}}{\bar{e}} \tag{3.19}$$

maximizes the LLR over H_1 [156]. This was the guiding principle for the formulation of the Dixon's test.

3.4.1 Outlier Factor in the Dixon's Test

Through his empirical evaluations, Dixon observed the following points for data sets of small sizes having a single outlier:

(i) The distance of the highest value $e_{[N]}$ from its nearest data value $e_{[N-1]}$ represents a more robust measure of the outlyingness of the data sample.

(ii) A test statistic expressed as a ratio of the above distance $e_{[N]} - e_{[N-1]}$ to the range of the data $e_{[N]} - e_{[1]}$ remains invariant of the location (mean) and the scale (variance) of the data sample.

A general expression for the Dixon's test can be expressed in terms of o_n as [156]

$$o_n = \frac{e_{[a]} - e_{[b]}}{e_{[c]} - e_{[d]}} \tag{3.20}$$

where $[a], [b], [c]$, and $[d]$ represent some order indices between $[i]$ and $[N]$. This can be seen as a simplification of the outlier factor in (3.10) for Grubbs test. Interestingly, both the Grubbs test and the Dixon's test were published in the same issue of the *Annals of Mathematical Statistics*. It was observed in [2], that the Dixon's test was able to outperform the Grubbs test in detecting an MU. Further, we demonstrate here that effective application of the Dixon's test after optimally grouping the data set into small sizes can enhance its performance in outlier rejection significantly.

For small datasets of sizes 3 to 7, Dixon derived the outlier factor for the Dixon's test for $e_{[N]}$ as

$$o_{[N]} = \frac{e_{[N]} - e_{[N-1]}}{e_{[N]} - e_{[1]}} \text{ for } 3 \leq N \leq 7 \tag{3.21}$$

For datasets of sizes greater than 7, Dixon empirically formulated the outlier factor for $e_{[N]}$ as

TH-1605_10610214

$$o_{[N]} = \begin{cases} \frac{e_{[N]}-e_{[N-1]}}{e_{[N]}-e_{[2]}} \text{ for } 8 \leq N \leq 10 \\ \frac{e_{[N]}-e_{[N-2]}}{e_{[N]}-e_{[2]}} \text{ for } 11 \leq N \leq 13 \\ \frac{e_{[N]}-e_{[N-2]}}{e_{[N]}-e_{[3]}} \text{ for } 14 \leq N \leq 20 \end{cases} \tag{3.22}$$

Similar expression for outlier factor $e_{[1]}$ for datasets of sizes 3 to 7 was derived as

$$o_{[1]} = \frac{e_{[2]} - e_{[1]}}{e_{[N]} - e_{[1]}} \text{ for } 3 \leq N \leq 7 \tag{3.23}$$

and for the datasets of sizes more than 7, $o_{[1]}$ was obtained as

$$o_{[1]} = \begin{cases} \frac{e_{[2]}-e_{[1]}}{e_{[N-1]}-e_{[1]}} for\, 8 \leq N \leq 10 \\ \frac{e_{[3]}-e_{[1]}}{e_{[N-1]}-e_{[2]}} for\, 11 \leq N \leq 13 \\ \frac{e_{[3]}-e_{[1]}}{e_{[N-2]}-e_{[1]}} for\, 14 \leq N \leq 20 \end{cases} \tag{3.24}$$

The outlier factors $o_{[1]}$ and $o_{[N]}$ are used to detect the outliers in the dataset.

3.4.2 Calculation of the Critical Value (C_v)

The next step in Dixon's test is the calculation of the critical values. Verma et al. presents a computational method for the calculation of the critical values in [157]. This method is outlined here: For independent and identically distributed data samples $e_1, e_2, \ldots, e_N$ with e_i having the pdf $\phi(e_i)$, the joint pdf is given by

$$p(e_1, e_2, ..., e_N) = \prod_{i=1}^{N} \phi(e_i) \tag{3.25}$$

It is known that Dixon's test is applicable to only normally distributed data samples. Hence,

$$\phi(e_i) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{1}{2}\left(\frac{e_i - \bar{e}}{\sigma}\right)^2\right) \tag{3.26}$$

where $\bar{e}$ and σ represent the mean and the standard deviation respectively. In (3.21-3.24), it can be seen that $o_{[N]}$ is a function of $e_{[i]}, e_{[N-j]}$, and $e_{[N]}$ and is independent of $\bar{e}$ and σ. It is found by integrating (3.26) over all the points except ($e_{[i]}, e_{[N-j]}$, and $e_{[N]}$). The points ($e_{[i]}, e_{[N-j]}$, $e_{[N]}$) have been expressed in terms of (t, u, v) by taking the transforms $t^2 = \frac{(1+o_{[N]}^2)v^2}{2}$, $u^2 = \frac{3e_{[N]}^2}{2}$ and $v = e_{[N]} - e_i$

TH-1605_10610214

and the pdf of $o_{[N]}$ has been obtained as

$$P(o_{[N]}) = \frac{N!}{(i-1)!(N-j-i-1)!(j-1)!} \int_{-\infty}^{\infty} \int_{0}^{\infty} \left(\int_{-\infty}^{e_{[N]}-v} \phi(t)dt \right)^{i-1} \left(\int_{e_{[N]}-v}^{e_{[N]}-o_N v} \phi(t)dt \right)^{N-j-i-1} \left(\int_{e_{[N]}-o_{[N]}v}^{e_{[N]}} \phi(t)dt \right)^{j-1} \phi(e_{[N]}-v)\phi(e_{[N]}-o_{[N]}v)\phi(e_{[N]})vdvde_{[N]} \tag{3.27}$$

For simplification, the following substitutions have been made:

$$L(e_{[N]},u,v) = \left(\int_{-\infty}^{e_{[N]}-v} \phi(t)dt \right)^{i-1} \left(\int_{e_{[N]}-v}^{e_{[N]}-o_{[N]}v} \phi(t)dt \right)^{N-j-i-1} \left(\int_{e_{[N]}-o_{[N]}v}^{e_{[N]}} \phi(t)dt \right)^{j-1} \tag{3.28}$$

and

$$N_1 = \frac{N!}{(i-1)!(N-j-i-1)!(j-1)!} \sqrt{\frac{2}{3}} \sqrt{\frac{2}{1+o_{[N]}^2}} \tag{3.29}$$

The objective of Verma et al. is to express (3.27) in a form suitable for solving by the Gauss-Hermite quadrature approach. Hence, the expression in (3.27) is expressed as

$$P(o_{[N]}) = N_1 \int_{-\infty}^{\infty} \exp(-u^2) \int_{0}^{\infty} \exp(-t^2) L(e(u),u,v) \exp\left(\frac{2ut(1+o_{[N]})}{\sqrt{3(1+o_{[N]}^2)}} \right) v_1 dtdu \tag{3.30}$$

where $e(u) = u\sqrt{\frac{2}{3}}$ and $v_1 = t\sqrt{\frac{2}{1+o_{[N]}^2}}$. The numerical integration of u is performed with Gauss-Hermite quadrature while for integrating v_1, half range Hermite polynomials are used. Finally, the approximation to (3.30) is obtained as

$$P(o_{[N]}) = N_1 \sum_{k=1}^{nH} w_{nH}(u_k) \sum_{l=1}^{nHH} w_{nHH}(t_l) L(e(u_k), v_1, o_{[N]}) \exp\left(\frac{2u_k t_l (1+o_{[N]})}{\sqrt{3(1+o_{[N]}^2)}} \right) v_1 \tag{3.31}$$

where u_k is the value of the kth abscissa of the nH-degree Hermite polynomial and $w_{nH}(u_k)$ is the corresponding weight associated. Similarly, t_l and $w_{nHH}(t_l)$ are the corresponding parameters for the nHH-degree half-range Hermite polynomial. The critical values for Dixon's test are calculated by integrating (3.31) for $r = 0$ to R, and the equation is evaluated using numerical quadrature approach using the legendre polynomials. The value of R is calculated by the bisection method for a given value of the cumulative distribution function (CDF) by using the initial values CDF=0, R=0 and CDF=1, R=1. The table of critical values [158] for different confidence levels has been presented in Table A.1 in Appendix A.

The SSDF attacks can be defeated by the proposed schemes, based on the Dixon's outlier test as

TH-1605_10610214

presented in the next section.

3.5 Proposed Method

The outlier factor for Dixon's test can be calculated for the data sets of different sizes [156]. The authors in [2] apply the test on the complete SU dataset at a particular sensing interval. This may at times prove less efficient for the following reasons: 1) The test is applicable for detecting outliers in normally distributed data samples [122]. 2) Dean and Dixon [122] observed that the test is efficient for normal data samples of size 10 or smaller. In average conditions, the number of cooperating users is likely to be more than 10. 3) The test application methodology in [2] can detect only a single outlier in data samples at one sensing interval.

In [159], Chernick studied the robustness of the Dixon's test over data sets of different sizes, following an assumed underlying distribution. It was concluded that the optimum size of a data set for the Dixon's test application, following an assumed underlying distribution, is $N = 3$, since the test is robust to the deviation from normality for this data set size.

We rewrite the Dixon's test expression for $o_{[N]}$ for a data set of size 3 by renaming it to $o_{[3]}$ as

$$o_{[3]} = \frac{e_{[3]} - e_{[2]}}{e_{[3]} - e_{[1]}} \tag{3.32}$$

and

$$o_{[1]} = \frac{e_{[2]} - e_{[1]}}{e_{[3]} - e_{[1]}} \tag{3.33}$$

The incoming energy values ideally follow a chi-square distribution. Considering the observations made in [159], one gets motivated to find a method for applying the Dixon's test on an energy data set of size three. Let there be P non-malicious SU energy values indexed as $e'_1(m), e'_2(m), \ldots, e'_P(m)$, after the outliers are discarded. The energies will be fused at the FC as,

$$E_P(m) = \frac{1}{P} \sum_{i=1}^{P} e'_i(m) \tag{3.34}$$

The new decision rule is given by

$$E_P(m) \underset{H_0}{\overset{H_1}{\gtrless}} \lambda \tag{3.35}$$

where λ is as mentioned in (3.6). The value of λ is determined by fixing (P_{fa}).

TH-1605_10610214

After the MUs are detected, (3.8) and (3.9) can be re-written as,

$$P_d = \Pr(E_P(m) > \lambda | H_1) \tag{3.36}$$

and

$$P_{fa} = \Pr(E_P(m) > \lambda | H_0) \tag{3.37}$$

The proposed three-point Dixon's test is applied in the form of two schemes presented below.

3.5.1 Scheme 1: Three-Point Dixon's Test over Non-Overlapping Blocks

Following the observations made in [159], the natural approach will be to apply the test on non-overlapping data segments of size 3. The incoming energy data values at the FC are first divided into groups of 3 each. Then Dixon's test is applied on each group to detect the possible outlier value in each group. Each outlier is discarded. Then, the pure values from each group are collected at the FC and the decision about spectrum occupancy is made. The implementation steps of this scheme is shown in Algorithm 3.1.

Simulations reveal that applying the Dixon's test on the blocks of 3 values improves the performance compared to its application on the whole data set. Also it is verified that the scheme 1 (the 3-point Dixon's test) performs well for detecting upto 20% MUs (Please refer Section 3.7). However, as the number of MUs increases, degradation in the performance of the test is observed. This degradation is the consequence of the fact that the applicability of the Dixon's test is restricted to only one outlier in a group. As the number of MUs in a CSS system increases, the probability of each small group of three containing more than one malicious value increases. The scheme 1 fails over such groups in detecting multiple outliers.

The limitation stated above motivated us to propose the three-point sliding window Dixon's test.

3.5.2 Scheme 2: Three-Point Sliding Window Dixon's Test

To overcome the drawback of applying the 3-point Dixon's test on non-overlapping blocks of the SU energy data (scheme 1), the SU energies are grouped into blocks with maximum overlaps. Thus, for an intermediate SU energy sample e_i, the block $\{e_{i-1}, e_i, e_{i+1}\}$ is considered for the 3-point Dixon's test. In this grouping, an e_i will be a part of three blocks $\{e_{i-2}, e_{i-1}, e_i\}$, $\{e_{i-1}, e_i, e_{i+1}\}$ and $\{e_i, e_{i+1}, e_{i+2}\}$. At one boundary of the data segment, the energy values are to be considered in a circular fashion. This arrangement enhances the detection of both single and multiple MUs.

TH-1605_10610214

Algorithm 3.1 Three point Dixon's test on non-overlapping blocks

N : length of the incoming energy data set
e : incoming energy data set
λ: Detection threshold
I: Rank of the values of e
C_v: critical value
for $i \leftarrow 2:3:[3 \times floor(\frac{N}{3}) - 1]$ **do**
  $Y == [e(i-1), e(i), e(i+1)]$ {Grouping the values}
  $[Y_s, I_n] == sort(Y)$ {Sorting the values with indices stored in I_n}
  $o_{[3]} == \frac{Y_s(I_n(3)) - Y_s(I_n(2))}{Y_s(I_n(3)) - Y_s(I_n(1))}$ {For suspected high values} and
  $o_{[1]} == \frac{Y_s(I_n(2)) - Y_s(I_n(1))}{Y_s(I_n(3)) - Y_s(I_n(1))}$ {For suspected low values}
  if $o_{[3]} > C_v$ **then**
    $e(I(Y_s(3))) == 0$
  end if
  if $o_{[1]} > C_v$ **then**
    $e(I(Y_s(1))) == 0$
  end if
end for
if $mod(N/3) \neq 0$ **then**
  $Y_r == [e(N-2), e(N-1), e(N)]$
  $[Y_{rs}, I_n] == sort(Y_r)$
  $o_{[3]} == \frac{Y_{rs}(I_n(3)) - Y_{rs}(I_n(2))}{Y_{rs}(I_n(3)) - Y_{rs}(I_n(1))}$
  $o_{[1]} == \frac{Y_{rs}(I_n(2)) - Y_{rs}(I_n(1))}{Y_{rs}(I_n(3)) - Y_{rs}(I_n(1))}$
  if $o_{[3]} > C_v$ **then**
    $e(I(Y_{rs}(3))) == 0$
  end if
  if $o_{[1]} > C_v$ **then**
    $e(I(Y_{rs}(1))) == 0$
  end if
end if
$P = count(e(i) > 0, i = 1, 2, \ldots, N)$ {Find the non zero values}
$E_P(m) = \frac{1}{P} \sum_{i=1}^{N} e(i)$
if $E_P(m) > \lambda$ **then**
  Decide H_1
else
  Decide H_0
end if

TH-1605_10610214

Under this scheme, each e_i will be subjected to the test in 3-point Dixon's test thrice. If any of the tests declares e_i as an outlier, the ith SU is considered as an MU. The algorithmic steps are described in Algorithm 3.2.

Algorithm 3.2 Sliding Window Dixon's test (Three point Dixon's test on overlapping blocks)

K : length of the incoming energy data set
X : $[e_1\ e_2\ \dots e_N]$
C_v: critical value
λ: Detection threshold {incoming energy data set}
rank I=$[I_1\ I_2\ \dots I_N]$ {index values of the X and Y}
$Y = X$ {Form an array Y having values same as that of X}
for $i \leftarrow 1 : N$ **do**
  X_{sort}=sort $[e_i\ e_{(i+1)modN}\ e_{(i+2)modN}]$
  $o_{[3]} = \frac{X_{sort}(3)-X_{sort}(2)}{X_{sort}(3)-X_{sort}(1)}$ {When MUs report high values}
  AND
  $o_{[1]} = \frac{X_{sort}(2)-X_{sort}(1)}{X_{sort}(3)-X_{sort}(1)}$ {When MUs report low values}
  if $o_{[3]} > C_v$ **then**
    $Y_{I(X_{sort}(3))} = 0$ {MUs reporting high values}
  end if
  AND
  if $o_{[1]} > C_v$ **then**
    $Y_{I(X_{sort}(1))} = 0$ {MUs reporting low values}
  end if
end for
$P = count(Y_i > 0, i = 1, 2, \dots, N)$ {Find the non zero values}
$E_P(n) = \frac{1}{P}\sum_{i=1}^{N} Y_i$
if $E_P(n) > \lambda$ **then**
  Decide H_1
else
  Decide H_0
end if

3.6 A Note on the Complexity of the Proposed Schemes

The N-point Dixon's test involves finding three extreme values. The worst case complexity of selecting these extreme values is of the order $O(N)$. The 3-point sliding window Dixon's test (scheme 2) involves sorting of three samples and the test is repeated at N sample points. Thus, the complexities for finding the extreme values is of the same order ($O(N)$) in both the N-point Dixon's test and the 3-point sliding window Dixon's tests (scheme 1 and scheme 2) applied at N sample points. The Dixon's outlier factor $o_{[N]}$ (or $o_{[1]}$) is to be computed once in the N-point Dixon's test while it is to be computed N times in the proposed 3-point sliding window Dixon's test applied at N sample points.

TH-1605_10610214

Thus the proposed method is more complex than the N-point Dixon's test in terms of the number of times the Dixon's quotient is computed.

3.7 Simulation Results and Performance Assessment

A CSS with 20 and 40 SUs is considered for simulations. Simulation experiments were carried out in MATLAB using the Monte-Carlo method as illustrated in Section 3.2.2 to study the performance of the proposed methods for MU detection. We assume that the SUs are deployed in the transmission vicinity of the PU, since, our work is based on the assumption that all the SUs will be able to perfectly receive the PU signal. A BPSK modulated signal is assumed to be transmitted by the PU transmitter which is subjected to independent Rayleigh fading and additive white Gaussian noise (AWGN) for each of the receiving SUs. The average receive SNR at the deployed SUs is 2dB. The time T allocated to the SUs for sensing the spectrum is 0.25s. This sensing time frame is sampled at a frequency of 200 samples/s. Hence, the energy at 50 instants ($M = 50$ in (3.3)) has been evaluated for all the investigations. We allot one flat fading channel to each SU. The channel bandwidth is 1×10^6 Hz. All the SU channels are assumed to be independent. The average receive SNR of the SUs accounts for all the transmission parameters. Performance evaluation is done in terms of Receiver Operating Characteristics (ROC) and the variations of P_d and P_{fa} with the detection threshold (λ). All the evaluations are done by observing the capability of a scheme to bring the ROC curves or the P_d vs λ and P_{fa} vs λ curves of a system affected by the MUs close to the case when there is no MU present in the system.

The captions used in the figures are as follows:

(i) CSS without MU: A normal CSS system without any MU.

(ii) CSS with MU untested: A CSS system with an MU without any detection test for it.

(iii) N-point Dixon's test: Test on the whole incoming energy data set (the proposition in [2]).

(iv) Scheme 1 (3-point Dixon's test (without overlapping)): Three-point Dixon's test over non-overlapping blocks.

(v) Scheme 2 (3-point Dixon's slider test (with maximal overlapping)): Three-point sliding window Dixon's test.

TH-1605_10610214

We first show the comparisons of the N-point Dixon's test with Grubbs' test 1, Grubbs' test 2, and Boxplot test in Figures 3.4 and 3.5. In both these investigations, $N = 20$. Similar to [2], we have considered only one MU in both the investigations.

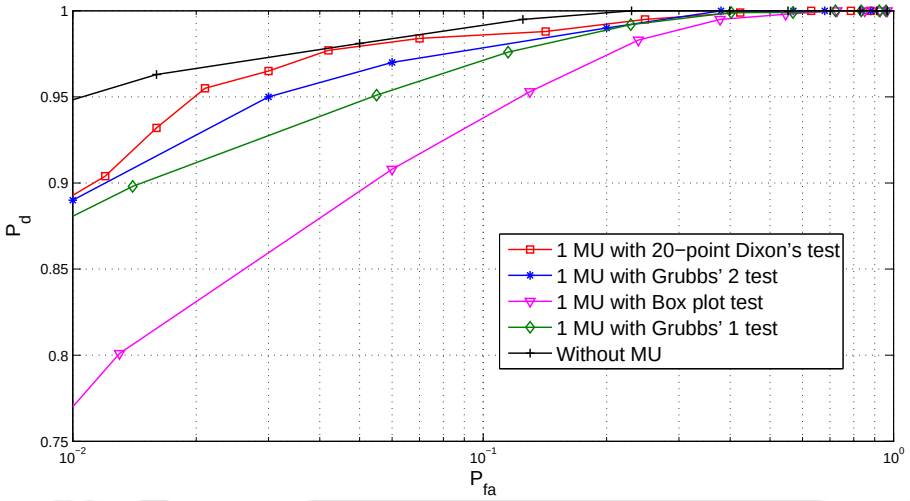

Figure 3.4: Comparison of MU detection performance of the N-point Dixon's tests with Grubbs tests and Boxplot test in a single high reporting MU case.

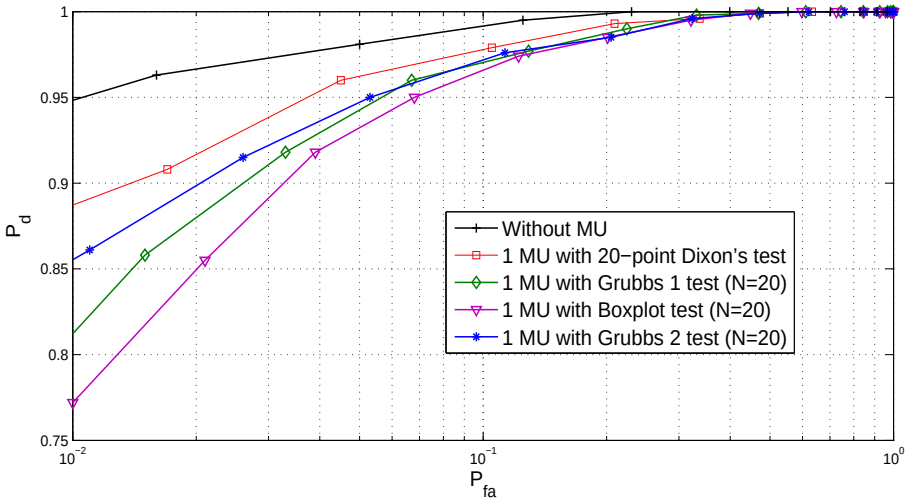

Figure 3.5: Comparison of MU detection performance of the N-point Dixon's tests with Grubbs tests and Boxplot test in a single low reporting MU case.

It is seen that Grubbs tests outperform the Boxplot test. Dixon's test shows better performance

TH-1605_10610214

than either of these tests.

3.7.1 Evaluating the Robustness of the Dixon's Test over Small Data Samples

In this set of experiments, we confirm the findings of Chernick. The different cases under evaluation are grouping the data into 3, 5, 7 and directly applying the test on the whole incoming data set, as done in [2]. Figures 3.6 and 3.7 show the comparisons when 1 MU is present whereas Figures 3.8 and 3.9 show the comparisons for the presence of 2 MUs. Figures 3.6 and 3.8 show the results for the high reporting MU case. Figures 3.7 and 3.9 show the comparisons for the low reporting MU case. It can be observed that in all the cases, the optimum grouping size comes out to be three, thus validating that the maximum performance is obtained for 3-point grouping test.

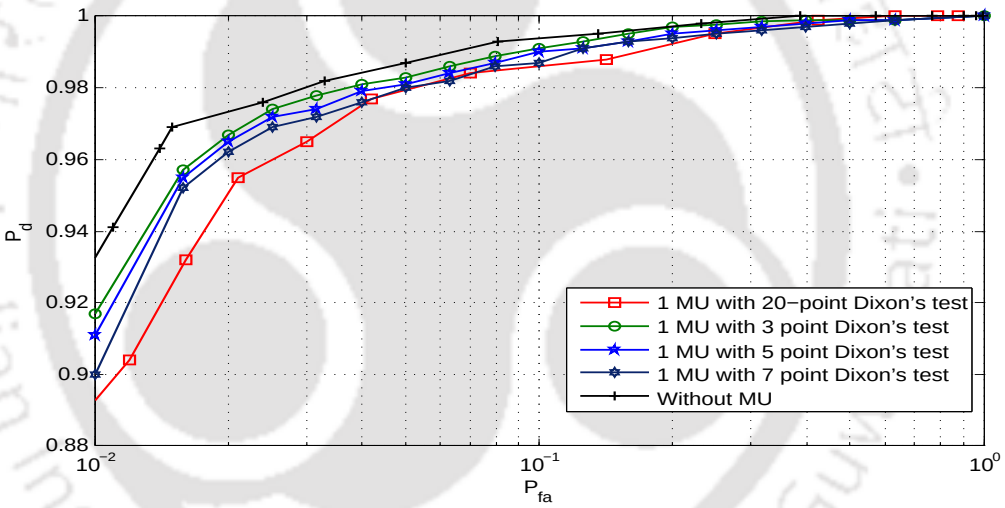

Figure 3.6: Comparison of MU detection performance of the N-point Dixon's tests for $N = 3, 5, 7$ and 20 in the single high reporting MU case.

3.7.2 Performance Evaluation in Suppressing a Single MU

This set of experiments compares the proposed algorithms with the 20-point Dixon's test in [2]. They are depicted in Figures 3.10- 3.15. All these evaluations are for a single MU. Figures 3.10 and 3.11 show the performance in terms of the ROC curves. The purpose of these figures is to study the achievement of schemes 1 and 2 in bringing the ROC curves close to the without-MU-case. In Figure 3.10, the MU is reporting high values whereas in Figure 3.11, it is reporting low values. It is seen that the scheme 1 outperforms the N-point Dixon's test. Further, the scheme 2 outperforms the scheme 1.

TH-1605_10610214

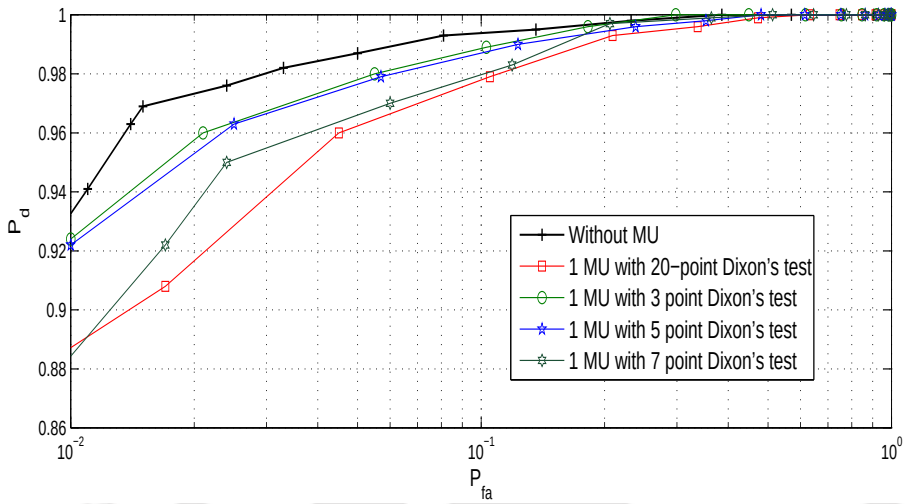

Figure 3.7: Comparison of MU detection performance of the N-point Dixon's tests for $N = 3, 5, 7$ and 20 in the single low reporting MU case.

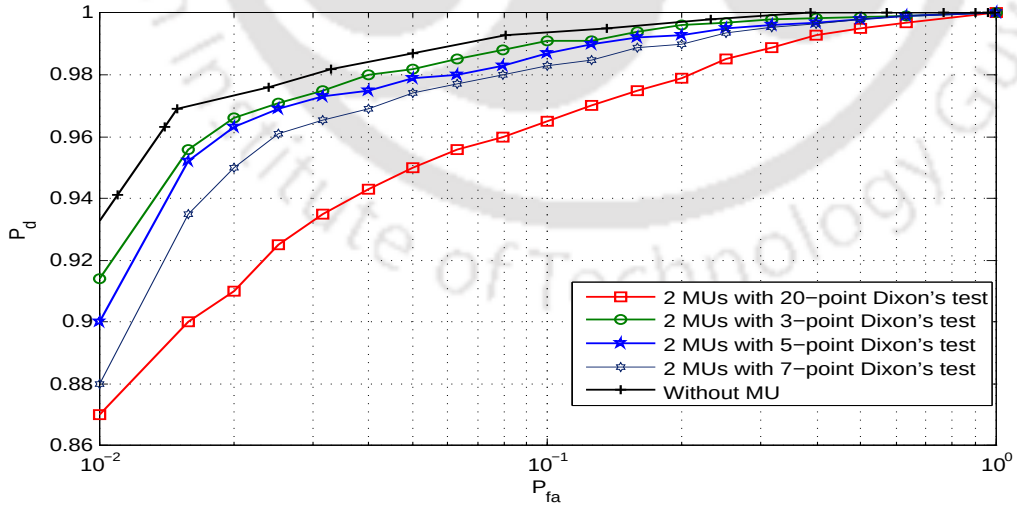

Figure 3.8: Comparison of MU detection performance of the N-point Dixon's tests for $N = 3, 5, 7$ and 20 in the two high reporting MUs case.

TH-1605_10610214

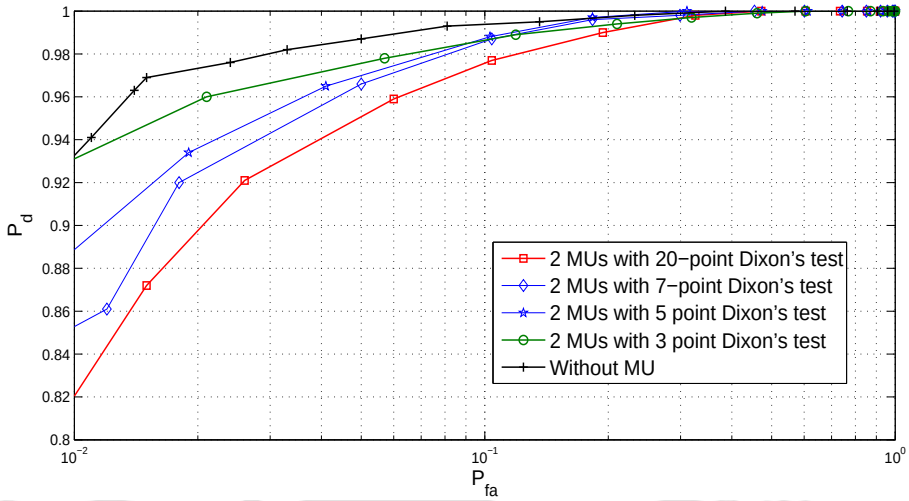

Figure 3.9: Comparison of MU detection performance of the N-point Dixon's tests for $N = 3, 5, 7$ and 20 in the two low reporting MUs case.

In Figures 3.12- 3.15 we show a more refined form of Figures 3.10 and 3.11. The effect of the MUs is found in the form of shifts in P_d and P_{fa} separately. The ROC curves may fail to reveal these shifts clearly. Hence, in Figures 3.12- 3.15, we show the variations of P_d and P_{fa} separately with λ. These values are compared with that of the CSS without an MU and the CSS with the MU removed using the 20-point Dixon's test. The plots show that the proposed schemes outperform the 20-point Dixon's test in [2]. It can also be observed that the scheme 2 performs better than the scheme 1. This is because, in the scheme 2, each SU is subjected to the Dixon's test thrice compared to once in the scheme 1.

TH-1605_10610214

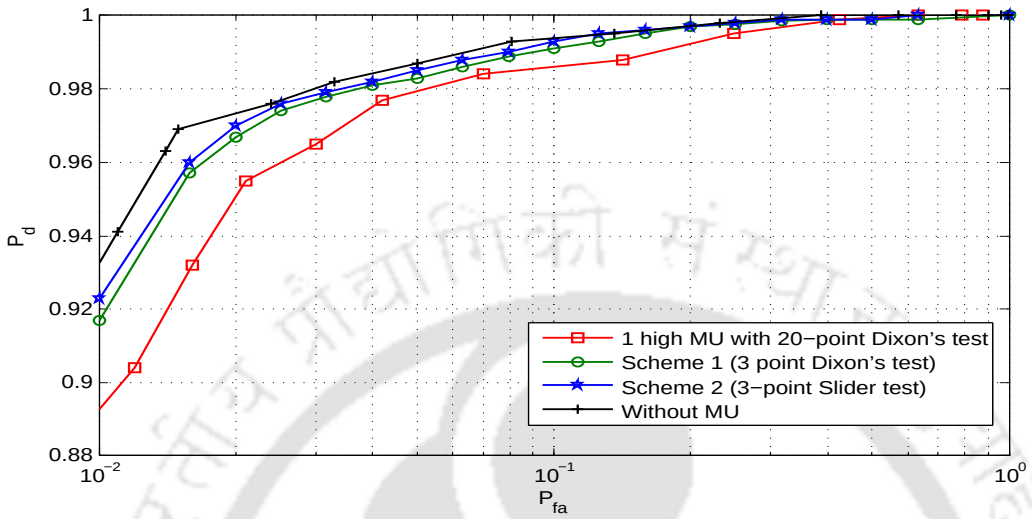

Figure 3.10: MU detection of the proposed schemes and the scheme in [2] for a single high reporting MU

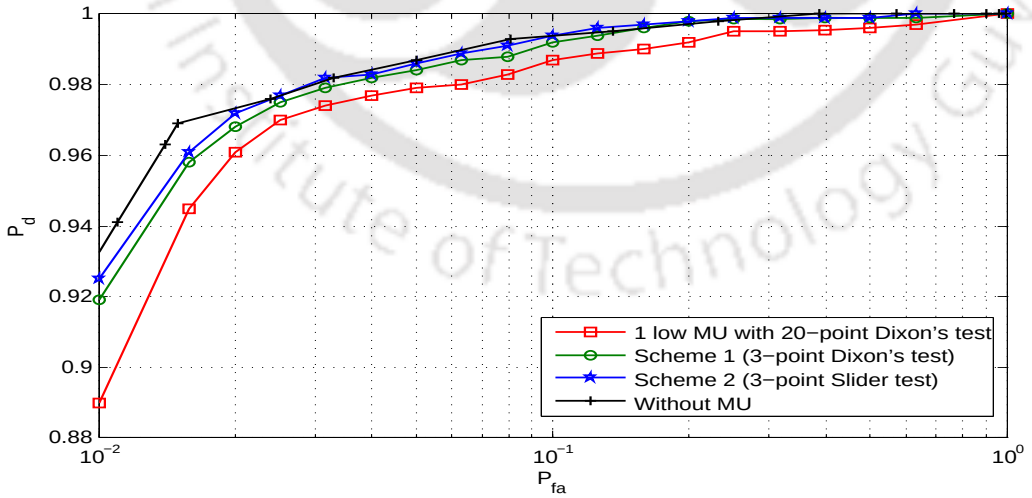

Figure 3.11: MU detection of the proposed schemes and the scheme in [2] for a single low reporting MU

TH-1605_10610214

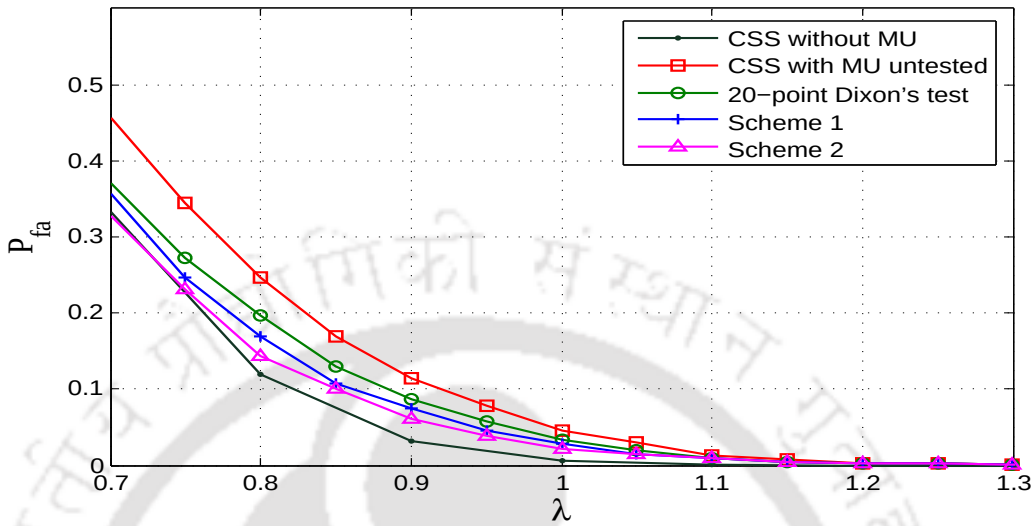

Figure 3.12: P_{fa} vs λ plot for a single MU reporting high value among 20 SUs showing the shift in P_{fa} reduced with the proposed schemes.

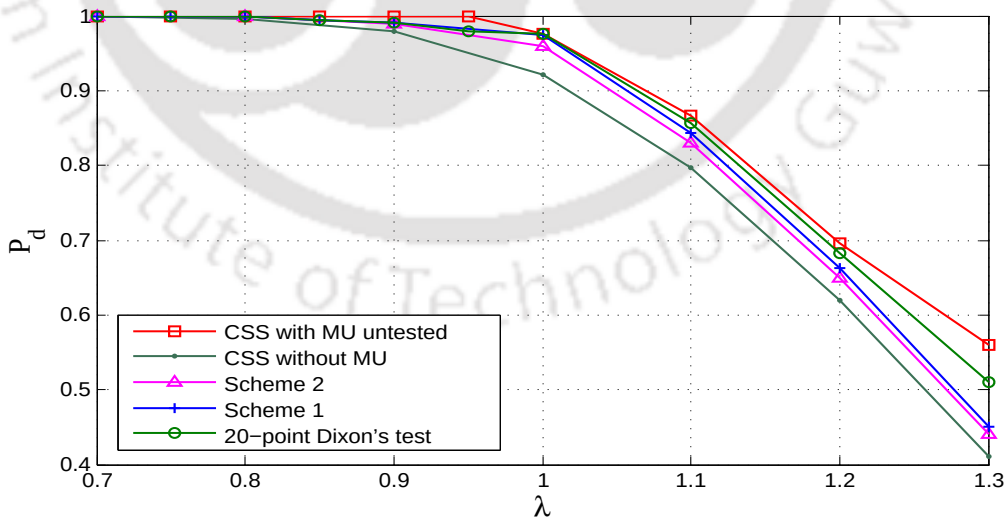

Figure 3.13: P_d vs λ plot for a single MU reporting high value among 20 SUs showing the shift in P_d reduced with the proposed schemes.

TH-1605_10610214

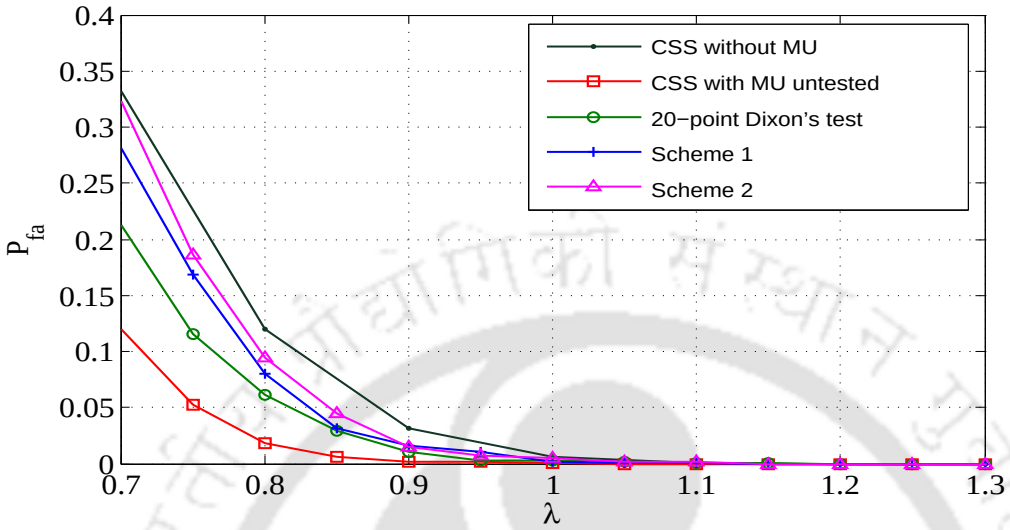

Figure 3.14: P_{fa} vs λ plot for a single MU reporting low value among 20 SUs showing the shift in P_{fa} reduced with the proposed schemes.

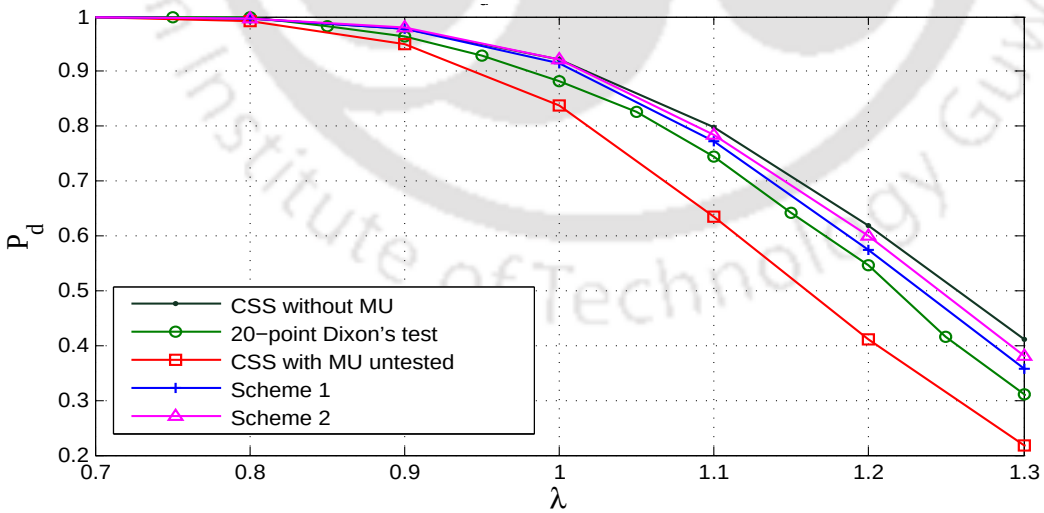

Figure 3.15: P_d vs λ plot for a single MU reporting low value among 20 SUs showing the shift in P_d reduced with the proposed schemes.

TH-1605_10610214

3.7.3 Performance Evaluation in Suppressing Multiple MUs

The multiple MUs are assumed to act independently. The performance of both the schemes has been evaluated. The number of cooperating SUs is taken to be 40. As in these evaluations, the MUs have been considered percentage wise, we consider 40 SUs to bring more generality in the results. Once again, the performance evaluation has been done by assessing the capability of the scheme to bring the values of P_d and P_{fa} close to the values when there are no MUs present, for varying λ. In order to clearly depict the shifts in P_d and P_{fa} caused by the MUs and the improvements brought by the proposed schemes, we have plotted them separately with λ in Figures 3.16- 3.23. Figures 3.16-3.19 show the performance of scheme 1 and Figures 3.20- 3.23 show the performance of scheme 2. Figures 3.16, 3.17, 3.20, and 3.21 show the investigations for low reporting MUs and Figures 3.18,3.19, 3.22, and 3.23 for high reporting MUs. The scheme 1 performs successfully when the fraction of MUs is increased up to 20% of the total SUs. The scheme 2 performs excellently when there are 10% MUs among the total cooperating SUs. It can be seen that the scheme performs well till the fraction of MUs is increased even up to 30%. Note that the evaluations for 10% MUs was shown in Figures 3.8 and 3.9.

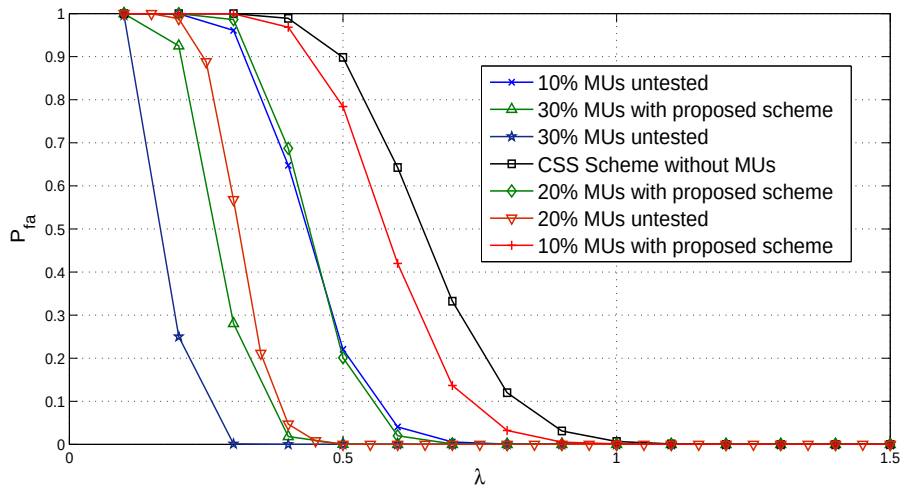

Figure 3.16: P_{fa} vs λ plot for MUs reporting low Values among $N = 40$ SUs when the PU signal is present, showing the shift in P_{fa} reduced with scheme 1.

TH-1605_10610214

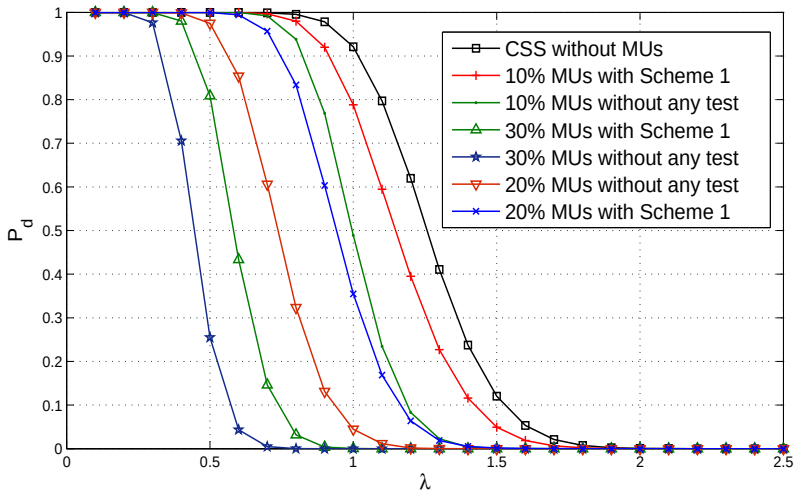

Figure 3.17: P_d vs λ plot for MUs reporting low values among $N = 40$ SUs when the PU signal is present showing the shift in P_d reduced with scheme 1.

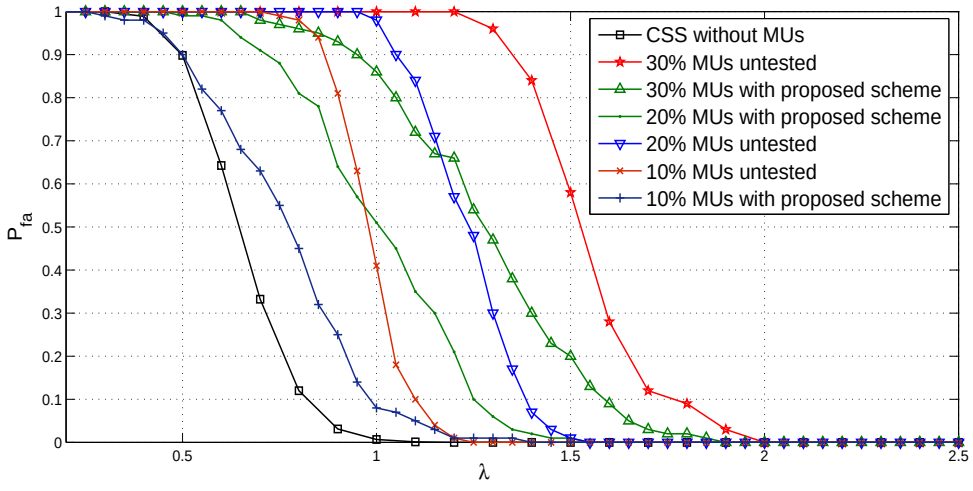

Figure 3.18: P_{fa} vs λ plot for MUs reporting high values among $N = 40$ SUs when the PU signal is absent showing the shift in P_{fa} reduced with scheme 1.

TH-1605_10610214

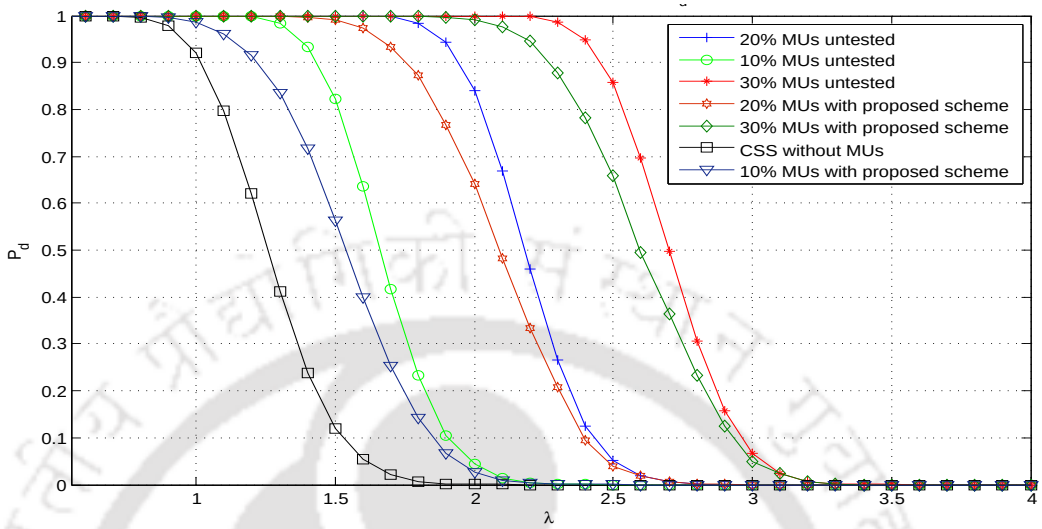

Figure 3.19: P_d vs λ plot for MUs reporting high values among $N = 40$ SUs when the PU signal is absent showing the shift in P_d reduced with scheme 1.

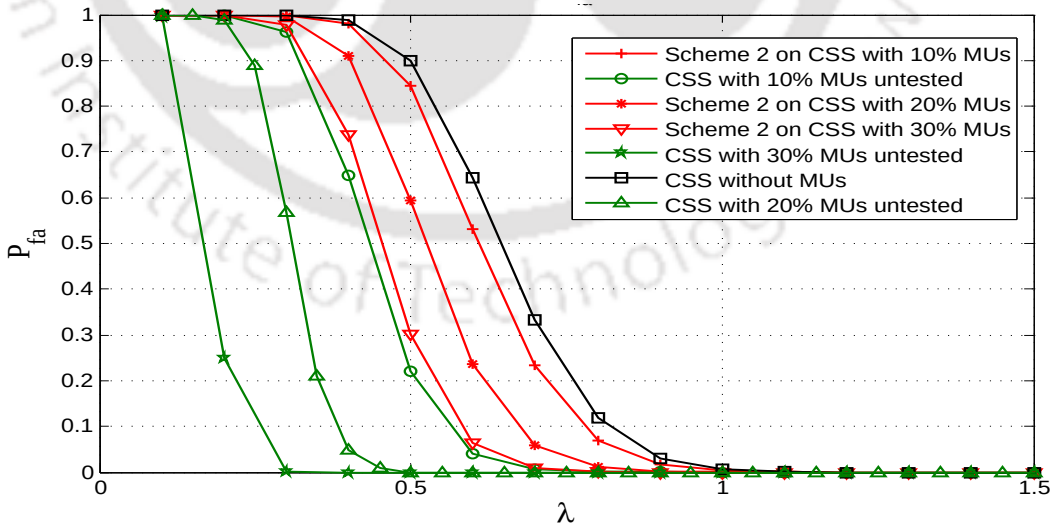

Figure 3.20: P_{fa} vs λ plot for MUs reporting low Values among $N = 40$ SUs showing the shift in P_{fa} reduced with scheme 2.

TH-1605_10610214

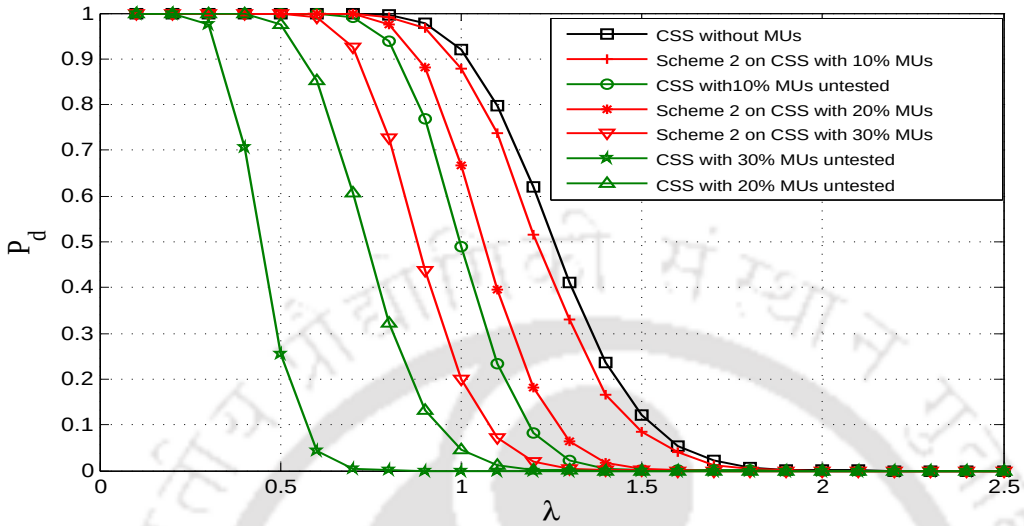

Figure 3.21: P_d vs λ plot for MUs reporting low values among $N = 40$ SUs showing the shift in P_{fa} reduced with scheme 2.

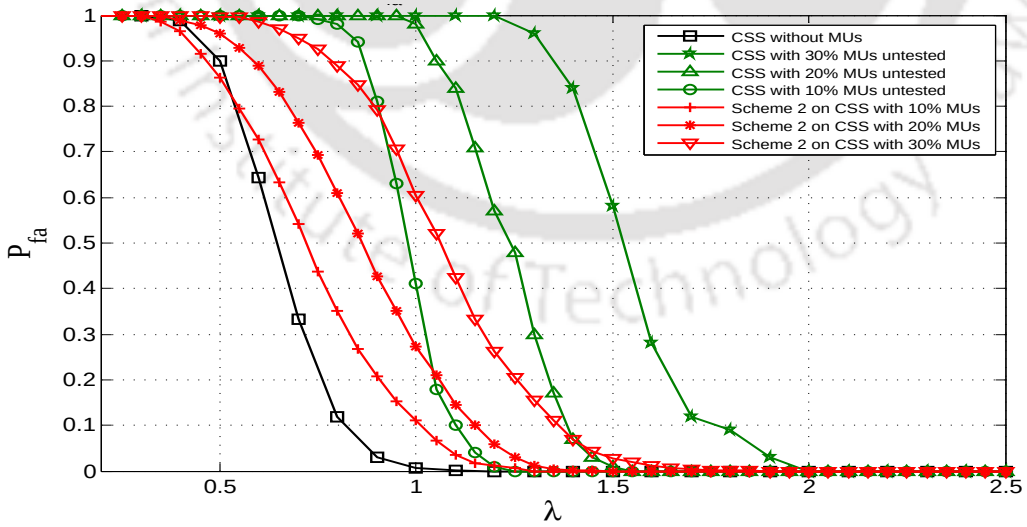

Figure 3.22: P_{fa} vs λ plot for MUs reporting high values among $N = 40$ SUs showing the shift in P_{fa} reduced with scheme 2.

TH-1605_10610214

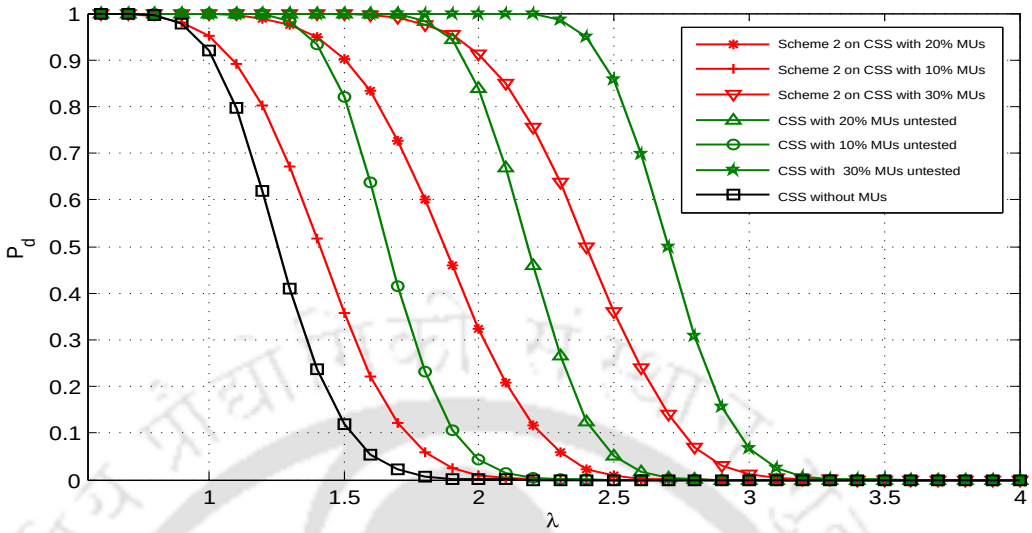

Figure 3.23: P_d vs λ plot for MUs reporting high values among $N = 40$ SUs showing the shift in P_{fa} reduced with scheme 2.

3.8 Conclusion

The chapter reported efficient schemes for the detection of malicious users present in a cooperative spectrum sensing system. It is based on the fact that Dixon's outlier detection test gives the best performance on groups of 3 users. Simulation results show that the proposed methods are efficient for the detection of malicious users present in fairly good numbers. In the next chapter, we will investigate the case when the MUs collude among themselves and launch attacks.

TH-1605_10610214

TH-1605_10610214

4

Collision Penalty based Mechanism for Countering Smart SSDF Attacks

Contents

4.1 Introduction 78
4.2 System Model 83
4.3 Proposed Scheme 85
4.4 Bounds on C_P for Attack Prevention 90
4.5 The Best Strategy for the SUs 102
4.6 Conclusion 104

TH-1605_10610214

In Chapter 3, we proposed methods to counter the MUs launching independent SSDF attacks. The schemes proposed in Chapter 3 are effective as long as the attacks are launched independently. The affect of the SSDF attacks increases severely if the MUs have the capability to collude. Such MUs can avoid getting detected by the methods reported in the Chapter 3. In this chapter, we extend the objective of the chapter 3 to countering smart SSDF attacks. The key idea is to identify the various malicious attacks possible in collusion and prevent them using suitable penalties. A game theoretic analysis of the proposed method proves that the system attains the Nash equilibrium when all the SUs are honest.

4.1 Introduction

One important fact that can be concluded from Chapter 3 is that the attack prevention mechanisms essentially need awareness about the level of intelligence of the MUs. They must be capable enough to break the strategy of the MUs. The designing of the attack prevention mechanisms involves computational complexities. The complexities increase for countering attacks made with higher intelligence. Higher intelligence also brings colluding capability in the MUs. Recall that in Chapter 3, the considered MUs attacked independently. They did not have any knowledge about the other SUs or the other MUs. The SSDF attacks can become more disastrous if the MUs have learning capabilities to collude among themselves. With such a capability, the MUs can manipulate their reports more intelligently and the schemes for independent attacks are likely to fail. In this chapter, we propose a mechanism to counter such smart attacks having colluding capabilities. As mentioned before, CSS can be performed in a centralized or a decentralized manner. Since, collusion attacks are caused with more easiness in decision fusion CSS [47], our analysis in this chapter is based on decision fusion CSS.

Collusion attacks have been extensively researched in CRs as well as in other areas of communications [47, 48, 61–66]. In [61], a CSS system facing collusion attacks from some cooperating SUs has been studied. The study of the attack scenario is based on a representative *distributed consensus-based spectrum sensing* algorithm. Distributed consensus-based spectrum sensing is a form of decentralized CSS. It is found that such a system is prone to the *covert adaptive data injection* attack. These attacks are caused by the MUs which are capable of adjusting attack strategies according to the decentralized CSS. They can manipulate the sensing results without being caught by conventional detection schemes. These MUs are some internal SUs participating in the CSS. The damage caused by these at-

TH-1605_10610214

tacks is magnified when they are launched in collusion. To counter the collusion attacks, a hash-based computation verification approach has been proposed. In this mechanism, each SU in the network has a unique ID and shares a unique key with every neighbor SU. Each pair of neighbor nodes has at least one common neighbor. There exists a secure neighborhood discovery mechanism, with which each SU can obtain two-hop neighborhood information. To implement the hash-based mechanism, the authors propose an iterative algorithm. In the first iteration, each SU reports its measurements to its neighbor SUs using an authenticated broadcast. After the SU collects all its neighbors' reports, it computes an updated information. Then it broadcasts this updated information to all the SUs. The broadcast contains a *hash commitment* of its inputs together with its own data. A hash commitment refers to a cryptographically encoded value which is hidden to the unintended SUs. Consequently, each SU receives a collection of updated reports from its neighbors. In the second round, each SU broadcasts the data of all its neighbors collected at the beginning of the first round. Finally, each SU receives a collection of data from the two-hop neighbors. Then, each SU checks whether the IDs in the collection are consistent with its stored neighbor IDs and whether its own data and the common neighbours' data are incorporated in each updated state by recomputing each updated state and commitment. It also sees that if the verification of an SU fails, the update process is stopped. The goal of this algorithm is to ensure that the state updates of each SU are trustworthy. With this algorithm, each SU can securely discover its two hop neighbors. As long as each pair of SUs can share one common neighbor, the collusion attacks can be identified.

In [62], the authors address the damage of collusion attacks on the information flowing around the network. The network has multiple copies of information published by multiple users. The authors asses the quality of the information from each user by evaluating its trustworthiness. A trust model is presented to evaluate the trustworthiness of the information as well as the users reporting them. This trustworthiness is based on *information provenance* which refers to the location history, the source of its origin, the details of the user reporting it, the details of the various users who have passed or processed it before it reaches the FC. The FC evaluates the information it receives from the users. This evaluation is updated repeatedly by considering two factors: *information similarity* and *path difference*. The information from different users has been grouped in sets known as information sets. Then, the similarity scores between two pairs of information are evaluated and based on it, the MU is identified. The MU is imposed with a penalty calculated on the basis of the feedbacks based on the

TH-1605_10610214

similarity scores obtained from the different users.

The authors in [63] study the CR security problem in the medium access control (MAC) layer. The analysis of a CR system in the MAC layer is based on the Markov chain model of carrier sense multiple access with collision avoidance (CSMA/CA). The CSMA/CA protocols depend on the random yield of the packets to use the spectrum efficiently. The MUs attack by picking short random yield and obtaining a larger share of the available bandwidth than the honest SUs. To address this problem, the authors use game theory and study the systematic cheating of the MUs. The behavior of the MUs and their effects on CSS is studied. All the cooperating SUs are viewed as players. Both the cases of a single and multiple attacks have been studied. The strategies of the honest players are arranged as *contention windows*, the size of the contention window is seen as their move, and their utilities are seen in the form of their throughputs. A contention window is a time division multiplexing mechanism. It refers to a collection of the strategies supposed to be processed on the first come first serve basis. The MUs break the contention window to gain additional utilities. First a desired point of operation of this CSS network is obtained such that the PUs do not suffer any collision and the SUs get equal utilities. Each contention window represents a set of strategies. For each set of strategies, a throughput value is obtained. Hence, every contention window gives a range of throughput values. The authors aim to obtain a contention window which gives the maximum SU throughput. It is shown that the desired throughput is obtained when the system reaches the Nash equilibrium that is also Pareto optimal. If any of the SUs deviates from its strategy to disturb the Nash equilibrium, it is penalized by all the cooperating SUs. The penalty any SU imposes on the other SU is the difference of its throughput from that of the other SU's throughput.

In [47], the authors first present a centralized collusion attack strategy. This strategy is made on a two-phase CSS system shown in Figure 4.1 with the help of an integer linear programming to compromise the decision of the FC. The strategy is named as energy efficient CSS (EE-CSS). The authors have designed a separate FC for the MUs known as the malicious FC. The MUs fuse their manipulated decisions at the malicious FC. The proposed strategy aims to attack only when it is likely to compromise the decision of the honest FC. It is shown that the proposed collusion attack can severely impact the global P_{fa} and P_{md}. A cross correlation filter identifies the difference in cross-correlations of the sensing reports of the MUs and the honest SUs. This difference in the cross-correlation of the sensing reports of the MUs and the SUs is used to identify and eliminate the MUs.

TH-1605_10610214

In [48], the authors have formulated a strategy against the jamming attacks. The SUs exploit the flexible access to multiple channels as the means of anti-jamming defense. First, investigations are made for the case where an SU can access only one channel at a time and hop among different channels. This strategy is used to model the system as an anti-jamming game. The authors formulate a Markov chain based channel hopping defense strategy by observing the interaction between the honest SUs and the MUs. Then, they propose two learning schemes for the honest SUs to gain the knowledge of the actions of the MUs. These schemes make the SUs capable of handling cases without perfect knowledge. The authors also extend the schemes to the scenario where the SUs can access all available channels simultaneously. The anti-jamming game with randomized power allocation as the counter strategy has been formulated for this case to make it a Colonel Blotto game, which is mainly a class of two player zero sum game. Each player has limited resources. The player which donates the maximum resources to the system finally wins. The paper formulates the case where the SUs can access all available channels as a Colonel Blotto game to detect the MUs. Finally a Nash equilibrium is derived for this game which minimizes the worst-case damages.

The authors in [64] have focussed specifically on the internal attacks. A distributed CSS based on the dynamic reputation model has been proposed to defend these attacks. The reputation values are used for performing weighted CSS. These values are based on the *Vickrey-Clarke-Groves (VCG)* mechanism. This mechanism is a sealed bid auction procedure among different bidders (SUs in the present case). The bidders report their evaluation of an event without knowing the reports of the other bidders in the auction. The auction system charges each of the bidders for the harm they cause to the other bidders. The VCG mechanism satisfies the following two conditions: 1) It should be incentive compatible and 2) It is individual rational. The condition in 1) means that the SUs should have no incentive to submit false information. The point 2) means that the rational users are expected to gain a higher utility form actively participating in the mechanism than from avoiding it. Based on the VCG mechanism, the authors design an algorithm for defending the system from MUs. In this algorithm, the application and the allocation of channels are done in two stages. In the first stage, the base station calculates the best allocation results. Then it allocates the channels based on the demands from the PUs. PUs can apply for consecutive slots to complete its transmission. In the second stage, the remaining vacant channels are allocated to the SUs by the the base station. After the allocation, the base station waits for the users to complete transmission and reallocate channels

TH-1605_10610214

in the next competing slot.

In [65], the authors aim to defend the MUs by collecting information on their reputation in the long term. A moral hazard principal-agent framework is constructed and an incentive compatible mechanism is designed to thwart the malicious behaviors of the MUs. This framework offers incentives to the MUs for not attacking. The authors consider external MUs. A malicious-behavior-resistant (MBR) mechanism with the above said framework is designed. The analysis of the malicious behavior is done by observing the utilities of the MUs. A penalty is exploited according to the conditions for the MUs to choose different malicious behaviors. The malicious behavior analysis provides an important basis to design appropriate MBR mechanisms. By analyzing the resistance cost of the MBR methods, it is concluded that the proposed MBR with SS could provide infinite punishment with resistance cost. Hence, an optimally joint SS and access mechanisms that provide an appropriately large incentive to the MUs with the least resistance cost has been proposed.

The authors in [66], have formulated a collision penalty mechanism for two kinds of proposed attacks naming them as *attack and run* and *stay with the attacks*. In the former attack, the MUs attack in the short term by attacking and running away and in the latter case, the MUs attack in the long run by staying after attacking and reap the benefits. To thwart these two attacks the authors have formulated two kinds of collision penalty: the direct collision penalty and the indirect collision penalty. The direct collision penalty can counter only the attack and run attacks whereas the indirect collision penalty can counter both the attacks.

The primary limitation in the above mentioned works is that they fail to provide a comprehensive categorization of the different possible attacks scenarios. The possibilities of attacks in different scenarios have not been considered in these works. In this chapter, we design a collision penalty mechanism keeping different attack scenarios in view. Bounds on the collision penalty are designed to counter the attacks in different scenarios. The effectiveness of the proposed method is proved using the concepts of game theory.

The rest of chapter is organized as follows: In Section 4.2, we explain the system model and the assumptions. The decision fusion rule and the parameters for our evaluations have also been explained in this section. In Section 4.3, we begin with our proposed idea. Section 4.3.1 presents the first bound on the collision penalty. In Section 4.3.2, we find the optimal decision fusion rule. In Section 4.4, we explain the different attack scenarios and derive additional bounds the collision penalty for their

TH-1605_10610214

prevention. In Section 4.5, a game theoretic analysis of the considered system has been presented. Section 4.6 concludes the chapter.

4.2 System Model

4.2.1 System Model and Assumptions

Let there be N SUs performing CSS. Let hypothesis H_0 imply the PU is idle and H_1 imply the PU is active. The ith SU senses the PU spectrum and reports a decision $D_i = 0$ for H_0 and $D_i = 1$ for H_1 to the FC. Let P_{di} and P_{fi} be its probability of detection and probability of false alarm respectively. The FC makes the final decision using the reports of the SUs and broadcasts it to all the SUs. Again, we adopt a periodic sensing model for opportunistic spectrum access illustrated in Figure 3.1 and again here in Figure 4.1. Each time slot consists of two phases:

- Phase 1- CSS: It is the reporting phase. In this phase, all the SUs report their decisions to the FC which uses them to make a global decision.
- Phase 2- Spectrum Sharing: This is the transmission phase. Based on its decision, the FC broadcasts 0 when the channel is available for transmission. If it broadcasts 1, none of the SUs should transmit.

Figure 4.1: Periodic Sensing

If the phase 1 is divided into $m = 1, 2, \ldots, M$ sensing instants, the received signal $y_i(m)$ at the ith SU by the mth sensing instant is given by

$$\begin{aligned} y_i(m) &= h_i s(m) + u_i(m) \quad : H_1 \\ y_i(m) &= u_i(m) \qquad\qquad\quad : H_0 \end{aligned} \tag{4.1}$$

TH-1605_10610214

4.2.2 Decision Fusion Rule

There are various decision fusion rules (DFRs) available in the literature [36]. The three DFRs widely used are:

n out of N rule: Suppose D represents the sum of the decisions of the N SUs at the FC as

$$D = \sum_{i=1}^{N} D_i, \tag{4.2}$$

Then n out of N DFR is given as

$$D \underset{H_0}{\overset{H_1}{\gtrless}} n. \tag{4.3}$$

AND rule: According to this rule, the FC decides for the presence of the PU only when all the N SUs report 1 at the FC. Hence, this rule is obtained after substituting $n = N$ in (4.3).

OR rule: By this rule, the FC decides for the presence of the PU if only one SU reports 1 at the FC. Hence, this rule is obtained after substituting $n = 1$ in (4.3).

4.2.3 Evaluation Parameters and Conditions

PU and SU utilities (U_{PU}, U_{SU}) : For each successful transmission, we assume that the PU and each SU gain utilities U_{PU} and U_{SU} respectively.

Collision Penalty (C_P) : Collision Penalty C_P is the amount charged on the FC by the PU if is suffers collision. The FC penalizes the SUs by dividing C_P equally among all of them, irrespective of an SU being honest or malicious [22].

4.2.4 Assumptions

We make the following assumptions

1: Both the SUs and the FC know the probability of the PU being idle ($P(H_0)$) [129].

2: The signal power of the PU is sufficiently higher than the noise power, hence the probability of successful transmission by an SU in the presence of the PU is negligible [9].

3: The FC follows the n out of N rule for making the global decision, since our study is based on a general decision fusion CSS.

TH-1605_10610214

4: The PU has a legitimate right over the spectrum while an SU is obliged by the PU to get only a part of it in its absence. This leads to the assumption $U_{PU} >> U_{SU}$.

5: We proceed with the assumption made in [22] that the smart MUs can overhear the decisions of the other SUs while reporting to the FC.

6: The SU will act maliciously only if it sees a gain in it.

4.3 Proposed Scheme

The proposed scheme finds bounds on C_P for countering smart SSDF attacks

4.3.1 Bound on C_P for Sharing the Spectrum by the PU

The utility point of view demands that sharing its spectrum with the SUs must be more beneficial for the PU than not sharing it. A CR network has three situations: 1) the SUs are present but do not cause collisions to the PU, 2) the SUs are present and cause collisions to the PU, and 3) the SUs are not present. If the PU gets a greater utility in situations 1 and 2 than in situation 3, it will share its spectrum even in hostile environments. If γ(N) is the probability of collision of the SU with the PU, then

$$(1-\gamma(\mathrm{N}))\mathrm{U}_{PU} + \gamma(\mathrm{N})\mathrm{C}_P \geq \mathrm{U}_{PU}. \tag{4.4}$$

On Solving (4.4), we obtain

$$C_P \geq U_{PU} \tag{4.5}$$

Therefore, $C_P = U_{PU}$ is the lower bound for sharing the spectrum by the PU.

4.3.2 Optimal Decision Fusion Rule

In an n out of N decision fusion CSS, $\forall n \in \{1, \ldots, N\}$, there exists an $n = n_{opt}$ which is optimal in some sense for the system [160, 161]. The $n = n_{opt}$ is known as the Optimal Decision Fusion Rule (ODFR). The FC uses the ODFR for deciding about the spectrum occupancy. The OFDR will be used for formulating bounds on C_P in different attack scenarios. There have been significant researches on finding the OFDR [160, 161]. In these papers, the OFDR has been obtained for minimizing the *total error* $P_e = P_{fa} + P_{md}$, where P_{fa} and P_{md} are the global probabilities of false alarm and miss detection respectively. Since, C_P has been proposed for preventing collisions with the PU, it improves

TH-1605_10610214

the throughput of the PU. In the next section, we find an n_{opt} aimed for the maximization of the SU throughput. The formulation of the SU throughput will appropriately consider C_P such that, maximizing the SU throughput should not harm the PU.

Let $P_{e_{\overline{PU}}}$ and $P_{e_{PU}}$ be the probabilities of error for each SU while transmitting in the absence and the presence of PU respectively. Assuming n out of N DFR, we formulate the expected throughput $E_{U_i}(n)$ of the ith SU as

$$\begin{aligned} E_{U_i}(n) = \mathrm{P}\left((D \leq n-1) \cap H_0\right)(1-P_{e_{\overline{PU}}})\tfrac{U_{SU}}{N} + \\ P\left((D \leq n-1) \cap H_1\right)\left\{(1-P_{e_{PU}})\tfrac{(U_{SU}-C_P)}{N} + P_{e_{PU}}\tfrac{-C_P}{N}\right\}, \end{aligned} \tag{4.6}$$

As mentioned before, the probability of successful transmission for the SU in the presence of the PU is negligible, hence $P_{e_{PU}} \approx 1$. Therefore, (4.6) can be written as

$$E_{U_i}(n) = \mathrm{P}\left((D \leq n-1) \cap H_0\right)\frac{S_P U_{SU}}{N} - P\left((D \leq n-1) \cap H_1\right)\frac{C_P}{N}, \tag{4.7}$$

where $S_P = 1 - P_{e_{\overline{PU}}}$, and $P_{e_{\overline{PU}}} = Q\left(\frac{d}{2\sigma_u}\right)$, d is the distance between the SU transmitter and the SU receiver, σ_u^2 is the noise variance, and $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty \exp\left(-\frac{t^2}{2}\right)dt$. Since the SUs report binary decisions at the FC, D follows a Binomial distribution. Expanding (4.7) will give

$$E_{U_i}(n) = P(H_0)\left[\sum_{j=0}^{n-1}\binom{N}{j}P_{f_i}^j(1-P_{f_i})^{N-j}\right]\frac{S_P U_{SU}}{N} - (1-P(H_0))\left[\sum_{j=0}^{n-1}\binom{N}{j}P_{d_i}^j(1-P_{d_i})^{N-j}\right]\frac{C_P}{N} \tag{4.8}$$

In the above expression, all the parameters except n are known. This simplifies the problem of maximizing $E_{U_i}(n)$. To find n_{opt}, the FC sets the penalty $C_P = U_{PU}$, the minimum penalty possible. From (4.8), the ratio $\frac{E_{U_i}(n+1)}{E_{U_i}(n)}$ is obtained as

$$\frac{E_{U_i}(n+1)}{E_{U_i}(n)} = \frac{P(H_0)\left[\sum_{j=0}^{n}\binom{N}{j}P_{f_i}^j(1-P_{f_i})^{N-j}\right]S_P\frac{U_{SU}}{N} - (1-P(H_0))\left[\sum_{j=0}^{n}\binom{N}{j}P_{d_i}^j(1-P_{d_i})^{N-j}\right]\frac{U_{PU}}{N}}{P(H_0)\left[\sum_{j=0}^{n-1}\binom{N}{j}P_{f_i}^j(1-P_{f_i})^{N-j}\right]S_P\frac{U_{SU}}{N} - (1-P(H_0))\left[\sum_{j=0}^{n-1}\binom{N}{j}P_{d_i}^j(1-P_{d_i})^{N-j}\right]\frac{U_{PU}}{N}} \tag{4.9}$$

On simplifying, we get

$$\frac{E_{U_i}(n+1)}{E_{U_i}(n)} = \frac{P(H_0)\begin{pmatrix} N \\ n \end{pmatrix} P_{f_i}^n (1-P_{f_i})^{N-n} S_P \frac{U_{SU}}{N} - (1-P(H_0))\begin{pmatrix} N \\ n \end{pmatrix} P_{d_i}^n (1-P_{d_i})^{N-n} \frac{U_{PU}}{N}}{P(H_0)\left[\sum_{j=0}^{n-1}\begin{pmatrix} N \\ j \end{pmatrix} P_{f_i}^j (1-P_{f_i})^{N-j}\right] S_P \frac{U_{SU}}{N} - (1-P(H_0))\left[\sum_{j=0}^{n-1}\begin{pmatrix} N \\ j \end{pmatrix} P_{d_i}^j (1-P_{d_i})^{N-j}\right] \frac{U_{PU}}{N}} + 1 \tag{4.10}$$

$$\frac{E_{U_i}(n+1)}{E_{U_i}(n)} = \frac{K_1\begin{pmatrix} N \\ n \end{pmatrix} P_{f_i}^n (1-P_{f_i})^{N-n} - K_2\begin{pmatrix} N \\ n \end{pmatrix} P_{d_i}^n (1-P_{d_i})^{N-n}}{K_1\left[\sum_{j=0}^{n-1}\begin{pmatrix} N \\ j \end{pmatrix} P_{f_i}^j (1-P_{f_i})^{N-j}\right] - K_2\left[\sum_{j=0}^{n-1}\begin{pmatrix} N \\ j \end{pmatrix} P_{d_i}^j (1-P_{d_i})^{N-j}\right]} + 1 \tag{4.11}$$

where $K_1 = P(H_0)S_P U_{SU}$ and $K_2 = (1-P(H_0))U_{PU}$. The ratio $\frac{E_{U_i}(n+1)}{E_{U_i}(n)}$ represents the slope of $E_{U_i}(n)$. It can be seen that $\frac{E_{U_i}(n+1)}{E_{U_i}(n)} > 1$ indicates that $E_{U_i}(n)$ is increasing with n, while $\frac{E_{U_i}(n+1)}{E_{U_i}(n)} < 1$ indicates $E_{U_i}(n)$ is decreasing with n. Expressing (4.11) as

$$\frac{E_{U_i}(n+1)}{E_{U_i}(n)} = A(n) + 1 \tag{4.12}$$

where

$$A(n) = \frac{K_1\begin{pmatrix} N \\ n \end{pmatrix} P_{f_i}^n (1-P_{f_i})^{N-n} - K_2\begin{pmatrix} N \\ n \end{pmatrix} P_{d_i}^n (1-P_{d_i})^{N-n}}{K_1\left[\sum_{j=0}^{n-1}\begin{pmatrix} N \\ j \end{pmatrix} P_{f_i}^j (1-P_{f_i})^{N-j}\right] - K_2\left[\sum_{j=0}^{n-1}\begin{pmatrix} N \\ j \end{pmatrix} P_{d_i}^j (1-P_{d_i})^{N-j}\right]} \tag{4.13}$$

It can be seen that,

$$\frac{E_{U_i}(n+1)}{E_{U_i}(n)} = \begin{cases} > 1 & if \quad A(n) > 0 \\ = 1 & if \quad A(n) = 0 \\ < 1 & if \quad A(n) < 0 \end{cases} \tag{4.14}$$

Note that at the value of n where $A(n)$ crosses from a positive value to a negative value, $E_{U_i}(n)$ reaches its maximum. This value of n will represent the OFDR ($n = n_{opt}$). Analytically, it is difficult to find n_{opt} for (4.11). We perform simulations in Figures 4.2-4.6 to observe the behavior of $A(n)$.

TH-1605_10610214

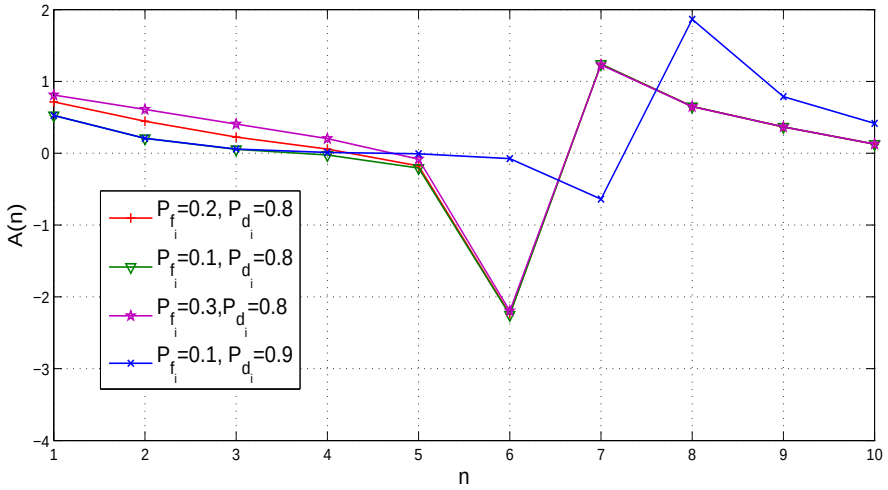

Figure 4.2: Variation of $A(n)$ vs n for N=10

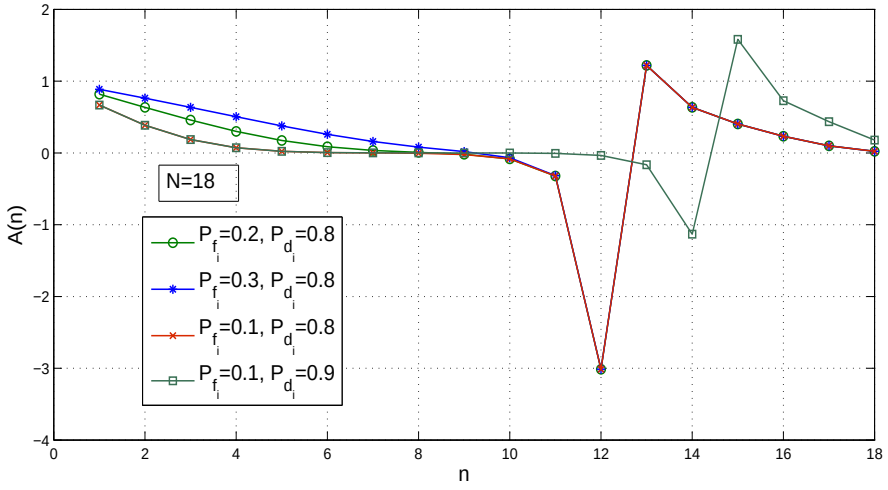

Figure 4.3: Variation of $A(n)$ vs n for N=18

TH-1605_10610214

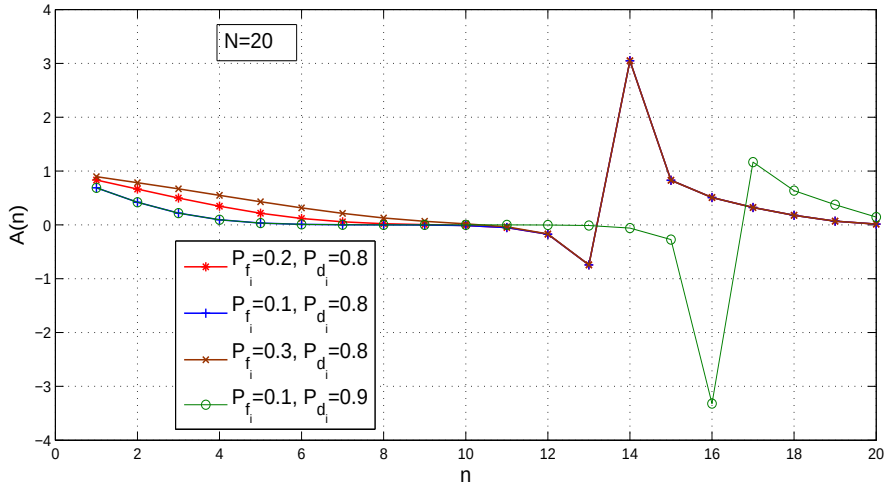

Figure 4.4: Variation of $A(n)$ vs n for N=20

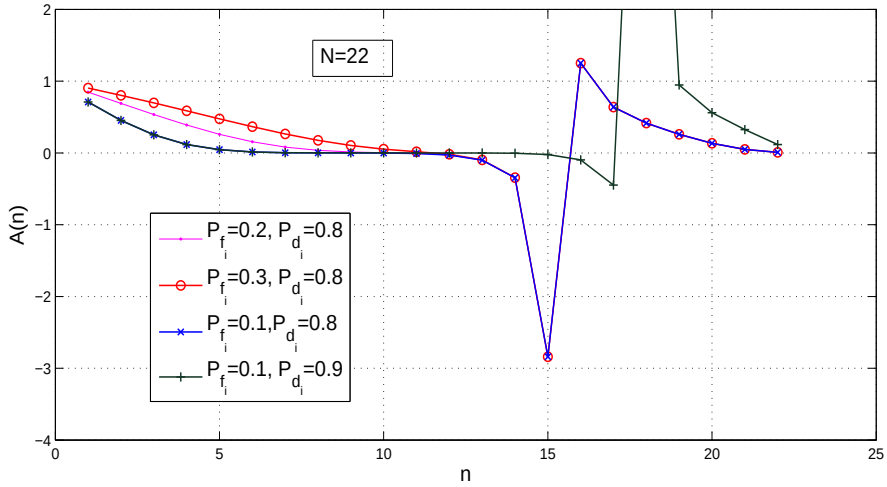

Figure 4.5: Variation of $A(n)$ vs n for N=22

TH-1605_10610214

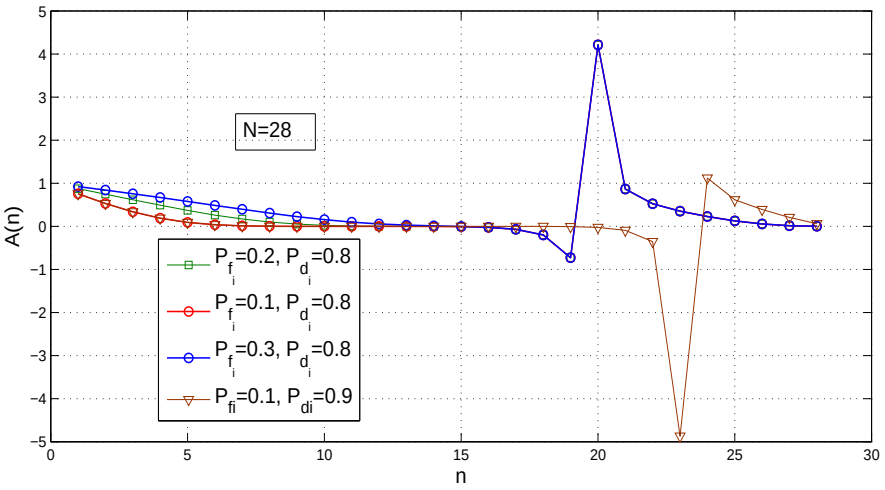

Figure 4.6: Variation of $A(n)$ vs n for N=28

Table 4.1: $E_{U_i}(n)$ at $n = N/2 - 3$ to $n = N/2 + 1$ for $P_{f_i} = 0.1$ and $P_{d_i} = 0.9$

N	$E_{U_i}(N/2-3)$	$E_{U_i}(N/2-2)$	$E_{U_i}(N/2-1)$	$E_{U_i}(N/2)$	$E_{U_i}(N/2+1)$
10	14.8769	15.7944	15.9592	15.8342	14.7203
14	15.8523	15.9763	15.9954	15.9816	15.8526
20	15.9933	15.9990	15.9998	15.9993	15.994
22	15.9976	15.9997	15.9999	15.9998	15.9979
28	15.9999	16.0000	16.0000	16.0000	15.9999

In Figures 4.2-4.6 the behavior of $A(n)$ has been shown for different values of N, P_{f_i} and P_{d_i}. We obtain K_1 and K_2 by assuming the values as $U_{PU} = 5U_{SU}$ and $P(H_0) = 9P(H_1)$. It can be seen that the smoothed $A(n)$ curve crosses zero slightly before $N/2$. This indicates that n_{opt} is either $N/2 - 1$ or $N/2$. Since n is an integer, we may conclude that $n_{opt} = N/2 - 1$. Tables 4.1, 4.2, and 4.3 show the values of $E_{U_i}(n)$ from $n = N/2 - 3$ to $n = N/2 + 1$ for different set of P_{f_i} and P_{d_i} values.

From Tables 4.1, 4.2, and 4.3, we conclude $n_{opt} = N/2 - 1$.

4.4 Bounds on C_P for Attack Prevention

Once the n_{opt} is determined, the FC analyzes all the possible malicious strategies of the MUs. We analyze the attack prevention mechanisms from the perspective of Game Theory. The reward obtained by an MU after playing maliciously will be expressed as utility. An MU may act maliciously in either one or both phases of periodic sensing. Any MU can play these strategies in the two phases:

TH-1605_10610214

Table 4.2: $E_{U_i}(n)$ at $n = N/2-3$ to $n = N/2+1$ for $P_{f_i} = 0.2$ and $P_{d_i} = 0.8$

N	$E_{U_i}(N/2-3)$	$E_{U_i}(N/2-2)$	$E_{U_i}(N/2-1)$	$E_{U_i}(N/2)$	$E_{U_i}(N/2+1)$
10	10.8370	13.9796	14.8384	12.6187	3.8988
14	13.9180	15.2601	15.5745	14.8007	11.6085
20	15.4842	15.8301	15.9021	15.7315	15.0002
22	15.6767	15.8953	15.9396	15.8354	15.3849
28	15.9204	15.9751	15.9856	15.9613	15.8545

Table 4.3: $E_{U_i}(n)$ at $n = N/2-3$ to $n = N/2+1$ for $P_{f_i} = 0.3$ and $P_{d_i} = 0.7$

N	$E_{U_i}(N/2-3)$	$E_{U_i}(N/2-2)$	$E_{U_i}(N/2-1)$	$E_{U_i}(N/2)$	$E_{U_i}(N/2+1)$
10	5.9655	8.3346	8.8608	0.2156	-19.2084
14	9.1807	11.2594	11.3606	6.1683	-6.0810
20	12.2285	13.3729	13.5181	10.9295	4.5846
22	12.9039	13.8872	13.9766	11.9010	6.7211
28	14.2815	14.8599	14.8928	13.7997	11.0489

$(H,H),(H,M),(M,H)$ and (M,M) where H and M represent 'Honest' and 'Malicious' strategies respectively. The only completely honest strategy is (H,H). The activity M in the phase 1 is reporting a false D_i to make the FC alter its decision. If the false D_i has not altered the FCs decision, then it is not considered malicious because none of the honest SUs or the PU will be adversely affected. The activity M in phase 2 is to disobey the FCs decision. Thus, the MUs know the number of SUs who have sensed the PU. Suppose n SUs have sensed the PU. Then the utility $G_{U_i}(m,n)$ seen by each of the m MUs if m MUs transmit during phase 2 is

$$G_{U_i}(m,n) = P\left((D=n)\cap H_0\right) S_P \frac{U_{SU}}{m} - P\left((D=n)\cap H_1\right)\frac{C_P}{N} \tag{4.15}$$

A plot of $G_{Ui}(m,n)$ with m MUs transmitting while n SUs have sensed the PU is shown in Figures 4.7 - 4.12. These plots are obtained after substituting $C_P = U_{PU}$ in (4.15) for different values of N. m and n have been varied from 1 to N. As mentioned in the Assumption 6, the SU will act maliciously only if it sees a positive value for $G_{Ui}(m,n)$. It can be seen in Figures 4.7 - 4.12 that $\forall n < N/2$, $G_{Ui}(m,n)$ attains significant positive values. Hence, $\forall n < N/2$, the MUs will become highly active. More importantly, it shows that setting $C_P = U_{PU}$ at $n = n_{opt}$ still makes $G_{Ui}(m,n)$ significantly positive for different values of m. Hence, even if the FC uses $n = n_{opt}$ for decision making, the MUs are highly likely to attack. It also indicates that the bound $C_P \geq U_{PU}$ is not enough to thwart the attacks and additional bounds on C_P are needed. We make analysis about the possible

TH-1605_10610214

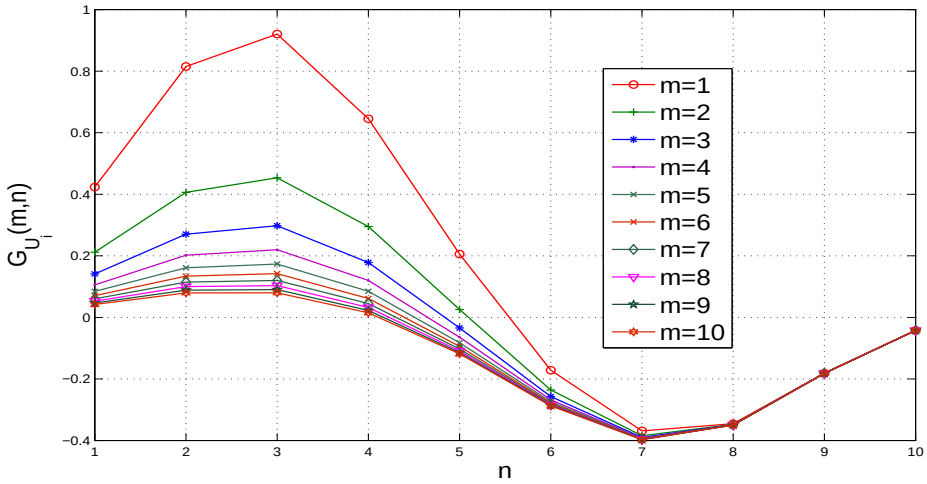

Figure 4.7: Variation of $G_{Ui}(m,n)$ vs n for N=10

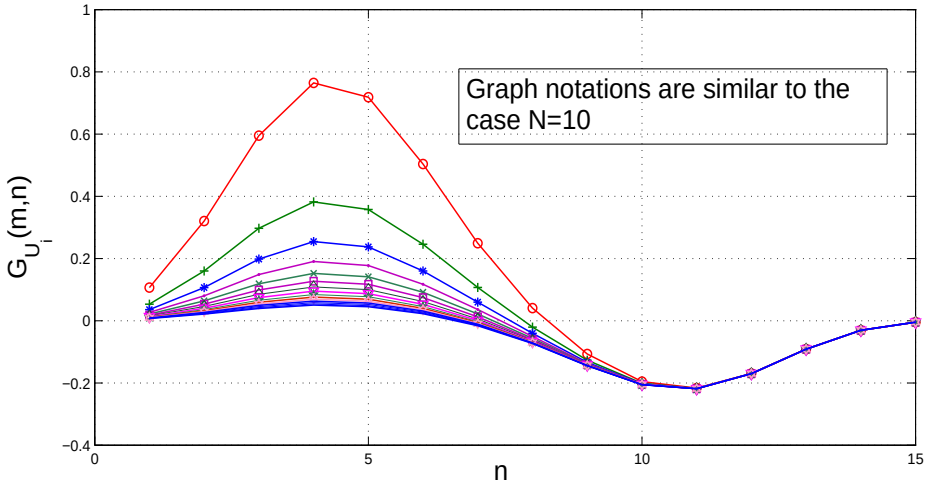

Figure 4.8: Variation of $G_{Ui}(m,n)$ vs n for N=15

TH-1605_10610214

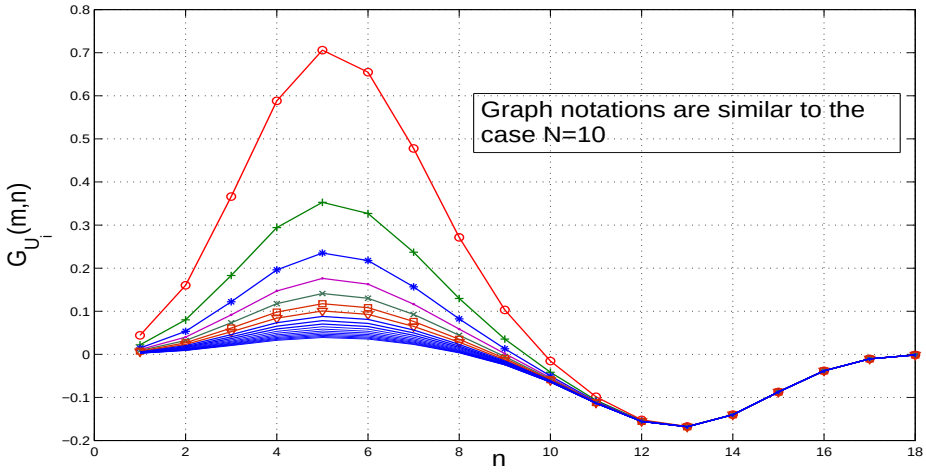

Figure 4.9: Variation of $G_{Ui}(m,n)$ vs n for N=18

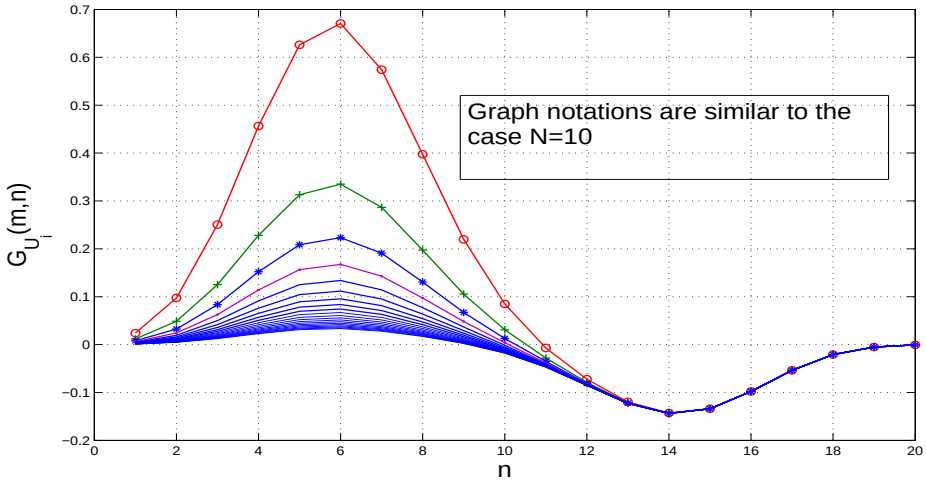

Figure 4.10: Variation of $G_{Ui}(m,n)$ vs n for N=20

TH-1605_10610214

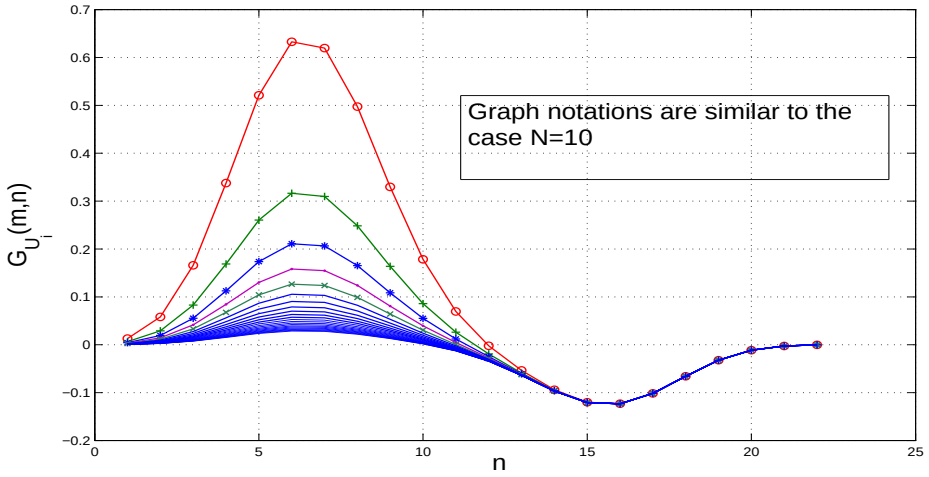

Figure 4.11: Variation of $G_{Ui}(m,n)$ vs n for N=22

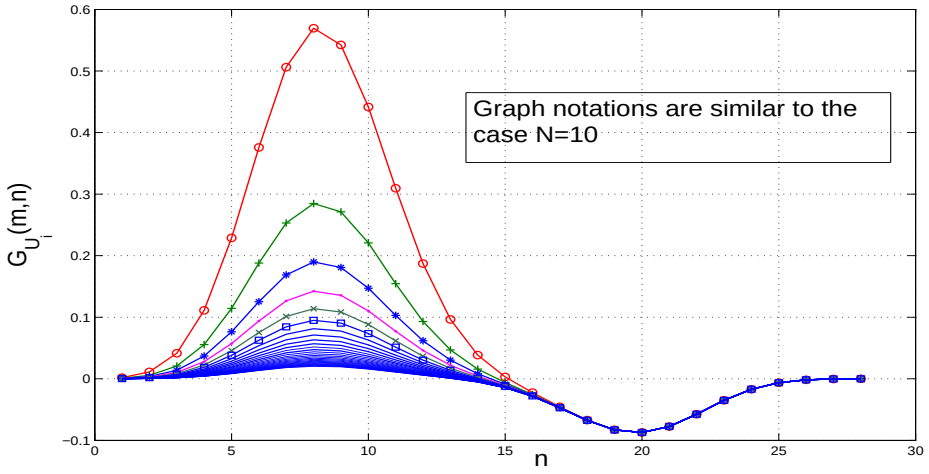

Figure 4.12: Variation of $G_{Ui}(m,n)$ vs n for N=28

TH-1605_10610214

attack scenarios to derive the additional bounds on C_P. Our analysis is based on two scenarios: When the FC declares H_1 and when it declares H_0.

4.4.1 Avoiding Malicious Strategies when the FC declares H_1

The FC declares H_1 in the following cases:

(i) When the MUs do not play malicious in the phase 1 and the PU is actually present. In this case the MUs will play (H, M).

(ii) When the PU is absent and it is forced by the MUs to declare H_1. In this case the strategy played by the MUs will be (M, M).

4.4.1.1 Avoiding (H, M)

This strategy is played when $n = n_{opt}$ SUs have sensed the PU. If $n < n_{opt}$ and the SUs are reporting honestly, then FC will never decide H_1. For $n = 1$ in Figure 4.7, $G_{Ui}(m, n)$ is positive for all values of m. This motivates the MUs for individual or collusion attacks. When $n = 5$, then it is positive only for $m = 1$ and $m = 2$. No attacks can happen for $n = 6$. To avoid the MUs playing (H, M), C_P should make $G_{Ui}(m, n)$s seen by the MUs which will result in (H, M) lower than zero. Thus,

$$P\left(D = n \cap H_0\right) S_P \frac{U_{SU}}{m} - P\left(D = n \cap H_1\right) \frac{C_P}{N} < 0 \quad \forall n \in \{1, 2, \ldots, N\} \tag{4.16}$$

$$C_P > \frac{P\left(D = n \cap H_0\right) S_P U_{SU} N}{P\left(D = n \cap H_1\right) m} \quad \forall n \in \{1, 2, \ldots, N\} \tag{4.17}$$

Let the RHS of (4.17) be the function $f(n)$. The ratio $\frac{f(n+1)}{f(n)} = \left(\frac{P_{d_i}(1-P_{f_i})}{P_{f_i}(1-P_{d_i})}\right)$ is less than 1 as $P_{di} > P_{fi}$ .Therefore, $f(n)$ is a monotonically decreasing function in n. Hence, it has the maximum value at $n = 1$. We denote this maximum value as $C_P^*(H, M)$. Thus the strategy (H, M) can be avoided if the following relation is satisfied

$$C_P > C_P^*(H, M) \tag{4.18}$$

Note that $C_P^*(H, M)$ is only the value which corresponds to $n = 1$. To avoid (H, M) attacks, C_P must be kept larger than $C_P^*(H, M)$.

TH-1605_10610214

4.4.1.2 Avoiding (M,M)

Suppose the PU is absent. The MUs will never play the strategies (H, M) and (M, H). This is because if they play H in the phase 1, the FC will declare H_0 and will allow the SUs to transmit in the phase 2. Now, playing M in the phase 2 means not obeying the FC, and hence not transmitting. Hence, by playing (H, M), the MUs do not gain anything. Now suppose they play M in the phase 1. This will force the FC to decide H_1 and deny transmissions for the SUs in the phase 2. In the phase 2, the MUs do not gain anything by playing H, which means obeying the FC and not transmitting. Hence, (M, H) will also not happen for this case. However, they do gain by disobeying the FC and transmitting in the phase 2. Hence, (M, M) strategy can be played when $n < n_{opt}$. On the other hand, if the PU is present, playing M in the phase 1 means making the FC declare H_0. It will be useless for the MUs to disobey the FC and do not transmit in the phase 2. Hence, (M, M) is not possible when the PU is present. The (M, M) strategy is possible only when $n < n_{opt}$. Let us consider the case of $N = 10$. It can be seen in Figure 4.7 that $G_{Ui}(m, n)$ is positive for $n < n_{opt}$. This motivates the MUs to play (M, M). If $n_{opt} - 1$ SUs have sensed the PU, then a single MU can make the FC decide H_1. Similarly, when $n_{opt} - 2$ SUs have sensed the PU signal, then at least $m = 2$ MUs need to collude in order to procure the spectrum by this strategy. We can generalize that when $n_{opt} - r$ SUs have sensed the PU, then at least $m = r$ MUs need to collude to attain the spectrum by this strategy. To avoid (M, M), C_P should be chosen to make the corresponding utilities negative. Therefore, $\forall r \in \{1, \ldots, n_{opt}\}$ and $\forall m \in \{r, \ldots, N\}$,

$$P\left((D = n_{opt} - r) \cap H_0\right) S_P \frac{U_{SU}}{m} - P\left((D = n_{opt} - r) \cap H_1\right) \frac{C_P}{N} < 0 \quad \forall n \in \{1, 2, \ldots, N\} \tag{4.19}$$

$$C_P > \frac{P\left((D = n_{opt} - r) \cap H_0\right) S_P U_{SU} N}{P\left((D = n_{opt} - r) \cap H_1\right) m} = h(m) \quad \forall n \in \{1, 2, \ldots, N\} \tag{4.20}$$

$$\frac{h(r+1)}{h(r)} = \frac{\frac{P_{f_i}^{n_{opt}-r-1}(1-P_{f_i})^{N-n_{opt}+r+1}}{P_{d_i}^{n_{opt}-r-1}(1-P_{d_i})^{N-n_{opt}+r+1}(r+1)}}{\frac{P_{f_i}^{n_{opt}-r}(1-P_{f_i})^{N-n_{opt}+r}}{P_{d_i}^{n_{opt}-r}(1-P_{d_i})^{N-n_{opt}+r}r}} \tag{4.21}$$

$$\underbrace{\frac{h(r+1)}{h(r)}}_{R} = \underbrace{\left(\frac{P_{d_i}(1-P_{f_i})}{P_{f_i}(1-P_{d_i})}\right)}_{R_1} \underbrace{\left(\frac{r}{r+1}\right)}_{R_2} \tag{4.22}$$

TH-1605_10610214

Table 4.4: Checking $\frac{1}{2}R_1$ for different P_{f_i} and P_{d_i}

P_{d_i}	P_{f_i}	R_1
0.57	0.4	1.19884
0.58	0.4	2.0714
0.6	0.2	6.0000
0.6	0.2	3.5600
0.6	0.4	2.25
0.7	0.2	9.3333
0.7	0.3	5.4444
0.7	0.4	3.5
0.8	0.2	16
0.8	0.4	6
0.8	0.3	9.33
0.9	0.3	21.0000
0.9	0.4	13.5
0.9	0.2	36.0000

Using the notations R, R_1 and R_2 as shown above and noting that $P_{di} > P_{fi}$, we see that $R_1 > 1$ and $R_2 < 1$. So the ratio R can be greater or lower than 1. The minimum value of R_2 for $r \in \{1, \ldots, n_{opt}\}$ is $\frac{1}{2}$. Hence the ratio $R > 1$ always if $\frac{1}{2}\left(\frac{P_{d_i}(1-P_{f_i})}{P_{f_i}(1-P_{d_i})}\right) > 1$. The generally desired value for P_{f_i} is as low as 0.1 while that P_{d_i} is as high as 0.9. We aim at a more general analysis and check the validity of $\frac{1}{2}\left(\frac{P_{d_i}(1-P_{f_i})}{P_{f_i}(1-P_{d_i})}\right) > 1$ for $P_{fi} < 0.4$. It can be seen in Table 4.4 that for $P_{fi} < 0.4$, this relation will be satisfied $\forall P_{di} > 0.58$.

We consider $P_{fi} < 0.4$ and $P_{di} > 0.57$ as the valid ranges for P_{fi} and P_{di} where $h(r)$ is an increasing function in r always. To avoid any kind of attacks in this scenario, C_P must be greater than the maximum of $h(r)$. Thus the maximum value is obtained at $r = n_{opt}$. We denote this value as $C_P^*(M, M)$. Note that $C_P^*(M, M)$ only corresponds to the C_P at $r = n_{opt}$. Therefore, the strategy (M, M) can be avoided if the following relation is satisfied:

$$C_P > C_P^*(M, M) \tag{4.23}$$

The strategies (H, M) and (M, M) can be avoided if C_P satisfies both (4.17) and (4.23). Also considering $C_P = U_{PU}$ as the lowest bound, we get

$$C_P \geq \max(C^*_{P_{(H,M)}}, C^*_{P_{(M,H)}}, U_{PU}) \tag{4.24}$$

TH-1605_10610214

4.4.2 Avoiding Malicious Strategies when the FC declares H_0

The FC declares H_0 in the following cases:

(i) When the PU is actually absent and the MUs play honestly in the phase 1. The strategy MUs will be left with in this case is (H, H).

(ii) When the PU is present but the FC is forced by the MUs to decide H_0. The strategy played by the MUs will be (M, H).

4.4.2.1 Avoiding (M,H)

The MUs try to make the FC decide H_0 so that both MUs and honest SUs transmit during phase 2. So (M, H) can happen only when $n = n_{opt}$ where the FC would have actually decided H_1. For the analysis of this strategy, expanding (4.8) gives

$$\begin{aligned} E_{U_i}(n_{opt}) = {} & P(H_0)\left[(1-P_{f_i})^N\right]\frac{S_P U_{SU}}{N} - (1-P(H_0))\left[(1-P_{d_i})^N\right]\frac{C_P}{N} + \\ & P(H_0)\left[P_{f_i}(1-P_{f_i})^{N-1}\right]\frac{S_P U_{SU}}{N} - (1-P(H_0))\left[P_{d_i}(1-P_{d_i})^N\right]\frac{C_P}{N} + \\ & \ldots + P(H_0)\left[\binom{N}{n_{opt}-1} P_{f_i}^{n_{opt}-1}(1-P_{f_i})^{N-(n_{opt}-1)}\right]\frac{S_P U_{SU}}{N} - \\ & (1-P(H_0))\left[\binom{N}{n_{opt}-1} P_{d_i}^{n_{opt}-1}(1-P_{d_i})^{N-(n_{opt}-1)}\right]\frac{C_P}{N} \end{aligned} \tag{4.25}$$

Rewriting (4.15) for $m = N$

$$G_{U_i}(N, n) = P\left((D = n) \cap H_0\right) S_P \frac{U_{SU}}{N} - P\left((D = n) \cap H_1\right) \frac{C_P}{N} \tag{4.26}$$

From (4.25) and (4.26), it can be seen that $E_{Ui}(n_{opt}) = G_{Ui}(N, 0) + G_{Ui}(N, 1) + \ldots + G_{Ui}(N, n_{opt}-1)$. Similarly $E_{Ui}(n_{opt}+1) = E_{Ui}(n_{opt}) + G_{Ui}(N, n_{opt})$. We have already seen that $\forall n \in [n_{opt}, \ldots, N]$, $E_{Ui}(n+1) < E_{Ui}(n)$. Hence, $E_{Ui}(n_{opt}) > E_{Ui}(n_{opt}+1)$ which shows that $G_{Ui}(N, n_{opt}) < 0$. Similarly, $G_{Ui}(N, n_{opt}+1), \ldots, G_{Ui}(N, N)$ are all negative. Therefore, as far as the collusion attacks are concerned, the MUs will never play (M, H). By considering that $C_P = U_{PU}$, FC sets $C_P = U_{PU}$.

Figures 4.7-4.12 show that the additional bounds on C_P make $G_{Ui}(m, n)$ negative for almost all the values of N, n and m. Though n_{opt} can still be seen as shifted from $N/2 - 1$. Nevertheless, our aim is to prevent the damage caused by the MUs. It has been accomplished by the additional bounds on C_P.

TH-1605_10610214

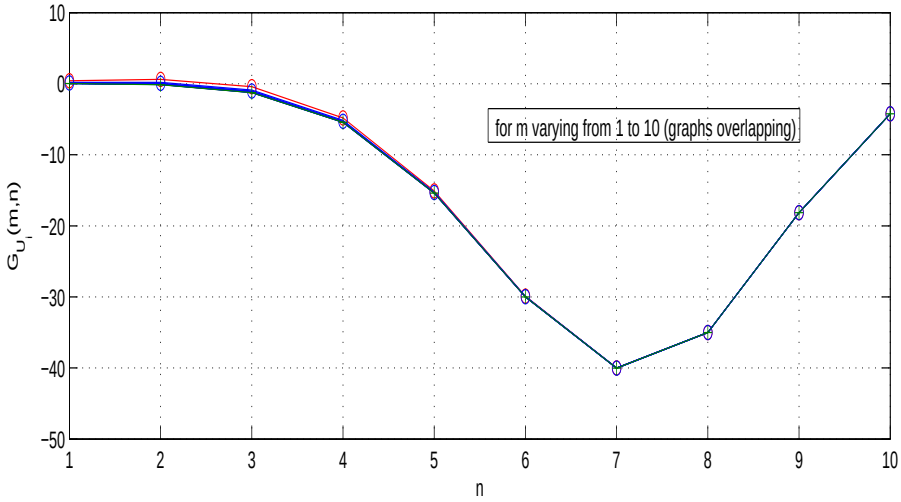

Figure 4.13: Variation of $G_{Ui}(m, n)$ vs n after using additional bounds on C_P for N=10

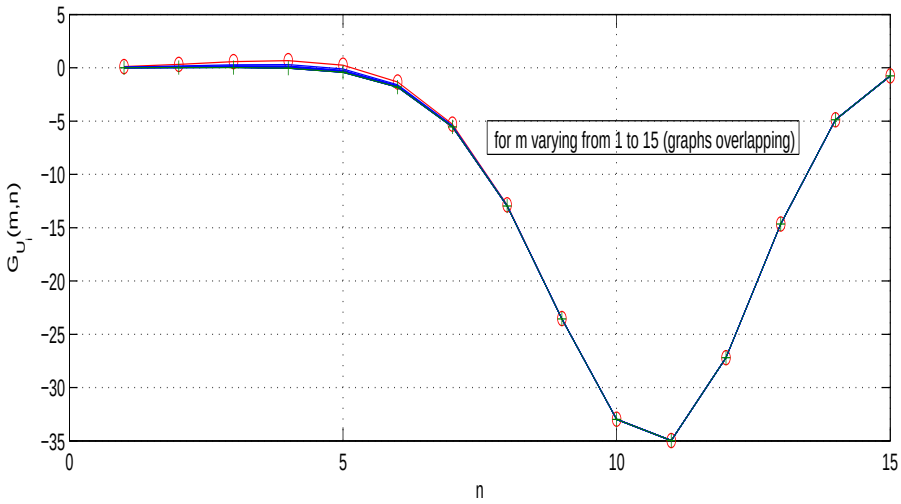

Figure 4.14: Variation of $G_{Ui}(m, n)$ vs n after using additional bounds on C_P for N=15

TH-1605_10610214

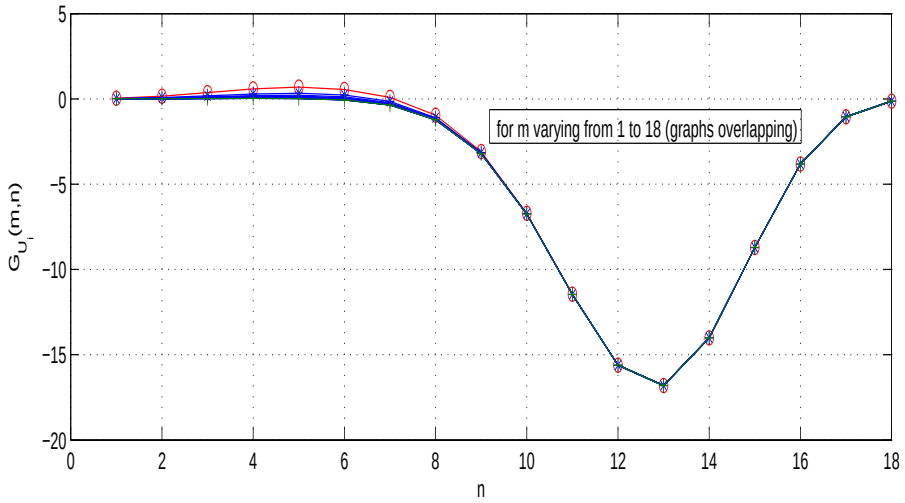

Figure 4.15: Variation of $G_{Ui}(m,n)$ vs n after using additional bounds on C_P for N=18

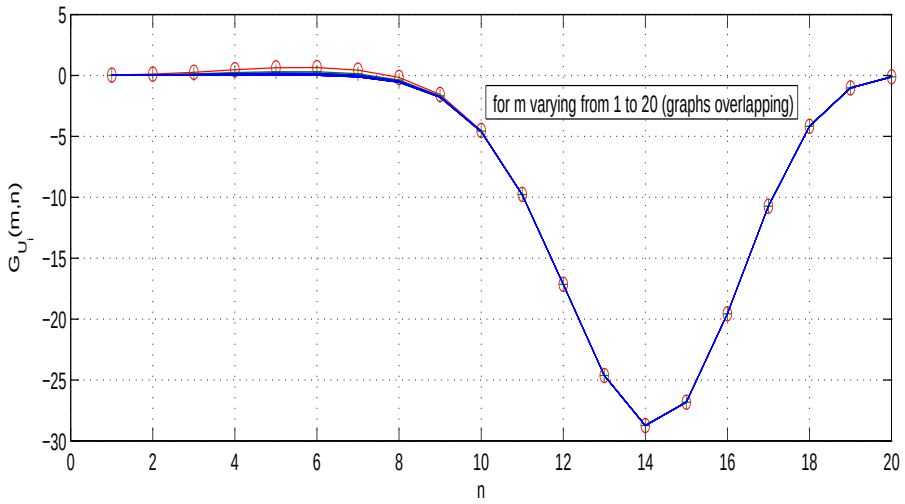

Figure 4.16: Variation of $G_{Ui}(m,n)$ vs n after using additional bounds on C_P for N=20

TH-1605_10610214

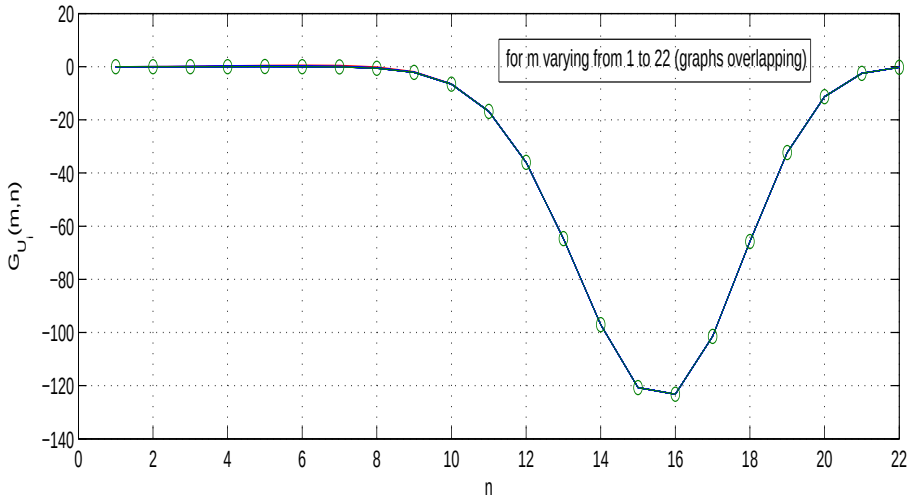

Figure 4.17: Variation of $G_{Ui}(m, n)$ vs n after using additional bounds on C_P for N=22

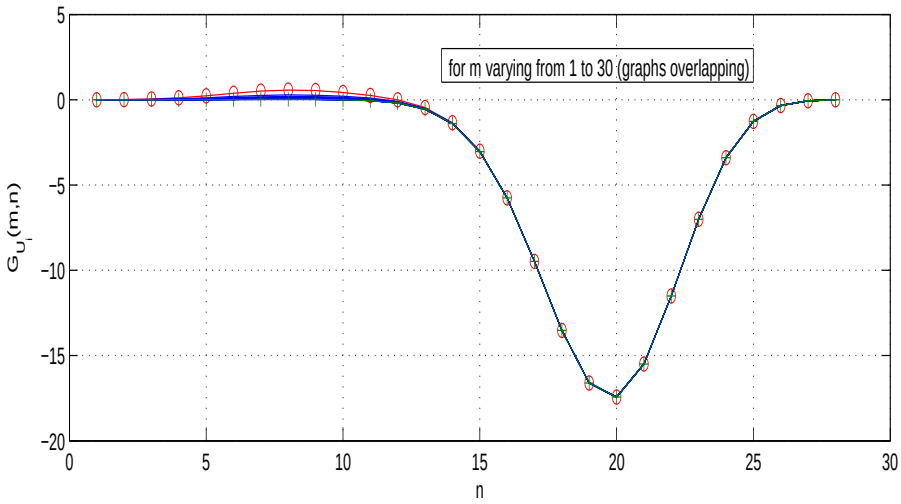

Figure 4.18: Variation of $G_{Ui}(m, n)$ vs n after using additional bounds on C_P for N=28

TH-1605_10610214

Table 4.5: Values for $L(n)$ for $n \in [1,3]$

n	1	2	3
$\frac{L(n+1)}{L(n)} = \frac{P_{di}(1-P_{fi})}{P_{fi}(1-P_{di})}$	0.4268	2.3333	12.7037

It can be seen from (4.24) that the value of C_P is large, since its lowest bound is U_{PU}. This can result to the honest SUs stop participating in CSS. To solve this problem, in the next section, we show with the help of Game Theory that the MUs lose heavily after playing malicious and the proposed C_P ensures avoidance of any malicious activity and complete safety to the honest SUs from being penalized unfairly.

4.5 The Best Strategy for the SUs

In this section, we use Game Theory to show that the best strategy for all the users is to be honest. The considered CSS has three basic elements if viewed as a strategic form game -

(i) A finite set of players $SU_1, SU_2, ..., SU_N$ with actions $a_1, a_2, ..., a_N$. Each a_i is either honest or malicious and is given as $a_i \in (H, M)$. The play (H, H) is the only strategy under H while $(H, M), (M, H)$ and (M, M) come under the strategy M.

(ii) The game is defined as $J(\{SU_i\}, \{a_i\})$.

(iii) A utility/payoff function- $G_{U_i}(m, n)$ as given in (4.15) is redefined as $G_{U_i}(a_1, a_2, ..., a_i, ..., a_N)$.

Our objective is to obtain the strategic profile which brings the game to Nash Equilibrium (NE) and Pareto Optimality. Such a strategic profile will give the ith player the maximum $G_{U_i}(m, n)$. Let a_i^* be the strategy of the ith SU at NE, where $i = 1, 2, ..., N$. NE is achieved when the ith player does not regret for its action, given the action chosen by the jth player is a_j^* where $j \neq i, j \in \{1, \ldots, N\}$. Hence, NE for this game can be expressed as

$$G_{U_i}(a_1^*, a_2^*, ..., a_i^*, ..., a_N^*) = \max_{a_i \in (H,M)} G_{U_i}(a_1^*, a_2^*, ..., a_i, ..., a_N^*) \tag{4.27}$$

The NE will be disturbed if any ith player deviates from action a_i^*.

Using C_P, we have made the utilities gained by even a single MU negative. Moreover, all the honest SUs also have to suffer a negative utility even if a single MU is present as the FC charges

TH-1605_10610214

Table 4.6: $G_{U_i}(m,n)$ for various n and m with $C_P = U_{PU}$

	n=0	n=1	n=2	n=3
$G_U(1,n)$	1.2536	-1.3546	-0.0194	-0.4694
$G_U(2,n)$	0.6043	0.5198	-0.3772	-0.5206
$G_U(3,n)$	0.3879	0.2415	-0.4965	-0.5376

Table 4.7: $G_{U_i}(m,n)$ for various n and m with $C_P = 722$

	n=0	n=1	n=2	n=3
$G_U(1,n)$	0.6488	-2.8790	-9.8978	-8.1526
$G_U(2,n)$	-0.0005	-3.7138	-10.2556	-8.2038
$G_U(3,n)$	-0.2169	-3.9961	-10.3749	-8.2208

the penalty equally on all SUs. This implies that the utility gained by each SU when at least one of them is malicious is negative. Hence, for $j \neq i$ and $\forall a_j = H$, the only a_i which maximizes $G_{U_i}(a_1, a_2, ..., a_i, ..., a_N)$ is H. Hence, NE can be achieved only when $a_i = H$ and the strategic profile which will result in non-negative utility to each SU is $(H, H, ..., H)$. It can also be seen that an NE also exists $\forall a_i = M$. However, that will make $G_{U_i}(a_1, a_2, ..., a_i, ..., a_N)$ negative, hence does not maximize it. Therefore, the NE obtained with $a_i = H, \forall i \in \{1, \ldots, N\}$ is Pareto-optimal.

Example:

We illustrate this for the case where only 3 SUs are involved. We assume that each SU has $P_{d_i} = 0.70$ and $P_{f_i} = 0.3$. We take $P(H_0) = 0.9$, $U_{SU} = 10$ and $U_{PU} = 5 \times U_{SU} = 50$. The ratio $\frac{K_1}{K_2} = 0.7572$. Table 4.5 shows that the value of the ratio $\frac{L(n+1)}{L(n)}$ crosses from less than 1 to greater than 1 for the first time at $n = 2$. Hence FC decides $n_{opt} = 2$. Table 4.6 shows $G_{U_i}(\mathrm{m}, \mathrm{n})$ seen by the SUs for various n when $C_P = U_{PU}$. None of the SUs will play (M, H) as $G_{U_i}(3,2)$ and $G_{U_i}(3,3)$ are negative. By (4.24), $C_P = \max(16.23, 721.45, 50)$. Let the FC set $C_P = 722$. The new values of $G_{U_i}(m,n)$ are

Table 4.8: Payoff matrix when the FC declares H_1

$SU_1 - H$	SU_2	H	M
SU_3	H	(0,0,0)	(-4.5,-2.9,-4.5)
	M	(-4.5,-2.9,-4.5)	(-4.5,-0.0005,-0.0005)

$SU_1 - M$	SU_2	H	M
SU_3	H	(-2.9,-4.5,-4.5)	(-0.0005,-0.0005,-4.5)
	M	(-0.0005,-4.5,-0.0005)	(-0.21,-0.21,-0.21)

TH-1605_10610214

shown in Table 4.7. We can see that the utilities which will result in (H, M) and (M, M) have become negative. Note that even if the utility $G_{U_i}(1, 0)$ is positive, none of the malicious strategies will make the SUs attain this value. Hence, the value $G_{U_i}(1, 1) = -2.9$ is the maximum possible utility when only 1 MU acts maliciously. Similarly, $G_{U_i}(2, 0) = -0.0005$ and $G_{U_i}(3, 0) = -0.21$ are the maximum possible utilities when 2 and 3 MUs act maliciously. Table 4.8 shows the payoff matrices when the FC decides H_1. The value -4.5 is the negative penalty suffered by the honest SUs.

The NEs are obtained for the strategic profiles (H, H, H) and (M, M, M). However, the strategic profile (H, H, H) is Pareto-optimal. Therefore the best strategy for all the SUs is to be honest. Thus, it is proved that C_P can avoid both (H, M) and (M, M) strategies.

4.6 Conclusion

CSS is highly vulnerable to the attacks by MUs. In this chapter, we focused on preventing both individual and collusion SSDF attacks. The proposed attack prevention method has been developed in the light of Game Theory. The ODFR that maximizes the throughput of each SU is found out first. It is seen that the effects of MUs are prevalent at the proposed OFDR. However, the MUs cause severe damage to the CSS Therefore, all possible malicious strategies of the MUs are identified and avoided by properly adjusting C_P. It is seen that C_P avoids all the malicious activities. The value of C_P is large, since its lowest bound is U_{PU}. This can result to the honest SUs stop participating in CSS. To solve this problem, we show with the help of Game Theory that the MUs lose heavily after playing malicious. Hence, the proposed C_P ensures avoidance of any malicious activity and complete safety to the honest SUs from being penalized unfairly. Also, it performs satisfactorily for a system with any value of n as its DFR.

TH-1605_10610214

5

Countering the Primary User Emulation Attacks

Contents

5.1 PUEAs 106
5.2 Approaches to Combat PUEAs 107
5.3 System Model, Sensing Mechanism and Parameters 110
5.4 Maximization of the SU Throughput under PUEAs 114
5.5 Obtaining Optimal Weights for Performing CSS 117
5.6 Experimental Results and Performance Evaluation 125
5.7 The Reason for using the NMA 136
5.8 Conclusion 137

TH-1605_10610214

In this chapter, we consider the second kind of attack mentioned in Chapter 1 : the primary user emulation attack (PUEA) [55]. An MU causes PUEA by transmitting emulated PU signals. Such an MU is known as a primary user emulator (PUE). The honest SUs mistake a PUE's signal to be coming from the PU and cease their transmissions. Hence, a PUE misleads the honest SUs about the licensed spectrum status. The PUE takes the advantage of this situation and starts transmitting on the spectrum.

We start the chapter with an introduction on PUEAsn in Section 5.1. Then we briefly describe about the existing works, their limitations and the significance of the SU throughput maximization problem in the presence of PUEs in Section 5.2. In Section 5.3, we explain the system model and the parameters considered for this investigation. Here, we discuss the expression for the throughput of an SU at the physical layer in detail. Subsequently in Section 5.4, we formulate the maximization problem of the SU throughput while giving sufficient protection to the PU. In Section 5.5, we present the proposed solution to the problem. We present the experimental results in Section 5.6 and summarize the chapter in section 5.8.

5.1 PUEAs

As mentioned earlier, PUEAs are caused when the MUs transmit emulated PU signals to misguide the cooperating SUs regarding the spectrum occupancy. The probability of these attacks is high since the MUs are installed with highly reconfigurable CRs [8]. With the learning and reconfiguring capabilities provided by the CR, it is not difficult for an MU to modify its air interface to emulate the PU signals. The SU system is required to differentiate the PU signal from the emulated PU signals, and it is a significantly difficult task. If an SU system misinterprets a signal to be coming from the PU, it has to terminate its communication which severely degrades its throughput. The PUEAs can also increase interference to the PU. Hence, the two major damages caused by the PUEAs can be categorized as:

- Degradation of the throughput of the SU system.
- Increased interference to the PU.

A successful implementation of the CR technology depends on robust security mechanisms against the PUEAs. The focus of our work is on the throughput degradation of the SU system.

TH-1605_10610214

There have been two kinds of PUEAs discussed in the literature [24]: *always-on PUEAs* and *smart PUEAs*. Always-on PUEAs are caused when the MUs transmit seamlessly irrespective of the presence of the PU. On the other hand, smart PUEAs are launched only when the PU is absent, thus saving its transmission power. In the following section, we detail about the existing works to counter PUEAs with their limitations and the problem addressed in this chapter.

5.2 Approaches to Combat PUEAs

As mentioned in the Chapter 2, there have been mainly two approaches in the literature to combat PUEAs:

(i) Direct approaches: These approaches aim at detecting the PUE. The detection is performed by identifying its location, differentiating the received signal power (RSS) or its features form those of the PU. The most significant work on detecting a PUE is in [55], where the authors have focussed on the vacant TV bands, since the FCC has recognized the TV bands suitable for the initial application for CR technology. The reason is that these TV bands experience lower dynamic traffic compared to the cellular networks. In this paper, a transmitter verification scheme termed as *LocDef (localization based defense)* has been proposed. In this scheme, the source of the signal is verified for being the PU by observing the signal characteristics. The location information of the PU has been used to distinguish between the PU and the PUE signal characteristics. The authors assume a stationary and known PU location. To implement this scheme, LocDef uses a *non-iterative localization* scheme. This method primarily depends on the modeling of the received signal from the PUE. Liu et al. in [162] aim at differentiating the PUE signal from the PU signal with the help of cryptography. The challenge in addressing this problem is that the FCC prohibits any modification to the PU signal. The authors develop an approach to authenticate the PU signal without violating the FCC norms. The wireless link signatures derived from the physical radio channel characteristics are integrated with the cryptographic signatures. To accomplish this, a *helper node* is kept physically near the PU. This node serves as a bridge between the PU and the SUs. The SUs first verify the wireless link signatures of the helper node. Then, they obtain the helper node's authentic link signatures to verify the PU's signals. The drawback of this mechanism is the requirement of the helper node near the PU. In [163], Pu et. al have used the cyclostationary features to differentiate between

TH-1605_10610214

the PU and the PUE signals. The classification of the features is done by feeding the signal into an artificial neural network. The authors aim at the following issues in detecting the PUEAs:

- The inability of the energy detection scheme based spectrum sensing systems in detecting PUEAs as the PUEs can easily transmit signals with the same energy as the PU.
- Localization based mechanisms being applicable only for static PUs
- Cryptographic signature based mechanisms requiring additional helper nodes near the PUs.

The proposed method has an advantage that it does not need a separate hardware for performing the cyclostationary feature classification. However, this method fails when the PUE is able to emulate the modulation scheme of the PU. In [164] and [165], Markov lower bound and *Wald's Sequential Probability Ratio Test (WSPRT)* based methods have been proposed to detect the PUEs. Both the methods are based on the analytical modeling of the received SU power. The authors in [56] and [57] have proposed a *belief propagation* based defense strategy, which uses the location information of the PU and the RSS from the PUEs.

The primary limitations of the above mentioned works is their dependence on the location identification, the features and the received power of the PU and PUE transmitted signals. The location identification based mechanisms distinguish the direction of arrival (DOA) of the received signal from the PUE and the PU. These mechanisms are efficient as long as the incoming PUE signals do not have the same DOA as the incoming PU signal. Also, the major requirement for the DOA differentiation based methods is a directional antenna or antenna arrays on each SU [166]. On the other hand, if the PU and PUE signals have the same signal power and features, the feature and RSS based mechanisms fail to differentiate them.

(ii) Indirect approaches: These approaches aim at thwarting the PUEAs by suppressing a specific damage caused by them rather than detecting them. The basis of these approaches is the estimation of the channel state information (CSI) of the PUE-SU links made in [167]. The estimated CSI is used to suppress the damage on a specific parameter by the PUEAs. For example, in [24], the authors use the CSI to reduce the damage caused by the PUEAs on P_d of the CSS system. The authors have considered an always-on PUEA model. A binary hypothesis testing problem for this model is considered and the expressions for P_d and P_{fa} are formulated. The authors use centralized weighted CSS for making the decision about the spectrum occupancy.

TH-1605_10610214

However, to simplify the calculations of P_d and P_{fa}, a modified weighted mechanism has been followed, where the received signals from all the SUs are weighted first and then summed at the FC. The FC calculates the energy of the weighted sum of the signals and P_d and P_{fa} are obtained. Then, P_d is maximized while keeping a bound on P_{fa}. A bound on P_{fa} is needed since the ROC curves show that P_d and P_{fa} monotonically increase with each other. On solving this optimization problem, the weights for performing weighted CSS are obtained. These weights are capable of suppressing the damage of PUEAs on P_d. It is known that the interference to the PU increases with a decreasing P_d. Hence, the authors have aimed at reducing the increased interference to the PU due to the PUEAs.

Some other major relevant works are [58–60, 67], where the authors have used the CSI obtained in [167] to minimize the *total error* of decision fusion based CSS systems. The total error is defined as the sum of P_{md} and P_{fa}. Unlike [24], the authors in [58–60, 67] consider a decision fusion based CSS. Saber et al. in [59] and [58] have obtained the optimal voting rule, the optimal number of samples needed for individual spectrum sensing and the optimal individual decision threshold which minimize the total error for the CSS model of smart PUEAs. In [59], the optimization of the number of samples and optimal voting rule have been presented whereas in [58], the optimal individual detection threshold has also been presented. The work in [58] is the extension of [59]. Further, Haghighat et al. in [60] have proposed different threshold values pertaining to different hypotheses arising in a smart PUEA model. These different threshold values are obtained with the help of simulations. The work in [60] is mainly an extension of the reference [67] by the same authors where only one threshold value has been obtained through simulations to mitigate the effects of the PUEAs. The authors in [168] have proposed a correlation matrix based detection method to detect the PUEAs. The authors consider the fact that the receivers closely placed have a high correlation in their received signals. The cooperating SUs placed closely will receive correlated signals from the PU going through almost identical fading. Such SUs will not help to exploit spatial diversity for CSS. Hence, the authors investigate over the receive signal correlation. They propose to select a few SUs with less correlation so that they can contribute to the purpose of CSS. This is done by forming a correlation matrix of the signals received by the SUs. After, selecting the few SUs, the MME detection is used to detect the presence of the PU. The authors assume that the PUE is located near to the SUs. Hence, in

TH-1605_10610214

the process of excluding the users with a high signal correlation, the PUE will also be excluded.

Note that the CSI estimation in [167] does not depend on the DOA, the RSS or the features of the PU signal. Therefore, the indirect approaches overcome these limitations of the direct approaches.

In this chapter, we follow an indirect approach to maximize the throughput of an SU participating in CSS in an environment facing PUEAs with a constraint on the interference to the PU. Our aim is to mitigate the effects of PUEAs on the SU throughput. To the best of our knowledge, this problem has not received focus in the physical layer. In honest sensing, the maximization of the SU throughput has been a subject of research [129, 169]. However, these references do not consider PUE in their cooperative model. On the other hand, the existing indirect approaches explained above consider the PUE in their cooperative models. However, they do not aim at mitigating the damages on the SU throughput by the PUE.

The objective of our work is to design a robust indirect PUE suppression scheme from the SU throughput perspective. Similar to [24], we consider the always-on PUEA CSS model and a weighted CSS scheme for fusing the SU energy data at the FC. An optimization problem is formulated to maximize the SU throughput with a constraint on the interference to the PU, in a CSS system facing PUEAs. The problem is solved with the help of the Nelder Mead Algorithm (NMA) [170] to obtain the optimal combining weights. The optimal weights generated are then used to combine the cooperating SUs' data at the FC. Our main contribution is the study of the CSS model in the presence of the PUEAs for maximizing the throughput of the SUs.

In the following section, we explain about the system model and the parameters considered for the evaluations in the chapter.

5.3 System Model, Sensing Mechanism and Parameters

5.3.1 System Model

Consider N SUs and 1 PUE in a CSS system as shown in the Figure 5.1. A periodic sensing scheme is considered for sensing the PU spectrum shown in Figure 5.2. Let H_0 and H_1 be the null and the alternative hypotheses respectively denoting the absence and the presence of the PU respectively in a PUEA environment. If the sensing time T is divided into M sampling instants, the signal $y_i(j)$ received by the ith SU at sampling instants $j = 1, 2, \ldots, M$ under H_0 and H_1 can be written as [24]

TH-1605_10610214

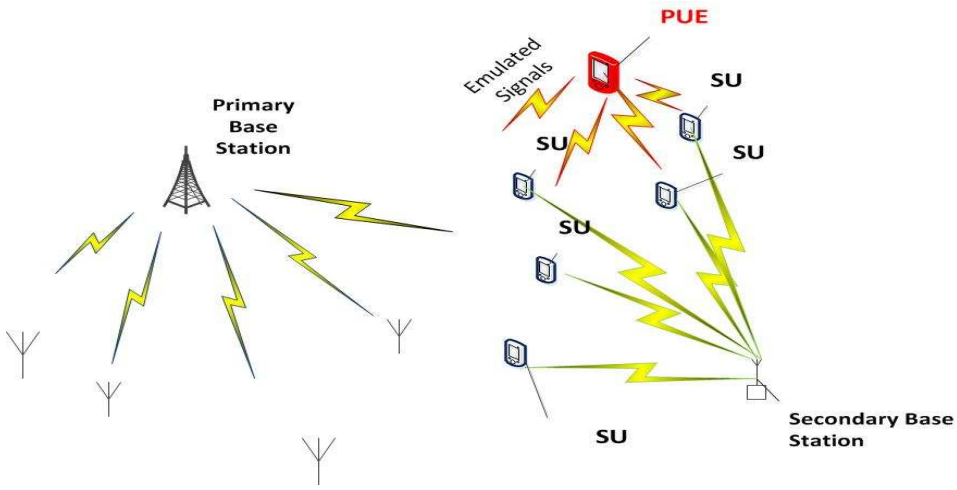

Figure 5.1: Primary User Emulation Attack Model

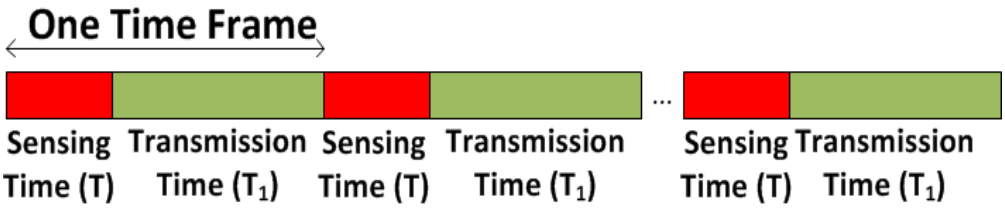

Figure 5.2: Periodic Sensing

$$y_i(j) = \begin{cases} \sqrt{\gamma_p} h_{p_i}(j) x_p(j) + \sqrt{\gamma_e} h_{e_i}(j) x_e(j) + u_i(j) & : H_1 \\ \sqrt{\gamma_e} h_{e_i}(j) x_e(j) + u_i(j) & : H_0 \end{cases} \tag{5.1}$$

where $h_{p_i}(j)$ denotes the channel coefficient of the PU-ith SU path, $h_{e_i}(j)$ denotes the channel coefficient of the PUE-ith SU path, $x_p(j)$ and $x_e(j)$ denote the PU and PUE signals assumed to be BPSK modulated, $u_i(j)$ denotes the noise at the ith SU assumed to be circularly symmetric complex Gaussian (CSCG) and γ_p and γ_e the SNRs of the PU to SU and the PUE to SU paths respectively. Without the loss of generality, the noise power of all the receivers has been assumed to be unity in all the investigations. $h_{p_i}(j)$ and $h_{e_i}(j)$ are assumed to be constant over one sensing interval and different

TH-1605_10610214

probability distributions are considered for $h_{p_i}(j)$ and $h_{e_i}(j)$ for evaluations in the Section 5.6.

At the end of T, the ith SU calculates its energy e_i as

$$e_i = \sum_{j=1}^{M} |y_i(j)|^2. \tag{5.2}$$

The SUs report their calculated e_is to the FC. The FC combines them to form a global decision regarding spectrum occupancy. Our aim is to weigh e_is at the FC for the maximization of the SU throughput. Unlike conventional combination, the FC performs a weighted combination of e_is to obtain its decision statistic E as

$$E = \sum_{i=1}^{N} w_i e_i, \tag{5.3}$$

where $w_1, w_2, \ldots, w_N$ are the combining weights to be optimized for maximizing the SU throughput. The decision regarding the PU presence is made at the FC by comparing E to a decision threshold λ. A value of E greater than λ concludes the decision in the favor of hypothesis H_1, otherwise H_0 is decided. Thus,

$$E \underset{H_0}{\overset{H_1}{\gtrless}} \lambda \tag{5.4}$$

5.3.2 Characterization of the Parameters

5.3.2.1 Probabilities of False Alarm and Miss Detection

As mentioned before, the performance evaluation of a SS system is based on two parameters, P_{fa} and P_{md}. P_{fa} is the probability of the FC wrongly declaring a vacant band as occupied. On the other hand, P_{md} is the probability of the FC declaring an occupied band as vacant. Mathematically, these probabilities are written as,

$$P_{fa} = \Pr(E > \lambda | H_0) \tag{5.5}$$

and

$$P_{md} = 1 - \Pr(E > \lambda | H_1). \tag{5.6}$$

A high efficiency of the SS system is ensured by low magnitudes of P_{fa} and P_{md}. The evaluation of P_{fa} and P_{md} is done by integrating the probability density function (pdf) of E over H_0 and H_1. For a large N, E approximately follows a complex Gaussian distribution [129] and the expressions for P_{fa} and P_{md} are obtained as

TH-1605_10610214

$$P_{fa}(\mathbf{w},\lambda) = Q\left(\frac{\lambda - \sum_{i=1}^{N} w_i(|h_{e_i}|^2\gamma_e + 1)}{\sqrt{\frac{1}{M}\sum_{i=1}^{N} w_i^2(|h_{e_i}|^2\gamma_e + 1)^2}}\right) \tag{5.7}$$

$$P_{md}(\mathbf{w},\lambda) = 1 - Q\left(\frac{\lambda - \sum_{i=1}^{N} w_i\,(R_i + 1)\,(|h_{e_i}|^2\gamma_e + 1)}{\sqrt{\frac{1}{M}\sum_{i=1}^{N} w_i^2\,(2R_i + 1)(|h_{e_i}|^2\gamma_e + 1)^2}}\right) \tag{5.8}$$

where $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^{\infty} e^{-\frac{u^2}{2}}du$ and $R_i = \frac{|h_{p_i}|^2\gamma_p}{|h_{e_i}|^2\gamma_e+1}$. The detailed derivations of (5.7) and (5.8) are given in Appendix B.

5.3.2.2 Throughput of an SU ($G_i(\mathbf{w},\lambda)$)

When the PU spectrum is detected vacant, it is allocated to the SUs depending on the spectrum allocation policy followed [171]. Without the loss of generality, we assume that for a period of one time span, the PU band is allocated to one SU [172]. One time span may contain one or more time frames $(T+T_1)$ as shown in the Figure 5.2. Our analysis here is confined over one time frame. Hence, only one SU will be active during all the evaluations. The SU transmits in two cases: 1) when the FC rightly recognizes the absence of the PU and 2) when the FC misses the presence of the PU. Accordingly, the effective throughput 'G_i' of the ith SU will be [129],

$$G_i(\mathbf{w},\lambda) = \frac{T_1}{T+T_1}\left(C_{0_i}(1 - P_{fa}(\mathbf{w},\lambda))P(H_0) + C_{1_i}(1 - P_d(\mathbf{w},\lambda))P(H_1)\right) \tag{5.9}$$

where T and T_1 are the sensing and the transmission times of the ith SU, C_{0_i} and C_{1_i} are the normalized capacities of the PU channel when used by the ith SU under the hypothesis H_0 and H_1 and $P_d(\mathbf{w},\lambda) = 1 - P_{md}(\mathbf{w},\lambda)$ is the probability of correct detection at the FC. In the above expression, the first term inside the bracket refers to the SU throughput when the PU is absent while the second term refers to the SU throughput when it is present. The normalized channel capacities are given as $C_{0_i} = \log_2(1+|h_i|^2\gamma_{s_{H_0}})$ and $C_{1_i} = \log_2(1+|h_i|^2\gamma_{s_{H_1}})$, where h_i is the channel coefficient of the ith SU transmitter receiver link and $\gamma_{s_{H_0}}$ and $\gamma_{s_{H_1}}$ are the corresponding SINRs under H_0 and H_1 given as $\gamma_{s_{H_0}} = \frac{\gamma_s}{|h_{e_i}|^2\gamma_e+1}$ and $\gamma_{s_{H_1}} = \frac{\gamma_s}{|h_{p_i}|^2\gamma_p+|h_{e_i}|^2\gamma_e+1}$, γ_s is the transmit power of the ith SU transmitter and $P_d(\mathbf{w},\lambda)$. Since it is known that, $P(H_0) >> P(H_1)$, $C_{0_i} >> C_{1_i}$ and $1 - P_{fa}(\mathbf{w},\lambda) > 1 - P_d(\mathbf{w},\lambda)$,

TH-1605_10610214

the throughput of the ith SU is approximated as

$$G_i(\mathbf{w}, \lambda) \simeq \frac{T_1}{T + T_1} C_{0_i}(1 - P_{fa}(\mathbf{w}, \lambda))P(H_0). \tag{5.10}$$

5.3.2.3 Effective Interference to the PU ($I_{eff}(\mathbf{w}, \lambda)$)

The interference is caused to the PU by the SUs and the PUEs. If the interference to the PU by the SU is $I_{SU}(\mathbf{w}, \lambda)$ and by the PUE is I_{PUE}, the total interference $I_t(\mathbf{w}, \lambda)$ to the PU is written as

$$I_t(\mathbf{w}, \lambda) = I_{SU}(\mathbf{w}, \lambda) + I_{PUE} \tag{5.11}$$

where

$$\begin{aligned} I_{SU}(\mathbf{w}, \lambda) &= \gamma_s |h_{i_p}|^2 P_{md}(\mathbf{w}, \lambda) \times P(H_1), \\ I_{PUE} &= \gamma_e |h_{e_p}|^2 \times P(H_1) \end{aligned} \tag{5.12}$$

γ_s is the transmission power of an SU, γ_e is as defined earlier, h_{i_p} is the channel gain of ith SU with the PU, and h_{e_p} of PUE with the PU. It can be seen that I_{PUE} is not a function of $P_{md}(\mathbf{w}, \lambda)$. It will be seen further that all the evaluations in this work are concerned only with $\mathbf{w}$ and λ. Secondly, the intention of the PUE is to mislead only the SUs. Hence, we assume that it has beamforming capability to direct its signals only towards the SUs and does not cause a significant interference to the PU. Therefore, the effective interference to the PU is obtained as

$$I_{eff}(\mathbf{w}, \lambda) \approx I_{SU}(\mathbf{w}, \lambda). \tag{5.13}$$

I_{eff} is not a function of I_{PUE}. However, I_{SU} is affected by the PUE, since $P_{md}(\mathbf{w}, \lambda)$ is an increasing function of $|h_{e_i}|^2 \gamma_e$ in (5.8). Hence, the effect of PUE on I_{SU} also appears in I_{eff}.

5.4 Maximization of the SU Throughput under PUEAs

As mentioned earlier, our objective is to maximize $G_i(\mathbf{w}, \lambda)$ in a CSS facing the PUEAs. However, maximizing G_i can increase I_{eff}. We explore the possible ways to maximize G_i and explain how its maximization can increase I_{eff} as follows: In (5.10), it can be seen that G_i depends on T_1, C_{0_i}, $P_{fa}(\mathbf{w}, \lambda)$, and $P(H_0)$. The maximization of G_i can be achieved by the following ways:

(i) Increasing $P(H_0)$, T_1, and C_{0_i}:

- $P(H_0)$ is decided by the frequency of the arrival of the PU. It cannot be controlled by

TH-1605_10610214

external factors.

- T_1 depends on the periodic sensing mechanism and its optimization has been an important subject of research. In the absence of PUE, it has been optimized in [129] for maximizing the SU throughput. In the presence of the PUE, it has been optimized in the form of number of samples over T for minimizing the total error in [58]. Note that for one time frame $(T_1 + T)$ is a constant. Hence, optimizing T essentially means optimizing T_1. The problem of optimizing T or T_1 for maximizing the SU throughput in the presence of the PUE has so far not been investigated to the best of our knowledge. However, in the present work, our aim is only to design a weighted CSS for maximizing the SU throughput. Hence, the optimization of T is out of the scope of our present work.
- The third factor affecting G_i is C_{0_i} which depends on $|h_i|^2\gamma_{s_{H_0}}$, where $\gamma_{s_{H_0}} = \frac{\gamma_s}{|h_{e_i}|^2\gamma_e+1}$. It can be seen that G_i can be increased by increasing γ_s. However, the magnitude of γ_s cannot be increased beyond a certain value since there are hardware constraints. From (5.13), it can be seen that increasing γ_s increases I_{SU} and I_{eff}.

(ii) Decreasing P_{fa}: It can be seen in (5.10) P_{fa} and G_i vary opposite to each other. Therefore, minimizing P_{fa} will maximize G_i. The receiver operating characteristics (ROC) curves show that P_{fa} also varies opposite to P_{md} [34]. On decreasing P_{fa}, P_{md} increases. Hence, decreasing P_{fa} will also increase I_{eff}.

It can be concluded from the above analysis that maximizing G_i increases I_{eff}. Hence, the maximization of $G_i(\mathbf{w}, \lambda)$ cannot be carried out without putting a constraint on $I_{eff}(\mathbf{w}, \lambda)$. To ensure sufficient protection to the PU, we formulate an optimization problem as

$$\begin{aligned} &\text{maximize} \quad G_i(\mathbf{w}, \lambda) \\ &\mathbf{w} \in \mathbb{R}_+ \\ &\text{subject to} \quad I_{eff}(\mathbf{w}, \lambda) \leq \widehat{I_{eff}}, \end{aligned} \tag{5.14}$$

where, $\widehat{I_{eff}}$ is the bound on $I_{eff}(\mathbf{w}, \lambda)$ and $\mathbb{R}_+$ represents the set of positive real numbers. In this chapter, we will focus only on P_{fa} for maximizing G_i. The reasons are as follows:

P_{fa} is more crucial for the maximization of G_i : The PUEAs damage the SU throughput in the form of interruptions in the SU network operation. These interruptions appear in the form of P_{fa}. The effects of PUE on P_{fa} and P_{md} can also be seen in (5.7) and (5.8).

TH-1605_10610214

Designing weighted CSS : Our aim in this chapter is to design a weighted CSS for SU throughput maximization while constraining interference to the PU. It can be seen in (5.10) and (5.11) that the only terms effective with respect to $\mathbf{w}$ and λ, are $P_{fa}(\mathbf{w}, \lambda)$ and $P_{md}(\mathbf{w}, \lambda)$.

Hence, our objective reduces to address the problem in (5.14) through P_{fa} and P_{md}. The problem in (5.14) reduces to

$$\begin{aligned} &\text{minimize} \quad P_{fa}(\mathbf{w}, \lambda) \\ &\mathbf{w} \in \mathbb{R}_+ \\ &\text{subject to } P_{md}(\mathbf{w}, \lambda) \leq \widehat{P_{md}}. \end{aligned} \tag{5.15}$$

where $\widehat{P_{md}}$ is the bound on P_{md} corresponding to $\widehat{I_{eff}}$. The bound $\widehat{I_{eff}}$ will involve various factors present in the expression for I_{eff} in (5.13). Hence, the calculation of $\widehat{P_{md}}$ might involve some more analysis. As of now for the purpose of evaluation, we consider $\widehat{P_{md}}$ only a theoretical value which corresponds to $\widehat{I_{eff}}$. For avoiding interference to the PU, a general upper bound on P_{md} is 0.2 [173]. For any detection system, the ROC curves show that P_{md} and P_{fa} vary opposite to each other [34]. On reducing P_{fa}, P_{md} increases. Suppose, for the optimal weight vector $\mathbf{w}^*$, λ_0 is the value of the threshold when the constraint in (5.15) is $P_{md}(\mathbf{w}^*, \lambda_0) = \widehat{P_{md}}$. If we chose a threshold $\lambda < \lambda_0$, then $P_{md}(\mathbf{w}^*, \lambda) < \widehat{P_{md}}$ and $P_{fa}(\mathbf{w}^*, \lambda) > P_{fa}(\mathbf{w}^*, \lambda_0)$. On the other hand, a $\lambda > \lambda_0$ will violate the constraint by making $P_{md}(\mathbf{w}^*, \lambda) > \widehat{P_{md}}$. Hence, the problem in (5.15) is justified only for an equality constraint as

$$\begin{aligned} &\text{minimize} \quad P_{fa}(\mathbf{w}, \lambda) \\ &\mathbf{w} \in \mathbb{R}_+ \\ &\text{subject to } P_{md}(\mathbf{w}, \lambda) = \widehat{P_{md}}. \end{aligned} \tag{5.16}$$

This is applicable as a general case for any weight vector $\mathbf{w}$. Now, λ in the constraint term of (5.16) can be written as a function of $\widehat{P}_{md}$ by using (5.8) as

$$\begin{aligned} \lambda(\mathbf{w}, \widehat{P_{md}}) = Q^{-1}(1 - \widehat{P_{md}}) \sqrt{\frac{1}{M} \sum_{i=1}^{N} w_i^2 \left(2 \frac{|h_{p_i}|^2 \gamma_p}{|h_{e_i}|^2 \gamma_e + 1} + 1\right) (|h_{e_i}|^2 \gamma_e + 1)^2} + \\ \sum_{i=1}^{N} w_i \left(\frac{|h_{p_i}|^2 \gamma_p}{|h_{e_i}|^2 \gamma_e + 1} + 1\right) (|h_{e_i}|^2 \gamma_e + 1). \end{aligned} \tag{5.17}$$

Substituting λ in (5.17) into the cost function of (5.16) transforms the optimization problem in (5.16) into an unconstrained problem as

TH-1605_10610214

$$\begin{aligned} &\text{minimize } P_{fa}(\mathbf{w}, \widehat{P_{md}}) \\ &\mathbf{w} \in \mathbb{R}_+ \end{aligned} \tag{5.18}$$

Elaborating (5.18) gives

$$\begin{aligned} &\text{minimize } Q\left(\frac{Q^{-1}(1-\widehat{P_{md}})\sqrt{\frac{1}{M}\sum_{i=1}^{N} w_i^2\left(2\frac{|h_{p_i}|^2\gamma_p}{|h_{e_i}|^2\gamma_e+1}+1\right)(|h_{e_i}|^2\gamma_e+1)^2}+\sum_{i=1}^{N} w_i|h_{p_i}|^2\gamma_p}{\sqrt{\frac{1}{M}\sum_{i=1}^{N} w_i^2(1+2|h_{e_i}|^2\gamma_e)^2}}\right). \\ &\mathbf{w} \in \mathbb{R}_+ \end{aligned} \tag{5.19}$$

5.5 Obtaining Optimal Weights for Performing CSS

The unconstrained non-linear optimization problem in (5.19) can be solved with two traditional approaches: the gradient based and the direct search methods. The direct search methods have become popular in solving complex optimization problems. In [174], it was observed that for small scale problems, the NMA [170] converges relatively faster and is easily implementable compared to the evolutionary computation or gradient based algorithms. Another significant characteristic of the NMA is its ability to to bring the approximate results even when it fails to converge. These features make it one of the most preferable algorithms for engineering applications [175], [176], [177]. Therefore, we apply the NMA to solve the problem in (5.19).

The first step in the application of the NMA is forming the working simplex of the objective function. The working simplex is formed with $K+1$ vertices $\mathbf{w}_0, \mathbf{w}_1, \ldots, \mathbf{w}_K$. $\mathbf{w}_0$ is the initial base point and vertex $\mathbf{w}_i$ $\forall i \in \{1, \ldots, K\}$ is found as follows [178]:

$$\mathbf{w}_i = \mathbf{w}_0 + cu_i + \sum_{j=1, j\neq i}^{K} dv_j, \tag{5.20}$$

where $c = \frac{s}{K\sqrt{2}}\left(\sqrt{K+1}+K-1\right)$, $d = \frac{s}{K\sqrt{2}}\left(\sqrt{K+1}-1\right)$, s is the size of the simplex (for example area of the simplex for the 2 dimensional case, volume for the 3 dimensional case and hyper-volume for higher dimensional cases), and u_i and v_j represent the unit vectors in the ith and jth directions respectively.

TH-1605_10610214

5.5.1 Calculation of $\mathbf{w}_0$

The choice of $\mathbf{w}_0$ is crucial for the performance of the algorithm. An arbitrary choice of $\mathbf{w}_0$ is less likely to cause the algorithm to converge to $\mathbf{w}^*$. A $\mathbf{w}_0$ nearer to $\mathbf{w}^*$ results into a lower algorithmic execution time. In this chapter, we carry out investigations with three choices of $\mathbf{w}_0$:

(i) **Arbitrary point**: $\mathbf{w}_0$ will be chosen randomly. We denote it as $\mathbf{w}_{0r}$.

(ii) **Solution of the existing SU throughput maximization technique**: In [129], efficient throughput maximization schemes were proposed for single sensing and CSS systems without PUEs. The weight vector obtained for combining the data at the FC were obtained as

$$\mathbf{w}_{0e} = \left[\frac{|h_{p_1}|^2}{\sqrt{\sum_{i=1}^{N} |h_{p_i}|^4}}, \frac{|h_{p_2}|^2}{\sqrt{\sum_{i=1}^{N} |h_{p_i}|^4}}, ..., \frac{|h_{p_N}|^2}{\sqrt{\sum_{i=1}^{N} |h_{p_i}|^4}} \right]. \tag{5.21}$$

These weights perform excellently for the maximization of the SU throughput in the absence of PUEAs. We denote it as $\mathbf{w}_{0_e}$ where subscript 'e' represents existing.

(iii) **A proposal for initial weight vector**:

In the presence of the PUE, $\mathbf{w}_0$ needs to be redesigned. In this regard, we aim to exploit the PU to SU and the PUE to SU channels gains. We start with investigating the individual received energies of the SU, represented as

$$E_i = \begin{cases} \sum_{m=1}^{M} |\sqrt{\gamma_p} h_{p_i}(m) x_p(m) + \sqrt{\gamma_e} h_{e_i}(m) x_e(m) + u_i(m)|^2 & : H_1 \\ \sum_{m=1}^{M} |\sqrt{\gamma_e} h_{e_i}(m) x_e(m) + u_i(m)|^2 & : H_0. \end{cases} \tag{5.22}$$

The individual energies are fused at the FC to form the decision about the spectrum occupancy as shown in (5.3). For clarity, (5.3) is rewritten in the expanded form as,

$$E = w_1 E_1 + w_2 E_2 + ... + w_N E_N. \tag{5.23}$$

It can be seen in (5.22) that the energy calculated by each SU depends on its path with respect to the PU (h_{p_i}) and the PUE (h_{e_i}). Different SUs may have good or bad paths with respect to the PU and the PUE depending upon their locations. For instance, the ith SU may have a good h_{p_i} but

TH-1605_10610214

a bad h_{e_i}, whereas jth SU may just have the opposites. Our objective is to use the estimated channel gains to appropriately scale the energy values of the SUs at the FC.

Under hypothesis H_0, $y_i(m)$ in (5.1) consists of the PUE signal and the noise. It can be concluded from (5.5) that a decrement in the PUE signal power decreases P_{fa}. In (5.23), each SU energy data has been scaled by some weight factor and added at the FC. Intuitively, a low weight value must be given to the energy of the SU which is at good channel conditions with the PUE. Mathematically, the received signal energy needs to be multiplied by a factor which deemphasizes it if it is from a good PUE-SU path. This will decrease the P_{fa}, since under H_0, only the PUE signal and noise are present. Let $\widetilde{h_{p_i}} = \frac{|h_{p_i}|^2}{\sqrt{\sum_{i=1}^{N} |h_{p_i}|^4}}$ and $\widetilde{h_{e_i}} = \frac{|h_{e_i}|^2}{\sqrt{\sum_{i=1}^{N} |h_{e_i}|^4}}$ be the normalized estimated channel gains of the PU-SU and the PUE-SU paths available at the FC. We propose to weigh the ith source's energy as

$$w_{0_i} \propto \frac{1}{\widetilde{h_{e_i}}}. \tag{5.24}$$

On the other hand, from (5.6), giving high weight value to the energy data of SUs having good channel condition with the PU will ensure the decrease in P_{md}. Therefore, we can consider

$$w_{0_i} \propto \widetilde{h_{p_i}}. \tag{5.25}$$

Combining (5.24) and (5.25), we get

$$w_{0_i} \propto \frac{\widetilde{h_{p_i}}}{\widetilde{h_{e_i}}}, \tag{5.26}$$

so that,

$$w_{0_i} = K_1 \frac{\widetilde{h_{p_i}}}{\widetilde{h_{e_i}}}, \tag{5.27}$$

where K_1 is the constant of proportionality. Without the loss of generality, we keep $K_1 = 1$. The proposed initial base point in this case denoted by the vector $\mathbf{w}_{0p}$ can be obtained as,

$$\mathbf{w}_{0p} = \left[\frac{\widetilde{h_{p_1}}}{\widetilde{h_{e_1}}}, \frac{\widetilde{h_{p_2}}}{\widetilde{h_{e_2}}}, \ldots, \frac{\widetilde{h_{p_N}}}{\widetilde{h_{e_N}}} \right]. \tag{5.28}$$

It can be seen that $\mathbf{w}_{0p}$ exploits the virtue and the adversity of the SU channel conditions with the PU and PUE. At every sensing instant, each SU reports the calculated energy value to the FC. It is assumed that the reporting channels are error free. Note that the channel estimation errors have also been ignored here.

TH-1605_10610214

Let us first compare the performances of $\mathbf{w}_{0p}$ and $\mathbf{w}_{0e}$ by directly using them as weights for weighted CSS. Substituting $\mathbf{w}_{0p}$ into (5.19) gives P_{fa} as

$$P_{fa}(\mathbf{w}_0, \widehat{P_{md}}) = Q\left(\frac{Q^{-1}(1-\widetilde{P_{md}})\sqrt{\frac{1}{M}\sum_{i=1}^{N}\frac{\widetilde{h_{p_i}}^2}{\widetilde{h_{e_i}}^2}\left(2\frac{|h_{p_i}|^2\gamma_p}{|h_{e_i}|^2\gamma_e+1}+1\right)\left(|h_{e_i}|^2\gamma_e+1\right)^2} + \sum_{i=1}^{N}\frac{\widetilde{h_{p_i}}}{\widetilde{h_{e_i}}}|h_{p_i}|^2\gamma_p}{\sqrt{\frac{1}{M}\sum_{i=1}^{N}\frac{\widetilde{h_{p_i}}^2}{\widetilde{h_{e_i}}^2}(1+2|h_{e_i}|^2\gamma_e)^2}} \right), \tag{5.29}$$

which is further substituted in (5.10) to give $G_i(\mathbf{w}, \lambda)$.

Figures 5.3-5.5 have been plotted for checking the suitability of $\mathbf{w}_{0p}$. These evaluations use the average SU throughput and average interference to the PU values (as shown ahead in (5.32) and (5.33)). The plots show the variation of the average SU throughput over the average interference values to the PU, the received PU SNRs at the ith SU, and the number of cooperating SUs. The comparison has been made for the initial weight vector $\mathbf{w}_{0e}$ in (5.21) and the proposed weight vector $\mathbf{w}_{0p}$ in (5.28). It can be seen that performing CSS with $\mathbf{w}_{0p}$ in (5.28) performs better than when performed with $\mathbf{w}_{0e}$ in (5.21).

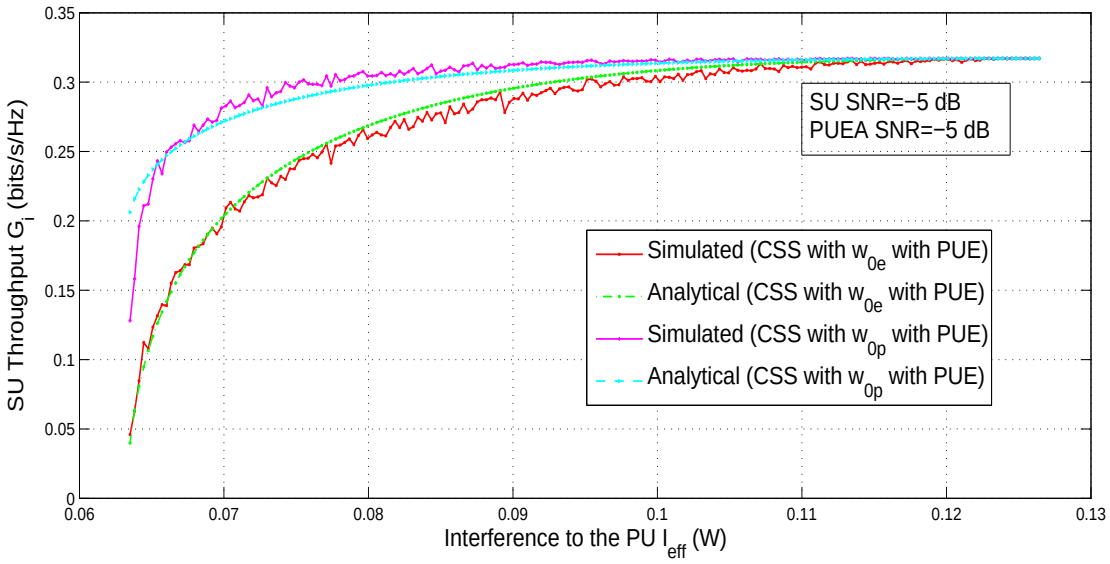

Figure 5.3: Plot of the $G_i(\mathbf{w}, \lambda)$ vs $I_{eff}(\mathbf{w}, \lambda)$

5.5.2 Obtaining w∗

After obtaining $\mathbf{w}_0$, the working simplex is formed with the expression in (5.20). The values of $P_{fa}(\mathbf{w}, \widehat{P_{md}})$ in (5.29) are compared at the points $\mathbf{w}_0, \mathbf{w}_1, \ldots, \mathbf{w}_K$. Then, these values are sorted in

TH-1605_10610214

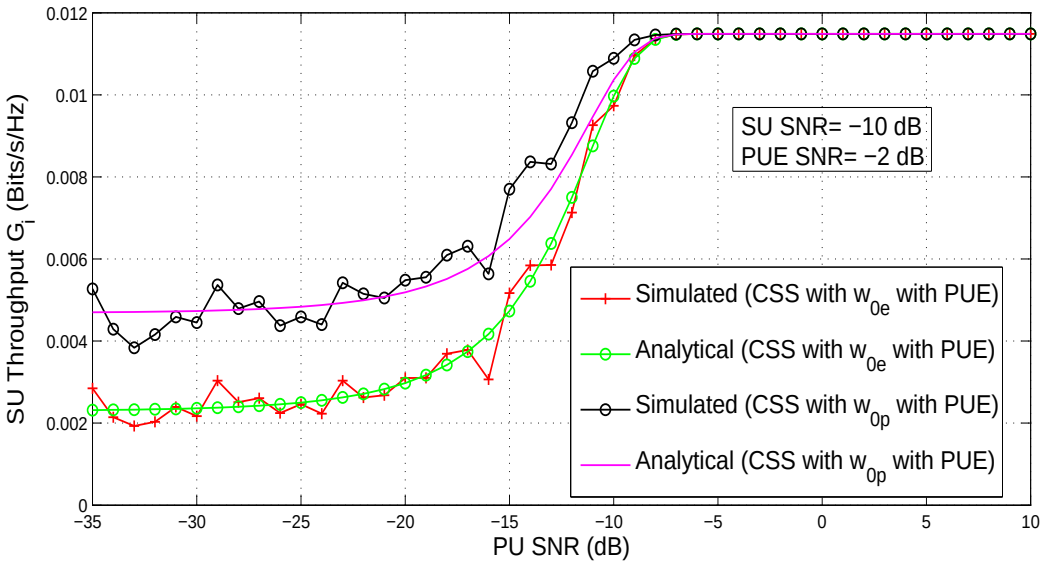

Figure 5.4: Plot of the $G_i(\mathbf{w}, \lambda)$ vs PU SNR (at $I_{eff} = 0.0695W$)

ascending order. If $\mathbf{w}_{(0)}, \mathbf{w}_{(1)}, ..., \mathbf{w}_{(K)}$ are the vertices at which $P_{fa}(\mathbf{w}, \widehat{P_{md}})$ comes in ascending order, then

$$P_{fa}(\mathbf{w}_{(0)}, \widehat{P_{md}}) < P_{fa}(\mathbf{w}_{(1)}, \widehat{P_{md}}) < ... < P_{fa}(\mathbf{w}_{(K)}, \widehat{P_{md}}). \tag{5.30}$$

In the next step, the points $\mathbf{w}_{(0)}, \mathbf{w}_{(K-1)}$, and $\mathbf{w}_{(K)}$ are chosen. Since $P_{fa}(\mathbf{w}, \widehat{P_{md}})$ has the lowest value at the point $\mathbf{w}_{(0)}$, this point is the best available vertex and is denoted as $\mathbf{w}_B$. Similarly, $\mathbf{w}_{(K-1)}$ and $\mathbf{w}_{(K)}$ are the second worst and the worst vertices and denoted as $\mathbf{w}_S$ and $\mathbf{w}_W$. The working simplex is shown in the Figure 5.6. All the vertices except $\mathbf{w}_B$, $\mathbf{w}_S$ and $\mathbf{w}_W$ lie on the line adjoining $\mathbf{w}_S$ and $\mathbf{w}_B$.

The next step is the calculation of the centroid '**c**' of all the points except $\mathbf{w}_W$. c is evaluated as

$$\mathbf{c} = \frac{1}{K} \sum_{i=0, i \neq W}^{K} \mathbf{w}_i. \tag{5.31}$$

Now, with each iteration, the simplex moves towards $\mathbf{w}*$. The iterations involve the following operations:

(i) Reflection: This operation gives $\mathbf{w}_r$ which is in the opposite face to $\mathbf{w}_W$. Since, $P_{fa}(\mathbf{w}, \widehat{P_{md}})$ has the highest value at $\mathbf{w}_W$, it expectedly has the lowest value at $\mathbf{w}_r$. The reflection point is found as, $\mathbf{w}_r = (1 + \alpha)\mathbf{c} - \alpha \mathbf{w}_W$. If $P_{fa}(\mathbf{w}_B, \widehat{P_{md}}) \leq P_{fa}(\mathbf{w}_r, \widehat{P_{md}}) < P_{fa}(\mathbf{w}_S, \widehat{P_{md}})$, $\mathbf{w}_W$ is replaced with $\mathbf{w}_r$ and the iteration is terminated. Here, $\alpha = \frac{D_{\mathbf{w}_r c}}{D_{\mathbf{w}_W c}}$ where D_{xy} represents the distance

TH-1605_10610214

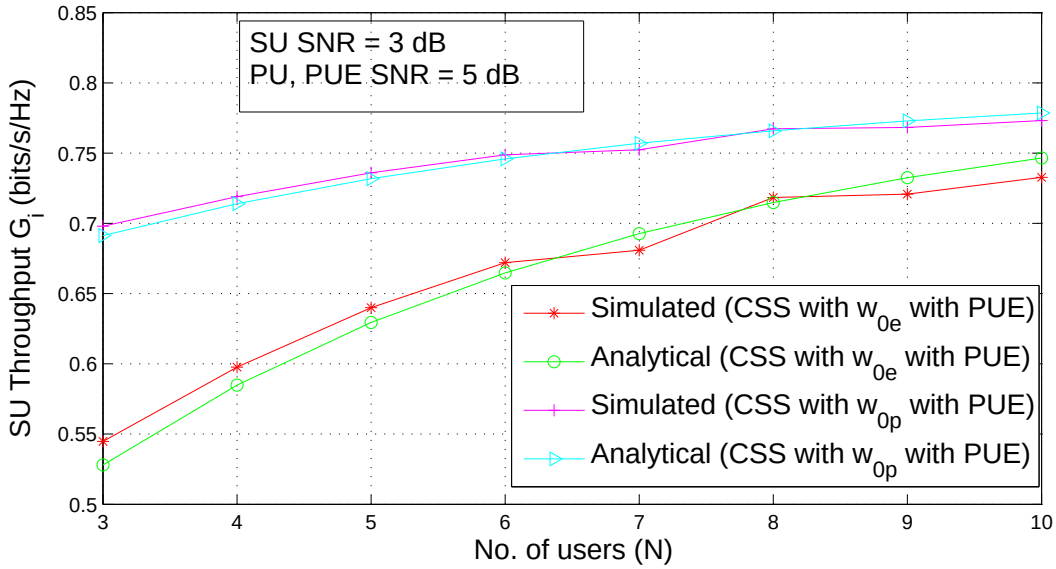

Figure 5.5: Plot of the $G_i(\mathbf{w}, \lambda)$ vs N ($I_{eff} = 0.0758$)

between points x and y.

(ii) Expansion: If the reflection point gives a new minimum as $P_{fa}(\mathbf{w}_r, \widehat{P_{md}}) < P_{fa}(\mathbf{w}_B, \widehat{P_{md}})$, then, the expansion point is calculated with the relation, $\mathbf{w}_e = \omega \mathbf{w}_r + (1-\omega)\mathbf{c}$. If $P_{fa}(\mathbf{w}_e, \widehat{P_{md}}) < P_{fa}(\mathbf{w}_B, \widehat{P_{md}})$, $\mathbf{w}_W$ is replaced by $\mathbf{w}_e$. If the case is opposite, $\mathbf{w}_W$ is replaced by $\mathbf{w}_r$ and the reflection process is started again. Here, $\omega = \frac{D_{\mathbf{w}_e c}}{D_{\mathbf{w}_r c}}$.

(iii) Contraction: If $P_{fa}(\mathbf{w}_r, \widehat{P_{md}}) < P_{fa}(\mathbf{w}_i, \widehat{P_{md}})$, where, $i \in \{0, \ldots, K\}, i \neq W$ and $P_{fa}(\mathbf{w}_r, \widehat{P_{md}}) < P_{fa}(\mathbf{w}_W, \widehat{P_{md}})$, the contraction point needs to be calculated. The contraction point may lie inside or outside depending on the following conditions:

- If $P_{fa}(\mathbf{w}_e, \widehat{P_{md}}) < P_{fa}(\mathbf{w}_r, \widehat{P_{md}}) < P_{fa}(\mathbf{w}_B, \widehat{P_{md}})$, the contraction point is found as, $\mathbf{w}_{c_{out}} = \mathbf{c} + \beta(\mathbf{w}_r - \mathbf{c})$.
- If $P_{fa}(\mathbf{w}_r, \widehat{P_{md}}) > P_{fa}(\mathbf{w}_W, \widehat{P_{md}})$, the contraction point lies inside and is given by the equation, $\mathbf{w}_{c_{in}} = \mathbf{c} + \beta(\mathbf{w}_h - \mathbf{c})$.

Here, $\beta = \frac{D_{\mathbf{w}_e c}}{D_{\mathbf{w}_W c}}$.

(iv) Shrink: If the contraction conditions fail, each vertex except $P_{fa}(\mathbf{w}_B, \widehat{P_{md}})$ is replaced by the point $P_{fa}(\mathbf{w}_i, \widehat{P_{md}}) = \delta P_{fa}(\mathbf{w}_i, \widehat{P_{md}}) + (1-\delta) P_{fa}(\mathbf{w}_B, \widehat{P_{md}})$. The simplex is said to shrink by the parameter δ.

TH-1605_10610214

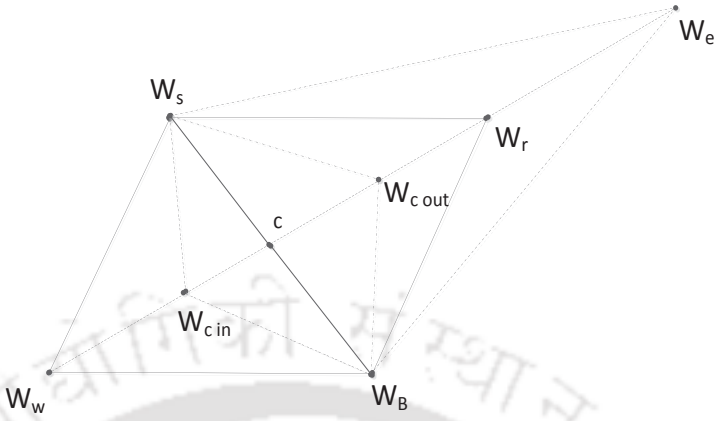

Figure 5.6: Working simplex with reflection, contraction and expansion points

A fixed value of 0.5 is recommended for the shrink coefficient (δ) in [170].

The last stage is the termination of the iterative process, and is decided by the following conditions:

(i) *The domain termination test*: This termination criterion depends on the difference in the vertices with largest and the smallest function values.

(ii) *The function termination test*: The decision of this criterion is based on the minimum difference between the smallest and the largest function values at the vertices of the simplex.

(iii) *Maximum iterations and function evaluations test*: At the beginning of the algorithm, the maximum number of iterations for the algorithm to converge has to be specified. If the number of iterations or the number of function evaluations at an iteration exceeds the specified maximum value, the algorithm stops and the final value obtained is to be taken as the optimal value.

We have showed the overall operation of our mechanism in the Algorithm 5.3.

5.5.3 Average Throughput and Interference

5.5.3.1 Average Throughput

The average throughput can be calculated as

$$E[G(\mathbf{w},\lambda)] = \int_0^\infty \int_0^\infty \int_0^\infty G(\mathbf{w},\lambda) f(h_i) f(h_{p_i}) f(h_{e_i}) dh_i dh_{p_i} dh_{e_i}, \tag{5.32}$$

where f(.) denotes the pdf, the channel gains h_{p_i}, h_{e_i} and h_i are assumed to be independent and Rayleigh distributed.

TH-1605_10610214

Algorithm 5.3 Designing CSS for defending the damage of PUEAs on SU throughput

Input N, $\widehat{P_{md}}$, $P(H_0)$, $P(H_1)$, Maximum Iterations Itr, Number of sensing time frames N_S,Index values I_K, α, β, ω, and δ
for $i \leftarrow 1 : N_S$ **do**
  e : incoming energy data set
  Calculate $\mathbf{w_{0_p}}$ from (5.28)
  Calculate c from (5.31)
  $P_{fa} \leftarrow P_{fa}(\mathbf{w}, \widehat{P}_{md})$
  $P_{fa}(I_K) = sort(P_{fa})$
  $\mathbf{w_{(K)}} = \mathbf{w}(P_{fa}(I_K))$ {Weights corresponding to the sorted P_{fa} values}
  Chose $\mathbf{w}_{(0)}, \mathbf{w}_{(K-1)}$, and $\mathbf{w}_{(K)}$
  Form simplex with (5.20)
  Motion of simplex towards $\mathbf{w}^*$ shown in the following loop
  for $j \leftarrow Itr$ **do**
    Perform reflection, expansion, contraction,shrink operations as mentioned in Section 5.5.2
    Test for the termination criteria based on domain, function, maximum iterations, and maximum function evaluation
    If algorithm terminated, perform $E = \sum_{i=1}^{N} w_i^* E_i$ {$\mathbf{w}^*$ is the numerical optimal weight vector generated by the simplex}
  end for
end for

5.5.3.2 Average Interference

The average interference is calculated as

$$E[I_{eff}(\mathbf{w}, \lambda)] = \int_0^\infty \int_0^\infty \int_0^\infty \int_0^\infty A dh_{p_i} dh_{i_p} dh_{e_p} dh_{e_i} \tag{5.33}$$

where

$$A = I_{eff}(\mathbf{w}, \lambda) f(h_{e_i}) f(h_{p_i}) f(h_{e_p}) f(h_{i_p}) \tag{5.34}$$

and $h_{e_i}, h_{p_i}, h_{e_p}$ and h_{i_p} are assumed to be independent and Rayleigh distributed.

The Algorithm 5.3 generates numerical values of $\mathbf{w}^*$ at every iteration. In such a case, it is not possible to evaluate $E[G(\mathbf{w}, \lambda)]$ and $E[I_{eff}(\mathbf{w}, \lambda)]$ in closed forms, since it requires the analytical model of $\mathbf{w}^*$. Therefore, $E[G(\mathbf{w}, \lambda)]$ and $E[I_{eff}(\mathbf{w}, \lambda)]$ have been evaluated by Monte Carlo simulations with the experimentally generated numerical values of $\mathbf{w}^*$.

TH-1605_10610214

5.6 Experimental Results and Performance Evaluation

The PU signal is considered to be BPSK modulated with a bandwidth (BW) 1 MHz (data rate 1 Mbps). The sampling frequency for energy detection is taken twice the BW, that is $M = 2 \times 10^6$. The sensing time T is taken to be 1 ms. The number of samples per sensing interval are 5100. The characteristics of the PUE signal are considered similar to the PU signal.

The evaluations are based on the results derived in (5.17), (5.19) and (5.29). $P(H_0)$ and $P(H_1)$ are assumed to be known *a priori*, in a particular geographical area or in a given time span and are taken as 0.8 and 0.2. Since, a unit noise power has been considered in all the evaluations, the transmit powers of the PU, PUE or the SU equate their transmit SNRs $\gamma_p, \gamma_e,$ and γ_s respectively. The noise at the SU receivers is considered to be CSCG distributed. In the Figures 5.3 and 5.4, the number of cooperating SUs was taken as 5 and the total time $(T + T_1)$ as 100 ms.

An upper bound of 400 on the number of iterations has been considered for the application of the NMA. The maximum number of function evaluations allowed per iteration has been taken as 1000. The termination criteria for function and domain tests are kept as low as 10^{-14} and 10^{-12} so that the solver may not fail to recognize convergence.

5.6.1 Static Transmitters and Receivers

In the subsequent experiments, the performance assessment of different weighted CSS schemes has been carried out. Figure 5.7 shows the comparison of $G(\mathbf{w}, \lambda)$ and $I_{eff}(\mathbf{w}, \lambda)$ for large number of obstacles present on the PU-SU and the PUE-SU path. The presence of large number of obstacles result into severe fading on these paths and hence the absence of the line-of-sight (LoS) components. Hence, h_{p_i} and h_{e_i} are assumed to be Rayleigh distributed. Like before, we consider a path loss exponent of 2. The average received SNR at the SU from the PU is 5 dB while from the PUE is 20 dB. The transmit powers of the PU and PUE are kept at 25 dB. The comparisons have been made between the weighted CSS schemes with the weights obtained after applying the NMA using $\mathbf{w}_{0r}$, $\mathbf{w}_{0e}$ in (5.21) and the proposed $\mathbf{w}_{0p}$ in (5.28). The evaluations have been carried out with different values of SU transmit SNRs.

TH-1605_10610214

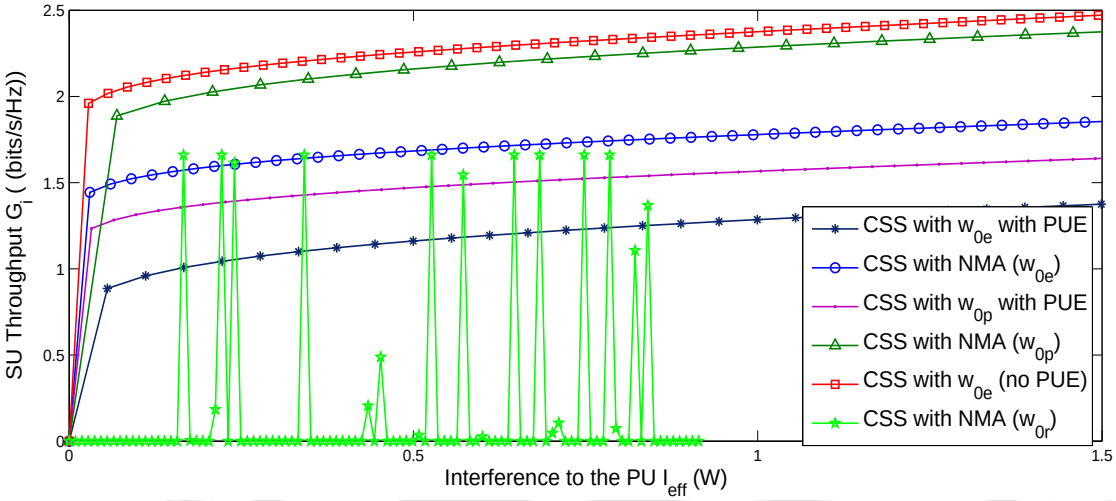

Figure 5.7: Plot of $G_i(\mathbf{w}, \lambda)$ vs $I_{eff}(\mathbf{w}, \lambda)$ when both PU-SU and PUE-SU channels are Rayleigh faded

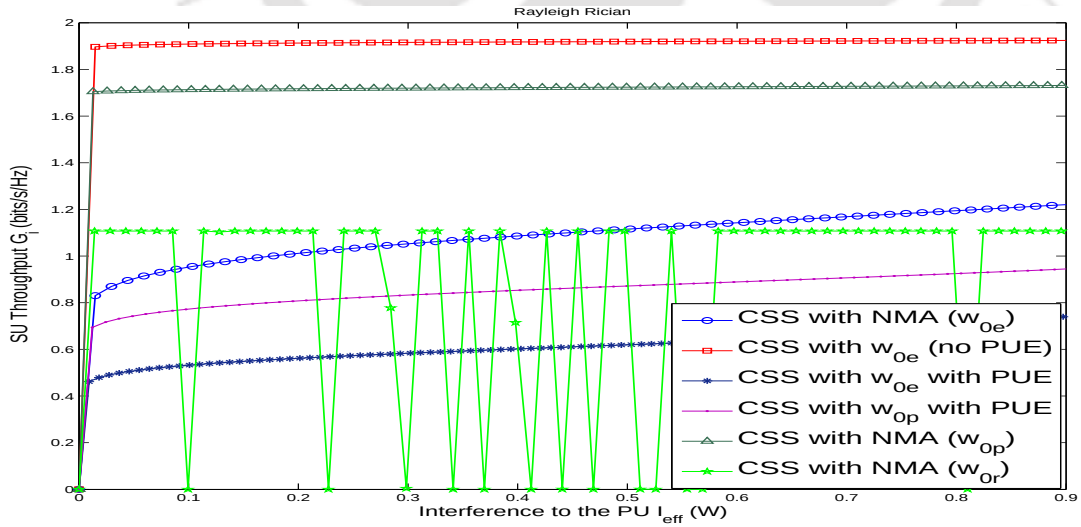

Figure 5.8: Plot of $G_i(\mathbf{w}, \lambda)$ vs $I_{eff}(\mathbf{w}, \lambda)$ when PU-SU and PUE-SU channels are Rayleigh and Rician faded respectively

TH-1605_10610214

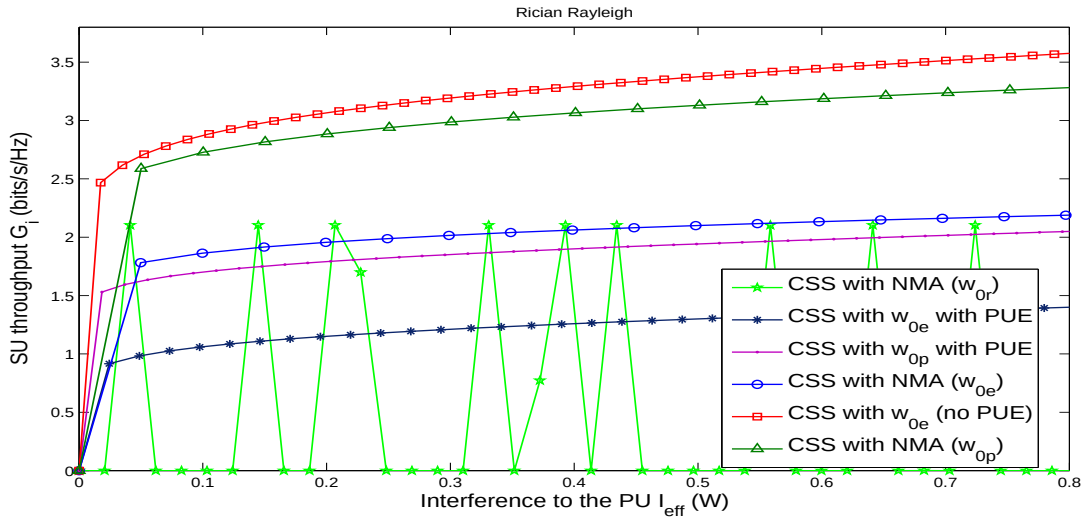

Figure 5.9: Plot of $G_i(\mathbf{w}, \lambda)$ vs $I_{eff}(\mathbf{w}, \lambda)$ when PU-SU and PUE-SU channels are Rician and Rayleigh faded respectively

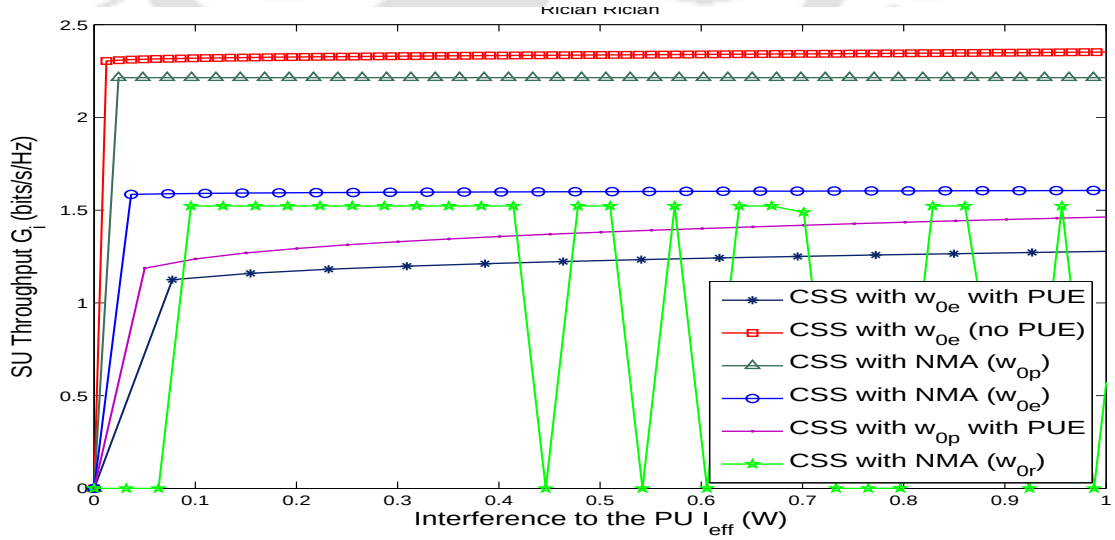

Figure 5.10: Plot of $G_i(\mathbf{w}, \lambda)$ vs $I_{eff}(\mathbf{w}, \lambda)$ when both PU-SU and PUE-SU channels are Rician faded

TH-1605_10610214

Therefore different ranges SU throughput values are observed in the evaluations. For completeness, CSS using $\mathbf{w}_{0e}$ and $\mathbf{w}_{0p}$ in (5.21) and (5.28) directly as weights has been performed to compare the improvement achieved by the NMA with the respective $\mathbf{w}_0$s. The performance of the CSS with $\mathbf{w}_{0e}$ in (5.21) as the combining weights in an honest CSS scenario (without PUE) has also been plotted. The performance in this case has been regarded as the ideal mark. All the evaluations are carried out by comparing the declination caused by the PUEAs in $G_i(\mathbf{w}, \lambda)$ with the ability of a scheme to bring it closer to the ideal mark. It can be seen that the NMA performed with a random $\mathbf{w}_{0r}$ gives highly non-convergent results. Thus, we see that for the particular system considered here, a random $\mathbf{w}_{0r}$ proves inefficient. It can be seen that the PUE is successful in severely damaging the weighted CSS performed with the $\mathbf{w}_{0e}$ in (5.21) as combining weights. However, applying the NMA with the same weight vector $\mathbf{w}_{0e}$ as the initial point brings a considerable improvement in the performance. In the next evaluation, the performance of the proposed initial point $\mathbf{w}_{0p}$ in (5.28) as the combining weights for CSS is seen to give better results than that for the case of (5.21). Similarly, the NMA applied with the $\mathbf{w}_{0p}$ in (5.28) as the initial base point shows a higher improvement than when applied with the $\mathbf{w}_{0e}$ in (5.21). The performance is the closest to the ideal mark when NMA is used with $\mathbf{w}_{0p}$ as the initial base point.

We extend our investigation in Figure 5.7 over more diverse scenarios by considering the presence of LoS components on the PU-SU and PUE-SU paths. LoS components are present when there are less number of obstacles on a path, and the transmitted signal is undergoing non-severe fading. The channel gains on such paths follow Rician distribution. We perform the simulations for the following cases:

Case 1: Severe fading on the PU-SU channel and non-severe fading on PUE-SU channel. h_{p_i} follows Rayleigh distribution and h_{e_i} follows Rician distribution.

Case 2: Non-severe fading on the PU-SU channel and severe fading on the PUE-SU channel. h_{p_i} follows Rician distribution and h_{e_i} follows Rayleigh distribution.

Case 3: Non-severe fading on both PU-SU and PUE-SU channels. h_{p_i} and h_{e_i} follow Rician distribution.

Figure 5.8 shows investigations for the Case 1. The environment between the PU and the ith SU is considered to have a large number of obstacles while the environment between the PUE and the ith

TH-1605_10610214

SU has been considered to have less obstacles.

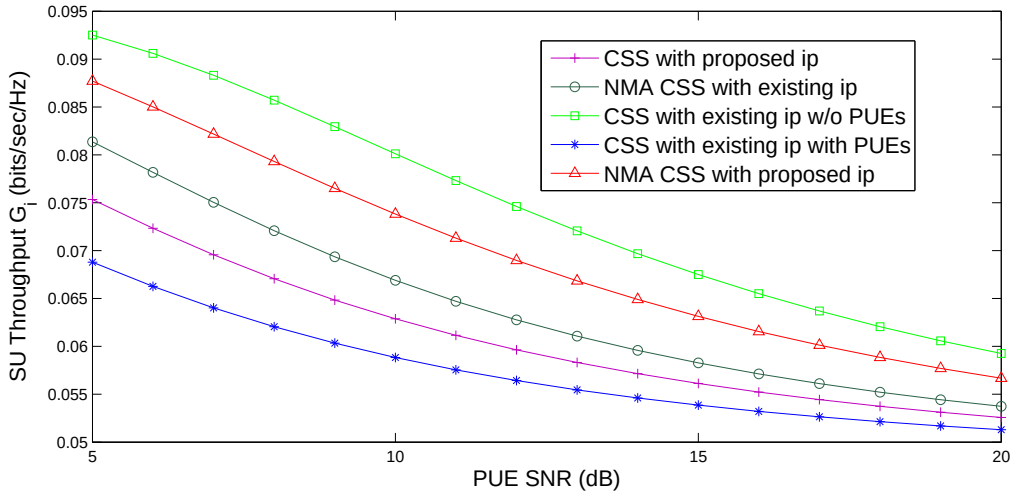

Figure 5.11: Plot of $G_i(\mathbf{w}, \lambda)$ vs PUE SNR at fixed interference ($P_{md} = 0.1$)

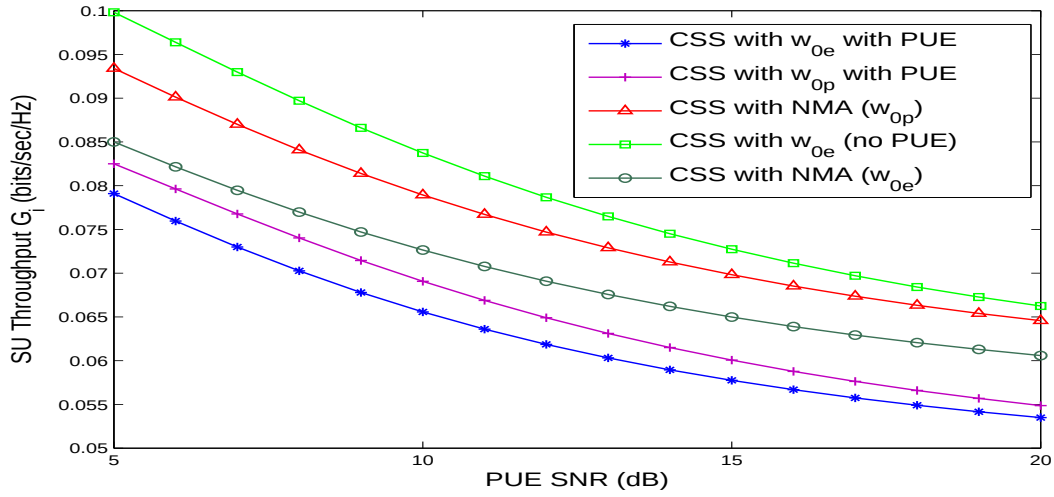

Figure 5.12: Plot of $G_i(\mathbf{w}, \lambda)$ vs PUE SNR at fixed interference ($P_{md} = 0.2$)

TH-1605_10610214

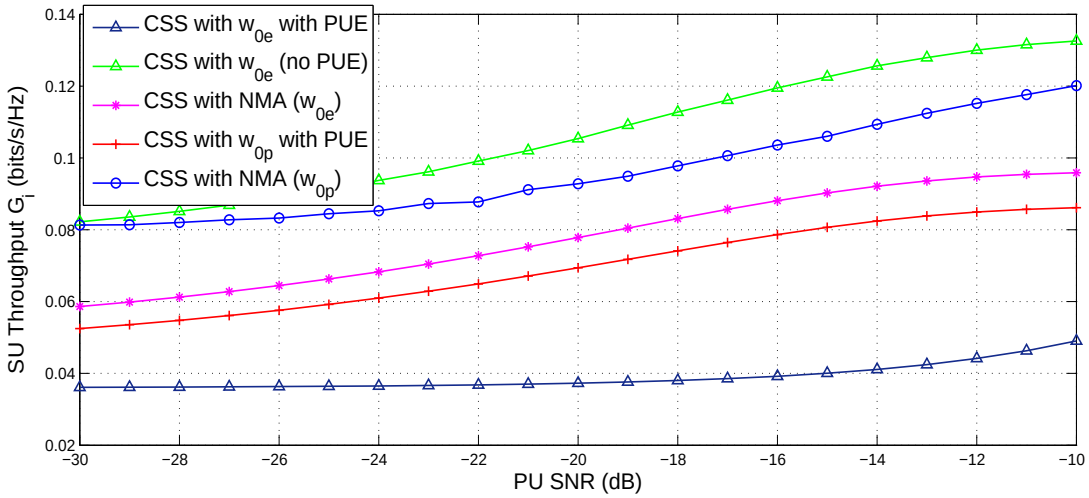

Figure 5.13: Plot of $G_i(\mathbf{w}, \lambda)$ vs PU SNR ($P_{md} = 0.1$)

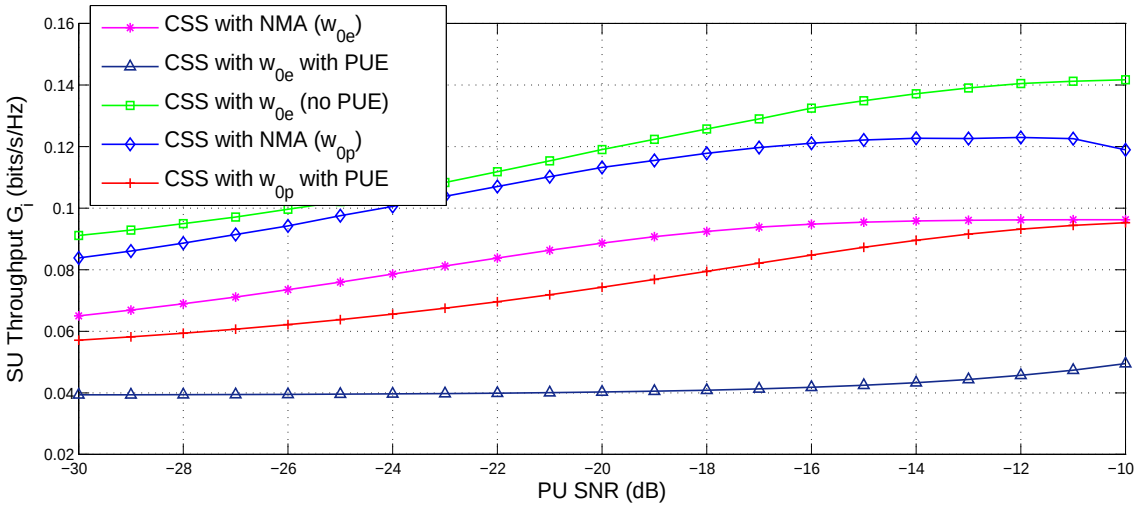

Figure 5.14: Plot of $G_i(\mathbf{w}, \lambda)$ vs PU SNR ($P_{md} = 0.2$)

TH-1605_10610214

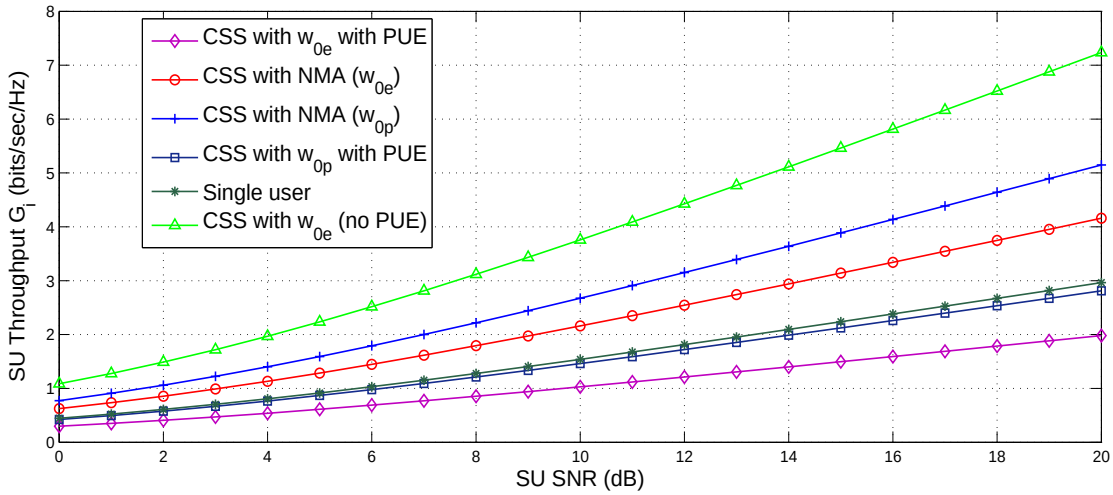

Figure 5.15: Plot of $G_i(\mathbf{w}, \lambda)$ vs SU SNR ($P_{md} = 0.1$)

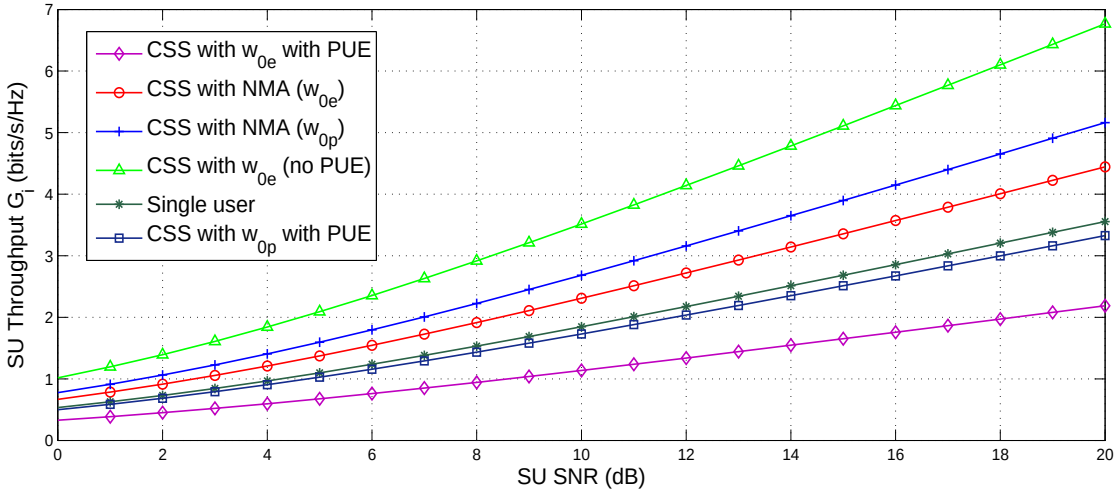

Figure 5.16: Plot of $G_i(\mathbf{w}, \lambda)$ vs SU SNR ($P_{md} = 0.2$)

TH-1605_10610214

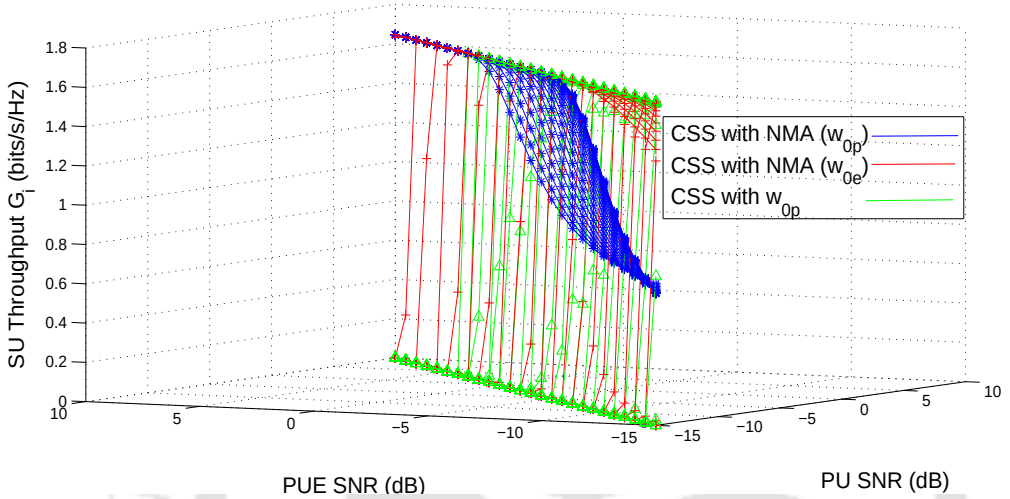

Figure 5.17: Plot of $G_i(\mathbf{w}, \lambda)$ vs PU SNR and PUE SNR moving away from each other

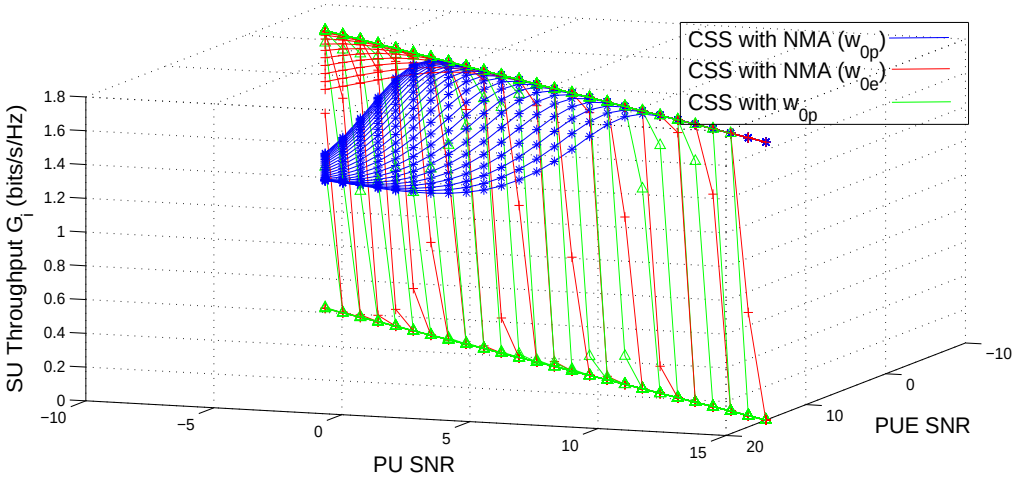

Figure 5.18: Plot of $G_i(\mathbf{w}, \lambda)$ vs PU SNR and PUE SNR moving towards each other

TH-1605_10610214

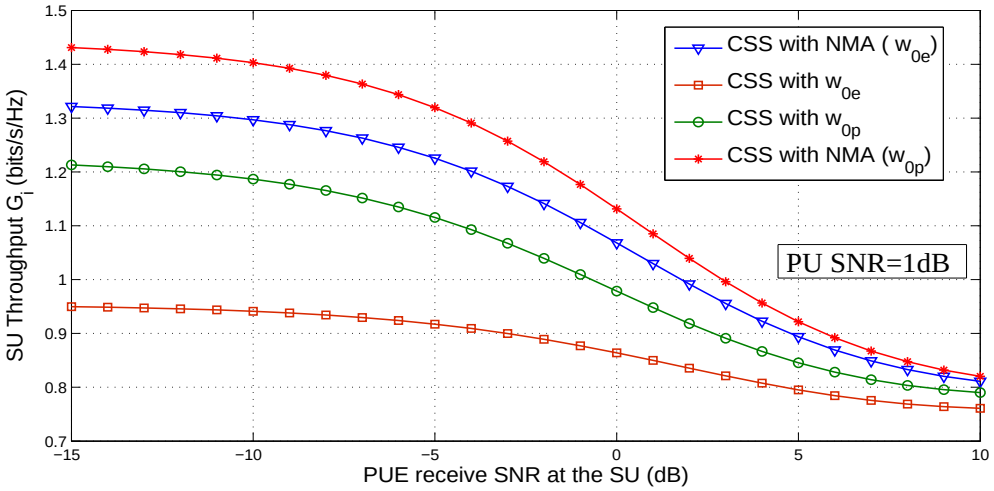

Figure 5.19: Plot of $G_i(\mathbf{w}, \lambda)$ vs PUE SNR for only PUE moving

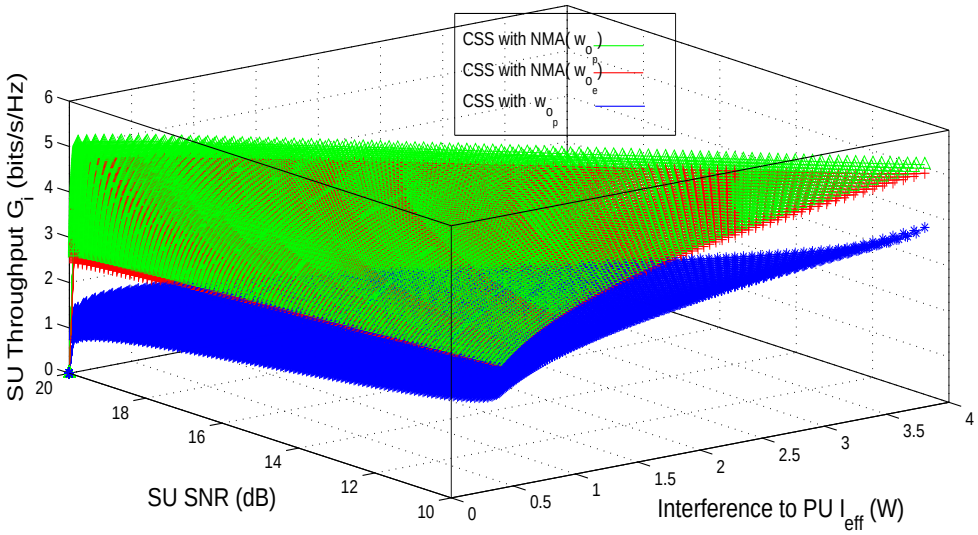

Figure 5.20: Plot of $G_i(\mathbf{w}, \lambda)$ vs SU SNR vs $I_{eff}(\mathbf{w}, \lambda)$

TH-1605_10610214

Hence, LoS components are highly possible on the PUE-SU path. This suggests to model the PUE-SU environment with Rician distribution. On the other hand, the environment between the PU and the SUs is still considered to be Rayleigh faded. Figure 5.9 shows the investigation in Case 2. Here the environment between the PU and the SU network has less obstacles, such that there exist LoS components between the PU and the SUs and the environment between PUE and the SU is considered to be suffering severe fading. Hence the PU-SU channel is considered to be Rician faded while the PUE-SU channel is considered to be Rayleigh faded. It can be seen that in all the fading scenarios, the proposed algorithm with $\mathbf{w}_{0p}$ outperforms its performance with $\mathbf{w}_{0e}$. Individually, $\mathbf{w}_{0p}$ used for CSS outperforms the CSS with $\mathbf{w}_{0e}$.

In Figure 5.10, the performance for the Case 3 has been plotted. Here, both the environments between the PU-SU and the PUE-SU are considered to have less obstacles so that both the PU-SU and the PUE-SU channels have LoS components and are Rician faded. It can be seen here that the same trend of performance as in Figures 5.7 5.8, and 5.9 is depicted.

Next, in Figures 5.11 and 5.12, the variation of the SU throughput over different PUE receive SNRs at the SU has been plotted at the two values of P_{md}. The path loss exponent is kept the same as before. The comparisons have been done for the weighted CSS systems employing weights obtained from the NMA with the proposed $\mathbf{w}_{0p}$ in (5.28) and the existing $\mathbf{w}_{0e}$ in (5.21). Clearly, the former case is seen to perform better than the latter. Similar to the previous experiment, the evaluations using $\mathbf{w}_{0p}$ and $\mathbf{w}_{0e}$ directly as the weight vector for the weighted CSS have also been carried out. It can be seen that the proposed algorithm with $\mathbf{w}_{0p}$ outperforms its performance with $\mathbf{w}_{0e}$. Also, CSS performed with $\mathbf{w}_{0p}$ outperforms the CSS when performed with $\mathbf{w}_{0e}$.

Figures 5.13 and 5.14 show the values of SU throughput at different receive SNRs of PU at the SUs for the two values of P_{md}. As before, the evaluations assess the ability of a scheme to bring the SU throughput of a PUEA affected system close to an honest weighted CSS system using the $\mathbf{w}_{0e}$ in (5.21) as weights. An identical nature of improvement with the previous plots is shown by the weighted CSS with weights obtained from the NMA using the $\mathbf{w}_{0p}$ in (5.28) over that in (5.21). Also, the weighted CSS with the proposed $\mathbf{w}_{0p}$ as weights outperforms the weighted CSS with the existing $\mathbf{w}_{0e}$. Figures 5.15 and 5.16 shows the plot of SU throughput with different SU transmit SNRs. The trend in the performance again shows that the proposed $\mathbf{w}_{0p}$ outperforms the existing $\mathbf{w}_{0e}$ both, when directly used as the weight vector and when used as $\mathbf{w}_0$ for obtaining the optimal weights with NMA.

TH-1605_10610214

Next, we observe the SU throughput for different interferences suffered by the PU with varying SU SNR in Figure 5.20. The SU, PUE, and PU transmit powers and the path loss exponent are kept same as before. One significant point to be noted in all the experiments is, since the PUE lies close to the SU, its receive SNR at the SU is likely to have lower pathloss effect compared to the PU. It can be clearly seen that for any set of (SU SNR, SU interference) values the $\mathbf{w}_0$ in (5.28) is a better choice than the one in (5.21) as a base point for the application of the NMA.

5.6.2 Transmitters and Receivers in Motion

In the evaluations so far, we have considered the PU, SUs, and PUEs. Now, we consider channels where relative motion between the PUE and the SUs causes a Doppler shift in the received signals at the SUs.

We assume the PU to be always static, since most PU systems like TV stations, mobile BS etc. are static. Hence the following cases occur:1) when both the ith SU and the PUE are mobile, 2) when only the PUE is mobile, and 3) when only the ith SU is mobile. Since the ith SU is moving in the cases 1 and 3, its receive SNR from both the PU and the PUE will fluctuate. Mathematically, both these cases are similar. Since only the PUE is moving, only the receive SNR from the PUE at the ith SU will fluctuate in case 2. First we consider the case 1 with the effective direction of the ith SU and the PUE away from each other. Without the loss of generality, we assume the movements of the ith SU and the PUE along the line joining them. The effective direction of the ith SU from the PU is assumed at 120°. The simulation results for this case have been shown in Figure 5.17. It can be clearly seen that for any set of (SU SNR, SU interference) values the $\mathbf{w}_0$ in (5.28) is a better choice than the one in (5.21) as a base point for the application of the proposed algorithm. The proposed algorithm with $\mathbf{w}_{0p}$ outperforms its performance with $\mathbf{w}_{0e}$. Also, CSS performed with $\mathbf{w}_{0p}$ outperforms the CSS when performed with $\mathbf{w}_{0e}$.

Figure 5.18 shows the case 1 with the relative motion between the PUE and the ith SU towards each other along the line joining them. For these evaluations, we consider the standard parameters for 3G/4G mobile systems [179]. We consider a carrier frequency $f_c = 1850$ MHz. In Figure 5.18, the relative velocity between the ith SU and the PUE have been considered to be 50 miles/hr or 22.36 m/s. For evaluating the Doppler shift f_d we consider $f_d = \frac{v}{c} f_c \cos\theta$, where θ is the angle between the direction of motion of the ith SU and the line joining it with the PUE, v is its velocity, and c is the velocity of light. We obtain $f_d = 137.886$Hz and the Doppler spread $2f_d = 275.76$Hz. The coherence

TH-1605_10610214

time T_c is obtained from $T_c = \frac{1}{4f_d}$ as 1.81ms. In Figure 5.17, the relative motion of the ith SU and the PUE is assumed to be in the opposite directions ($\theta = 180$), with the same relative velocity. Hence f_d will be obtained as -137.886 Hz. The effect of doppler shift on the channel coefficient is given in the following expression

$$h(t) = \sum_{i=0}^{L-1} a_i e^{-j2\pi f_c \tau_i} e^{j2\pi f_d t} \tag{5.35}$$

It can be seen that the when the Doppler shift is negative, the channel coefficient suffers more distortions compared to when the doppler shift is positive. Hence lower values of the SU throughput can be seen in Figure 5.17 compared to those in Figure 5.18. It can be observed that the Doppler shifts produce the least fluctuations when NMA is used with the initial base point as $\mathbf{w_{0p}}$ and gives a consistently high SU throughput. Similarly, in the evaluation done in Figure 5.19, only the PUE is moving towards the ith SU which signifies the case 2. The magnitude of the relative velocity has been taken as $v = 40$ miles/hr, and correspondingly f_d is obtained as 110.31Hz, and the Doppler spread is obtained as 220.62Hz. The coherence time in this case is obtained as 2.2ms. The symbol duration time for 3G/4G systems is taken to be approximately 3ms, hence the channel is a fast fading channel. Note that in both the investigations in Figures 5.17 and 5.18, the obtained values of T_c are greater than $T = 1$ ms assumed in our simulations. Hence, even if the channels are fast fading, they do not change over T.

5.7 The Reason for using the NMA

The major reason for considering the NMA in this chapter is its fast convergence and its ability to bring satisfying results even when it fails to converge completely. Compared to the derivative based methods, the NMA converges faster because it need not have to calculate derivatives. Derivative calculation is a complicated and computationally involved task specially when the problem is as complicated as in (5.16). On the other hand, it performs faster than the widely used evolutionary algorithms because of simple calculations [174]. It has been observed in [174] that for problems of small dimensions (up to N=15), the NMA gives a better performance than most of the derivative and non-derivative based algorithms in terms of convergence speed. Since the networks we have considered in our simulations comprise of $8-10$ SUs needing quick decisions, our choice for the NMA is justified.

The reason for prioritizing the convergence speed while choosing our optimization algorithm is that in CR systems, the most important parameter is the quickness in sensing the spectrum. A slightest

TH-1605_10610214

delay in the sensing process can cause a severe increase in interference to the PU. Hence, we aim at an algorithm which is fast yet accurate enough not to compromise on the system robustness. The NMA has been widely known as the most preferable algorithm in Engineering problems for its property of giving approximately optimal solutions even when it fails to converge. Also, most of the non-linear optimization algorithms have a drawback of getting stuck to a suboptimal solution. However, it has been found that the NMA doesn't get stuck to a suboptimal solution [176].

It is possible that there are some algorithms which may give better results than the NMA in terms of accuracy, however considering the trade-off between the accuracy and convergence time [180], we found NMA be the best available option for our work.

Also, note that we have formulated an initial base point $\mathbf{w_{0p}}$ in (23) (5.28). The efficiency of $\mathbf{w_{0p}}$ has been investigated in Figures 5.3, 5.4, and 5.5, which indicates its closeness to the optimal point. It has been proved that when an initial base point closer to the optimal solution is available, the simplex algorithms are more preferable over other algorithms ([175] and [177]).

5.8 Conclusion

The chapter reported redesigning of the SU throughput maximization scheme necessitated by the presence of a PUE in the physical layer. We aimed at saving the SU throughput from getting affected by the PUEAs in CSS. To suppress the damage caused by the PUEAs, an optimally weighted CSS scheme is proposed for energy data combination at the FC. The optimally weighted combination of the energy values at the FC maximizes the SU throughput while providing sufficient protection to the PU in a CSS network facing the PUEAs. It can be seen that the proposed scheme does not depend on the differences in the DOA and the features of the PU and the PUE signals. Simulation results demonstrate that the proposed scheme is effective in suppressing the effects of PUEAs on the SU throughput.

TH-1605_10610214

TH-1605_10610214

6

Conclusions

Contents

6.1 Summary of Contributions and Discussions 140
6.2 Suggestions for Future Research 142

TH-1605_10610214

6.1 Summary of Contributions and Discussions

This thesis dealt with some security issues in a CSS system. The main objective of this thesis is to suppress effects of the MUs in CR systems. The contributions of the thesis can be mainly categorized into three parts, containing the research on non-colluding SSDF attacks, colluding SSDF attacks and the PUEAs respectively. We studied the existing mechanisms to counter each of these attacks. The issues with the existing mechanisms were investigated and work was done to provide some possible solutions. In the first part, we countered the actions of the MUs. This was done by discarding the wrong reports of the MUs. In the second part, we proposed a mechanism to counter the intentions of the MUs. This was carried out by penalizing them for a wrong activity. Instead of allowing them to report wrongly as done in the part 1, we attempted to stop them from even acting maliciously. In the third part, we suppressed a particular effect caused by the MUs. In this thesis, we have focussed on the effects of the PUEAs on the throughput of the SUs. The attacks considered in all these parts were different. While collusion SSDF attacks are an enhanced form of individual SSDF attacks, the reader can see that PUEAs are relatively more stand-alone from the individual and collusion SSDF attacks. The contributions of this thesis are summarized as follows:

(i) We provided a comprehensive literature review of all the major researches in the security issues in CRs. Starting with the first work which had expressed the possibility of the security issues in CRs [40], we elaborated on every major research in this area. We categorized the SSDF attacks and the PUEAs as active and passive. All the major existing counter mechanisms for each of the categorizations have been explained.

(ii) The next chapter of the thesis investigated on the non-colluding SSDF attacks. We studied various statistical methods for suppressing the SSDF attacks. We showed that the major difficulty with the existing statistical methods is to obtain a statistic to measure the deviation of the MUs' data from those of the SUs' data. We showed that Dixon's test has been a very simple mechanism to obtain this deviation. We illustrated the application of Dixon's test in Analytical Chemistry. We threw light on the motivation for using it in Communication and Signal Processing problems. Then we showed how it was used to detect MUs causing SSDF attacks. We conducted a thorough study to find the Dixon's test as an appropriate method to make the MU suppression less complex because it does not depend on the estimation of the statistical parame-

TH-1605_10610214

ters. We later found that the application of Dixon's test has certain drawbacks in the form of its inapplicability to the detection of multiple MUs. Our objective was to design a simple method which can detect multiple MUs efficiently. We used the idea that applying the test on smaller groups can enhance it to detect anomalies in each of the groups. Secondly if the smaller groups show optimality in terms of the application of the Dixon's test, we can enhance its performance. We proposed to extend the capability of the Dixon's test to multiple MUs detection by applying it over smaller groups of 3. Further if each data element undergoes the test multiple times, the efficiency of the algorithm can be significantly enhanced. To further enhance its capability, we applied it over groups with maximum overlap of the SU data. This size of the overlapping groups is set as the optimal size at which Dixon's test gives the best performance. Simulation results showed that the proposed mechanisms are efficient in suppressing multiple MUs.

(iii) The above mechanism was proposed for suppressing individual MUs. However, the mechanism for suppressing individual MUs fails if they launch attacks in collusion. In the next part of the thesis, we studied on the colluding MUs. We found that most of the existing mechanisms on collusion attack scenario were based on the collision penalty C_P. Unlike the first part where our focus was on the actions of the MUs, here the focus was on the intentions of the MUs. Suppressing the malicious intentions can assure a much higher capability to counter these attacks. This idea was expected to work since the collusion SSDF attacks are more harmful than the individual SSDF attacks. In hostile environments, specially when the MUs are colluding, the PU becomes reluctant to share its spectrum with the SUs. The existing mechanisms of designing C_P in hostile environments did not consider incentives for the PU to share its spectrum. Also, they did not consider different collusion attack scenarios in the context of the CRs. We designed a mechanism to counter the collusion attacks where C_P ensures sufficient incentives for the PU to make it share its spectrum in hostile environments. We started with formulating the expression for the expected utility of an SU. The expected utility was defined as the net throughput gain obtained by the SU after considering its successful transmission and C_P imposed on it by the PU for causing collision to it. The expected utility was a function of C_P. The different attack scenarios were considered next and the bounds on C_P to counter them were obtained. After considering all the bounds, the final range of C_P obtained is successful in suppressing the collusion attacks.

(iv) The third part of the thesis studied the PUEAs. Our idea was that reducing the damage caused

TH-1605_10610214

by the PUEAs rather than discarding it altogether can produce a significantly simpler and flexible counter mechanism. The possibility of successfully discarding it is more dependent on factors like RSS, DOA, signal features etc. On the other hand, reducing the damage depends only on efficient channel estimation. Our objective was to reduce the damage caused by the PUE on the throughput of the SUs. The maximization of the throughput of an SU has been an important subject of study in an honest SS environment. However, if PUEAs are launched, the architecture of the network is changed which necessitates the redesigning of the scheme for the maximization of the SU throughput. Such redesigning of maximization of the SU throughput required due the presence of a PUE was carried out for CSS. Our objective was to combine the data of the cooperating SUs in a manner that the effects of the PUEAs on the SU throughput are suppressed. To serve this purpose, a weighted scheme for combining the SU data at the FC was considered for the CSS. The optimal combining weights were obtained by solving an optimization problem which maximizes the SU throughput while protecting the PU from interference in a network facing the PUEAs. The optimal weights generated were used to combine the SU energy data at the FC. The experiments carried out endorsed the effectiveness of the proposed scheme compared to the existing combination schemes.

6.2 Suggestions for Future Research

The thesis points to several important research directions. Some of these are discussed below:

6.2.1 Suppression of Multiple Malicious Users

(i) The present work is for a data fusion CSS system. However, in data fusion systems, the major issue is the required bandwidth for reporting the data to the FC. The present work can be extended for decision fusion systems. However, applying statistical tests on decision fusion systems can be difficult since the values reported are binary. Hence, the work can be extended with a quadrature system which may support some statistical tests.

(ii) The present work assumes error free reporting channels. However, if the reporting channels are erroneous, the sliding window Dixon's mechanism will likely reject the reports from some honest SUs, since it is highly robust towards any deviation from the normal values. An efficient scheme which considers the error in the reporting channels while rejecting the reports is necessary.

TH-1605_10610214

6.2.2 Suppressing Collusion Attacks

(i) The proposed mechanism for suppressing collusion attacks is for n out of N decision fusion CSS. A similar study needs to be carried out for OR and AND rule decision fusion CSS systems.

(ii) Additional categorizations can be incorporated in the work like the attack and run and stay with the attacks.

6.2.3 Suppressing PUEAs

(i) The present work is for a basic "always on" PUE Model. However, smart PUEs represent a more practical scenario. Smart PUEs can manipulate their transmissions according to the presence of the PU and hence are more harmful than the always on PUEs. Designing an efficient scheme for the maximization of the SU throughput under smart PUEAs is a significant direction for future work.

(ii) The interference to the PU considered in the present work is only because of the SUs. However formulating a scheme that considers the interference from the PUEs to the PU too will make the solution more robust for both kinds of PUEs.

(iii) The channel estimations have been considered error free in the present work. Considering channel estimation error in the present work is an important future work to be done.

(iv) The derivations for the closed form expressions for the average throughput and average interference in the present work is a significant problem that needs attention.

6.2.4 Security issues in frequency selective fading channels

This research work has been performed over flat fading channels. However, a more practical scenario is obtained when frequency selective fading channels are considered. The PU signal reaching the SUs may experience a frequency selective fading for the reason that the signal reaches the SU receiver through multiple propagation paths. It has been found that the additional multipaths in frequency selective channels improve the detection performance in the case of energy detection based sensing [181, 182]. Consider a frequency selective fading channel condition and let $\mathbf{h} = [h_1, h_2, ..., h_L]$ be the channel gain vector [181, 182]. The elements of $\mathbf{h}$ are circularly symmetric complex Gaussian RVs, that is $CalN\left(0, E|h_l|^2\right)$ where $l = 1, 2, ..., L$. We assume a uniformly distributed power delay

TH-1605_10610214

profile. The power of the channel is normalized as $\sum_{l=1}^{L} E|h_l|^2$. Let $y(n)$ be the received signal at an SU as shown in (2.1). For frequency fading channels, the hypotheses are

$$\begin{aligned} H_0: &\quad y(n) = w(n) \\ H_1: &\quad y(n) = e^{j(2pin\Delta f + \phi(n))} \sum_{l=0}^{L-1} h_l s(n-l) + w(n) \end{aligned} \tag{6.1}$$

where n is the number of samples collected by the secondary user, $s(n)$ is the signal transmitted by the PU, Δf is the frequency offset that results from the oscillator frequency mismatch between the transmitter and the receiver or the relative motion of the receiver $\phi(n)$ is the phase noise. The instantaneous signal to noise ratio is $\gamma = \sigma_s^2 \sum_{l=0}^{L-1} |h_l|^2/\sigma_w^2$. The noise $w(n)$ is assumed to be iid samples $CN\left(0, \sigma_w^2\right)$. It can also be seen that on considering the frequency selective channels, frequency offset will appear between the transmitter and the receiver. It can be seen that considering frequency selective fading changes the basic system model. The study of security issues on frequency selective channels and noise correlation model may be an area for our future research.

6.2.5 Research on military applications

Cognitive radios have a tremendous application in military applications. The cognitive radio technology has the capability to support waveforms of various frequencies. They can help in providing a cost effective solution for a platform to support communications in various ranges of frequency spectrum after sensing for their availability. They can jump to the available frequency band and help in adjusting the radio parameters accordingly for providing effective communications. Cognitive radios have a tremendous application in enabling network centric warfare (NCW) or network enabled operations (NEOps) [183]. NEOps refer to the sharing of information among the frontline forces, decision makers, weapons, sensors, etc. The need for sharing this information is awareness about the situation for making quick decisions. The information needs to be transferred wirelessly. On the other hand, the commercial interests in civilian applications of the wireless technology are leading to huge investments over frequency bands. This is pressurizing the military to reduce their allocated bands. As a result of this, the use of CR has been widely proposed for military applications over the parts of the VHF and the UHF bands most parts of which remains unused.

In the military applications of CRs, it might not be difficult for the enemy side to disrupt the SS process, particularly on the border areas. In most of the border areas, the communication systems of the warring sides are likely to be located within an area of 0-30 Kms. If one party has the

TH-1605_10610214

required information about the characteristics of the transmitted signals on its counter side, it can easily transmit fake signals of similar characteristics and cause PUEAs. As far as SSDF attacks are concerned, there is a high possibility of external SSDF attacks to cause interference at the enemy side FC. A proper investigation of this thesis work in military applications can open interesting and useful research.

TH-1605_10610214

TH-1605_10610214

A

Table for Critical Values for Dixon's Test

Contents

A.1 Table for Critical Values 148

TH-1605_10610214

A.1 Table for Critical Values

Table A.1: Critical values for different confidence limits (CLs)

N / CL	70%	80%	90%	95%	98%	99%	99.5%
3	0.6836	0.7808	0.8850	0.9411	0.9763	0.9881	0.9940
4	0.4704	0.5603	0.6789	0.7651	0.8457	0.8886	0.9201
5	0.3730	0.4508	0.5578	0.6423	0.7291	0.7819	0.8234
7	0.2811	0.3444	0.4340	0.5077	0.5864	0.6371	0.6809
8	0.2550	0.3138	0.3979	0.4673	0.5432	0.5914	0.6336
9	0.2361	0.2915	0.3704	0.4363	0.5091	0.5554	0.5952
10	0.2208	0.2735	0.3492	0.4122	0.4813	0.5260	0.5658
11	0.2086	0.2586	0.3312	0.3922	0.4591	0.5028	0.5416
12	0.1983	0.2467	0.3170	0.3755	0.4405	0.4831	0.5208
13	0.1898	0.2366	0.3045	0.3615	0.4250	0.4664	0.5034
14	0.1826	0.2280	0.2938	0.3496	0.4118	0.4517	0.4869
15	0.1764	0.2202	0.2848	0.3389	0.3991	0.4385	0.4739
16	0.1707	0.2137	0.2765	0.3293	0.3883	0.4268	0.4614
17	0.1656	0.2077	0.2691	0.3208	0.3792	0.4166	0.4504
18	0.1613	0.2023	0.2626	0.3135	0.3711	0.4081	0.4423
19	0.1572	0.1973	0.2564	0.3068	0.3630	0.4002	0.4333
20	0.1535	0.1929	0.2511	0.3005	0.3562	0.3922	0.4247

TH-1605_10610214

B

Evaluation Parameters for PUEA Model

Contents

B.1 Probability of False Alarm 150
B.2 Probability of Miss Detection 151

TH-1605_10610214

The calculations of P_{fa} and P_{md} follow the procedure similar to [129]. The only difference made here is the inclusion of PUE channels and power in the expressions as shown below:

B.1 Probability of False Alarm

The probability of false alarm can be mathematically written as $P_f = \Pr(E > \lambda | H_0)$. For simplicity we write, $E(y) = E$. Considering the distribution for E as given in Section 2, we get

$$P_f = \int_{\lambda}^{\infty} B dE$$
$$B = \frac{1}{\sqrt{2\pi \frac{1}{M} \sum_{i=1}^{N} w_i^2 (\gamma_e+1)^2}} \exp\left(\frac{-\left(E - \sum_{i=1}^{N} w_i(|h_{e_i}|^2\gamma_e+1)\right)^2}{2.\frac{1}{M}\sum_{i=1}^{N} w_i^2(|h_{e_i}|^2\gamma_e+1)^2} \right). \tag{B.1}$$

Substituting

$$\frac{E - \sum_{i=1}^{N} w_i(|h_{e_i}|^2\gamma_e + 1)}{\sqrt{\frac{1}{M}\sum_{i=1}^{N} w_i^2(|h_{e_i}|^2\gamma_e + 1)^2}} = z, \tag{B.2}$$

gives

$$dE = dz \sqrt{\frac{1}{M}\sum_{i=1}^{N} w_i^2(|h_{e_i}|^2\gamma_e + 1)^2}. \tag{B.3}$$

With the substitutions, P_f is obtained as

$$P_f(\mathbf{w}, \lambda) = \frac{1}{\sqrt{2\pi}} \int_{L_{l_1}}^{\infty} \exp\left(-\frac{z^2}{2}\right) dz, \tag{B.4}$$

where $L_{l_1} = \frac{\lambda - \sum_{i=1}^{N} w_i(|h_{e_i}|^2\gamma_e+1)}{\sqrt{\frac{1}{M}\sum_{i=1}^{N} w_i^2(|h_{e_i}|^2\gamma_e+1)^2}}$.

Finally, P_f comes out to be

$$P_f(\mathbf{w}, \lambda) = Q\left(\frac{\lambda - \sum_{i=1}^{N} w_i(|h_{e_i}|^2\gamma_e + 1)}{\sqrt{\frac{1}{M}\sum_{i=1}^{N} w_i^2(|h_{e_i}|^2\gamma_e + 1)^2}} \right), \tag{B.5}$$

where $Q(.)$ is as defined in (5.7).

TH-1605_10610214

B.2 Probability of Miss Detection

We simplify the analysis by writing $P_m = 1 - P_d$, where P_d is the probability of detection. The probability of detection is mathematically written as $P_d = \Pr(E(y) > \lambda | H_1)$. Considering the distribution as given in section 2, we get,

$$P_d(\mathbf{w}, \lambda) = \int_{\lambda}^{\infty} \frac{1}{\sqrt{2\pi \frac{1}{M} \sum_{i=1}^{N} w_i^2 \left(\frac{2|h_{p_i}|^2\gamma_p}{|h_{e_i}|^2\gamma_e+1} + 1\right)(\gamma_e+1)^2}} \exp\left(\frac{-\left(E - \sum_{i=1}^{N} w_i \left(\frac{|h_{p_i}|^2\gamma_p}{|h_{e_i}|^2\gamma_e+1} + 1\right)(|h_{e_i}|^2\gamma_e + 1)\right)^2}{2.\frac{1}{M} \sum_{i=1}^{N} w_i^2 \left(2\frac{|h_{p_i}|^2\gamma_p}{|h_{e_i}|^2\gamma_e+1} + 1\right)(|h_{e_i}|^2\gamma_e + 1))} \right) dE \tag{B.6}$$

Substituting

$$\frac{E - \sum_{i=1}^{N} w_i \left(\frac{|h_{p_i}|^2\gamma_p}{|h_{e_i}|^2\gamma_e+1} + 1\right)(|h_{e_i}|^2\gamma_e + 1)}{\sqrt{\frac{1}{M} \sum_{i=1}^{N} w_i^2 \left(2\frac{|h_{p_i}|^2\gamma_p}{|h_{e_i}|^2\gamma_e+1} + 1\right)(|h_{e_i}|^2\gamma_e + 1))}} = z \tag{B.7}$$

gives

$$dE = dz \sqrt{\frac{1}{M} \sum_{i=1}^{N} w_i^2 \left(2\frac{|h_{p_i}|^2\gamma_p}{|h_{e_i}|^2\gamma_e + 1} + 1\right)(|h_{e_i}|^2\gamma_e + 1))}. \tag{B.8}$$

Writing (B.6) as

$$P_d(\lambda, \mathbf{w}) = \frac{1}{\sqrt{2\pi}} \int_{L_{l_2}}^{\infty} \exp\left(\frac{-z^2}{2}\right) dz, \tag{B.9}$$

where

$$L_{l_2} = \frac{\lambda - \sum_{i=1}^{N} w_i \left(\frac{|h_{p_i}|^2\gamma_p}{|h_{e_i}|^2\gamma_e+1} + 1\right)(|h_{e_i}|^2\gamma_e + 1)}{\sqrt{\frac{1}{M} \sum_{i=1}^{N} w_i^2 \left(2\frac{|h_{p_i}|^2\gamma_p}{|h_{e_i}|^2\gamma_e+1} + 1\right)(|h_{e_i}|^2\gamma_e + 1))}}. \tag{B.10}$$

The probability of detection is found as,

$$P_d(\mathbf{w}, \lambda) = Q\left(\frac{\lambda - \sum_{i=1}^{N} w_i \left(\frac{|h_{p_i}|^2\gamma_p}{|h_{e_i}|^2\gamma_e+1} + 1\right)(|h_{e_i}|^2\gamma_e + 1)}{\sqrt{\frac{1}{M} \sum_{i=1}^{N} w_i^2 \left(2\frac{|h_{p_i}|^2\gamma_p}{|h_{e_i}|^2\gamma_e+1} + 1\right)(|h_{e_i}|^2\gamma_e + 1))}} \right). \tag{B.11}$$

TH-1605_10610214

TH-1605_10610214

Bibliography

[1] C. Consulting, "https://www.slideshare.net/stefanzehle/spectrum-auction-failure-in-india-october-2016," *Spectrum auction failure in India, October 2016*, 2016.

[2] S. Kalamkar, A. Banerjee, and A. Roychowdhury, "Malicious user suppression for cooperative spectrum sensing in cognitive radio networks using dixon's outlier detection method," in *National Conference on Communications (NCC), 2012*, 2012, pp. 1–5.

[3] J. McMillan, "Why auction the spectrum?" *Telecommunications Policy, Elsevier*, vol. 19, no. 3, pp. 191–199, April 1995.

[4] R. S. Jain, "Spectrum auctions in india: lessons from experience," *Telecommunications Policy, Elsevier*, vol. 25, no. 10-11, pp. 671–688, October-November 2001.

[5] "Spectrum policy task force," in *ET Docket No. 02-135*, 2002.

[6] J. M. III, "Cognitive radios: An integrated agent for software defined radio," *Dissertation for Doctor of Technology*, 8 May 2000.

[7] "Notice of proposed rule making and order," in *ET Docket No. 03-108*, 2003.

[8] S. Hakin, "Cognitive radio: Brain empowered wireless communications," *IEEE Journals on Selected Areas in Comunications.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[9] R. Tandra and A. Sahai, "Snr walls for signal detection," *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, no. 1, pp. 4–17, Feb 2008.

[10] M. Gandetto and C. Regazzoni, "Spectrum sensing: A distributed approach for cognitive terminals," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 3, pp. 546–557, April 2007.

[11] J. M. Peha, "Approaches to spectrum sharing," *IEEE Communications Magazine*, vol. 43, no. 2, pp. 10–12, Feb 2005.

[12] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio, part i: Two user networks," *IEEE Transactions on Wireless Communications*, vol. 6, no. 6, pp. 2204–2213, June 2007.

[13] G. Xiong and S. Kishore, "Cooperative spectrum sensing in cognitive radio networks under gaussian fusion channels," in *2009 43rd Annual Conference on Information Sciences and Systems*, March 2009, pp. 675–680.

[14] S. M. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative sensing among cognitive radios," in *2006 IEEE International Conference on Communications*, vol. 4, June 2006, pp. 1658–1663.

[15] S. E. Ghasemi, A., "Collaborative spectrum sensing for opportunistic access in fading environments," in *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, (DySPAN) 2005*, 8-11 Nov. 2005, pp. 131–136.

[16] A. Sahai, N. Hoven, and R. Tandra, "Some fundamental limits on cognitive radio," in *Proc. Allerton Conf. Commun., Contr. Comput.*, Oct 2004.

[17] Z. Ma, W. Chen, K. B. Letaief, and Z. Cao, "A semi range-based iterative localization algorithm for cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 704–717, Feb 2010.

TH-1605_10610214

[18] S. Li, H. Zhu, Z. Gao, X. Guan, K. Xing, and X. Shen, "Location privacy preservation in collaborative spectrum sensing," in *INFOCOM, 2012 Proceedings IEEE*, March 2012, pp. 729–737.

[19] H. Li and Z. Han, "Catch me if you can: An abnormality detection approach for collaborative spectrum sensing in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3554–3565, November 2010.

[20] P. L. Yu, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 38–51, March 2008.

[21] N. T. Nguyen, R. Zheng, and Z. Han, "On identifying primary user emulation attacks in cognitive radio systems using nonparametric bayesian classification," *IEEE Transactions on Signal Processing*, vol. 60, no. 3, pp. 1432–1445, March 2012.

[22] L. Duan, A. Min, J. Huang, and K. Shin, "Attack prevention for collaborative spectrum sensing in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 9, pp. 1658–1665, October 2012.

[23] R. Chen and J. M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in *1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, 2006. (SDR) '06.*, Sept 2006, pp. 110–119.

[24] C. Chen, H. Cheng, and Y.-D. Yao, "Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack," *IEEE Transactions on Wireless Communications*, vol. 10, no. 7, pp. 2135–2141, 2011.

[25] Q. Zhao and B. M. Sadler, "A survey of dynamic spectrum access," *IEEE Signal Processing Magazine*, vol. 24, no. 3, pp. 79–89, May 2007.

[26] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proceedings of the IEEE*, vol. 55, no. 4, pp. 523–531, April 1967.

[27] F. F. Digham, M. S. Alouini, and M. K. Simon, "On the energy detection of unknown signals over fading channels," in *Communications, 2003. ICC '03. IEEE International Conference on*, vol. 5, May 2003, pp. 3575–3579 vol.5.

[28] ——, "On the energy detection of unknown signals over fading channels," *IEEE Transactions on Communications*, vol. 55, no. 1, pp. 21–24, Jan 2007.

[29] S. P. Herath, N. Rajatheva, and C. Tellambura, "Energy detection of unknown signals in fading and diversity reception," *IEEE Transactions on Communications*, vol. 59, no. 9, pp. 2443–2453, September 2011.

[30] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer Networks*, vol. 50, no. 13, pp. 2127 – 2159, 2006. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128606001009

[31] Z. Quan, S. Cui, A. H. Sayed, and H. V. Poor, "Wideband spectrum sensing in cognitive radio networks," in *IEEE International Conference on Communications 2008*, May 2008, pp. 901–906.

[32] P. De and Y.-C. Liang, "Blind spectrum sensing algorithms for cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 5, pp. 2834–2842, September 2008.

[33] D. Cabric, S. M. Mishra, and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, 2004*, vol. 1, Nov 2004, pp. 772–776 Vol.1.

[34] S. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*, ser. Prentice Hall signal processing series. Prentice-Hall PTR, 1998, no. v. 1. [Online]. Available: http://books.google.co.in/books?id=aFwESQAACAAJ

[35] F. F. Digham, M. S. Alouini, and M. K. Simon, "On the energy detection of unknown signals over fading channels," in *IEEE International Conference on Communications, 2003. ICC '03*, vol. 5, May 2003, pp. 3575–3579 vol.5.

TH-1605_10610214

[36] K. B. Letaief and W. Zhang, "Cooperative communications for cognitive radio networks," *Proceedings of the IEEE*, vol. 97, no. 5, pp. 878–893, May 2009.

[37] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity. part i. system description," *IEEE Transactions on Communications*, vol. 51, no. 11, pp. 1927–1938, Nov 2003.

[38] ——, "User cooperation diversity. part ii. implementation aspects and performance analysis," *IEEE Transactions on Communications*, vol. 51, no. 11, pp. 1939–1948, Nov 2003.

[39] B. L. To, M. Otmani, T. M. T. Nguyen, A. Fladenmuller, and G. Pujolle, "Decentralized cooperative spectrum sensing for cognitive radio ad-hoc network: Hidden terminal awareness approach," in *2012 11th International Conference on Information Science, Signal Processing and their Applications (ISSPA)*, July 2012, pp. 146–151.

[40] S. Mishra, A. Sahai, and R. Brodersen, "Cooperative sensing among cognitive radios," in *IEEE International Conference on Communications, 2006. (ICC '06)*, vol. 4, June 2006, pp. 1658–1663.

[41] J.-M. P. Ruiliang Chen and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *The IEEE 27th Conference on Computer Communications INFOCOM*, April 2008, pp. 1876–1884.

[42] Y. S. Z. H. Wenkai Wang, Husheng Li, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *43rd Annual Conference on Information Sciences and Systems*, 18-20 March 2009, pp. 130–134.

[43] F. Yu, H. Tang, M. Huang, Z. Li, and P. Mason, "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," in *IEEE Military Communications Conference (MILCOM), 2009*, Oct 2009, pp. 1–7.

[44] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE Transactions on Wireless Communications*, vol. 9, no. 8, pp. 2488–2497, 2010.

[45] S. Shrivastava, A. Rajesh, and P. Bora, "Sliding window dixon's tests for malicious users' suppression in a cooperative spectrum sensing system," *IET Communications*, vol. 8, no. 7, pp. 1065–1071, May 2014.

[46] C. Chen, M. Song, C. Xin, and J. Backens, "A game-theoretical anti-jamming scheme for cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 22–27, May 2013.

[47] S. Mousavifar and C. Leung, "Centralized collusion attack in cognitive radio collaborative spectrum sensing," in *2014 IEEE 80th Vehicular Technology Conference (VTC Fall)*, Sept 2014, pp. 1–6.

[48] Y. Wu, B. Wang, K. J. R. Liu, and T. C. Clancy, "Anti-jamming games in multi-channel cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 1, pp. 4–15, January 2012.

[49] S. Marano, V. Matta, and L. Tong, "Distributed detection in the presence of byzantine attacks," *IEEE Transactions on Signal Processing*, vol. 57, no. 1, pp. 16–29, Jan 2009.

[50] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in *2008 IEEE International Conference on Communications*, May 2008, pp. 3406–3410.

[51] R. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, April 2008.

[52] F. Zhu and S. W. Seo, "Enhanced robust cooperative spectrum sensing in cognitive radio," *Journal of Communications and Networks*, vol. 11, no. 2, pp. 122–133, April 2009.

[53] W. Wang, H. Li, Y. Sun, and Z. Han, "Catchit: Detect malicious nodes in collaborative spectrum sensing," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, Nov 2009, pp. 1–6.

[54] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 2, pp. 774–786, Feb 2011.

[55] P. J.-M. Chen, Ruiliang. and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on selected areas in Communications*, vol. 26, pp. 25–37, 2008.

TH-1605_10610214

[56] Z. Yuan, D. Niyato, H. Li, and Z. Han, "Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks," in *IEEE Wireless Communications and Networking Conference (WCNC), 2011*, March 2011, pp. 599–604.

[57] Z. Yuan, D. Niyato, H. Li, J. B. Song, and Z. Han, "Defeating primary user emulation attacks using belief propagation in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 10, pp. 1850–1860, November 2012.

[58] S. M. J. and S. S. S. M, "Optimisation of cooperative spectrum sensing for cognitive radio networks in the presence of smart primary user emulation attack," *Trans. Emerging Tel. Tech*, October 2014.

[59] M. J. Saber and S. M. S. Sadough, "Optimal energy detection in cognitive radio networks in the presence of malicious users," in *ICCKE 2013*, Oct 2013, pp. 173–177.

[60] M. Haghighat and S. M. S. Sadough, "Cooperative spectrum sensing for cognitive radio networks in the presence of smart malicious users," {*AEU*} - *International Journal of Electronics and Communications*, vol. 68, no. 6, pp. 520 – 527, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S143484111300318X

[61] Q. Yan, M. Li, T. Jiang, W. Lou, and Y. T. Hou, "Vulnerability and protection for distributed consensus-based spectrum sensing in cognitive radio networks," in *Proceedings of IEEE INFOCOM 2012*, March 2012, pp. 900–908.

[62] X. Wang, K. Govindan, and P. Mohapatra, "Collusion-resilient quality of information evaluation based on information provenance," in *2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, June 2011, pp. 395–403.

[63] H. Kahsay, Y. Z. Jembre, and Y. J. Choi, "Game-theoretic analysis of selfish secondary users in cognitive radio networks," *Journal of Communications and Networks*, vol. 17, no. 4, pp. 440–448, Aug 2015.

[64] H. Lin, J. Hu, C. Huang, L. Xu, and B. Wu, "Secure cooperative spectrum sensing and allocation in distributed cognitive radio networks," *International Journal of Distributed Sensor Networks*, vol. 11, no. 10, pp. 440–448, Jan 2016.

[65] W. Wang, L. Chen, K. G. Shin, and L. Duan, "Secure cooperative spectrum sensing and access against intelligent malicious behaviors," in *IEEE Conference on Computer Communications (INFOCOM) 2014*, April 2014, pp. 1267–1275.

[66] ——, "Thwarting intelligent malicious behaviors in cooperative spectrum sensing," *IEEE Transactions on Mobile Computing*, vol. 14, no. 11, pp. 2392–2405, Nov 2015.

[67] M. Haghighat and S. M. S. Sadough, "Cooperative spectrum sensing in cognitive radio networks under primary user emulation attacks," in *6th International Symposium on Telecommunications (IST)*, Nov 2012, pp. 148–151.

[68] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proceedings of the IEEE*, vol. 55, no. 4, pp. 523–531, 1967.

[69] V. Turunen, M. Kosunen, A. Huttunen, S. Kallioinen, P. Ikonen, A. Parssinen, and J. Ryynanen, "Implementation of cyclostationary feature detector for cognitive radios," in *2009 4th International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, June 2009, pp. 1–4.

[70] X. Zhang, R. Chai, and F. Gao, "Matched filter based spectrum sensing and power level detection for cognitive radio network," in *2014 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Dec 2014, pp. 1267–1270.

[71] A. Nasser, A. Mansour, K. C. Yao, H. Charara, and M. Chaitou, "Efficient spectrum sensing approaches based on waveform detection," in *The Third International Conference on e-Technologies and Networks for Development (ICeND2014)*, April 2014, pp. 13–17.

[72] T. S. Dhope and D. Simunic, "Performance analysis of covariance based detection in cognitive radio," in *2012 Proceedings of the 35th International Convention MIPRO*, May 2012, pp. 737–742.

TH-1605_10610214

[73] B. Shaikh, S. M. Z. Shah, and F. Umrani, "An unsigned autocorrelation based blind spectrum sensing approach for cognitive radio," in *2016 International Conference on Open Source Systems Technologies (ICOSST)*, Dec 2016, pp. 48–53.

[74] R. K. Sharma and J. W. Wallace, "Improved spectrum sensing by utilizing signal autocorrelation," in *IEEE 69th Vehicular Technology Conference VTC Spring 2009*, April 2009, pp. 1–5.

[75] M. Naraghi-Pour and T. Ikuma, "Autocorrelation-based spectrum sensing for cognitive radios," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 718–733, Feb 2010.

[76] A. Al-Abbasi and T. Fujii, "A novel blind diversity detection scheme for multi-antenna cognitive radio spectrum sensing," in *2010 IEEE 72nd Vehicular Technology Conference - Fall*, Sept 2010, pp. 1–5.

[77] A. Eslami and S. Karamzadeh, "Double threshold maximum to minimum eigen-value spectrum sensing proposal and performance analysis," in *2016 National Conference on Electrical, Electronics and Biomedical Engineering (ELECO)*, Dec 2016, pp. 646–649.

[78] J. Luo, G. Zhang, H. Xu, Y. Zhou, and W. Yang, "An energy detection based signal detection method with multiple antennas in cognitive radio," in *2015 IEEE Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, Dec 2015, pp. 187–191.

[79] W. Wang and Q. Zhang, "Privacy-preserving collaborative spectrum sensing with multiple service providers," *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 1011–1019, Feb 2015.

[80] A. W. Min and K. G. Shin, "Robust tracking of small-scale mobile primary user in cognitive radio networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 4, pp. 778–788, April 2013.

[81] M. Ghaznavi and A. Jamshidi, "A reliable spectrum sensing method in the presence of malicious sensors in distributed cognitive radio network," *IEEE Sensors Journal*, vol. 15, no. 3, pp. 1810–1816, March 2015.

[82] F. Adelantado and C. Verikoukis, "A non-parametric statistical approach for malicious users detection in cognitive wireless ad-hoc networks," in *2011 IEEE International Conference on Communications (ICC)*, June 2011, pp. 1–5.

[83] S. Srinu and S. L. Sabat, "Cooperative wideband sensing based on entropy and cyclic features under noise uncertainty," *IET Signal Processing*, vol. 7, no. 8, pp. 655–663, October 2013.

[84] H. Tang, F. R. Yu, M. Huang, and Z. Li, "Distributed consensus-based security mechanisms in cognitive radio mobile ad hoc networks," *IET Communications*, vol. 6, no. 8, pp. 974–983, May 2012.

[85] W. Ren and R. W. Beard, "Consensus seeking in multiagent systems under dynamically changing interaction topologies," *IEEE Transactions on Automatic Control*, vol. 50, no. 5, pp. 655–661, May 2005.

[86] L. Xiao, S. Boyd, and S. Lall, "A scheme for robust distributed sensor fusion based on average consensus," in *IPSN 2005. Fourth International Symposium on Information Processing in Sensor Networks, 2005.*, April 2005, pp. 63–70.

[87] M. Huang and J. H. Manton, "Stochastic consensus seeking with measurement noise: Convergence and asymptotic normality," in *2008 American Control Conference*, June 2008, pp. 1337–1342.

[88] X. He, H. Dai, and P. Ning, "Hmm-based malicious user detection for robust collaborative spectrum sensing," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 11, pp. 2196–2208, November 2013.

[89] S. Jana, K. Zeng, and P. Mohapatra, "Trusted collaborative spectrum sensing for mobile cognitive radio networks," in *INFOCOM, 2012 Proceedings IEEE*, March 2012, pp. 2621–2625.

[90] S. Jana, K. Zeng, W. Cheng, and P. Mohapatra, "Trusted collaborative spectrum sensing for mobile cognitive radio networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 9, pp. 1497–1507, Sept 2013.

[91] A. Wald, "Sequential tests of statistical hypotheses," *Ann. Math. Statist.*, vol. 16, no. 2, pp. 117–186, 06 1945. [Online]. Available: http://dx.doi.org/10.1214/aoms/1177731118

TH-1605_10610214

[92] S. Althunibat, V. Sucasas, H. Marques, J. Rodriguez, R. Tafazolli, and F. Granelli, "On the trade-off between security and energy efficiency in cooperative spectrum sensing for cognitive radio," *IEEE Communications Letters*, vol. 17, no. 8, pp. 1564–1567, August 2013.

[93] A. W. Min, K. H. Kim, and K. G. Shin, "Robust cooperative sensing via state estimation in cognitive radio networks," in *New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2011 IEEE Symposium on*, May 2011, pp. 185–196.

[94] S. Srinivasa and M. Haenggi, "Path loss exponent estimation in large wireless networks," in *2009 Information Theory and Applications Workshop*, Feb 2009, pp. 124–129.

[95] Z. Qin, Q. Li, and G. Hsieh, "Defending against cooperative attacks in cooperative spectrum sensing," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2680–2687, June 2013.

[96] A. Monticelli, F. F. Wu, and M. Yen, "Multiple bad data identification for state estimation by combinatorial optimization," *IEEE Power Engineering Review*, vol. PER-6, no. 7, pp. 73–74, July 1986.

[97] E. Soltanmohammadi and M. Naraghi-Pour, "Fast detection of malicious behavior in cooperative spectrum sensing," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 3, pp. 377–386, March 2014.

[98] Y. Tan, S. Sengupta, and K. P. Subbalakshmi, "Analysis of coordinated denial-of-service attacks in ieee 802.22 networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 890–902, April 2011.

[99] Y. Wu, B. Wang, K. J. R. Liu, and T. C. Clancy, "Anti-jamming games in multi-channel cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 1, pp. 4–15, January 2012.

[100] C. Chen, M. Song, C. Xin, and J. Backens, "A game-theoretical anti-jamming scheme for cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 22–27, May 2013.

[101] R. Macedo, Y. Ghamri-Doudane, and M. Nogueira, "Mitigating dos attacks in identity management systems through reorganizations," in *2015 Latin American Network Operations and Management Symposium (LANOMS)*, Oct 2015, pp. 27–34.

[102] E. Hyytia and J. Virtamo, "Dynamic routing and wavelength assignment using first policy iteration," in *Proceedings ISCC 2000. Fifth IEEE Symposium on Computers and Communications*, 2000, pp. 146–151.

[103] N. Mokari, S. Parsaeefard, H. Saeedi, and P. Azmi, "Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users," *IEEE Transactions on Wireless Communications*, vol. 13, no. 2, pp. 1058–1073, February 2014.

[104] D. T. Hoang, D. Niyato, P. Wang, and D. I. Kim, "Performance analysis of wireless energy harvesting cognitive radio networks under smart jamming attacks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 1, no. 2, pp. 200–216, June 2015.

[105] A. Garnaev and W. Trappe, "One-time spectrum coexistence in dynamic spectrum access when the secondary user may be malicious," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 1064–1075, May 2015.

[106] Y. Zou, J. Zhu, L. Yang, Y. c. Liang, and Y. d. Yao, "Securing physical-layer communications for cognitive radio networks," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 48–54, September 2015.

[107] A. A. Sharifi and M. J. M. Niya, "Defense against ssdf attack in cognitive radio networks: Attack-aware collaborative spectrum sensing approach," *IEEE Communications Letters*, vol. 20, no. 1, pp. 93–96, Jan 2016.

[108] K. M. Borle, B. Chen, and W. K. Du, "Physical layer spectrum usage authentication in cognitive radio: Analysis and implementation," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2225–2235, Oct 2015.

[109] Y. Tan, S. Sengupta, and K. P. Subbalakshmi, "Primary user emulation attack in dynamic spectrum access networks: a game-theoretic approach," *IET Communications*, vol. 6, no. 8, pp. 964–973, May 2012.

[110] S. Chen, K. Zeng, and P. Mohapatra, "Hearing is believing: Detecting wireless microphone emulation attacks in white space," *IEEE Transactions on Mobile Computing*, vol. 12, no. 3, pp. 401–411, March 2013.

TH-1605_10610214

[111] S. U. Rehman, K. W. Sowerby, and C. Coghill, "Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios," *IET Communications*, vol. 8, no. 8, pp. 1274–1284, May 2014.

[112] C. Xin and M. Song, "Detection of pue attacks in cognitive radio networks based on signal activity pattern," *IEEE Transactions on Mobile Computing*, vol. 13, no. 5, pp. 1022–1034, May 2014.

[113] D. Pu and A. M. Wyglinski, "Primary-user emulation detection using database-assisted frequency-domain action recognition," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 9, pp. 4372–4382, Nov 2014.

[114] N. Nguyen-Thanh, P. Ciblat, A. T. Pham, and V. T. Nguyen, "Surveillance strategies against primary user emulation attack in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 9, pp. 4981–4993, Sept 2015.

[115] A. Alahmadi, Z. Fang, T. Song, and T. Li, "Subband puea detection and mitigation in ofdm-based cognitive radio networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2131–2142, Oct 2015.

[116] H. Li and Z. Han, "Dogfight in spectrum: Jamming and anti-jamming in multichannel cognitive radio systems," in *IEEE Global Telecommunications Conference (GLOBECOM), 2009*, Nov 2009, pp. 1–6.

[117] ——, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, part i: Known channel statistics," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3566–3577, November 2010.

[118] ——, "Blind dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems with unknown channel statistics," in *IEEE International Conference on Communications (ICC), 2010*, May 2010, pp. 1–6.

[119] ——, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems 2014;part ii: Unknown channel statistics," *IEEE Transactions on Wireless Communications*, vol. 10, no. 1, pp. 274–283, January 2011.

[120] R. W. Thomas, B. J. Borghetti, R. S. Komali, and P. Mahonen, "Understanding conditions that lead to emulation attacks in dynamic spectrum access," *IEEE Communications Magazine*, vol. 49, no. 3, pp. 32–37, March 2011.

[121] W.J.Dixon, "Analysis of extreme values," *The Annals of Mathematical Statistics*, vol. 21, no. 4, pp. 488–506, Dec. 1950.

[122] R. Dean and W. Dixon, "Simplified statistics for small numbers of observations," *Analytical Chemistry.*, vol. 23, no. 4, pp. 636–638, April 1951.

[123] M. Zabet-Moghaddam, E. Heinzle, and A. Tholey, "Qualitative and quantitative analysis of low molecular weight compounds by ultraviolet matrix-assisted laser desorption/ionization mass spectrometry using ionic liquid matrices," *Rapid Communications in Mass Spectrometry*, vol. 18, no. 2, pp. 141–148, 2004. [Online]. Available: http://dx.doi.org/10.1002/rcm.1293

[124] Fisher and Yates, *Statistical tables for biological, agricultural, and medical research.* Oliver and Boyd Edinburgh, 1943. [Online]. Available: http://hdl.handle.net/2027/mdp.39015010175332

[125] S. Kim, S. Lee, H. J. Ju, D. Ko, and S. An, "Priority-based hybrid routing in wireless sensor networks," in *IEEE Wireless Communications and Networking Conference (WCNC), 2010*, April 2010, pp. 1–6.

[126] Y. Lu, A. Vervisch-Picois, and N. Samama, "Cycle slips detection and repair for high accuracy gnss-based indoor positioning," in *International Conference on Indoor Positioning and Indoor Navigation (IPIN), 2014*, Oct 2014, pp. 481–490.

[127] A. Kundu and J. Zhou, "Combination median filter," *IEEE Transactions on Image Processing*, vol. 1, no. 3, pp. 422–429, Jul 1992.

[128] A. Mariani, S. Kandeepan, and A. Giorgetti, "Periodic spectrum sensing with non-continuous primary user transmissions," *IEEE Transactions on Wireless Communications*, vol. 14, no. 3, pp. 1636–1649, March 2015.

TH-1605_10610214

[129] Y.-C. Liang, Y. Zeng, E. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1326–1337, 2008.

[130] M. ney and M. etin, "An efficient monte carlo approach for optimizing communication constrained decentralized estimation networks," in *2009 17th European Signal Processing Conference*, Aug 2009, pp. 1047–1051.

[131] K. Zeng, P. Paweczak, and D. Cabric, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Communications Letters*, vol. 14, no. 3, pp. 226–228, 2010.

[132] K. Arshad and K. Moessner, "Robust collaborative spectrum sensing in the presence of deleterious users," *IET Communications*, vol. 7, no. 1, pp. 49–56, Jan 2013.

[133] H. Bu, Q. Xu, S. Wu, Y. Guo, and M. Sbert, "Detection and removal for impulse noise in monte carlo global illumination rendered images of highly glossy scenes," in *2015 International Conference on Virtual Reality and Visualization (ICVRV)*, Oct 2015, pp. 125–129.

[134] R. J. Hagerty, "Determination of measurement limits to optimize production losses," *IEEE Transactions on Aerospace and Electronic Systems*, vol. AES-3, no. 3, pp. 390–399, May 1967.

[135] M. Urvoy, D. Goudia, and F. Autrusseau, "Perceptual dft watermarking with improved detection and robustness to geometrical distortions," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 7, pp. 1108–1119, July 2014.

[136] X. Wu, B. Hong, X. Peng, F. Wen, and J. Huang, "Radial basis function neural network based short-term wind power forecasting with grubbs test," in *2011 4th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT)*, July 2011, pp. 1879–1882.

[137] S. Peng, X. Lian, X. Wang, and J. Xu, "Optimization of water quality monitoring section based on comprehensive hierarchical clustering," in *Fuzzy Systems and Knowledge Discovery (FSKD), 2015 12th International Conference on*, Aug 2015, pp. 124–129.

[138] T. E. M. Nordling, N. Padhan, S. Nelander, and L. Claesson-Welsh, "Identification of biomarkers and signatures in protein data," in *e-Science (e-Science), 2015 IEEE 11th International Conference on*, Aug 2015, pp. 411–419.

[139] J. H. Xue and D. M. Titterington, "t -tests, f -tests and otsu's methods for image thresholding," *IEEE Transactions on Image Processing*, vol. 20, no. 8, pp. 2392–2396, Aug 2011.

[140] G. D. Tourassi, C. E. Floyd, M. T. Munley, J. E. Bowsher, and R. E. Coleman, "Improved lesion detection in spect using mlem reconstruction," *IEEE Transactions on Nuclear Science*, vol. 38, no. 2, pp. 780–783, Apr 1991.

[141] S. MacDougall, A. K. Nandi, and R. Chapman, "Multiresolution and hybrid bayesian algorithms for automatic detection of change points," *IEE Proceedings - Vision, Image and Signal Processing*, vol. 145, no. 4, pp. 280–286, Aug 1998.

[142] M. Anbar, L. Milescu, A. Naumov, C. Brown, T. Button, C. Carly, and K. AlDulaimi, "Detection of cancerous breasts by dynamic area telethermometry," *IEEE Engineering in Medicine and Biology Magazine*, vol. 20, no. 5, pp. 80–91, Sept 2001.

[143] C. Lee, H. Jung, K. H. Lam, C. Yoon, and K. K. Shung, "Ultrasonic scattering measurements of a live single cell at 86 mhz," *IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control*, vol. 62, no. 11, pp. 1968–1978, November 2015.

[144] A. P. Nanthagopal and R. Sukanesh, "Wavelet statistical texture features-based segmentation and classification of brain computed tomography images," *IET Image Processing*, vol. 7, no. 1, pp. 25–32, February 2013.

[145] M. H. Pinson, L. Janowski, R. Pepion, Q. Huynh-Thu, C. Schmidmer, P. Corriveau, A. Younkin, P. L. Callet, M. Barkowsky, and W. Ingram, "The influence of subjects and environment on audiovisual subjective tests: An international study," *IEEE Journal of Selected Topics in Signal Processing*, vol. 6, no. 6, pp. 640–651, Oct 2012.

TH-1605_10610214

[146] B. Jovanovic, K. Stankovic, M. Vujisic, and P. Osmokrovic, "Initiation and progress of breakdown in the range to the left of the paschen minimum," *IEEE Transactions on Dielectrics and Electrical Insulation*, vol. 18, no. 4, pp. 954–963, August 2011.

[147] S. Pop, I. Ciascai, and D. Pitica, "Statistical analysis of experimental data obtained from the optical pendulum," in *Design and Technology in Electronic Packaging (SIITME), 2010 IEEE 16th International Symposium for*, Sept 2010, pp. 207–210.

[148] S. Sabade and H. Walker, "Evaluation of statistical outlier rejection methods for iddq limit setting," in *Design Automation Conference, 2002. Proceedings of ASP-DAC 2002. 7th Asia and South Pacific and the 15th International Conference on VLSI Design. Proceedings.*, 2002, pp. 755–760.

[149] A. Nasser and D. Hamad, "Detection and visualisation of outliers using kernel principal components," in *Fifth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, April 2015, pp. 119–124.

[150] A. Fiche, J. C. Cexus, A. Khenchaf, M. Rochdi, and A. Martin, "Characterization of em sea clutter with α stable distribution," in *IEEE International Geoscience and Remote Sensing Symposium*, July 2012, pp. 6059–6062.

[151] D. Apetrei, I. Silvas, G. Chicco, R. Neurohr, M. Albu, and P. Postolache, "Voltage and frequency time series analysis improvements in transforming data from quality survey into information," in *9th International Conference on Environment and Electrical Engineering (EEEIC*, May 2010, pp. 265–268.

[152] W. Chai, H. Dong, J. He, and W. Shang, "A biogeography-based optimization algorithm with multiple migrations," in *2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)*, June 2016, pp. 1–8.

[153] A. B. Aicha and S. B. Jebara, "Statistical selection of relevant objective criteria for speech enhancement assessment," in *Advanced Technologies for Signal and Image Processing (ATSIP), 2014 1st International Conference on*, March 2014, pp. 429–433.

[154] M. V. Liarokapis, P. K. Artemiadis, P. T. Katsiaris, K. J. Kyriakopoulos, and E. S. Manolakos, "Learning human reach-to-grasp strategies: Towards emg-based control of robotic arm-hand systems," in *Robotics and Automation (ICRA), 2012 IEEE International Conference on*, May 2012, pp. 2287–2292.

[155] Y. Benjamini, "Opening the box of a boxplot," *The American Statistician*, vol. 42, no. 4, pp. 257–262, 1988. [Online]. Available: http://www.jstor.org/stable/2685133

[156] V. Barnett and T. Lewis, *Outliers in Statistical Data*, ser. Wiley series in probability and mathematical statistics: Applied probability and statistics. Wiley, 1994. [Online]. Available: http://books.google.co.in/books?id=B44QAQAAIAAJ

[157] M. Verma and M. Suarez, "Dixontest.criticalvalues: A computer code to calculate critical values for the dixon statistical data treatment approach," *Journal of Statistical Software*, vol. 57, no. 1, pp. 1–12, 2014. [Online]. Available: https://www.jstatsoft.org/index.php/jss/article/view/v057i02

[158] S. P. Verma and A. Quiroz-Ruiz, "Critical values for six dixon tests for outliers in normal samples up to sizes 100, and applications in science and engineering." *Revista Mexicana de Ciencias Geologicas*, vol. 23, pp. 133–161, 2006.

[159] M. R. Chernick, "A note on the robustness of dixon's ratio test in small samples," *The American Statistician*, vol. 36, p. 140, 1982.

[160] J. M. J. Ashish Rauniyar and S. Y. Shin, "Optimal hard decision fusion rule for centralized and decentralized cooperative spectrum sensing in cognitive radio networks," *Journal of Advances in Computer Networks*, vol. 3, no. 3, pp. 207–212, January 2015.

[161] W. Zhang, R. Mallik, and K. Letaief, "Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks," *IEEE Transactions on Wireless Communications,*, vol. 8, no. 12, pp. 5761–5766, December 2009.

[162] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *2010 IEEE Symposium on Security and Privacy*, May 2010, pp. 286–301.

TH-1605_10610214

[163] D. Pu, Y. Shi, A. Ilyashenko, and A. M. Wyglinski, "Detecting primary user emulation attack in cognitive radio networks," in *IEEE Global Telecommunications Conference (GLOBECOM 2011), 2011*, Dec 2011, pp. 1–5.

[164] S. Anand, Z. Jin, and K. P. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in *Proc. IEEE International Dynamic Spectrum Access Netw.*, Oct. 2008, pp. 1–6.

[165] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in *Proc. IEEE International Conf. Commun.*, Jun. 2009, pp. 1–5.

[166] R. Peng and M. Sichitiu, "Angle of arrival localization for wireless sensor networks," in *3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, 2006. SECON '06.*, vol. 1, Sept 2006, pp. 374–382.

[167] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Raez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in *IEEE 28th International Performance Computing and Communications Conference (IPCCC), 2009*, Dec 2009, pp. 208–215.

[168] F. Liu, H. Chen, L. Xie, and K. Wang, "Maximum-minimum eigenvalue detection-based method to mitigate the effect of the puea in cognitive radio networks," in *2011 International Conference on Wireless Communications and Signal Processing (WCSP)*, Nov 2011, pp. 1–5.

[169] Z. Quan, S. Cui, A. Sayed, and H. Poor, "Optimal multiband joint detection for spectrum sensing in cognitive radio networks," *IEEE Transactions on Signal Processing,*, vol. 57, no. 3, pp. 1128–1140, March 2009.

[170] J. Nelder and M. R., "A simplex method for function minimization," *Computer Journal*, vol. 7, no. 4, pp. 308–313, 1965.

[171] I. F. Akyildiz, W. y. Lee, M. C. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 40–48, April 2008.

[172] J. Lehtomaki, J. Vartiainen, and M. Juntti, "Combined wideband and narrowband signal detection for spectrum sensing," in *Second International Workshop on Cognitive Radio and Advanced Spectrum Management, 2009. CogART 2009.*, May 2009, pp. 91–95.

[173] A. A. Owayed, Z. A. Mohammed, and A. A. R. Mosa, "Probabilities of detection and false alarm in multitaper based spectrum sensing for cognitive radio systems in awgn," in *2010 IEEE International Conference on Communication Systems*, Nov 2010, pp. 579–584.

[174] N. Pham, A. Malinowski, and T. Bartczak, "Comparative study of derivative free optimization algorithms," *IEEE Transactions on Industrial Informatics,*, vol. 7, no. 4, pp. 592–600, Nov 2011.

[175] S. Singer, Sanja; Singer, "Complexity analysis of nelder–mead search iterations," in *Proceedings of the 1.Conferenceon Applied Mathematics and Computation*, September 1318 1999, p. 1999.

[176] W. M. H. W. P. E. Lagarias J. C., Reeds J. A., "Advanced search include citations convergence properties of the nelder-mead simplex method in low dimensions," *SIAM Journal of Optimization*, vol. 9, no. 1, pp. 112–147, 1998.

[177] L. R. M. Kolda T. G. and T. v., "Optimization by direct search: New perspectives on some classical and modern methods*," *SIAM Journal of Optimization*, vol. 45, no. 3, pp. 385–482, 2003.

[178] W. Spenley, G. R. Hext, and F. R. Himsworth, "Sequential application of simplex designs in optimisation and evolutionary operation," *Taylor and Francis Ltd. on behalf of American Statistical Association and American Society for Quality*, vol. 4, no. 4, pp. 441–461, 1962.

[179] L. Sun, G. x. Zhang, B. h. Sun, W. d. Tang, and J. p. Yuan, "A single patch antenna with broadside and conical radiation patterns for 3g/4g pattern diversity," *IEEE Antennas and Wireless Propagation Letters*, vol. 15, pp. 433–436, 2016.

[180] J. M. Renders and S. P. Flasse, "Hybrid methods using genetic algorithms for global optimization," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 26, no. 2, pp. 243–258, Apr 1996.

TH-1605_10610214

[181] J. K. Tugnait, "Spectrum sensing for cognitive radios over frequency selective channels in white noise," in *2011 IEEE International Conference on Communications (ICC)*, June 2011, pp. 1–5.

[182] Y. F. Sharkasi, D. McLernon, and M. Ghogho, "Performance analysis of a cognitive radio energy detector over frequency-selective channels," in *2012 International Symposium on Wireless Communication Systems (ISWCS)*, Aug 2012, pp. 51–55.

[183] T. Willink, "Sdr and cognitive radio for military applications," *Emerging Wireless Technologies*, pp. 1–20, 2007.

TH-1605_10610214

TH-1605_10610214

List of Publications

In Journal

- Shivanshu Shrivastava, Allentatil Rajesh and Prabin Kumar Bora,"Sliding Window Dixon's test for Malicious Users' Suppression in a Cooperative System,"*IET, Communications*, 2014, Vol. 8, Iss. 7, pp. 1065-1071.

In Conference Proceedings

- Shivanshu Shrivastava, A. Rajesh and P. K. Bora,"A Simplified Counter Approach to Primary User Emulation Attacks from Secondary User Perspective,"*IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (26thIEEE-PIMRC)*, Hong Kong, Sep 2015, pp. 2344-2349.(*This work was the departmental* 2^{nd} *runner up in the Research Conclave 2016, IIT Guwahati*)

Presented in Seminars (Refereed)

- Shivanshu Shrivastava, A. Rajesh and P. K. Bora,"On countering Primary User Emulation Attacks from Secondary User Perspective," *Xerox Research Center India (XRCI) Open-2016, Bengaluru, 21-22 Jan. 2016.*

- Shivanshu Shrivastava, A. Rajesh and P. K. Bora,"A Simplified Method for Multiple Malicious Users Suppression in a Cooperative Spectrum Sensing System,"*Presented at the Research Scholars Congress (RSC) 2015*, IIT Guwahati, 23-24 May 2015.

Under Review

- Shivanshu Shrivastava, A. Rajesh and P. K. Bora, "Countering Primary User Emulation Attacks from the Secondary User Throughput Perspective,"*Under Review in Elsevier AEU International Journal of Electronics and Communications.*

- Shivanshu Shrivastava,S.John, A. Rajesh and P. K. Bora, "Bounds on the Collision Penalty for Suppressing Collusion Attacks in Cooperative Systems" *Under Review in IET Communications.*

TH-1605_10610214

TH-1605_10610214