Trust-based Mechanisms for Secure Communication in Cognitive Radio Networks

Sazia Parvin

School of Information Systems, Curtin Business School

Curtin University

A thesis submitted for the degree of

Doctor of Philosophy

June 2013

Declaration

To the best of my knowledge and belief this thesis contains no material previously published by any other person except where due acknowledgment has been made.

This work has not been submitted for any other degree or diploma in any other university.

Signature: .....

Date: .....

Contents

List of Figures xv

List of Tables xxi

Acronyms xxiv

Abstract xxvi

Acknowledgements xxviii

List of Publications xxx

1 Introduction 1

1.1 Introduction 1

1.2 Characteristics of CRNs 4

1.2.1 CRN working process 4

1.2.1.1 Sense (Cognitive capability) 5

1.2.1.2 Understand (Self-Organized capability) 6

1.2.1.3 Decide (Decision capability) 7

1.2.1.4 Adapt (Reconfigurable capability) 8

1.2.2 CRN architecture 8

1.2.2.1 Infrastructure architecture 9
1.2.2.2 Ad-hoc architecture 10
1.2.2.3 Mesh architecture 10
1.2.3 Layered architecture of CRN 10
1.2.4 Application scenarios of CRNs in real-life applications . . 13
1.3 Security Challenges in CRNs 15
1.3.1 Security threats in CRNs 15
1.3.2 Security attacks on protocol layers in cognitive radio node 17
1.3.3 Security requirements in CRNs 20
1.4 Importance of Trust Management for Ensuring CRN Security . 24
1.5 Research Gaps in CRN Security 30
1.5.1 Trust management 30
1.5.2 Authentication 31
1.5.3 Secure routing 32
1.5.4 Spectrum management 33
1.6 Objectives of the Thesis 36
1.7 Scope of the Thesis 37
1.8 Significance of the Research 39
1.8.1 Social and economic significance 39
1.8.2 Scientific significance 40
1.9 The Structure of the Thesis 41
1.10 Conclusion 44

2 Literature Review **45**

2.1 Introduction 45
2.2 Challenges and Threats in the Various Functionalities of CRNs . 46

2.2.1 Spectrum Sensing 47
2.2.1.1 Spectrum sensing challenges 47
2.2.1.2 Spectrum sensing threats 50
2.2.2 Spectrum decision 50
2.2.2.1 Spectrum decision challenges 51
2.2.2.2 Spectrum decision threats 52
2.2.3 Spectrum sharing 52
2.2.3.1 Spectrum sharing challenges 53
2.2.3.2 Spectrum sharing threats 53
2.2.4 Spectrum mobility 54
2.2.4.1 Spectrum Mobility Challenges 54
2.2.4.2 Spectrum mobility threats 55
2.3 Countermeasures for Various Attacks on CRNs 56
2.3.1 Jamming countermeasures 56
2.3.2 Primary user emulation attack countermeasures 57
2.3.3 Objective function attacks countermeasures 58
2.3.4 Lion attack countermeasures 59
2.4 Secure Spectrum Management Schemes in CRNs 59
2.4.1 Secure spectrum sensing scheme 59
2.4.2 Secure spectrum decision scheme 63
2.4.3 Secure spectrum sharing scheme 64
2.4.4 Secure spectrum mobility scheme 66
2.5 Trust-based Schemes to Ensure Security in CRNs 67
2.5.1 Trust-based schemes in secure spectrum sensing in CRNs 71
2.5.2 Trust-based spectrum decision schemes in CRNs 73
2.5.3 Trust-based schemes in secure spectrum sharing in CRNs 75

2.6 Authentication-based Schemes for CRN Security 75
2.6.1 Location-based authentication schemes 76
2.6.2 Identity-based authentication schemes 79
2.7 Critical Evaluation of the Existing Approaches to Maintain Secure Communication in CRNs 82
2.8 Conclusion 87

3 Problem Definition **88**
3.1 Introduction 88
3.2 Key Concepts and Preliminaries 89
3.2.1 Trust 89
3.2.2 Security 90
3.2.3 Trustworthiness 90
3.2.4 Authentication 90
3.2.5 Availability 91
3.2.6 Unavailability 91
3.2.7 Reliability 91
3.2.8 Downtime 91
3.2.9 Trusted Third Party(TTP) 92
3.2.10 Trust Repository 92
3.2.11 User/Node 92
3.2.12 Deprivation rate 93
3.2.13 Blocking rate 93
3.2.14 Utilization ratio 93
3.3 Problem Definition 93

3.3.1 Trust-based authentication schemes for improving secure communication in CRNs 94
3.3.1.1 Existing solutions of trust establishment in CRNs 94
3.3.1.2 Research gaps in existing trust establishment schemes in CRNs 96
3.3.1.3 Existing solutions in authentication mechanisms in CRNs 98
3.3.1.4 Research gaps in authentication mechanisms in CRNs 99
3.3.2 Mechanisms for secure spectrum sharing in CRNs 100
3.3.2.1 Existing solutions in spectrum sharing in CRNs 100
3.3.2.2 Research gaps in secure spectrum sharing in CRNs 101
3.3.3 Mechanisms for improving system availability in CRNs . 102
3.3.3.1 Existing solutions in system availability in CRNs 102
3.3.3.2 Research gaps in system availability in CRNs . 103
3.4 Research Issues 106
3.4.1 Issue 1: Propose a trust-based authentication framework which improves the security of communication 107
3.4.2 Issue 2: Propose a trust-based spectrum sharing scheme for secure communication in CRNs 108
3.4.3 Issue 3: Propose a model for minimizing disruption to an SU's service during spectrum sharing in CRNs 109
3.4.4 Issue 4: Propose a scheme for balancing the number of SUs and PUs during spectrum sharing in CRNs 109

3.4.5 Issue 5: Propose a trust-based mechanism for node selection and secure node joining and leaving the network 110
3.4.6 Issue 6: Propose a framework for system availability enhancement in CRNs . . . 111
3.5 Research Methodology . . . 111
3.5.1 The science and engineering-based research method . . . 111
3.5.2 Research stages . . . 112
3.6 Conclusion . . . 118

4 Solution Overview 120

4.1 Introduction . . . 120
4.2 Solution Overview for Trust Establishment Between Different Nodes in CRNs . . . 121
4.2.1 Overview of the solution for establishing trust-based authentication . . . 122
4.2.2 Overview of the solution for solving the biasing problem 123
4.3 Solution Overview for Secure Spectrum Sharing Mechanisms in CRNs . . . 125
4.3.1 Overview of the solution to minimize disruption in the SU's service . . . 125
4.3.2 Overview of the solution for a conjoint trust assessment mechanism for secure spectrum sharing . . . 128
4.3.3 Overview of the solution for balancing the CRNs for multiple PUs, SUs and sub-bands . . . 131
4.4 Solution Overview for System Availability Enhancement Mechanisms in CRNs . . . 132

4.4.1 Overview of the solution for selecting the key nodes in CRNs based on their trust value . . . 133
4.4.2 Overview of the solution for the process of secure node joining and leaving the network and its effect on the trust value . . . 134
4.4.3 Overview of the solution for increasing system availability and reliability by introducing multiple backup CAs in CRN . . . 136
4.5 Conclusion . . . 139

5 Framework for Trust-based Secondary Node Authentication in Cognitive Radio Networks 140

5.1 Introduction . . . 140
5.2 Proposed Framework for Trust-based Secondary Node Authentication (TSNA) in CRNs . . . 142
5.2.1 System model and architecture . . . 142
5.2.2 Working of the proposed TSNA framework in CRNs . . . 144
5.2.2.1 Trust calculation between different nodes . . . 146
5.2.2.2 Authenticating an SU's request . . . 147
5.2.2.3 Solution to avoid the biasing problem . . . 148
5.3 Trust Calculation Methods Between Different Nodes in the TSNA Framework . . . 149
5.3.1 Direct trust calculation . . . 152
5.3.2 Indirect trust calculation . . . 155
5.3.3 Integrated trust calculation . . . 157
5.3.4 Bootstrapping of a new SU in the primary network . . . 158

5.3.4.1 Triangular trust calculation 159
5.3.4.2 Reference trust calculation 160
5.4 Authenticating an SU's Request in the TSNA Framework 162
5.5 Solution to Avoid the Biasing Problem During Trust Recommendation 163
5.6 Example of Trust Calculation to Authenticate an SU's Request in CRNs 166
5.6.1 Example of direct trust calculation 166
5.6.2 Example of indirect trust calculation 168
5.6.3 Example of integrated trust calculation 169
5.7 Verification of the TSNA Framework 170
5.7.1 Phases in the trust-based SU authentication framework verification 171
5.7.2 Scenario 1: Authenticating the SU's request based on the trust value 172
5.7.2.1 *Case 1: Candidate node's request authentication process in the secondary network ('Network 1')* 173
5.7.2.2 *Case 2: Candidate node's request authentication process in the primary network ('Network 2')* 178
5.7.2.3 *Case 3: Candidate node's request is not authenticated either in the 'Network 1' or in the 'Network 2'* 183

5.7.3 Scenario 2: Member nodes are biased by malicious users to assign a biased trust value for the candidate node and its solution 184
5.8 Conclusion 191

6 Mechanisms for Secure Spectrum sharing in CRNs 193

6.1 Introduction 193
6.2 Service Continuity Enhancement (SCE) Approach for Authenticated SUs During Spectrum Sharing 196
6.2.1 Defining different working states to enhance an SU's service continuity 196
6.2.2 Defining the transition rates and probabilities of an SU being in different states during spectrum sharing 199
6.3 Conjoint Trust Assessment for Secure Spectrum Sharing (CTAS^3) Framework in CRNs 205
6.3.1 Working of the proposed CTAS^3 framework 206
6.3.2 Trust calculation of the requesting node from the secondary network 209
6.3.3 Trust calculation of the requesting node from the primary network 213
6.3.4 Checking the trust value of the requesting node for spectrum access 215
6.4 B-CRN Framework for Multiple Users for Efficient Spectrum Sharing in CRNs 217
6.4.1 B-CRN system model and architecture 218
6.4.2 Balancing the number of PUs and PUs in CRNs 218

6.4.2.1 For a fixed sub-band network 219
6.4.2.2 For a fixed number of PUs in a network 220
6.4.3 Efficient spectrum sharing in the presence of multiple PUs and SUs in CRNs 222
6.4.3.1 Defining states during spectrum sharing for multiple SUs and PUs 223
6.4.3.2 Defining transition rates during spectrum sharing for multiple SUs and PUs 224
6.4.3.3 Probability of the model being in each state during spectrum sharing for multiple SUs and PUs 225
6.4.4 Criteria to evaluate system performance for a balanced multi-user network during spectrum sharing 229
6.4.4.1 The mean number of SUs 229
6.4.4.2 Deprivation rate 229
6.4.4.3 Blocking rate 230
6.4.4.4 Utilization ratio 230
6.5 Verification and Numerical Results 231
6.5.1 Enhancing the SU's service continuity through the SCE framework 231
6.5.2 Secure spectrum sharing through CTAS^3 framework . . . 236
6.5.2.1 Trust calculation from the secondary network . 237
6.5.2.2 Trust calculation from the primary network . . 239
6.5.3 Evaluation of network statistics for a B-CRN framework 241
6.5.3.1 Mean number of SUs analysis 241
6.5.3.2 Deprivation rate analysis 243

6.5.3.3 Blocking rate analysis 244
6.5.3.4 Utilization ratio analysis 246
6.6 Conclusion 247

7 Mechanisms for Enhancing System Availability of CRNs 248

7.1 Introduction 248
7.2 Proposed Framework for Node Selection and Secure Node Joining and Leaving (NSSJL) the Network to Increase the System Availability 251
7.2.1 System model and architecture 251
7.2.2 Working steps of the NSSJL framework 252
7.3 Trustworthy Node Selection to Work as a CA and BCA 254
7.3.1 Trust calculation method 258
7.3.2 Selection of CA and BCA based on the trust value . . . 265
7.3.3 Selection of CA and BCA node when there is more than one possible node 266
7.3.3.1 *CA Selection Process* 267
7.3.3.2 *BCA Selection Process* 268
7.4 Process of Secure Node Joining and Leaving the CRN and its Effect on Trust Value 270
7.4.1 Secure joining the network and its effect on a node's trust value 270
7.4.2 Secure leaving process from the network and its effect on the node's trust value 276
7.5 Enhancing the Availability of the CRN System using the NSSJL Framework 280

7.5.1 Defining multi-states in a CA and the transition between them . . . 283
7.5.2 Defining the transition rates and probabilities of CAs being in different states . . . 286
7.5.3 Determining the probability of the system being in a healthy state . . . 290
7.5.3.1 Probability of the system being in a healthy state in a single-CA system ($n = 1$) . . . 290
7.5.3.2 Probability of the system being in a healthy state in a multi-BCA System ($n >= 2$) . . . 291
7.5.4 Criteria to evaluate the availability of the CRN . . . 292
7.5.4.1 Availability . . . 292
7.5.4.2 Downtime and downtime cost . . . 293
7.5.4.3 Reliability . . . 293
7.5.4.4 Trustworthiness . . . 294
7.6 Verification Results and Discussion . . . 294
7.6.1 Selection of the CA and BCA from the member nodes in CRNs . . . 296
7.6.2 Secure node joining and leaving process which affects the node's trust value . . . 300
7.6.3 System availability and reliability enhancement in CRNs using the NSSJL framework . . . 304
7.6.3.1 Availability analysis . . . 305
7.6.3.2 Downtime cost analysis . . . 308
7.6.3.3 Reliability analysis . . . 309
7.6.3.4 Trustworthiness analysis . . . 310

7.7 Conclusion 311

8 Recapitulation and Future Work **313**

8.1 Introduction 313

8.2 Recapitulation of Research Issues 314

8.3 Contributions of the Thesis 316

8.3.1 Contribution 1: Methodology to establish trust between different CR nodes to authenticate the node's request . . 318

8.3.2 Contribution 2: Methodology to solve the biasing problem to obtain the node's actual trust value 319

8.3.3 Contribution 3: Methodology to propose different working states of an SU to minimize the disruption to its service when it needs to vacate the spectrum for the PU in CRNs 320

8.3.4 Contribution 4: Methodology for a conjoint trust assessment to share the spectrum securely in CRNs . . . 321

8.3.5 Contribution 5: Methodology for balancing the number of PUs and SUs for efficient spectrum sharing in CRNs . 322

8.3.6 Contribution 6: Methodology for selecting the key nodes to perform the major functionalities 323

8.3.7 Contribution 7: Methodology for proposing a secure node joining and leaving process in CRNs 324

8.3.8 Contribution 8: Methodology for system availability and reliability enhancement in CRNs 324

8.4 Future Work 325

8.4.1 Consider the dynamic behaviours of CR nodes to obtain the most recent trust value . . . 326
8.4.2 Extend the proposed framework for multi-hop CRNs . . 327
8.4.3 Consider soft encryption-based techniques during message transmission in CRNs . . . 328
8.4.4 Establish certificate-based trust to ensure the integrity and authenticity of the trust value for the candidate node in CRNs . . . 328
8.4.5 Consider communication overheads for cryptography techniques and huge data in the co-operation record table 329
8.5 Conclusion . . . 330

References **331**

Appendix **352**

A The Selected Publications **353**

A.1 Multi-Cyber Framework for Availability Enhancement of Cyber Physical Systems . . . 353
A.2 Conjoint Trust Assessment for Secure Communication in Cognitive Radio Networks . . . 353
A.3 Cognitive Radio Network Security:A Survey . . . 353
A.4 Trust-Based Spectrum Sharing for Cognitive Radio Networks . . 353

List of Figures

1.1 Difference between wireless networks and CRNs 4
1.2 Working process of CRNs 5
1.3 Basic architecture of CRNs 9
1.4 Infrastructure architecture 10
1.5 Ad-hoc architecture 10
1.6 Mesh architecture 11
1.7 Standard layered architecture for CRNs 11
1.8 Main functions of different protocol layers in CRNs 12
1.9 Cognitive radio applications 14
1.10 Defense of soft security issues using trust 26
1.11 Position of trust management in a secured system architecture . 27
1.12 Architecture of trust management in secured CRN 29
1.13 Relationship between the chapters of this thesis 43

2.1 Security threats in CRNs sensing 51
2.2 Secure spectrum sensing scheme 61
2.3 Location-based authentication protocol 78
2.4 Improved identify authentication process 81

3.1 The general process of a standard trust establishment paradigm 95

3.2 A conceptual framework for secure trust-based communication in cognitive radio networks 114

4.1 Overview of the solutions proposed in this thesis 121
4.2 Overview of trust establishment scheme 124
4.3 Working states of an SU during spectrum sharing 127
4.4 Overview of the secure spectrum sharing scheme 130
4.5 Overview of secure spectrum with multiple users in a balanced network 132
4.6 Overview of the node selection scheme 134
4.7 Overview of secure node joining and leaving process 136
4.8 System availability enhancement scheme 138

5.1 System model of the TSNA framework 142
5.2 Flowchart illustrating steps performed by the TSNA framework 145
5.3 Different trust relationships between the candidate node and member nodes 151
5.4 Flowchart of trust calculation phase performed by the TSNA framework 152
5.5 Triangular trust calculation to bootstrap a new SU node 160
5.6 Reference trust calculation to bootstrap a new SU node 161
5.7 Flowchart of the authentication checking step performed by the TSNA framework 162
5.8 Flowchart for the biasing problem solution phase performed by the TSNA framework 164
5.9 Example of indirect trust calculation 168
5.10 Example of integrated trust calculation 170

5.11 Snapshot Network Set-up 173
5.12 Input for 'Network 1' 174
5.13 Trustworthiness of the candidate node from four nodes in 'Network 1' for criteria 1 175
5.14 Trustworthiness of the candidate node from four nodes in 'Network 1' for criteria 2 176
5.15 Trustworthiness of the candidate node from four nodes in 'Network 1' for criteria 3 177
5.16 Candidate node's final trust value computed by the SUBS in 'Network 1' 177
5.17 Input for 'Network 2' 179
5.18 Trustworthiness of the candidate node from different nodes in 'Network 2' for criteria 1 180
5.19 Trustworthiness of the candidate node from different nodes in 'Network 2' for criteria 2 181
5.20 Trustworthiness of the candidate node from different nodes in 'Network 2' for criteria 3 181
5.21 Candidate node's final trust value computed by the PUBS in 'Network 2' 182
5.22 Trust value for the candidate node in 'Network 1' for criteria 1 185
5.23 Trust value for the candidate node in 'Network 1' for criteria 2 186
5.24 Trust value for the candidate node in 'Network 1' for criteria 3 186
5.25 Query response for the candidate node's trust value in 'Network 1' 188
5.26 Checking of the candidate node's trust value assigned by each individual member node in 'Network 1' 191

6.1 Transition between different working states of an SU during spectrum sharing . . . 198
6.2 Stochastic model for an SU's activity. . . . 201
6.3 System architecture . . . 205
6.4 Flowchart illustrating the steps performed by the CTAS^3 framework . . . 208
6.5 Flow of controls between different nodes in the CTAS^3 framework 209
6.6 Frequency band sharing in CRNs . . . 218
6.7 State transition diagram of spectrum sharing for multiple users in CRNs . . . 222
6.8 Service continuity vs access rate . . . 235
6.10 Average trust value of the requesting node from the other 5 nodes in the secondary network . . . 237
6.9 Trust value of the requesting node from each member node in the secondary network for 1000 services . . . 238
6.11 Trust value of the requesting SU from each member node for the 1000 services in the primary network . . . 239
6.12 Average trust value of the requesting node from the primary network . . . 240
6.13 Mean number of SUs vs. arrival rate of PUs (λ_p) . . . 242
6.14 Deprivation rate vs. arrival rate of PUs (λ_p) . . . 244
6.15 Blocking rate vs. arrival rate of SUs (λ_s) . . . 245
6.16 Utilization ratio vs. arrival rate of SUs (λ_s) . . . 246

7.1 Proposed model using multiple BCAs in the NSSJL framework . 251

7.2 Flowchart illustrating the steps performed by the NSSJL framework . . . 253
7.3 Working steps for the node selection phase in the NSSJL framework . . . 256
7.4 Communication between CR Nodes . . . 257
7.5 Example to illustrate the trust calculation method . . . 260
7.6 Working steps of the secure joining process in the NSSJL framework . . . 272
7.7 Flow of the secure joining process between different nodes in the network in the NSSJL framework . . . 276
7.8 Working steps of the secure leaving process in the NSSJL framework . . . 278
7.9 Flow of the secure node leaving process in the NSSJL framework 280
7.10 CA and BCA's cooperation to maintain smooth communication in CRNs . . . 282
7.11 Multiple BCAs framework . . . 284
7.12 Multi-BCA model using Markov Chain . . . 287
7.13 Single-CA system . . . 290
7.14 Node 1's trust value with the other five nodes in the NSSJL framework . . . 296
7.15 Node 2's trust value with the other five nodes in the NSSJL framework . . . 297
7.16 Node 3's trust value with the other five nodes in the NSSJL framework . . . 297
7.17 Node 4's trust value with the other five nodes in the NSSJL framework . . . 298

7.18 Node 5's trust value with the other five nodes in the NSSJL framework . . . 298
7.19 Node 6's trust value with the other five nodes in the NSSJL framework . . . 299
7.20 Trust value of member nodes during the joining process to the network . . . 301
7.21 Trust value of member nodes after new node's trust value is updated for the successful joining of the NSSJL framework . . . 302
7.22 Trust value increased after normal leaving in the NSSJL framework . . . 303
7.23 Trust value decreased after abnormal leaving in the NSSJL framework . . . 304
7.24 Availability vs. different reconfiguration rates for different numbers of CAs . . . 306
7.25 Availability vs. different reconfiguration time for different numbers of CAs . . . 307
7.26 Availability vs. different reconfiguration times and different failure rates . . . 308
7.27 Downtime cost vs. different reconfiguration rates for different numbers of CAs . . . 309
7.28 Reliability vs. different reconfiguration rates . . . 310
7.29 Trustworthiness for different CA options . . . 311

List of Tables

1.1 Attacks on different protocol layers in CRNs 18

1.2 Name and description of different attacks in CRNs 19

1.3 Scope of attacks 24

5.1 Cooperation record table 154

5.2 Cooperation record table for direct trust calculation 167

5.3 Node initialization from 'Network 1' 174

5.4 Trustworthiness comparison to decide to authenticate the candidate node's request in 'Network 1' 178

5.5 Nodes initialization from 'Network 2' 179

5.6 Trustworthiness comparison to decide to authenticate the candidate node's request in 'Network 2' 182

5.7 Trustworthiness comparison to decide to authenticate 'node 4' in 'Network 1' 183

5.8 Saving trust value of candidate node in CA repository 187

5.9 Nodes initialization in 'Network1' 187

5.10 The candidate node's trust value computed by the SUBS in 'Network 1' after the biasing problem 188

5.11 Comparison of candidate node's trust value 189

5.12 Trust value comparison from every individual node for different criteria in 'Network 1' 190
5.13 Decision by the SUBS based on the biasing value 191

6.1 Cooperation record table of node 2 with requesting node 211
6.2 System operation oarameters. 231
6.3 Service continuity level of the SU depending on various transition rates 234
6.4 Trust value of the requesting node from the secondary network . 238
6.5 Trust value of the requesting node from the PUBS 240
6.6 System operation parameters for mean number of SU analysis for multiple users during spectrum sharing 242
6.7 System operation parameters for deprivation rate analysis for multiple users during spectrum sharing 243
6.8 System operation parameters for blocking rate analysis for multiple users during spectrum sharing 245
6.9 System operation parameters for utilization rate analysis for multiple users during spectrum sharing 246

7.1 The trust value received by the SUBS for the CR node 262
7.2 The trust value received by the PUBS for the CR node 263
7.3 The average trust value of nodes calculated by the SUBS 264
7.4 The average trust value of nodes calculated by the PUBS 264
7.5 Local trust relationship table stored in the PUBS 265
7.6 Candidate list for CA and BCA selection 266
7.7 Example when both nodes have the same trust value 269
7.8 Behaviour-based event table 274

7.9 Each member node's trust value 300

Acronyms

CR: Cognitive Radio

CRN: Cognitive Radio Network

PU: Primary User

SU: Secondary User

CA: Certificate Authority

BCA: Back-up Certificate Authority

SN: Secondary Network

PN: Primary Network

SUBS: Secondary User Base Station

PUBS: Primary User Base StationInput/Output

PKC: Public Key Cryptography

PKI: Primary Key Infrastructure

CTMC: Continuous Time Markov Chain

PUEA: Primary User Emulation Attack

LV: Location Verifiers

OFA: Objective Function Attack

SSDF: Secondary Sensing Data Falsification

RSS: Received Signal Strength

RFF: Radio Frequency Fingerprinting

AI: Artificial Intelligence

DSA: Dynamic Spectrum Access

PMF: Probability Mass Function

SOC: Spectrum Opportunity Clustering

OFDM: Orthogonal Frequency Division Multiplexing

EAP: Extensible Authentication Protocol

RFF: Radio Frequency Fingerprinting

TSNA: Trust-based Secondary Node Authentication

CTAS^3: Conjoint Trust Assessment for Secure Spectrum Sharing

SCE: Service Continuity Enhancement

B-CRN: Balance the number of PUs and SUs in CRN

NSSJL: Node Selection and Secure Node Joining and Leaving

Abstract

The advancement of wireless communication has led to the problem of growing spectrum scarcity due to an increasing demand. Cognitive radio technology as a concept was introduced to solve the problem of spectrum scarcity and improve spectrum utilization to support such growth in wireless communication. Cognitive radio provides a key enabling function in next generation (xG) mobile communication by being aware of the changes of its surrounding environment and modifying its operating parameters dynamically to adapt to such changes to solve spectrum scarcity issues. However, the inherent properties of cognitive radio technology make such networks more vulnerable to attacks compared to other traditional wireless networks. Therefore, the security concerns of cognitive radio networks (CRNs) have attracted a great deal of attention in the literature recently to obtain maximum benefits from the technology.

In the literature, several approaches have been proposed to defend against the different types of attacks in CRNs, but the majority of these have focused on specific vulnerabilities along with corresponding traditional countermeasures such as cryptographic measures, secure routing and data aggregation etc. Though some types of conventional attacks in CRNs can be countered by applying such conventional mechanisms, there are some other types of attacks that cannot be countered by them. These are the threats and attacks that are

brought by unreliable or malicious nodes to the CRNs. These type of threats are classified as *soft security threats* and in such scenarios, 'trust' plays an important role to defend against them. In the literature, many solutions have been proposed to address the non-conventional threats of malicious nodes in CRNs by using the notion of trust, but no trust-based mechanisms have been proposed in the literature to maintain secure communication between different nodes in CRNs. Therefore, to address this gap, this thesis is an effort in such a direction to assess, analyse and utilize trust to maintain secure communication in CRNs.

In order to address the problem, this thesis develops a trust-based framework and specific schemes by which trust can be established to solve the security threats brought about by untrustworthy entities. It proposes a framework that authenticates only trustworthy nodes to share spectrum securely and increases CRN availability and reliability by selecting the trustworthy nodes as the key nodes of the CRN. The proposed solutions provide reliable and robust security infrastructure for facilitating secure communications in CRNs. The functionality and features proposed in each approach are validated by experiments and evaluated to highlight the effectiveness of the overall proposed solution.

Acknowledgement

First and foremost, I would like to thank Almighty Allah for His immense blessings bestowed upon me throughout my life and particularly during my PhD.

I would like to express my gratitude and heartfelt thanks to my supervisors, Dr. Omar Khadeer Hussain and Dr. Farookh Khadeer Hussain, for enabling me to complete my Doctoral dissertation under their supervision and their continued support, excellent guidance and encouragement throughout my research. Especially, I am indebted to Dr. Omar Khadeer Hussain. He patiently and gracefully provided advice that was crucial and invaluable for the completion of this thesis and assisted each stage of my study. I want to thank the other members of my thesis committee, including Dr. Song Han and Dr. Jaipal Singh, for their support and advice when I needed them most. I thank Professor Tharam Dillon and Professor Elizabeth Chang for their help and guidance in assisting me to enrol at Curtin University and supporting me during the course of my studies.

I would like to thank my friends, as they deserve a big 'thank you' for sharing with me the simple joys along the way. I thank Dinusha, Olivia, Biming, Jamshaid, Bambang, Naeem, Adil and Lainey for helping me to have such a wonderful time at Curtin University. A special thanks to Zia-ur-Rehman for his continuous help, support and assistance.

A major part of what I am today is credited to my family. I gratefully acknowledge my parents, siblings and parents-in-laws for their affection, prayers, understanding and encouragement. I thank my mother, Rezia Khatun, who always inspired me and encouraged me to embark on higher

studies. I am also grateful and indebted to my husband, Abdullah Al Faruque. He has continuously been a source of strength and courage and has done every possible thing to make this a pleasant and comforting journey. Without his consistent support and motivation, I would not have been able to overcome the difficulties and challenges of this undertaking. To my son, Shafeer Ahmad, thanks to you for being a wonderful source of joy and pleasure. Though you are so young, I am impressed by your level of understanding and support you have demonstrated over the last few months.

Last but certainly not least, I dedicate this thesis to my husband, Abdullah Al Faruque and my son, Shafeer Ahmad, who gave the best of themselves to make sure that we have the best life. Without their sacrifices, I would not have made it this far.

List of Publications

Refereed journal articles arising from this thesis

1. Sazia Parvin, Farookh Khadeer Hussain, and Omar Khadeer Hussain "Multi-Cyber Framework for Availability Enhancement of Cyber Physical Systems", The Computing Journal, Springer, DOI 10.1007/s00607-012-0227-7, 2012. (**ERA Rank A, Impact Factor 0.701**)

2. Sazia Parvin, Farookh Khadeer Hussain, Omar Khadeer Hussain, Song Han, Biming Tian, and Elizabeth Chang "Cognitive radio network security: A survey", Journal of Network and Computer Applications, Elsevier, http://dx.doi.org/10.1016/j.jnca.2012.06.006, 35(6): 1691-1708, 2012. (**ERA Rank A, Impact Factor 1.067**)

3. Sazia Parvin, Farookh Khadeer Hussain, and Omar Khadeer Hussain "Conjoint Trust Assessment for Secure Communication in Cognitive

Radio Networks", Mathematical and Computer Modelling, Elsevier, doi:10.1016/j.mcm.2013.01.001, 2013. (**ERA Rank B, Impact Factor 1.346**)

4. Sazia Parvin, Farookh Khadeer Hussain, Song Han, and Omar Khadeer Hussain "Trust-based Spectrum Sharing for cognitive Radio Networks", Journal of Interconnection Networks, World Scientific, DOI: 10.1142/S0219265911002927, 12(3):155-171, 2011. (**ERA Rank B, Impact Factor 0.12**)

Refereed journal articles related to this thesis

5. Sazia Parvin, Farookh Khadeer Hussain and Sohrab Ali "A methodology to counter DoS attacks in mobile IP communication", Mobile Information Systems, IOS press, DOI 10.3233/MIS-2012-0135, 8(2):127-152, 2011. (**Impact Factor 1.3**)

6. Sazia Parvin, Farookh Khadder Hussain, Jong Sou Park, and Dong Seong Kim "A Survivability Model in Wireless Sensor Networks", Computers and Mathematics with Applications, Elsevier, doi:10.1016/j.camwa.2012.02.027, 64(12):3666-3682, 2012. (**Impact Factor 1.747**)

7. Biming Tian, Song Han, Sazia Parvin, Jiankun Hu, and Sajal Das "Self-healing Key Distribution Schemes for Wireless Networks: A Survey", The Computer Journal, doi:10.1093/comjnl/bxs016, 54(4):549-569, 2011. (**ERA Rank A*, Impact Factor 0.943**)

8. Miao Xie, Song Han, Biming Tian, and Sazia Parvin "Anomaly Detection in Wireless Sensor Networks: A Survey", Journal of Network and Computer Applications, Elsevier, doi:10.1016/j.jnca.2011.03.004, 34(4):1302-1325, 2011. (**ERA Rank A, Impact Factor 1.346**)

9. Biming Tian, Song Han, Liu Liu, Saghar Khadem and Sazia Parvin "Towards enhanced key management in multi-phase ZigBee, network architecture", Journal of Computer Communications, Elsevier, doi:10.1016/j.comcom.2011.12.004, 35(5):579-588, 2012. (**Impact Factor 0.958**)

Refereed conference articles arising from this thesis

10. Sazia Parvin, Farookh Khadeer Hussain, Omar Khadeer Hussain, *Digital Signature-based Authentication Framework in Cognitive Radio Networks*, Proceedings of the 10th International Conference on Advances in Mobile

Computing and Multimedia (MoMM'12), December 3-5, 2012, Bali, Indonesia, pp. 136-142.

11. Sazia Parvin, Farookh Khadeer Hussain, Omar Khadeer Hussain, Mohammad Abdullah Al Faruque, *Trust-based Throughput in Cognitive Radio Networks*, Proceedings of the 9th International Conference on Mobile Web Information Systems (MobiWIS'12), Elsevier, August 27-29, 2012, Canada, Procedia CS 10: 713-720.

12. Sazia Parvin, Farookh Khadeer Hussain, Song Han, Zia Ur Rehman, Abdullah Al Faruque, *A New Identity-based Group Signature Scheme based on Knapsack ECC*, Proceedings of the 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS'12), July 4-6, 2012, Italy, pp. 73-80.

13. Sazia Parvin, Farookh Khadeer Hussain, *Trust-based Security for Community-based Cognitive Radio Networks*, Proceedings of the 26th International Conference on Advanced Information Networking and Applications (AINA-2012), March 26-29, 2012, Fukuoka, Japan, pp. 518-525.

14. Sazia Parvin, Farookh Khadeer Hussain, *Digital Signature-based Secure Communication in Cognitive Radio Networks*, Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA'11), October 26-28, 2011, 10.

15. Sazia Parvin, Song Han, Farookh K. Hussain, and Biming Tian, *A Combinational Approach for Trust Establishment in Cognitive Radio*

Networks, Proceedings of the 5th International Conference on Complex, Intelligent, and Software Intensive Systems(CISIS'11), June 30th-July 2nd, 2011, Seoul, Korea, pp. 227-232.

16. Sazia Parvin, Song Han, Biming Tian, Farookh K. Hussain, *Trust Based Authentication for Secure Communication in Cognitive Radio Networks*, Proceedings of the 6th IEEE/IFIP International Symposium on Trusted Computing and Communications (TrustCom'10), December 11-13, 2010, Hongkong, pp.589-596.

17. Sazia Parvin, Song Han, Farookh Khadeer Hussain, Mohammad Abdullah Al Faruque, *Trust based security for cognitive radio networks.* Proceedings of the 12th International Conference on Information Integration and Web-based Applications and Services (iiWAS'10), November 8-10, 2010, Paris, France, pp. 743-748.

18. Sazia Parvin, Song Han, Biming Tian, Miao Xie, *Authenticated Spectrum Sharing for Secondary Users in Cognitive Radio Networks*, Proceedings of the 2nd IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC'10), September 24-26, 2010, Beijing, Chaina, pp.509-513.

19. Sazia Parvin, Song Han, Li Gao, Farookh Hussain,Elizabeth Chang, *Towards Trust Establishment for Spectrum Sensing in Cognitive Radio Networks*, Proceedings of the 24th Annual Conference of the IEEE Advanced Information Networking and Applications(AINA'10), April 20-23, 2010, Perth, Australia, pp. 579-583.

Refereed conference articles related to this thesis

20. Biming Tian, Song Han, Sazia Parvin, Miao Xie, *Generalized hash-binary-tree based self-healing key distribution with implicit authentication.* Proceedings of the 7th International Wireless Communications and Mobile Computing Conference (IWCMC'11), July 4-8 2011, Istanbul, Portugal, pp. 213-219.

21. Biming Tian, Song Han, Sazia Parvin, Tharam S. Dillon, *A Key Management Protocol for Multiphase Hierarchical Wireless Sensor Networks*, the 6th IEEE/IFIP International Symposium on Trusted Computing and Communications (TrustCom'10), December 11-13, 2010, Hongkong, pp.617-623 .

22. Li Gao, Elizabeth Chang, Sazia Parvin, Song Han, *A Secure Key Management Model for Wireless Mesh Networks*, Proceedings of the 24th Annual Conference of the IEEE Advanced Information Networking and Applications(AINA'10), April 20-23, 2010, Perth, Australia, pp. 655-660.

23. Sazia Parvin, Sohrab Ali, Jaipal Singh, Farookh Hussain, Song Han, *Towards DoS Attack Prevention based on Clustering Architecture in*

Mobile IP, Proceedings of the 35th Annual Conference of the IEEE Industrial Electronics Society (IECON'09) , November 3-5, 2009, Porto, Portugal, pp. 3183-3188.

24. Sazia Parvin, Shohrab Ali, Song Han, Tharam.S.Dillon, *Security against DoS Attack in Mobile IP Communication*, Proceedings of the 2nd International ACM Conference on Security of Information and Networks (SIN'09), October 6-10, 2009, Gazimagusa, North Cyprus, pp.152-157.

Chapter 1

Introduction

1.1 Introduction

With the advancement of Information Communication Technologies, there has been an exponential growth in mobile computing and the number of interconnected digital devices in the world. Depending upon their location, most of these devices communicate with one another wirelessly by using distribution mechanisms and radio spectrum bands. As a result, there is an ever-increasing demand for spectrum to support such growth of wireless communication devices by orders of magnitude over the next decade. This problem must be addressed via technology and regulatory innovations for significant improvements in spectrum efficiency and increased robustness and performance of wireless devices [1]. Keeping this in view, the Federal Communications Commission (FCC) has considered making the unused licensed spectrum available to unlicensed users to continue smooth operation [2]. Having this unused licensed spectrum usage will allow unlicensed users to use the empty spectrum, under the condition that they cause no interference

to licensed users.

To address the problem of spectrum shortage, cognitive radio was pioneered by J.Mitola [3] from software defined radio (SDR) [4] to improve spectrum utilization. Cognitive radio is a new research area for wireless communication in which either a network or a wireless node is able to change its transmission or reception parameters to communicate efficiently by avoiding interference with either licensed or unlicensed users [5]. Cognitive radio allows nodes to find opportunities for communication using the "spectrum holes"and transports the packets of communication on top of cognitive radio links in order to successfully facilitate useful applications and services [6]. A cognitive radio node senses available spectrum, occupies it for communication and vacates the spectrum on sensing the return of the licensed user. A mobile terminal with cognitive radio communication capabilities can always ***sense*** the communication environments (e.g. spectrum holes, geographic location, available wire/wireless communication system or networks, and available services), ***analyze*** the environment and ***learn*** information from the environment with the user's requirements and ***reconfigure*** itself by adjusting system parameters to conform to certain policies and regulations. Cognitive radio nodes and the radio links form the cognitive radio network (CRN) which uses several factors for active monitoring, either in the external or internal radio environment, such as radio frequency spectrum, user behavior and network state. In the literature, the future wireless network is termed the 'cognitive radio network' (CRN), which is quite consistent with Haykins's definition of cognitive radio [4]: "*Cognitive radio is an intelligent wireless communication system that is aware of its surrounding environment (i.e.,*

outside world), and uses the methodology of understanding-by-building to learn from the environment and adapt its internal states to statistical variations in the incoming RF stimuli by making corresponding changes in certain operating parameters (e.g., transmit power, carries-frequency, and modulation strategy) in real time, with two primary objectives in mind: highly reliable communication whenever and wherever needed and efficient utilization of the radio spectrum".

Even though a CRN is a wireless communication network, there are several differences between cognitive and traditional non-cognitive wireless networks. One notable difference between them is that nodes in CRNs need to be aware of the dynamic environment, find a suitable frequency band for their operation and adaptively adjust their operating parameters based on the interactions with the environment and other users in the network. This is contrary to nodes in the traditional wireless network which cooperate unconditionally in a static environment for spectrum sharing and other management approaches [7]. In other words, the major difference between the CRN and the traditional wireless network is that it doesn't operate on a fixed frequency spectrum i.e. the frequency spectrum is being used dynamically [8]. However, such features are beneficial and advantageous in certain studies. Figure 1.1 shows a basic difference between wireless networks and CRNs, where in CRN, a cell phone is able to identify a newly available communication cell through spectrum opportunistic access to communicate and establish a connection with other nodes in an emergency situation whereas it is not possible for a cell phone in a traditional wireless network to identify a newly available communication cell and establish a connection to make a call. This is achieved by the sense,

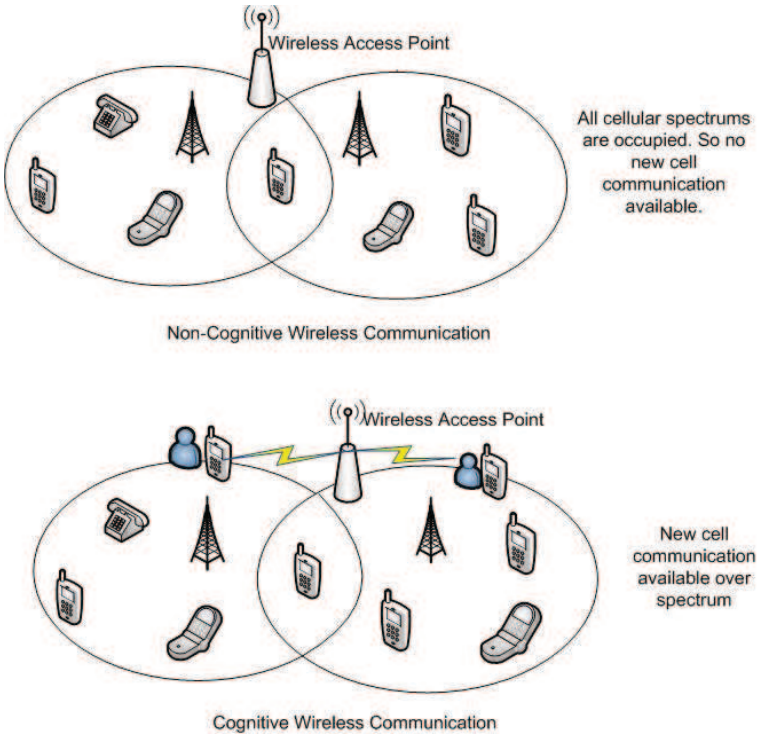

Figure 1.1: Difference between wireless networks and CRNs

understand, adapt and decide capability of CRN. This is explained further in the next section.

1.2 Characteristics of CRNs

1.2.1 CRN working process

As mentioned in Section 1.1 and as shown in Figure 1.2, a cognitive radio senses the environment (cognitive capability), then analyzes and understands the sensed information (self-organized capability), makes decisions (decision capability) and adapts to the environment (reconfigurable capabilities). In this subsection, for completeness, an overview is given of the different features

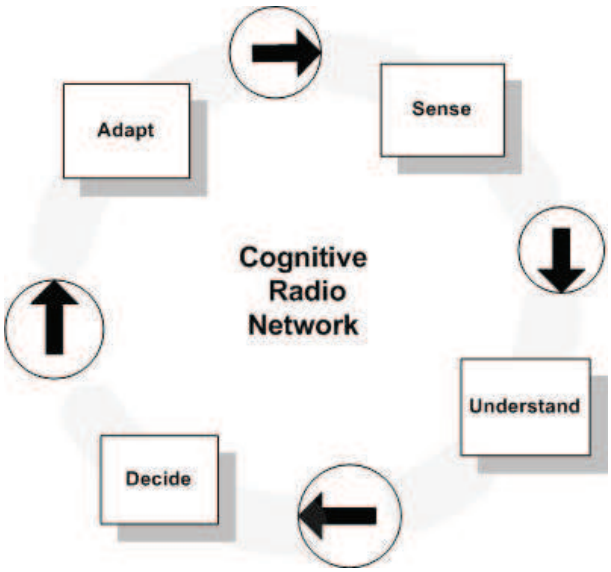

Figure 1.2: Working process of CRNs

that come under each functionality.

1.2.1.1 Sense (Cognitive capability)

In this section, an overview of the various sensing capabilities of a CRN is given.

- *Spectrum Sensing* : Spectrum sensing is a mechanism that allows a cognitive radio node to sense spectrum by adopting different sensing techniques [9–15] and detect "spectrum holes" which are those frequency bands not used by licensed users or which have limited interference with the surrounding nodes in the network.

- *Spectrum Sharing*: Spectrum sharing is a mechanism that helps to share spectrum by adopting different sharing techniques [7, 16, 17]under different terms of agreement and policies between a licensee and a third party without the need for prior agreement between all parties.

- *Location Identification*: Location identification is a mechanism that allows a cognitive radio node to select the appropriate operating parameters, such as power and frequency, depending on various location technologies [6, 18, 19] to avoid interference.

- *Network/System and Service Discovery*: Network/system discovery is a mechanism that enables a cognitive radio node to discover the available networks around it to communicate between nodes via either directed one-hop communication or multi-hop relay nodes [6]. Service discovery mechanisms [20] that allows a cognitive radio terminal to discover a service by identifying nearby Bluetooth, WiFi devices.

1.2.1.2 Understand (Self-Organized capability)

In this section, an overview of the various self-organizing capabilities of CRNs is presented. Like wireless sensor networks (WSNs), CRNs have a limited availability of energy supply and hence the CR nodes need to cooperate and self-organize to provide smooth network operation by going into idle/sleep mode and giving permission to other nodes to use the unused spectrum [21]. This is done by using the self-organizing capability of CRNs. The features that come under this functionality are :

- *Spectrum/Radio Resource Management:* Spectrum management is a process that allows cognitive radio nodes to manage and organize spectrum holes information between them by adopting a reputed model such as the Preemptive Resume Priority (PRP) M/G/1 queuing model [22].

- *Mobility and Connection Management:* Mobility and connection

management is a technique that allows cognitive radio nodes to detect the available Internet access and support vertical hand-offs to select routes and networks [6].

- *Trust/Security Management:* Trust/security management is a technique which enables cognitive radio nodes to defend different types of attacks introduced by the various heterogeneities nature of CRNs (e.g. wireless access technologies, system/network operators). Security becomes a very challenging issue in CRNs as different types of attacks are very common to cognitive radio technology compared to the general wireless network. In this case, trust is a prerequisite for securing operations in CRNs. Different trust-based approaches are used in CRNs for better performance.

1.2.1.3 Decide (Decision capability)

Decision capability enables unlicensed users to select a reasonable spectrum channel from the licensed users, based on spectrum characteristics and other quality of service (QoS) requirements. So, it is very important to have a sound understanding of the CRN's fundamental precondition before deployment with a view to ensure reliable outcomes of the decision making process. Zheng and Cao in [23] proposed a device-centric spectrum management scheme, and five spectrum decision rules to regulate users' access, trading off fairness, utilization with communication costs, and algorithm complexity.

1.2.1.4 Adapt (Reconfigurable capability)

Reconfigurable capability aims to enable the radio to be dynamically programmed according to the radio environment and change the appropriate operating frequency by selecting frequency agility, adaptive coding and transmit power control for smooth communication[6] and to detect signals from other radio frequency systems to avoid co-channel interference [24].

In the next subsection, the basic architecture of CRN and the different network architectures for communication is discussed.

1.2.2 CRN architecture

A CRN is formed by a group of users (nodes/stations) who collaborate to share a frequency band by using cognitive radio. CRN consists of various kinds of communication systems and networks, and can be viewed as a heterogeneous network. The basic components of CRNs shown in Figure 1.3 are as follows:

- **Mobile Station (MS)**: A mobile station is the normal wireless node equipped with a cognitive capability of cognitive radio for communication with a mobile network. There are two types of mobile stations (users): Primary User (PU) and Secondary User (SU). The PU is the licensed user of a particular radio frequency band and the SU is an unlicensed user who cognitively operates without causing harmful interference to the PU [25].

- **Base Station/Access Point (BS/AP)**: An access point (AP) is a device that allows wireless devices to connect to a wired or wireless network using Wi-Fi, or related standards. There are two types of base

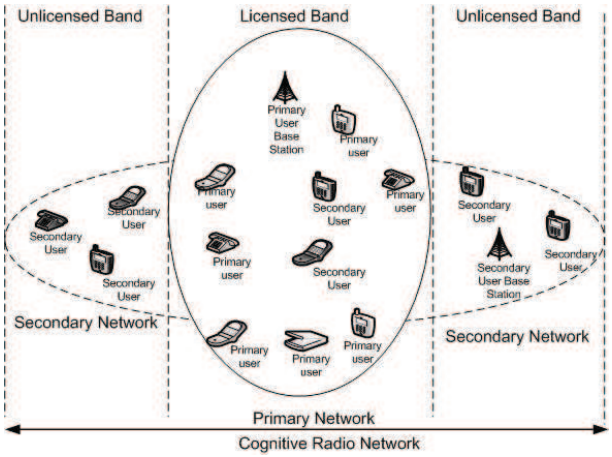

Figure 1.3: Basic architecture of CRNs

stations: the Primary User Base Station (PUBS) and Secondary User Base Station (SUBS).

- **Backbone/ Core Networks**: A backbone or core network is the central part of a communication network that provides various services to the users who are connected by the access network

These three basic components of CRN communicate with each other by using any of the following network architecture [6]:

1.2.2.1 Infrastructure architecture

In the infrastructure architecture, as shown in Figure 1.4, an MS can access a BS/AP only in a one-hop manner. MSs under the transmission range of the same BS/AP communicate with each other through the BS/AP. Communications between different cells are routed through backbone/core networks. The BS/AP may be able to execute one or multiple communication standards/protocols to meet different demands from MSs.

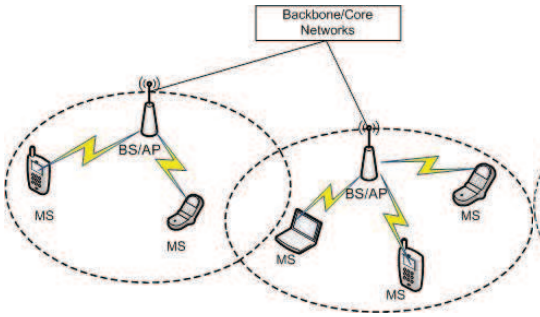

Figure 1.4: Infrastructure architecture

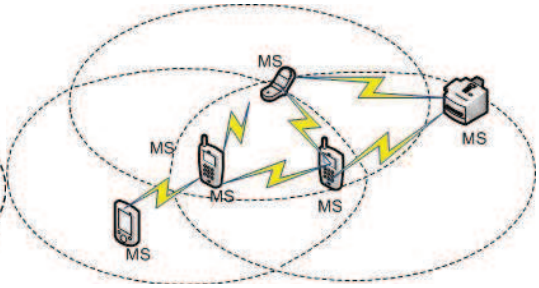

Figure 1.5: Ad-hoc architecture

1.2.2.2 Ad-hoc architecture

In ad-hoc architecture, there is no infrastructure backbone. If an MS recognizes that there are other MSs nearby and are connectable through certain communication standards/protocols, they can set up a link with both licensed and unlicensed users [26] and thus form an ad-hoc network such as cognitive maritime wireless ad-hoc network [27].

1.2.2.3 Mesh architecture

This architecture, as shown in Figure 1.6, is a combination of infrastructure and ad-hoc architectures by enabling the wireless connections between BSs/APs, which is similar to the Hybrid Wireless Mesh Networks [6].

The abovementioned architecture shows how the different nodes in a CRN communicate with each other. Within each node, the communication process goes through different layers as presented in the next subsection.

1.2.3 Layered architecture of CRN

The standard layered network architecture is usually used with some additional modules to convert it into an architecture for the CRN.

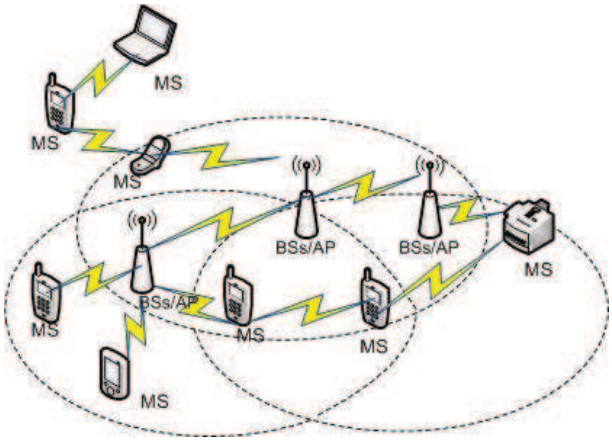

Figure 1.6: Mesh architecture

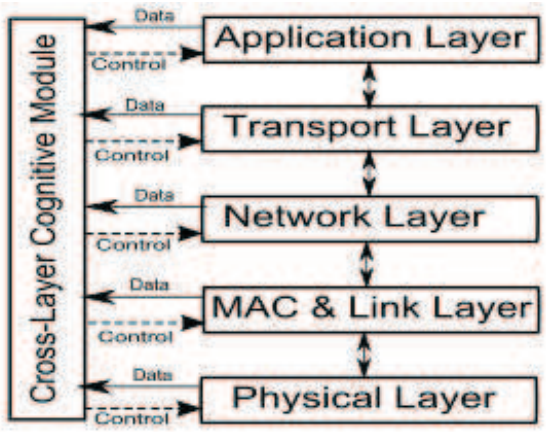

Figure 1.7: Standard layered architecture for CRNs [28]

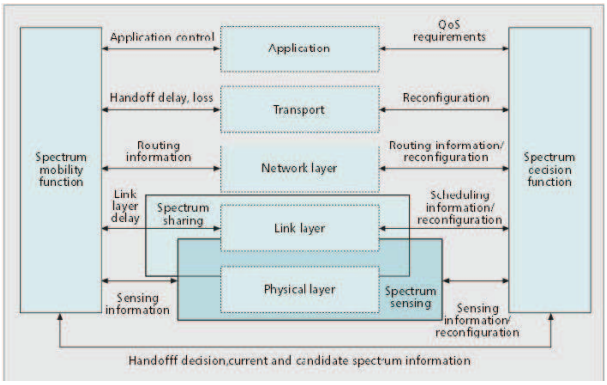

Figure 1.8: Main functions of different protocol layers in CRNs [29]

As shown in Figure 1.7, the cross-layer approach adds a new module to the existing layered network architecture for incorporating cognitive functions of all the layers [28].

Descriptions and key functionalities of different protocol layers of a CR node are as follows:

- Physical Layer: This layer is the lowest layer in the layered architecture and the essential component that enables CR users to identify a spectrum hole [30].

- Link Layer: This layer is responsible for transferring data from one node to other in a single hop. Specific tasks such as sensing scheduling, sensing-access tradeoff design, spectrum-aware access control etc. are performed by this layer of a CR node.

- Network Layer: The main objective of the network layer is end-to-end packet delivery. Functions of the network layer are spectrum-aware routing, flow control, error control and ensuring quality of service (QoS).

- Transport Layer: This is responsible for transferring data between two

end hosts. It is responsible for flow control, congestion control and end-to-end error recovery, reconfiguration and hand-off delay.

- Application Layer: This is the top most layer of the protocol stack. Protocols that run at the application layer completely rely on the services provided by the underlying lower layers.

The key functions of different protocol layers in CRNs are shown in Figure 1.8.

1.2.4 Application scenarios of CRNs in real-life applications

In the literature, CRNs have been applied in various real-life applications, as shown in Figure 1.9. Some of the applications are as follows:

- **Emergency Management or Disaster Recovery:** Cognitive radio resolves problems in disaster situations [31, 32] by providing a significant amount of bandwidth through Opportunistic Spectrum Access [33].
- **Search and Rescue:** The GPS capability of cognitive radio helps to rescue the person by establishing a short range communication link, like a beacon, without any central control [31, 34].
- **Mining:** CR chooses an appropriate waveform to establish a clear signal between the adverse environment in the mine and the outside world [31].
- **Traffic Control:** Cognitive sensors at each signal location gather traffic information and make appropriate decisions locally or via a central location and send an alternate route to the mobile user [31].

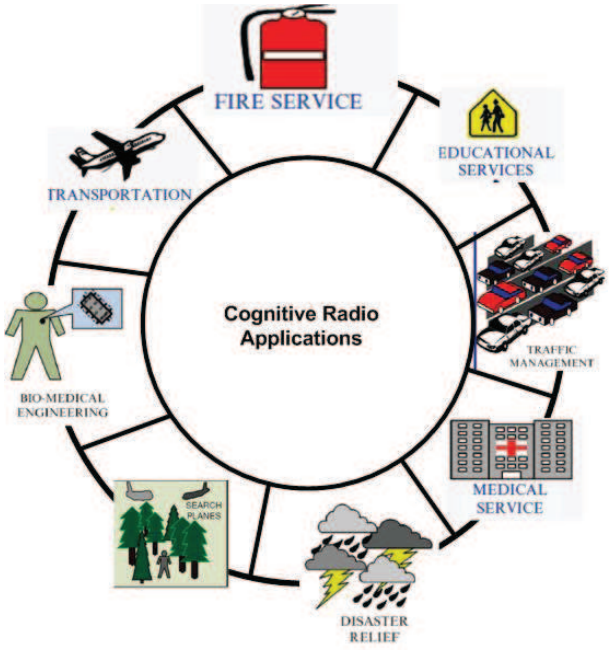

Figure 1.9: Cognitive radio applications

- **Medical Applications:** Cognitive radio uses cognitive ID tags to intelligently detect abnormal tissues or blood cells in a human body and intelligently inform the respective authority to take appropriate action [31].

- **Public Safety Networks:** A public safety CRN provides a substantially improved communication by providing more bandwidth through Opportunistic Spectrum Access and allows interpretability across different public safety services [33, 35].

These applications show the enormous advantages that CRN provides in real-life applications. But apart from these advantages, an important consideration for users to consider is the notion of security, as CRNs are susceptible to various security threats and attacks. Therefore, proper security mechanisms have to be used in order to keep networks secure. In the next

section, the different security threats and attacks and the security requirements that are needed to address these threats are described.

1.3 Security Challenges in CRNs

As mentioned in Section 1.1, CRNs are more flexible and exposed to wireless networks compared to other traditional radio networks. Hence, there are many security threats to CRNs because of their special characteristics, such as intelligence functionality and dynamic spectrum access application, more so than other traditional radio environments. Since cognitive radios can adapt to their environment and change how they communicate, it is crucial that they select an optimal and secure means of communication. Several survey papers [36–40] have presented an analytical survey for the detection of several attacks in CRNs and examine only a small number of general security requirements of CRNs. In the next subsection, some of the security threats for CRNs are summarized.

1.3.1 Security threats in CRNs

- **Sensing Problem Threats:** Cognitive radio technology provides more opportunities for attackers due to its intrinsic nature. For example, spectrum sensing is a key characteristic used in CRNs, which scans a certain range of the spectrum to detect unoccupied spectrum [29, 41, 42]. Through this process, an unlicensed user can determine whether the radio can be used. However, if the spectrum sensing result is modified maliciously, normal network activities will be disabled; it is possible that all network traffic may collapse. Other types of threats include spectrum

decision threats, spectrum sharing and spectrum mobility threats.

- **Hidden Terminal Problem Threats:** Another important challenge facing a cognitive radio system is to identify the presence of PUs over a wide range of spectrum [42]. This process is very difficult as different modulation schemes, employed by PUs, need to be identified. There is also a need to identify different data rates and transmission powers in the presence of variable propagation losses, interference generated by other SUs, and thermal noise. For example, if the channel between the primary transmitter and the sensing device is under a deep fade, it is possible that the sensing device may not detect the primary signal. As a result, the cognitive radio might transmit a signal in the corresponding PU band, causing interference to the nearby primary receiver. This issue is commonly referred to as the *Hidden Terminal Problem.*

- **Policy Threats:** In order to communicate more effectively in an intelligent way, a cognitive radio node needs policies for reasoning in different environments or under different conditions. Two types of threats which are possible in the use of policies [36] are :(1) policies may be modified by attackers who can obtain control of a CR, or obtain permission from the policy database administration to modify the internal policies; and (2) false policies also lead to security threats so that attacker can try to inject false policies into the CR policy database and thereby cause interference.

- **Learning Threats:** Some CRs are designed with the capability of learning. These CRs can learn from past experiences or current situations to predict the future environment and select optimal operations. But

attackers can modify past statistics or spoof current conditions to prevent the CR from predicting accurately [43].

- **Parameter threats:** An attacker can manipulate a CR to behave maliciously and alter the parameters to conduct sub-optimal operations for CRNs [36].

Apart from these overall threats, a CRN is also susceptible to various threats and attacks on the protocol layers of CRN during communication. This is explained in the next subsection.

1.3.2 Security attacks on protocol layers in cognitive radio node

In this subsection, the attacks on various protocol layers of a cognitive radio node are described. The motivations for attacks on CRNs are discussed in [38], which classifies the motivation into two broad categories namely: selfish attack and malicious attack [44].

1. Selfish Attack: A selfish attack occurs in a situation where the attacker wants to use the spectrum with higher priority. This attack meets its target by misleading other unlicensed users to believe that he is a licensed user. As a result, the adversarial user can occupy the spectrum resource as long as it wants. Since this selfish behaviour does not obey the spectrum sharing scheme [29], this attack is called a selfish attack. The CR network is vulnerable to selfish attacks, where selfish SUs increase their accessing probability by changing the transmission parameters to

Protocol Layers	Attacks
Physical Layer	International Jamming Attack; Primary Receiver Jamming Attack; Sensitivity Amplifying Attack; Overlapping Secondary User Attack; Primary User Emulation Attack; Objective Function Attack; Common Control Data Attack
Link Layer	Spectrum Sensing Data Falsification Attack; Denial of Service Attack; Biased Utility Attack; Asynchronous Sensing Attack; False Feedback Attack; Fabrication Attack
Network Layer	Resource Hungry Attack; Network Endo-Parasite Attack; Channel Ecto-Parasite Attack (CEPA); Low cOst Ripple effect Attack (LORA)
Transport Layer	Key Depletion Attack; Jellyfish Attack; Lion Attack; DoS Attack
Application Layer	Any attack on physical, link, network or transport layers impact adversely on the application layer as application layer is the final layer of the communication protocol stack.

Table 1.1: Attacks on different protocol layers in CRNs

enhance their own utilities by degrading the performance of other users that, in turn, degrades the CR network's performance.

2. Malicious Attack: A malicious attack means that the adversary prevents other unlicensed users from using the spectrum and causes a denial of service (DoS). As a result, a malicious attack will drastically decrease the available bandwidth and break down the whole traffic and turn the cognitive radio into a jammer.

There are different types of attacks that come under each category. The different types of attacks are named in Table 1.1 and a description of these attacks is given in Table 1.2. It is important to note that the abovementioned threats and attacks in Table 1.2 are not exhaustive and it is quite possible that with the advent of new threats, there may be a new requirement that needs to be improved to ensure the security in CRNs. In the next subsection, an overview of security requirements that need to be established to facilitate and enhance secure communication in CRNs is given.

Name of Attack	Description
Intentional Jamming Attack	The malicious SU jams PU and other SUs by intentionally and continuously transmitting in a licensed band [39]
Primary Receiver Jamming Attack	This attack occurs whenever a malicious entity closer to the victim primary receiver participates in a collaborative protocol and requests transmissions from other SUs to be directed towards the malicious user [39]
Sensitivity Amplifying Attack	A malicious entity can amplify the sensitivity and hence increases the number of missed opportunities and false detections by replaying the primary transmissions [39]
Overlapping Secondary User Attack	In both centralized and distributed architectures in CRNs, multiple secondary networks may coexist over the same geographical region [39]
Primary User Emulation Attack	The attacker may jam the licensed band and emulate the PU, thereby limiting the CRN to operating in the unlicensed bands and limiting CRN capacity [36]
Objective Function Attacks (OFA)	An adversary forces a radio to use some high security level, thus the system's objective function decreases
Common Control Channel Jamming	The attacker transmits periodical pulses in the control channel spectrum and blocks probable communication between all cognitive radio nodes
Spectrum Sensing Data Falsification Attack	An attacker may send false local spectrum sensing results to a data collector, causing the data collector to make a wrong spectrum sensing decision in CRNs [45]
Denial of Service Attack	The attackers generate sensing results showing that the PU spectrum band is occupied by PUs. If their sensing results are aggregated into the final decision making process without proper filtering, they could adversely influence the final decision, resulting in false alarm errors and a loss of opportunity to utilize the PU spectrum bands when they are actually available [46]
Biased Utility Attack	A malicious SU may intentionally tweak parameters of the utility function to increase its bandwidth [39]
Asynchronous Sensing Attack	A malicious SU may transmit asynchronously instead of synchronizing the sensing activity with other SUs in the network during sensing operations
False Feedback Attack	In CRNs, false feedback from one or a group of malicious user could make other SUs take inappropriate action and violate the terms of the protocol
Fabrication Attack	A malicious SU deliberately reports inverted sensing results to a SU base-station (SUBS) all the time and causes deterioration to the overall performance of all the CRNs [46]
Resource Hungry Attack	Malicious SUs always report to SUBS that the PU spectrum band is not in use and this misdetection introduces undue interference to PU using the same spectrum band
Network Endo-Parasite Attack (NEPA)	In CRNs, the malicious nodes attempt to increase the interference at a heavily loaded high priority channel but the neighbors are not informed about the change [41]
Channel Ecto-Parasite Attack (CEPA)	In CRNs, a compromised node launches CEPA by switching all its interfaces to the channel that is being used by the highest priority link [41]
Low cOst Ripple effect Attack (LORA)	Misleading information about spectrum assignments is transmitted to all the neighbors to push the network into a quasi-stable state [41]
Key Depletion Attack	Transport layer sessions in CRNs last only for a short duration because of frequently occurring retransmissions in the network [39]
Jellyfish Attack	An attacker causes the cognitive node to switch from one frequency band to another frequency band, thereby causing considerable delay in the network and transport layers and reduces the throughput of the TCP protocol [39]
Lion Attack	Lion attack actually causes the jamming to slow down the throughput of the Transmission Control Protocol by forcing frequency handoff [47]

Table 1.2: Name and description of different attacks in CRNs

1.3.3 Security requirements in CRNs

As is the case in any interacting and facilitating medium, security in CRNs is vital to ensure secure communication in CRN [37]. Although security requirements may vary in different application environments, there are, in fact, general requirements that provide basic safety controls, as follows [38]:

- **Access Control:** Access control is a security requirement for the physical layer. Users must be guaranteed to have access to the network, and they must obey their organization's policy. Since different SUs coexist in CRNs, collisions may happen if they simultaneously move to and use the same spectrum band, according to their spectrum sensing results [48]. Thus, an access control property should coordinate the spectrum access of different SUs to avoid collisions.

- **Integrity:** Data that is in transit in the network needs to be protected from malicious modification, insertion, deletion or replay. Integrity is extremely important in a wireless network because, unlike their wired counterparts, the wireless medium is easily accessible to intruders. Hence, in wireless local area networks (WLANs), an additional layer of security is added at the link layer to make the wireless links as secure as wired links. The security protocol used in this layer is called the CCMP [49] (counter-mode encryption with CBC-MAC authentication protocol). The CCMP protocol uses a state-of-the art advanced encryptions standard (AES) [50] in cipher block chaining mode [51] to produce a message integrity check. Data integrity can be achieved by applying higher cryptographic techniques in CRNs.

- **Confidentiality:** Confidentiality is closely related to integrity. While integrity ensures that data is not maliciously modified in transit, confidentiality ensures that the data is transformed in such a way that it is not understood to an unauthorized entity [39]. This issue is even more pronounced in CRNs, where the SU's access to the network is opportunistic and spectrum availability is not guaranteed [39].

- **Authentication:** The primary objective of an authentication scheme is to prevent unauthorized users from gaining access to protected systems [39]. In CRNs, there is an inherent requirement to distinguish between PUs and SUs. Therefore, authentication can be considered as one of the basic requirements for CRNs. The authentication problem occurs in CRNs in the situation when a receiver detects signals at a particular spectrum, but is not sure if the signal has infact been sent by the primary owner of the spectrum or not. This situation outlines the authentication problem in CRNs. Tan et al. [52] mentioned that it is impossible to conduct authentication in CRNs other than on the physical layer. For example, a cognitive radio receiver may be able to receive signals from TV stations, process them at the physical layer, but it may lack the component to understand the data in the signals. Therefore, if the authentication depends on the correct understanding of the data (done at upper layers), the cognitive radio receiver will be unable to authenticate the PU. Tan et al. [52] proposed a method that allows PUs to add a cryptographic link signature to its signal, so the spectrum usage by PUs can be authenticated. Zhu et al. [53] proposed an authentication mechanism for CRNs which is based on third-party

Certification Authority (CA). However, in CRNs with a number of SUs dispersed over a large geographical area, providing the functionalities of a CA can be quite challenging [54].

- **Identification.** Identification is one of the basic security requirements for any communication device. It is a method whereby an user is associated with his name or identity [39]. For example, in cellular networks, the mobile devices are provided with an equipment identification device called an international mobile equipment identifier (IMEI). A tamper-proof identification mechanism is built into the SU (unlicensed) devices in CRNs. Miller et al. [20] described identification in CRNs, saying that it would be advantageous for a CR to know how many networks exist, how many users are associated with each network, and even certain properties about the devices themselves. To achieve this level of information, it is essential for a cognitive radio to gather an accurate picture of the RF (Radio Frequency) environment. CRs identify different network services (e.g. Bluetooth, WiFi), and devices. Service discovery and device identification provide the necessary building blocks for constructing efficient and trustworthy CRNs [20].

- **Non-repudiation:** Non-repudiation techniques prevent either the sender or receiver from denying a transmitted message. In a cognitive radio ad-hoc network setting, if malicious SUs violating the protocol are identified, non-repudiation techniques can be used to prove the misbehavior and disassociate/ban the malicious users from the secondary network [39]. The proof that an activity has already happened should be available in CRNs.

- **Availability:** Availability refers to the ability of PUs and SUs to access the spectrum in CRNs. For PUs, availability refers to the ability to transmit in the licensed band without harmful interference from the SUs. From the definition of dynamic spectrum access policies [2], spectrum availability for PUs is guaranteed. For SUs, availability refers to the existence of chunks of spectrum, where the SU can transmit without causing harmful interference to the PU. In CRNs, one of the important functions of this service is to prevent energy starvation and denial of service attacks, as well as misbehaviour, such as selfishness [45].

The various types of attacks described in subsection 1.3.2 are classified depending on whether their goal is to compromise the confidentiality of stored data, alter the integrity of such data or disrupt the availability of the victim communications. Table 1.3 shows different attacks according to their impact on the basic CIA (Confidentiality, Integrity, Availability) security model.

In the next section, the importance of trust management in the defense against various security threats to enhance secure communication in CRNs is described.

Name of Attacks	Confidentiality	Availability	Integrity
PUEA	✓	✓	
OFA	✓	✓	✓
False Feedback Attack		✓	
Lion Attack		✓	
On-Off Attack			✓
DoS Attack		✓	✓
Resource Hungry Attack		✓	✓
Fabrication Attack			✓
Primary Receiver Jamming Attack		✓	
CCDA	✓		
Biased Utility Attack		✓	
SSDF			✓
International Jamming Attack		✓	
Key Depletion Attack		✓	
NEPA		✓	
CEPA		✓	
LORA		✓	
Jelly Fish Attack	✓		

Table 1.3: Scope of attacks

1.4 Importance of Trust Management for Ensuring CRN Security

Security threats to CRNs can be categorized into two, namely ***hard security*** issues and ***soft security*** issues. Hard security issues are traditional threats from outside users which aim to disrupt the normal functioning of the network. Soft security issues are traditional threats from inside users with the same aim i.e. to disrupt the normal functioning of the network, namely authentication, integrity and availability. However, the issues related to both these security categories are different and hence need to be addressed in order to improve the authentication, integrity and availability of the CRN and ensure a secure communication platform in CRN. But it is not easy to implement security defences in CRNs. One of the major obstacles in deploying security on CRNs is that the current CRNs have limited computation and communication

capabilities and resource constraints such as power and memory [55] and it is impossible to manually replace the battery due to the unattended nature and hazardous sensing of environments. The constraints make the provision of adequate security countermeasures even more difficult.

In such situations, 'trust' is an important concept to defend against soft security threats in CRNs, especially when authentication has to be achieved to ensure secure communication on the basis of believing that an SU using the PU's spectrum will not cause interference to the PU. In the literature, the notion of trust is defined in two ways: the first one is related to the notion of 'trusted computing' which is formed by an alliance of Microsoft, Intel, IBM and HP in providing a platform which can not be tampered with, and where the applications can communicate securely with each other [56]. In the context of trusted computing, trust refers to the interacting entity accepting the provided security mechanisms adopted by the other entity in the interaction by which it feels safe and not vulnerable to the outside forces which might hamper its interaction. The other notion of trust is related to the level of confidence that an entity has in the other entity's ability to achieve its desired outcomes through the communication. The role of trust in this context is defined in CRNs as the belief that the security of a network will not be compromised as a result of a user's action after that user is permitted to share the PU's free spectrum. Ensuring authentication by establishing and understanding trust relationships among different CR nodes is the foundation to implement security in CRNs. Having such a trust-based authentication mechanism allows only non-malicious SUs to gain access to the licensed spectrum and network resources, thereby playing a complementary role in improving the overall

security and creating a balance in the whole CRN. In other words, having a trusted relationship among nodes assists security for improving the overall performance of the CRN. Figure 1.10 shows how trust is used to protect soft security issues in CRNs.

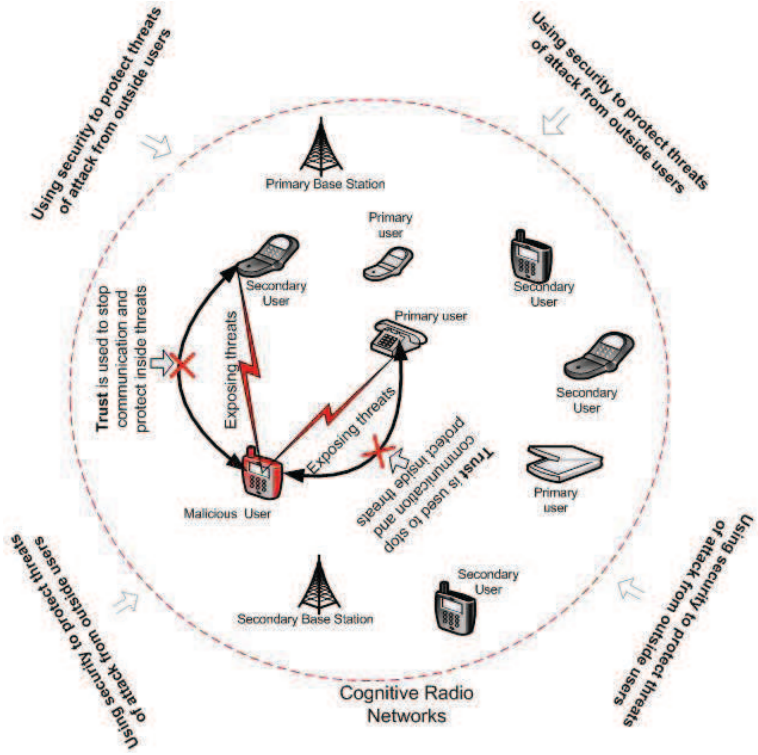

Figure 1.10: Defense of soft security issues using trust

However, the unique characteristics of CRNs render the trust management schemes of wired and general wireless networks ineffective to be applied in such instances. With this in mind, some researchers have begun to safeguard CRNs with simplified and lightweight trust management mechanisms. Compared with general trust management schemes, lightweight trust management schemes provide security support with reduced overhead and thus are more suitable for CRNs. Although considerable developments have been made in trust management in general wireless networks, and researchers have begun

to study the trust mechanism in CRN, most of them use it to solve only one problem in certain processes instead of designing it to address from the overall demand for CRN, hence research for the trust mechanism in CRN is still in its infancy, and there is no complete trust management system for building, assessment, and updating as yet. The position of trust management in a general secured system is shown in Figure 1.11.

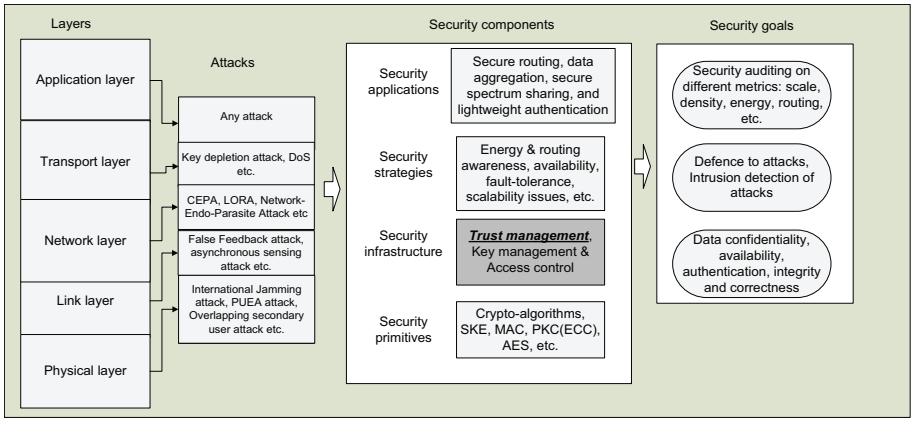

Figure 1.11: Position of trust management in a secured system architecture

However CRNs are application-specific networks. Except for some common features, a CRN for a specific application has some unique features and correspondingly, has some unique security requirements. The solution proposed for one particular application is unlikely to be readily applicable to another environment. Suppose a cognitive radio-based sensor network is deployed in the military surveillance environment and another in an agricultural base; the requirements of security would be different, based on the resource that the nodes possess and the risks they face. It is impossible to reach a one-fits-all trust management solution. Trust management, including trust establishment, trust update, and trust revocation, is much more challenging in mobile networks than in traditional centralized environments [57]. For

example, collecting trust information or evidence to evaluate trustworthiness is difficult due to mobility induced changes in network topology. To date, there has been no comprehensive analysis or discussion of security threats caused specifically by cognitive radio techniques and the special characteristics of cognitive radio in CRNs and there are still several gaps in CRNs research which have not yet been addressed, resulting in there being no effective defense mechanism against attacks in CRNs, as well as no guideline for the selection of defense mechanisms. Theses issues motive me to propose a comprehensive defense mechanism by incorporating trust to enhance secure communication in CRNs.

SUs in CRNs cooperate with each other to make decisions in the spectrum sensing and the channel allocation process, so SUs should be trustworthy to PUs. In other words, the PUs need be provided with a trust guarantee by the SUs. However, some untrustworthy, selfish and malicious users may send false data or falsify the sensing data to damage the profits of the other legitimate second users. These problems can be overcome by using trust and reputation management-based security schemes to make the CRN much more robust and secure by ensuring secure data transfer, authentication, secure data aggregation, secure resource sharing etc., as shown in Figure 1.12.

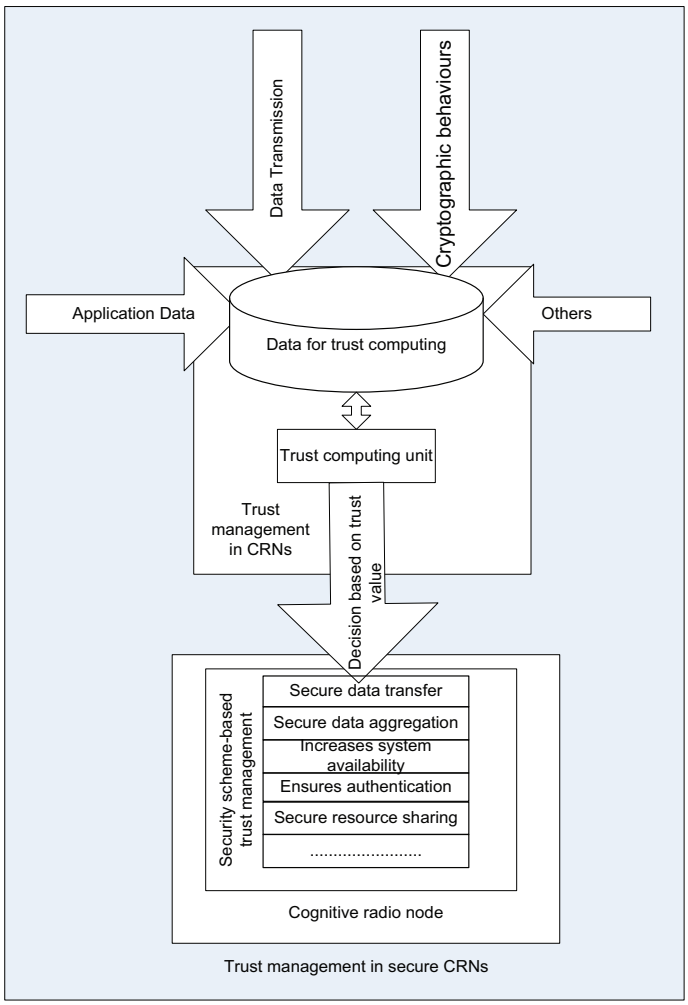

Figure 1.12: Architecture of trust management in secured CRN

Therefore, security in CRNs is a particularly challenging task and attracts great interest from researchers world-wide. One of the ways by which some of the security issues can be solved is by using the notion of trust. In the next subsection, the gaps in the research into improving the security of CRNs from the view point of trust are discussed.

1.5 Research Gaps in CRN Security

In this section, the current popular research interest in CRN security is reviewed. It is important to note that this section only lists the current hot research topics in the field of CRN security and highlights the importance of trust management in the whole security framework, rather than giving a comprehensive coverage of existing security techniques currently being researched.

1.5.1 Trust management

Trust management can solve some problems in CRNs that traditional cryptographic security mechanisms cannot deal with. For example, trust mechanisms are effective in judging the quality and reliability of cognitive nodes and wireless links, spectrum sensing, data aggregation, reliability and correctness of sensing information and spectrum sharing. However, it is not easy to build a good trust model within a CRN given the resource constraints [58]. Many existing security mechanisms assume that a trust relationship between CR nodes exists in advance.

Trust establishment techniques in cognitive networks are not new. Blaze et al. [59] introduced the term "trust management" in mobile networks and defined it as one of the components of security services in networks. Chen et al. [45] defined trust by showing a mathematical framework in the CRN working process. Although there is no concrete experiment that is carried out in [45], it expresses a first attempt to theoretically introduce the idea of applying trust and reputation modeling to CRNs. Qin et al. [46] also proposed a

novel trust-based spectrum sensing scheme which can identify misbehaving SUs and make the overall sensing decision by filtering out their reported spectrum sensing results.

Trust management usually involves computation overhead, so building an efficient scheme for resource-constrained CRN is a very challenging task. A typical public key infrastructure (PKI) scheme which achieves secure routing and other purposes in typical ad-hoc networks is not enough to guarantee the security of CRNs, given their limited communication and computation resources as mentioned above. This gives rise to the need for a trusted mechanism in CRNs, and authentication is a part of trust, along with other technical or non-technical factors.

1.5.2 Authentication

Authentication guarantees that the entities with whom a CR node communicates are the expected ones and the received data is the original sent by the counterparts. Generally speaking, a trust management scheme is required to authenticate messages in CRNs. However, due to the resource constraints at the cognitive nodes, solutions based on trust have intolerable storage and computation overheads on CRNs. Current research on authentication in CRNs focuses on identity and location-based authentication.

Identity-based authentication is one of the key factors for ensuring secure communications in CRNs. Zhu et al. [53] proposed a new authentication mechanism for CRNs which is based on third-party Certification Authority (CA). Zhao et al. [60] proposed an authentication scheme in the physical

layer by identifying the transmitter in CRNs to differentiate between the PU signal transmitter and the PUE attacker. Kuroda et al. [61] proposed a radio-independent authentication protocol for CRNs that is able to support EAP (Extensible Authentication Protocol) transport. Observing the necessity of a secure PU detection method, Liu et al. [62] proposed a novel approach for authenticating the PU's signal in CRNs in the presence of attackers by integrating traditional cryptographic signatures and link signatures. Wassim et al. [63] reported that cryptographic authentication mechanisms, such as digital signatures, cannot be implemented in the PU's identification because of the FCC regulation that prohibits altering PU systems. Hence there is a need to establish trust-based authentication in CRNs.

1.5.3 Secure routing

Routing protocols, to some extent, have received maximum attention from researchers both in wired networks and wireless networks. Therefore, most current research primarily focuses on providing the most energy efficient routing scheme. In CRNs, routing is considered inherently fragile and can easily be compromised by unknown attacks, malicious behaviors and even unintentional misconfigurations. Zhu et al. [64] reported that many attacks occur in CRNs, such as primary user emulation attacks [65], jamming attacks [66], false reporting of sensing data in collaborative spectrum sensing [67], denial-of-service attacks [68], and possibly some other attacks in the network layer. So, it is essential to design secure routing schemes that can enhance the security of routing in CRNs [36]. Clancy et al. [36] reported that trust information about the broader network is used to develop policy about routing and forwarding of traffic in a secure way in CRNs. Zhu et al. [64] mentioned

the routing technique as a mechanism that considers multi-hop packet error probability and delay from the source to the destination as performance metrics to be optimized in an adversarial and evolving environment populated by jammers who can cooperate and deteriorate the performance. Hossain et al. [69] reported that PUs can affect the spectrum opportunities available for SUs, leading to dynamically changing network topology in multi-hop CR networks. Therefore, a secure routing scheme should be implemented in CRNs that allows SUs to obtain knowledge about their environment in a distributed and dynamic fashion and use optimal routing decisions that can defend against malicious attacks with a minimum level of compromise in performance [64]. As different types of attacks can degrade network performance and reliability in an exponential way by attacking the routing techniques in distributed wireless networks such as CRNs, there is an urgent need to enhance security in routing in CRNs. Although some cryptographic techniques are employed at the physical layer in CRNs, the routing is still vulnerable to attacks. This leads to critical deterioration in the performance and reliability of CRNs. Zhu et al. [64] proposed a dynamic routing algorithm that can guarantee a performance level given by the value of the game in CRNs. Chen et al. [45] proposed trust through a mathematical framework for secure routing in CRNs. So, it is crucial to consider security issues at the beginning of a routing protocol design in CRNs.

1.5.4 Spectrum management

CRNs are proposed in order to provide high bandwidth to mobile users via heterogeneous wireless architectures and dynamic spectrum access techniques [29]. This goal can be achieved only through dynamic and efficient

spectrum management techniques and functions that address four main challenges: spectrum sensing, spectrum decision, spectrum sharing, and spectrum mobility.

Spectrum sensing enables CR users to adapt to the environment by detecting spectrum holes without causing interference to the primary network. Lee at al. [70] proposed an optimal sensing framework to avoid interference and the sensing limitation problem in CRNs as well as to maximize spectrum access opportunities. One of the major technical challenges in spectrum sensing is the problem of precisely distinguishing incumbent signals from SU signals. To distinguish the two signals, existing spectrum sensing schemes based on energy detectors [71, 72] implicitly assume a "naive" trust model. When energy detection is used, an SU can recognize the signal of other SUs but cannot recognize the PU's signal. When an SU detects a signal that it recognizes, it assumes that the signal is that of an SU; otherwise, it concludes that the signal is that of a PU. Under such an overly simplistic trust model, a selfish or malicious SU (i.e. an attacker) can easily exploit the spectrum sensing process [73].

Based on the spectrum availability, CR users allocate a channel depending not only on spectrum availability but also on internal policies. Spectrum decision depends on two factors: first, each spectrum band is characterized by local observations of CR users and statistical information of primary networks. Then, based on this characterization, the most appropriate spectrum band can be chosen. But a CR user may select the wrong band or a sub-optimal band, and communication may be impaired [43]. Akyildiz et al. [74] proposed a spectrum capacity estimation method that takes into consideration the

bandwidth and the permission power to mitigate this threat. Zheng et al. [23] proposed a management system and specified five rules that regulate CR users to act based on local observations and access the spectrum with limited communication cost and low complexity. But none of the rules considers user's behavior under faulty conditions.

A policy management mechanism needs to be implemented in CRNs to avoid harmful interference and misuse of the spectral bands caused by either intentionally or unintentionally. But the unique characteristics of CRs causes CRNs to face different challenges for spectrum sharing in CR networks. Baldini et al. [75] describe policy management architecture to validate the spectrum sharing approaches in the face of possible security threats and their reflection on network behavior and performance. Wang et al. [76] proposed a basic spectrum sharing scheme considering a model with one PU and multiple SUs and analyzed important statistics including mean number of radio bands used by the second users, deprivation rate and blocking rate of the second users, and the utilization ratio of the spectrum. Based on the scheme [76], Patil et al. [77] also proposed a Continuous Time Markov Chain (CTMC)-based spectrum sharing scheme for CRNs and analyzed the same statistics in [76]. But both schemes [76, 77] did not consider any threats or misbehaving during spectrum sharing.

The function of spectrum mobility is to ensure a seamless connection when a CR vacates a channel and moves to a better channel. After a CR captures the best available spectrum, PU activity on the selected spectrum may require the user to change their operating spectrum band(s), which is referred to as spectrum mobility [74]. Spectrum mobility introduces a new type

of handoff in CR networks which is termed 'spectrum handoff'. The intrinsic characteristics of a CR network give rise to research efforts to address the problems of spectrum handoff during spectrum mobility. The mobility-based handoff mechanisms that have been already investigated in cellular networks may serve as the groundwork in this area but there are still open research topics that need to be investigated.

In this thesis, some of these identified gaps in the research to enhance CRN security by incorporating trust-based mechanisms will be addressed. In the next section, the main research objectives of this thesis are discussed.

1.6 Objectives of the Thesis

This thesis focuses on developing trust-based schemes to improve the security in CRNs. The aim of this thesis is to design, specify, and analyze trust management frameworks in CRNs to ensure secure communication and enhance the system availability.

The main research objectives of this thesis are as follows:

1. To present the security requirements and challenges of CRNs. Based on the acquired information and with a clear understanding of the challenges involved in implementing security mechanisms, a security model is defined according to the security requirements and will work as a performance metrics to evaluate the proposed trust-based schemes. The development of security metrics, measurements, and evaluation based on the trust of approaches is of great importance in order to establish a scientific methodology for the field of entire cognitive network security

research.

2. To propose a methodology to establish trust between different CR nodes in the network for **authentication** purposes so that it can effectively prevent malicious and selfish users's interaction in the network.

3. To propose a conjoint trust assessment approach (combining trust assessment from the Primary User Network and Secondary User Network) in CRNs to solve the security threats brought about by untrustworthy entities, such as selfish, malicious, and faultless nodes, and to ensure secure **spectrum sharing** in CRNs.

4. To propose multiple back-up Certificate Authority (BCA)-based system architecture and enhance system **availability** and reliability by reducing the downtime cost due to an attack on the CRN's key nodes.

5. To propose a methodology where nodes can **join and leave the network securely** without introducing any selfish behaviors in the network and show how the trust value can be updated according to their manners.

6. To validate the aforementioned proposed approaches to improve secure communication in CRNs.

1.7 Scope of the Thesis

This thesis presents a methodology that will enable a trusting relationship to gain access to the network resources in CRNs after trust has been determined and established. The scope of this thesis can be specified as follows:

1. Trust is not a separate component of security architecture for CRNs. Trust management provides a security infrastructure for other security services. At the same time, it relies on other security services. Trust management and other security services together make up the security architecture of CRNs (shown in Figure 1.11). A comprehensive consideration is compulsory when designing a trust management scheme for a CRN. However, to limit the scope of this thesis, only secure communication in CRNs is focused from the view point of trust. The existence of other security aspects, such as Intrusion Detection Systems (IDS) and secure routing are not considered.

2. This thesis is concerned with the development of trust-based mechanisms for secure communication in CRNs. It should be noted that the methodology proposed in this thesis relates purely to the domain of trust. It encompasses trust calculation in different ways which focuses on issues involving trust establishment, maintenance, and update. Related topics, including algorithm selection for the highest trusted node for CA and BCA selection, are also included in this thesis to ensure secure communication in CRNs. The proposed trust establishment algorithm can be applied to different applications where the threshold value may change according to the system criteria. As the threshold value depends on the specific application domain, the method of determining it is out of scope of this thesis.

3. The proposed trust-based mechanisms in this thesis for secure communication in CRNs focuses on small scale networks which do not require any additional resources as the trust calculation process is carried

out by using the computational capacity which is present in each node. Other processing relevant factors such as cost, memory, time etc are not considered within the scope of this thesis.

4. The proposed methodologies in thesis are verified by considering different case studies. Validation of the proposed algorithms on a synthetic real world CRN is beyond the scope of the thesis.

5. This thesis focuses on trust-based spectrum sharing in CRNs. The trust in spectrum sensing, spectrum mobility is not provided in this thesis. It is assumed that the SUs will use existing spectrum sensing approaches presented in the literature.

1.8 Significance of the Research

1.8.1 Social and economic significance

The significance of the proposed research, from a social and economic point of view, includes:

1. Saving resources: Current spectrum management schemes consume valuable resources such as memory, network bandwidth, and power. The proposed approaches are efficient and can reduce the consumption of resources and thus can be used in large-scale CRNs.

2. Low-cost network maintenance: The introduced authentication schemes make the establishment of trust over an unreliable network possible. Hence, it can address the network maintenance problem without increasing hardware costs.

3. Provision of lightweight trust management: The application of CRNs calls for corresponding security mechanisms. The lack of a matching lightweight security mechanism hinders the wide application of CRNs. However, the challenges of CRNs render most security mechanisms infeasible. The trust-based schemes in this research pave the way for access control and establishment of secure communication channels in CRNs.

1.8.2 Scientific significance

The significance of the proposed research, from a scientific point of view, includes:

1. proposing trust-based authentication schemes in CRNs which fix the security problems brought by untrustworthy users in CRNs and can be seamlessly used to enhance secure communication in CRNs.

2. proposing multiple back-up of the Certificate Authority (BCA) scheme which increases system availability and reliability and decreases the downtime cost of the system. This thesis also proposes a trust-based election procedure to select the CA and back-up CA in the system to act as the key nodes in CRNs.

3. proposing a trust-based spectrum sharing scheme for secure communication in CRNs. This is the first time a trust-based spectrum sharing scheme has been developed and the first its experimental details have been explored. It also proposes mechanisms to determine the right balance of multiple nodes for spectrum sharing in CRNs to ensure a smooth communication.

1.9 The Structure of the Thesis

As mentioned earlier, in this thesis, a trust-based methodology is proposed and developed for secure communication in CRNs whereby trust can be established, distributed and updated with lightweight overhead. Incase, an attack occurs during transmission, the multiple back-up mechanism can proceed in a fault-tolerant manner. In order to achieve the aforementioned objectives, this thesis is organized as follows:

- In Chapter 2, an in-depth survey of the state-of-the-art techniques for trust-based security in CRNs is presented. The proposed techniques in the literature is reviewed in terms of each aspect and summarized the weaknesses and existing problems in each aspect. The literature review in this chapter provides the foundation for the problem definition in the following chapter.

- In Chapter 3, the problem definition is formally presented. The problem definition is divided into different research issues. The terms and terminologies are also defined in this chapter that will be used while solving each issue.

- In Chapter 4, an overview of the solution to each of the issues identified in Chapter 3 is presented. Chapter 4 also provides pointers to the chapters containing the overview of the solutions for the identified research issues.

- In Chapter 5, a trust-based framework is proposed for establishing trust between CR nodes that authenticates SU's request of CRN to access the network resources on the level of belief that the security of a network

will not be compromised as a result of that user's action after it joins the network.

- In Chapter 6, trust-based secure spectrum sharing mechanisms are proposed to solve the security threats brought about by untrustworthy entities, such as selfish, malicious, and faulty nodes, and to ensure secure communication through trustworthy spectrum sharing in CRNs.

- In Chapter 7, system availability enhancement mechanisms are proposed in CRNs by selecting the key nodes based on the level of trust and proposing trust-based secure node joining and leaving process in the network.

- In Chapter 8, the thesis concludes with a summary of the work developed in this thesis and the potential further work is identified.

The structure of the chapters and the relationship between the chapters is shown in Figure 1.13.

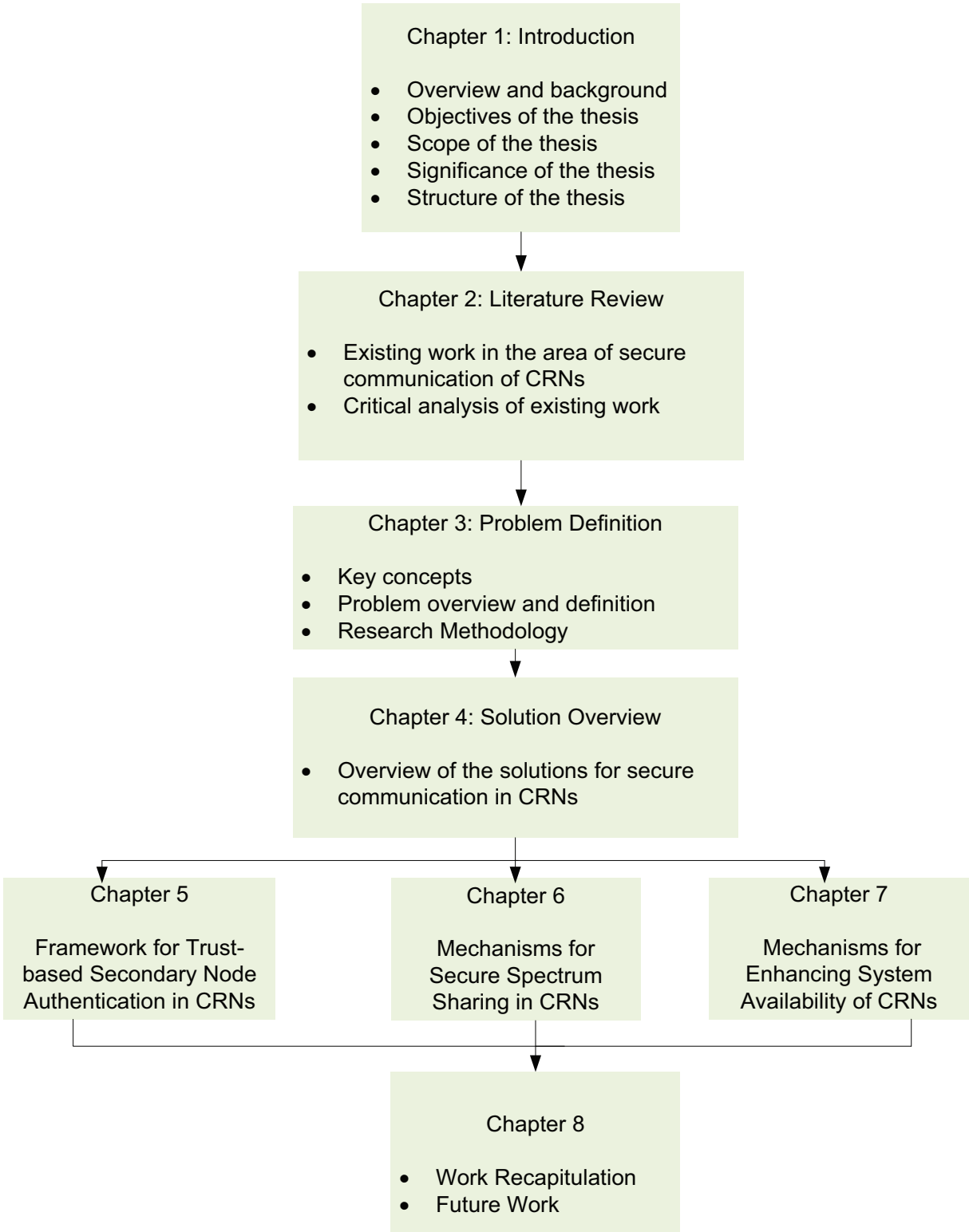

Figure 1.13: Relationship between the chapters of this thesis

1.10 Conclusion

The proliferation of CRNs has driven research into CRN security, with trust being the cornerstone of the research area. In this chapter, a comprehensive overview of CRN security, including the application, architecture, vulnerabilities, security requirements, and current hot research topics in the field of CRN security is provided. The overview helps in understanding of the characteristics of CRNs and the importance of trust in CRN security research. Then, the motivation is introduced that drives me to carry out this research, followed by a description of the significance of my work. The scope and objectives of this study were identified and discussed and the structure of the thesis was presented.

Chapter 2

Literature Review

2.1 Introduction

In chapter 1, security was highlighted as a crucial issue in cognitive radio networks (CRNs) due to its inherent network characteristics. One of the ways by which it can be addressed is by using the notion of trust. In this chapter, an overview of the existing literature on trust-based security issues in CRNs is presented. Substantial progress has been made on providing a sound, practical basis for a number of problems that are associated with trust for CRN security. A number of trust management techniques has been documented in the literature. In the following sections, the work that has been previously undertaken to solve some of the issues related to security and trust in CRNs are discussed. The research areas investigated in this thesis can be grouped into the following categories:

1. Challenges and threats in CRNs

2. Countermeasures for various attacks on CRNs

3. Secure spectrum management scheme for CRNs

4. Trust-based schemes for CRN security

5. Authentication-based schemes for CRN security

This research focuses on trust-based schemes for ensuring security in CRNs. Different types of trust-based schemes are proposed in order to meet security requirements in CRNs and these will be discussed in this chapter with the aim to highlight their drawbacks. A discussion on the challenges and threats related to various functionalities in CRNs is given in Section 2.2. Section 2.3 describes the different countermeasures in CRNs. Existing approaches in the literature to secure each phase in spectrum management is given in Section 2.4. In Section 2.5, the key aspect for improving the security using the notion of trust in different phases in spectrum management in CRNs is discussed. Section 2.6 describes the authentication-based schemes in the literature to improve security in CRNs. In Section 2.7, an integrative view of all these approaches from the literature is discussed with a view to ascertaining the trust to be utilized for ensuring secure communication in CRNs. Finally, 2.8 concludes the chapter.

2.2 Challenges and Threats in the Various Functionalities of CRNs

In this section, the different types of challenges and threats that are common to CRNs are described.

2.2.1 Spectrum Sensing

A CR is considered to be aware of and sensitive to changes in its surroundings, which makes spectrum sensing an important requirement for the realization of CRNs. Spectrum sensing enables CR users to adapt to the environment by detecting spectrum holes without causing interference to the primary network. This task can be accomplished by a real-time wide band sensing capability to detect weak primary signals within a broad spectrum range. Generally, spectrum sensing techniques can be classified into three groups: primary transmitter detection, primary receiver detection and interference temperature management [29].

2.2.1.1 Spectrum sensing challenges

Several open research challenges currently exist which must be investigated for the development of spectrum sensing techniques [29]:

- *Interference temperature measurement:* Due to the lack of interaction between primary networks and CR networks, generally a CR user is not aware of the precise locations of the primary receivers. Thus, new techniques are required to measure or estimate the interference temperature at nearby primary receivers.

- *Spectrum sensing in multi-user networks:* The multi-user environment, consisting of multiple CR users and primary users (PUs), makes it more difficult to sense spectrum holes and estimate interference. Hence, spectrum sensing functions should be developed which take into consideration the multi-user environment. In multi-user CRNs,

different users share their sensing results and collaboratively decide on the presence of the licensed band. To address these challenges, different sensing schemes in multi-user networks have been proposed. Ghasemi et al. [78] discussed the effectiveness of collaborative sensing in multi-user CRNs. In multi-user CRNs, CR users can achieve the desired performance through collaborative sensing, even if individual users do not meet the minimum SNR (Signal to Noise Ratio) requirement. Shahid et al. [15] proposed a new cooperative spectrum sensing scheme in multi-user CRNs where each users contribution is weighted by a factor that depends on received power and path loss.

- *Spectrum-efficient sensing:* In CRNs, CR users cannot perform sensing and transmission at the same time, which inevitably decreases their transmission opportunities. This problem is termed the so-called sensing efficiency problem. Hence, CR users should stop transmitting while sensing. For this reason, balancing spectrum efficiency and sensing accuracy is an important issue. Moreover, because sensing time directly affects transmission performance, novel spectrum sensing algorithms must be developed so that the sensing time is minimized within a given sensing accuracy. To solve this sensing efficiency problem, Lee at al. [70] proposed an optimal sensing framework to avoid interference and the sensing limitation problem in CRNs as well as to maximize spectrum access opportunities. To solve the interference problem in spectrum sensing, Shahid et al. [79] proposed a new method of agile spectrum evacuation through the formation of a set of users that are able to detect the return of PUs while SUs continue to use the spectrum band in a

cooperative manner.

- *Hardware Attachment :* Spectrum sensing in CRNs requires a high sampling rate, high resolution analog to digital converters (ADCs) with large dynamic range, and high speed signal processors [9]. Cognitive radio terminals are required to process transmission over a larger, wider band for searching and utilizing any opportunity. So, a cognitive radio node needs to capture and analyze a large band to determine the spectrum opportunity. This large operating bandwidth adds additional requirements, such as antennas and power amplifiers, etc. and increases the cost.

- *Hidden Primary User Problem:* This problem is a well known problem in CRNs. Cognitive radio devices cause unwanted interference to the PU as the primary transmitter's signal can not be detected because of the location of devices.

- *Detecting Spread Spectrum Primary Users:* PUs that use spread spectrum signaling are difficult to detect as the power of the PU is distributed over a wide frequency range.

- *Security:* In CRNs, a selfish or malicious user can alter its air interference to the PU. So, it can give false information to the networks regarding the PU's spectrum sensing performance. This problem is termed a Primary User Emulation (PUE) attack. It is very difficult and challenging to develop countermeasures when an attack is already identified. A PU identification method is proposed, based on the public key encryption in [25] to prevent SUs masquerading as PUs.

2.2.1.2 Spectrum sensing threats

One of the major technical challenges in spectrum sensing is the problem of precisely distinguishing the incumbent signals from the SU signals. To distinguish the two signals, existing spectrum sensing schemes based on energy detectors [71, 72] implicitly assume a "naive" trust model. When energy detection is used, an SU can recognize the signal of other SUs but cannot recognize the PU's signal. When an SU detects a signal that it recognizes, it assumes that the signal is that of an SU; otherwise, it concludes that the signal is that of a PU. Under such an overly simplistic trust model, a selfish or malicious SU (i.e., an attacker) can easily exploit the spectrum sensing process [73]. The malicious SU can send false information and mislead the spectrum sensing results to cause collision or inefficient spectrum usage. For example, some SUs always report the existence of the PU so that they can occupy the spectrum themselves [80]. The problem of dishonest users in distributed spectrum sensing is discussed in [81]. From the literature review [34, 36, 37, 39, 43], it can be seen that some attackers can seriously affect the spectrum sensing scheme in CRNs, as depicted in Figure 2.1.

2.2.2 Spectrum decision

CRNs need to be able to decide which of the available bands is the best spectrum band according to the QoS requirements of the applications. This notion is called spectrum decision and constitutes an important topic in CRNs. A spectrum decision is closely related to the channel characteristics and operations of PUs. Furthermore, a spectrum decision is affected by the activities of other CR users in the network. A spectrum decision usually

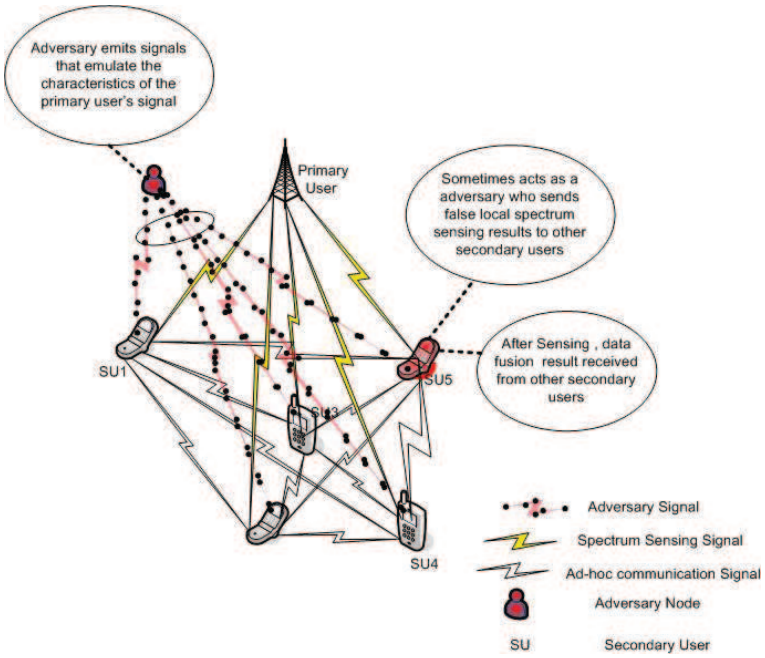

Figure 2.1: Security threats in CRNs sensing

consists of two steps: first, each spectrum band is characterized, based on not only local observations of CR users but also statistical information of primary networks. Then, based on this characterization, the most appropriate spectrum band can be chosen. The challenges and threats in spectrum decision phase are discussed in the next section.

2.2.2.1 Spectrum decision challenges

In the development of the spectrum decision function, there are several challenges still need to be addressed:

- *Decision Model:* Spectrum capacity estimation using signal-to-noise (SNR) is not sufficient to characterize the spectrum band in CRNs. Also, applications require different QoS requirements. Thus, the design of application and spectrum-adaptive spectrum decision models is still an open issue.

- *Cooperation with reconfiguration:* CR techniques enable transmission parameters to be reconfigured for optimal operation in a certain spectrum band. For example, even if the SNR is changed, bit rate and bit error rate (BER) can be maintained by exploiting adaptive modulation instead of spectrum decision technique.

- *Spectrum decision over heterogeneous spectrum bands:* Currently, certain spectrum bands are assigned to different purposes, whereas some bands remain unlicensed. Thus, a CR network should support spectrum decision operations on both licensed and unlicensed bands.

2.2.2.2 Spectrum decision threats

CRNs need to be able to decide which is the best spectrum band to use from the available bands, according to the QoS requirements of the applications. The threats come from the possibility of false or fake spectrum characteristic parameters. The false or fake parameters affect the outcome of spectrum decisions. So, a CR may select the wrong band or a sub-optimal band, and communication may be impaired [43]. Akyildiz et al. [74] proposed a spectrum capacity estimation method that takes into consideration the bandwidth and the permission power to mitigate this threat.

2.2.3 Spectrum sharing

Spectrum sharing is one of the main challenges of CRNs. Its techniques actually follow two types of architecture: spectrum sharing inside a CR network (intra-network spectrum sharing) and among multiple coexisting CR networks (inter-network spectrum sharing) [31]. There are two main reasons

for the challenges of spectrum sharing in CRNs: (1) co-existence with licensed users; and (2) a wide range of available spectrum.

2.2.3.1 Spectrum sharing challenges

There are many open challenges for spectrum sharing in CRNs such as:

- *Common Control Channel:* A common control channel (CCC) is associated with many spectrum sharing functionalities. But implementation of a fixed CCC is infeasible because a channel must be vacated whenever a PU chooses it.

- *Dynamic radio range:* The cognitive radio nodes, as well as their neighbours, often change the operating frequency because of the interdependence between radio range and operating frequency. So far, no prior work has addressed this important issue of spectrum sharing in CRNs.

- *Location Information:* In most of the existing work, it is assumed that SUs are always informed about the PU's location and transmission power. Such an assumption is always valid [29]. The authors in [82] proposed a protocol which uses location information as a key factor to authenticate each other to provide privacy and confidentiality in CRNs.

2.2.3.2 Spectrum sharing threats

Different users can share the same spectrum bands in CRN technology. A policy management mechanism is implemented to avoid harmful interference and misuse of spectral bands caused by malicious users. Malicious users can deny spectral bands to other CR networks and devices for selfish reasons and

disrupt the communication of other wireless networks. So, the security in spectrum sharing in CRNs is treated as one of the crucial problems in cognitive environments. Baldini et al. [75] described policy management architecture to validate the spectrum sharing approaches in the face of possible security threats and their reflection on the network behavior and performance.

2.2.4 Spectrum mobility

After a CR captures the suitable available spectrum, PU activity on the selected spectrum may require the user to change its operating spectrum band, which is referred to as 'spectrum mobility'. Spectrum mobility is associated with 'spectrum hand-off', where the users transfer their connections to an unused spectrum band in CRNs and ensure smooth communication during spectrum hand-off. Whenever the CR user tries to modify the operating frequency, the network protocol needs to be modified according to the operating parameters as well. The challenges and threats in this area are as follows:

2.2.4.1 Spectrum Mobility Challenges

The following are the open research issues for spectrum mobility in CRNs.

- *Spectrum mobility in time domain:* CR networks always adjust to the wireless spectrum, based on the availability of the free bands. As these free available channels alter over time, this makes QoS in this spectrum sharing environment a challenging issue.

- *Spectrum mobility in space:* The availability of the bands also changes as the CR user can move at any time from one place to another in the

network. Hence, continuous spectrum allocation in CRNs is a major and challenging issue.

2.2.4.2 Spectrum mobility threats

The function of spectrum mobility is to ensure a seamless connection when a CR vacates a channel and moves to a better channel. According to [43], in CRNs, one should vacate the current spectrum band whenever the PU is active. In order to establish smooth communication as soon as possible, the SU needs to select a new appropriate spectrum band, and move to the band immediately. This process is called "spectrum hand-off". During hand-off, the security threats are serious. An attacker can induce a failed spectrum hand-off by means of: compelling the CR to vacate the current band by masking the PU, jamming to slow the process of selecting a new available band or causing a communication failure, etc. To mitigate this kind of threat, an SU can randomly hop over multiple channels. This opens a trade-off between choosing good channels and evading an attacker's jamming when different channels have different qualities (e.g. the probability of being idle, propagation characteristics, etc.). The interaction between the SU and the attacker has been called a 'dogfight' in the spectrum due to the dynamics of pursuit and evasion [66]. In [66], Li et al. analyzed one-stage and multi-stage cases by numerical simulation results, showing that the performance of an SU was improved when the number of channels was increased or the channel state certainty was reduced.

In the next section, the different countermeasures for various attacks in CRNs are discussed.

2.3 Countermeasures for Various Attacks on CRNs

In this section, the various possible countermeasures to potential attacks on CRNs are discussed. The authors in [55] proposed various possible countermeasures on different attacks in CRNs.

2.3.1 Jamming countermeasures

Most of the attacks targeting CRNs are associated with jamming specified frequencies. Security protocols can mitigate many of the attacker's goals but cannot effectively deal with DoS or channel degradation due to jamming [47]. Therefore, it is essential to identify the source of attack. An Intrusion Detection System (IDS) has the ability to identify which nodes are suspicious or malicious, and supply this information to other protocols of the node such as routing and aggregation. So IDS is considered an important tool for detecting attackers. In CRNs, feedback from the CR devices can enhance the efficiency of IDS. The redundancy of the network is used as an advantage because the feedback of many participants can lead to easier detection of the jamming source [47]. The authors in [83] proposed a new model for intrusion detection and response for mobile, ad-hoc wireless networks in a distributed and cooperative manner. The same idea could be applied to CRNs where cooperation is an integral part of their architecture. The best approach is probably based on the detection of abnormal operation through traffic analysis and cooperation [47].

IDS must be executed in every networking layer in a cross-layer manner

with a view to performing this task. There are many IDS approaches [16, 83–85], which are adequate for other wireless networks but not sufficient for CRNs. Filho et al. [86] described two types of CRN intrusion detection mechanisms, namely the localization mechanism (LM) and the reputation mechanism (RM). LMs of malicious users in CRNs will make possible the determination of the radio's geographical positioning. RMs are necessary to validate the confidence of the data supplied for the radios. The architecture of an IDS entity for distributed systems is based on its basic elements: a local packet monitoring module that receives the packets from the neighborhood, a statistics module that stores the information derived from the packets and information regarding the neighborhood, a local detection module that detects the existence of the different attacks, an alert database that stores information about possible attacks, a cooperative detection module that collaborates with other detection entities located within the neighborhood, and a local response module that makes decisions according to the output of the detection modules [87]. Focusing on the detection modules used in these IDS for CRNs, they must make use of first-hand information, second-hand information, statistical data, and the data acquired by the CRs during its normal operation. These modules can then use this data to distinguish between normal and abnormal activities, thus discovering the existence of intrusions.

2.3.2 Primary user emulation attack countermeasures

The prevention of a Primary User Emulation Attack (PUEA) in CRNs is vital. A detection technique to verify the authenticity of primary signals is an essential issue for protection against PUEA. The authors in [47] proposed various techniques to counter this attack in CRNs. The simplest way is to

embed a signature in an incumbent signal or to use an authentication protocol between primary users (PUs) and secondary users (SUs) [47]. However, these approaches do not ensure the requirement established by the FCC [51] which states that *no modification to the incumbent system should be required to accommodate the opportunistic use of the spectrum by secondary users*. The authors in [65] proposed a technique to use signal energy level detection in accordance with the location of transmitters to deal with PUEA in CRNs. This approach is based on the existence of a set of nodes known as Location Verifiers (LV) in CRNs, these nodes being responsible for measuring the received signal strength (RSS). But the authors in [47] criticized this approach as it does not work in network environments where PUs are not fixed and transmit with low transmission, such as wireless microphones. There are alternative countermeasures against PUEA in CRNs such as *radio frequency fingerprinting* (RFF), which has been broadly discussed in the literature as a method of transmitter identification [88].

2.3.3 Objective function attacks countermeasures

Objective function attacks (OFAs) attempt online learning of the AI protocol used by CR devices. OFAs always modify the behavior of the wireless media by jamming at specific times and frequencies in respect to a policy-defined parameter, such as the security level, and thus change the learning curve to make it favorable to the attacker. As a result, low level security is achieved in this case. The authors in [47] proposed a naive solution for updatable radio parameters for the selection of threshold values. This scheme can prevent the situation where only one or a set of parameters do not meet the predefined threshold requirements.

2.3.4 Lion attack countermeasures

As explained previously in the section on Lion Attack, TCP throughput becomes lower because of frequency hand-offs as the transport layer is not informed about the physical/link layer information and this situation causes a network disconnection due to network congestion. The authors in [89] proposed several cross-layer solutions in order to obtain better TCP performance in the context of wireless networks, especially ad hoc networks. These TCP performance improvement techniques can be used as directions to develop new protocols which are appropriate for CRNs with a view to increasing efficiency and making them strong enough against cross-layer attacks. In the next section, the schemes in various activities during spectrum management to ensure security are discussed.

2.4 Secure Spectrum Management Schemes in CRNs

2.4.1 Secure spectrum sensing scheme

One of the functionalities of CRNs is to detect spectrum holes by spectrum sensing which continually monitors a given spectrum band and captures the information. CR users may temporarily use the spectrum holes without creating any harmful interference to the PUs. However, CRs must periodically sense the spectrum to detect the presence of incumbents and quit the band once detected. The detection techniques which are often used in local sensing are energy detection, matched filter, and cylcostationary feature detection.

However, few studies have considered a novel security threat of spectrum sensing which is called spectrum sensing data falsification [38], whereby an attacker or malicious user sends false local spectrum sensing results to a data fusion center which causes the data fusion center to make an incorrect spectrum sensing decision. This kind of security attack was first mentioned in [90] and further considered in [38, 81]. In [81], the spectrum sensing data falsification problem was solved by a Weighted Sequential Probability Ratio Test which gives good performance. However, this method requires knowledge of the physical location of sensing terminals and the position of the PU in order to obtain some required prior probabilities. This is inappropriate to apply to a mobile CR system, and to such systems in which the information about the PU is completely unknown.

In other work [91], the authors proposed a robust secure distributed spectrum sensing scheme that uses robust statistics to approximate the distributions for both hypotheses of all nodes, discriminatingly, based on their past data reports. The achieved parameters are used for the testing of malicious users and calculating the necessary information for data fusion by means of D-S theory. This scheme has the powerful capability to eliminate malicious users due to the abnormality of distribution of malicious users compared with that of legitimate users. Their algorithm, taking advantage of an appropriate method of data fusion and the benefit of robust statistics for outlier testing based on two estimated distributions separately, can operate without needing knowledge of primary systems, even in very adverse circumstances where there are numerous malicious users. After sensing, each CU (CR User) sends its own received power data to a DFC (data fusion center)

where the global sensing decision is made. For the purpose of improving security and cooperative sensing gain, the proposed robust secure distributed spectrum sensing scheme by Nhan et al. [91] is depicted in Figure 2.2.

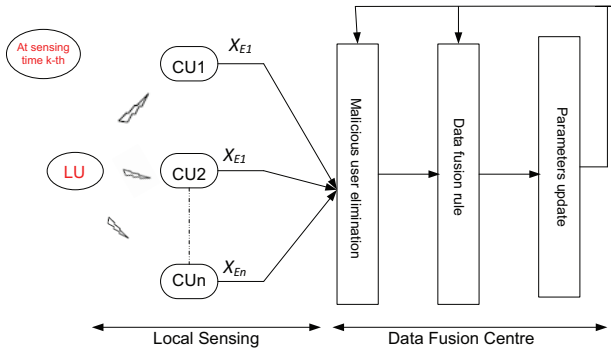

Figure 2.2: Secure spectrum sensing scheme [91]

In the proposed scheme [91], the authors consider two kinds of malicious nodes: the "always-yes" node and the "always-no" node. The "always-no" node always reports the absence of a primary signal, whereas the "always-yes" node always informs of the presence of the LU (Licensed User). "Always-yes" users increase the probability of false alarm P_f while "always-no" users decrease the probability of detection P_d. A malicious user will have abnormal estimated parameters. Based on this feature, it can easily detect consistent malicious users by the following test condition: $|\hat{\mu}_{1i} - \hat{\mu}_{oi}| < \varepsilon_1$ where N= 2TW where T and W are detection time and signal bandwidth, respectively, and ε_1 is the detection thresholds which is predefined based on N so that the malicious users can be removed completely [91]. This test is used for detecting "consistent malicious" nodes which generate false sensing data from one hypothesis. An "always-yes" or "always-no" node will have very small difference between two hypotheses means and deviations since its data set $\{x_{Ei}|H_0\}$ and $\{x_{Ei}|H_1\}$ are derived from one hypothesis distribution or even

from a constant value. If a node has a smaller distance between two mean values of two hypotheses than a minimum tolerable value, it is considered a consistent malicious user.

Several studies address the security issues of spectrum sensing in CRNs. Primary user emulation attack is analyzed in [65, 92]. In this attack, malicious users transmit false signals which have features similar to those of a primary signal. In this way, the attacker can mislead legitimate SUs to believe that a PU is present. The defense scheme in [65] is designed to identify malicious users by estimating location information and observing received signal strength (RSS). In [92], signal classification algorithms are used to distinguish between primary and secondary signals. Primary user emulation attack is an outsider attack, targeting both collaborative and non-collaborative spectrum sensing. Another type of attack is insider attack that targets collaborative spectrum sensing. In current collaborative sensing schemes, SUs are often assumed to report their sensing information honestly. However, it is quite possible that wireless devices are compromised by malicious parties. Compromised nodes can send false sensing information to mislead the system.

A natural defense scheme [90] is used to change the decision rule. The revised rule is: when there are $k-1$ malicious nodes, the decision result is based on there being at least k nodes being reported on. However, this defense scheme has three disadvantages. First, the scheme does not specify how to estimate the number of malicious users, which is difficult to measure in practice. Second, the scheme will not work in soft-decision cases, where SUs report sensed energy levels instead of binary hard decisions. Third, the scheme has a very high false alarm rate when there are multiple attackers.

The problem of dishonest users in distributed spectrum sensing is discussed in [81]. The defense scheme in this work requires SUs to collect sensing reports from their neighbors when a confirmatory decision cannot be made. Moreover, the scheme is applied only to hard-decision reporting cases. Finally, current security issues in CRNs, including attacks and corresponding defense schemes, are summarized in [36].

2.4.2 Secure spectrum decision scheme

The main benefit of introducing security in the spectrum decision process is a stronger guarantee that the service of PUs will not be significantly disrupted. At no additional cost, the resilience of the spectrum decision against malicious attackers protects the secondary network as well. For instance, the DoS types of attacks presented in [68] will not be applicable if the spectrum decision is secure. The authors proposed a protocol designed to provide secure spectrum decisions in a clustered infrastructure-based network where spectrum decisions are made periodically and independently in each cluster. The proposed protocol guarantees that a malicious outsider and a limited number of corrupt insiders (i.e., nodes that participate in the protocol) cannot have a significant impact on the spectrum decision. The protocol is provably secure, and it is more efficient than the straightforward solutions involving digital signatures or key establishment protocols.

Many existing dynamic spectrum access protocols make spectrum decisions based on the assumption that all parties involved in the spectrum decision are honest and there is no malicious outsider that can manipulate the spectrum decision process. The authors [93] assume that there is some sort

of synchronization among the nodes in the cluster in the network. The time is divided into equal length intervals (or cycles). The nodes know when each cycle begins and ends, and they are also aware of the schedule of events during a cycle (e.g., which node sends its channel availability data, which channels it uses, etc.). There are three main events that are handled in a given cycle: one or more nodes may join the spectrum decision process in a given cluster, the nodes of the cluster send their spectrum sensing data, and the cluster head sends to the other nodes the final channel assignment. They also describe how each of these operations can be accomplished in a secure and efficient manner. But they do not deal with the details of the data sent by the nodes during the spectrum decision. They simply present techniques that enable secure transmission.

2.4.3 Secure spectrum sharing scheme

As spectrum sharing is one of the most important functions in CRNs, which allows CRNs to fairly share the available spectrum bands among the coexisting cognitive radios, it is very important to ensure security for spectrum sharing in CRNs. In the existing literature, it appears that, to date, no work has been done to ensure security during spectrum sharing in CRNs, although, some work has been done on spectrum sharing mechanisms in CRNs only.

Wang et al. [76] also proposed a spectrum sharing scheme for CRNs. In their model [76], they assume a CRN consists of one PU and N SUs. PUs are licensed users whereas SUs are unlicensed users. PU's spectrum band is divided into N sub-bands by maintaining the properties of Orthogonal Frequency Division Multiplexing technology. The proposed spectrum sharing scheme is based on the following statistics:

- The arrival of the PU to access the spectrum is a Poisson process with rate λ_p
- The time of the PU occupying the spectrum is a random variable that follows a negative exponential distribution with mean time $\frac{1}{\mu_p}$
- The inter-arrival time of SUs accessing the spectrum is a random variable that follows a negative-exponentially distributed with mean time $\frac{1}{\lambda_s}$
- The time of each SU using a radio band is a random variable obeying negative-exponential distribution with mean $\frac{1}{\mu_s}$

The proposed spectrum sharing scheme [76] evaluated and discussed different network parameters such as mean number of radio bands used by the SUs, deprivation rate of the SUs, blocking rate of the SUs, and utilization ratio of spectrum.

Patil et al. [77] proposed a spectrum sharing scheme in CRNs based on the Continuous Time Markov chain (CTMC) model. In their model [77], they assume a CRN consists of two PUs and $2N$ SUs. PUs are licensed users whereas SUs are unlicensed users. They considered two licensed frequency bands f_x and f_y, licensed to PU1 and PU2, respectively. Each band is divided into N sub-bands by maintaining the properties of Orthogonal Frequency Division Multiplexing technology. So the 2N SUs can use the sub-bands in parallel when the PUs are not using their own spectrum. All the SUs have to stop using the radio bands and vacate them when the PU comes back to use the spectrum. The proposed spectrum sharing scheme is based on the same assumption in [76]. The proposed spectrum sharing scheme [77] also evaluated and discussed different network parameters such as the mean number of radio bands used

by SUs, the deprivation rate of the SUs, the blocking rate of the SUs, and the utilization ratio of the spectrum. Although some work has been done in spectrum sharing, none considers security issues during spectrum sharing. This thesis is the first attempt to address security in spectrum sharing.

2.4.4 Secure spectrum mobility scheme

The protocols of different layers of CRNs must be able to adapt to the channel parameters of the operating frequency. As well, they must be apparent to the spectrum hand-off and related latency. An algorithm should be implemented and the best available spectrum should be chosen, depending on the channel characteristics of the available spectrum and the Quality of Service requirements of the CR user. There is no work on secure spectrum mobility in CRNs. Only a few studies have addressed spectrum mobility in CRNs.

Chen et al. [94] developed a cross-layer protocol for both spectrum mobility and handover in long-term evolution (LTE) cognitive networks. They developed a cross-layer handoff protocol considering the Poisson distribution of spectrum resources with the minimum expected transmission time in cognitive LTE networks. They considered two cases during their protocol development:

- The first case is that the SU's initial location is not in the overlapped area. If a PU appears and attempts to use its own spectrum which is temporarily occupied by the SU, the SU performs spectrum mobility processing to select a new spectrum hole, move to the new spectrum hole to continue its transmission, and vacate the occupied spectrum for the PU.

- The second case is when the SU's initial location is in the overlapped area, as it continually moves between two adjacent networks.

In the next section, the trust-based scheme for addressing security in CRNs is discussed.

2.5 Trust-based Schemes to Ensure Security in CRNs

A variety of techniques by which security can be achieved in CRNs has been proposed in the literature. But sometimes these security protocols are difficult to implement due to severe resource constraints in bandwidth, memory size, battery life, computational power, and unique wireless characteristics such as openness to eavesdropping, high security threats or vulnerability, unreliable communication, and rapid changes in topologies or memberships due to user mobility or node failure [57]. To address this, Blaze et al. [59] introduced the term "trust management" in mobile networks and defined it as one of the components of security services in networks. However, in the context of CRNs, 'trust' is an important concept to consider when authentication has to be achieved to ensure secure communication on the basis of believing that an SU, using the PU's spectrum, will not cause interference to the PU. Trust in this context is defined as the belief that the security of a network will not be compromised as a result of a user's action after that user has been permitted to share the PU's free spectrum. Having such a trust-based mechanism allows only non-malicious SUs to access the licensed spectrum and network resources. Trust management, including trust establishment, trust update, and trust

revocation, is much more challenging in mobile networks than in traditional centralized environments due to its various characteristics [57]. For example, collecting trust information or evidence to evaluate trustworthiness is difficult due to mobility-induced changes in network topology. The idea of applying trust and reputation modeling in CRNs has attracted research interest.

Chen et al. [45] define trust by showing a mathematical framework in the CRN working process in the following ways:

(a) A cognitive radio node senses a spectrum hole and to dynamically access the spectrum for transmission requires "trust" from the originally existing system, i.e. primary system (PS) and regulator, without creating interference to the PS.

(b) A cognitive radio node may want to leverage another existing cognitive radio node to route its packets, even though another CR is not the targeted recipient terminal. It requires "trust" from another CR.

(c) A cognitive radionode can even leverage the PS to forward its packets to realize the goal of packet switching networks. It needs "trust" from the PS, not only at the network level but from the service provider (or network operator).

Detailed definitions of trust in CRNs are defined under the trusted routing context. Although there is no concrete experiment that is carried out in [45], it expresses as a first attempt to theoretically introduce the idea of applying trust and reputation modeling to CRNs.

The proposed approach suffers from the following drawbacks:

- The authors do not show trust measurement for spectrum sensing or decisions. They only show trust for trusted routing in CRNs.
- The authors do not provide any performance evaluation for how trust

mechanisms could improve the security in CRNs.

- The authors define different types of attacks but they do not show how trust evaluation can defend against these attacks to ensure security in CRNs.

- The authors do not propose a methodology by which trust can be determined at the node level for both networks in CRNs.

Pei et al. [95] proposed a trust management model through the whole cognitive cycle for centralized CRNs to solve the security threats brought by untrustworthy entities, such as selfish, malicious, and faultless nodes. The cognitive base station (CBS) is actually responsible for taking the charge of the establishment and management of the trust mechanism to ensure the safety and reliability of the cognitive cycle. The base station is responsible for monitoring the overall performance of the SUs in the network, and implementing the appropriate incentive or punishment mechanisms to ensure the safety and reliability of the cognitive cycle. The base station can distinguish between legitimate users and malicious users based on the long-term behavior records of the users. Their trust mechanism consists of four parts: trust initialization, updating of reputation, trust assessment and a reward mechanism.

- Trust initialization: The base station establishes the trust list for SUs. The reputation for SUs i is denoted as R_i. At first, the reputation of each SU who passed the authentication is initialized as indefinite.

- Updating of reputation: Reputation is updated using the following equation:

$$R_{i(updated)} = \rho_1 R_{i(past)} + \rho_2 r_i \tag{2.1}$$

where $R_{i(updated)}$ is the updating reputation of user i,

$R_{i(past)}$ is the historical reputation of user i recorded by base station,

r_i is the current trust evidence of user i observed by base station,

ρ_1, ρ_2 is the fading factor, $\rho_1 + \rho_2 = 1$. ρ_1, ρ_2 can be changed according to the security requirements of the network.

- Trust assessment: When the SU gains access to the channel after successful spectrum sensing along the cognitive cycle round, the cognitive base station updates the reputation of that user once. After updating the reputation, the base station classifies it into the corresponding interval of trust to identify the trust state of the user, and then records it in the list of trust.

- Reward mechanism: After the trust mechanism is established, SUs continue to operate along the cognitive cycle. Based on these operations, their reputations and trust states are recorded and updated. The cognitive base station takes appropriate decision depending on the trust assessment result to adjust their strategies within the network so that the network maintains a trend of equal treatment to fair treatment from the beginning to ensure a secure network environment.

The proposed approach suffers from the following drawbacks:

- The authors do not propose any trust-based framework for detecting and solving security threats brought by untrustworthy entities.

- The authors only show the trust value for different types of misbehaving nodes but they do not propose any mechanism to defend against these nodes.

In the next subsection, trust in different working phases in spectrum management is discussed.

2.5.1 Trust-based schemes in secure spectrum sensing in CRNs

Qin et al. [46] proposed a novel trust-based spectrum sensing scheme which can identify misbehaving SUs and make an overall sensing decision by filtering out their reported spectrum sensing results. In their scheme [46], SUs send the sensing results to the Secondary User Base Station (SUBS) and the SUBS aggregates the sensing results depending on each SU's confidence level, θ using equation 2.2.

$$R_p = \theta\Gamma_{BS} + (1-\theta)\frac{\sum_{i=1}^{M}\tau_{ip}\Gamma_{ip}}{\sum i = 1^{M}\tau_{ip}} \tag{2.2}$$

where R_P is the overall sensing result for PU spectrum band p;

θ is the confidence level of the SUBS;

Γ_{BS} is the sensing result provided by the SUBS;

τ_{ip} is the trustworthiness of SU i in the context of the PU spectrum band p;

Γ_{ip} is the sensing result for PU spectrum band p provided by SU i;

M is the number of SUs whose trustworthiness with respect to PU spectrum band p is above a predefined threshold η.

The final decision D_p is made based on the sign of R_p for spectrum usage using equation 2.3.

$$D_p = \begin{cases} 1, & R_p < 0 \\ 0, & R_p = 0 \\ 1, & R_p > 0 \end{cases} \tag{2.3}$$

Qin et al. [46] showed their proposed trust-based approach is able to defend against fabrication attack, on-off attack, denial of service attack, resource hungry attack but the proposed approach does not have a trust-based framework to calculate the node's level of trustworthiness to determine whether it is able to detect and defend against these kinds of attacks.

Kaligineedi et al. [42] also proposed trust-based methods for secure cooperative spectrum sensing in CRNs by detecting the malicious nodes in CRNs which have a significant effect on the performance of the cooperative sensing system. They assign a trust factor $\lambda[u;k]$ for each user, $u \in 1, 2, 3, ...U$ in CRNs.

$$\sum_{u=1}^{U} \lambda[u;k] = 1 \tag{2.4}$$

The trust factor denotes the measurement of reliability of a particular user. Trust factors are used as the weighting factors for calculating the mean of the energy values received from various users. The final decision is made using the trust factors as follows:

$$\sum_{u=1}^{U} \lambda[u;k]e[u;k] \gtrless_{H_0}^{H_1} e_T \tag{2.5}$$

where

e_T is the threshold;

$e[u;k]$ represents the outputs of the energy detectors at various nodes at time instant k for user $u = 1, 2, 3, ...U$;

hypothesis H_0 indicates the absence of the primary signal and

hypothesis H_1 indicates the presence of the primary signal. No prior work has

been done on collaborative spectrum sensing under attacks due to the mobility of CR nodes in CRNs. The proposed approach has the following shortcomings:

- The authors use trust-based methods only for spectrum sensing but they do not show how trust is used in spectrum sensing in CRNs.
- The authors maintain security for spectrum sensing but they do not consider secure communication.
- The authors do not discuss anything about the spectrum availability based on spectrum sensing results.

Jana et al. [96] proposed trusted collaborative spectrum sensing under different path-loss and fading conditions in CRNs using two trust parameters, Location Reliability and Malicious Intention (LRMI), to detect malicious users in CRNs. Location Reliability (LR) reflects the path loss characteristics of the wireless channel and Malicious Intention (MI) captures the true intention of SUs, respectively. Each SU sends spectrum sensing information to the fusion center. The reports for one particular SU at the fusion center are evaluated based on two sources of evidence associated with each report: LR and MI. If the reliability of the user assigned by fusion center drops below a certain threshold (ξ), the user is considered a malicious user. But the proposed approach does not show the complete framework to avoid the malicious user's behavior.

2.5.2 Trust-based spectrum decision schemes in CRNs

Pang et al. [97] also proposed a trust-based spectrum decision scheme to secure cooperative spectrum sensing in CRNs. In their scheme [97], each SU executes spectrum sensing by itself and sends the spectrum sensing

information to a DC (Data Collector) which uses an appropriate data fusion technique to make a final spectrum sensing decision. Nodes which send false information to a DC are identified and their effect is discarded on the cooperative spectrum sensing system. By detecting and analyzing behaviors of SUs in cooperative sensing, the DC can establish a trust model with a PID (Proportional-Integral-Derivative) which can acquire relatively high speed to track the behaviors of neighbors. There are two hypotheses for detecting the PU in a data fusion technique: H_1 and H_0. (H_1 means a PU exists, and H_0 means the channel is free. The problems of existing data fusion techniques have been overcome by the proposed new Weighted Bayesian Detection (WBD) technique. This scheme is able to defend against three types of spectrum spoofing attacks: always-false, always-busy and always-free. An always-false attacker always sends spectrum reports that are opposite to its real local sensing results, an always-busy attacker always indicates that the spectrum is busy while an always-free attacker always reports contrary results. The proposed approach suffers from the following drawbacks:

- The authors determine trust only for cooperative spectrum sensing.
- The authors use trust to analyse anomalous behaviors of selfish nodes but they do not propose any framework to defend against these types of attacks to prevent selfish nodes taking part in CRN communication.
- The prior probability values in the behavior analysis model play a key role, but this calculation needs many priori messages about the CR networks which may limit the deployment of secure cooperative sensing techniques.

2.5.3 Trust-based schemes in secure spectrum sharing in CRNs

Qin et al. [98] proposed a novel trust-aware resource allocation scheme in a centralized CRN in which trustworthiness is measured as a key factor for detecting misbehaving SUs, filtering out their sensing results and allowing trustworthy nodes to gain access to the system resources. The proposed scheme maximizes the total bit rate of SUs by utilizing a system level trust measure. In their scheme, the SUs trustworthiness is first measured and then, depending on the sensing result, the SUBS will decide whether the requesting SUs will be given access to the resources or not. In fact, the SUBS decides whether the PU spectrum band is active or not active. If the PU spectrum band is active, then it will not allocate resources to SUs. If the SUBS decides that the PU spectrum band is inactive and the SUBS is not in a shutdown (penalty) period, it will allocate resources to SUs. But the proposed approach does not include a framework to calculate the trustworthiness of nodes in CRNs nor does it discuss security aspects. Very little work has been conducted on trust used during spectrum sharing to ensure security in CRNs. In the next section, authentication-based mechanisms to ensure security are discussed.

2.6 Authentication-based Schemes for CRN Security

An SU in a CRN always searches for PU's free spectrum for communication. But an attacker or a selfish SU may express itself as a PU to other SUs to gain illegal access to radio channels. Therefore, a secure PU detection mechanism

is necessary in CRNs to distinguish the PU's signal from an attacker's signal.

2.6.1 Location-based authentication schemes

Kuroda et al. [61] proposed a radio-independent authentication protocol for CRNs that is able to support EAP (Extensible Authentication Protocol) transport. This protocol uses user-specific information, such as location information, as a key factor. The factors for authentication and encryption are derived from the historical location registry of a mobile terminal. As the position of the mobile user always varies, the location information is frequently updated. Location information is used in this protocol as the basis for extracting secrecy, and can reduce the costs of AAA consultation using a long-term credential during switchover. The key factor of this protocol is a location-carousel, which is a data structure that represents the unique location information of every mobile terminal as well as the notion of synchronization between location-carousels at the mobile device and the corresponding network node. The key management protocol assumes user-specific information as an initial bootstrap, and subsequent keys for authentication and encryption are derived from the location-carousel. This protocol supports light weight mutual authentication and could be implemented on a mobile node that has limited memory and power. This protocol is able to defend against man-in-the middle attacks. However, Kuroda et al.'s [61] protocol is based on the strong assumption that consumer premise equipment should be registered in the co-located CRN offline via a robust and secure method and does not consider privacy issues. Therefore, the protocol cannot be applied to the IEEE 802.22 Wireless Regional Area Network (WRAN).

In order to overcome Kuroda et al.'s [61] shortfall, Hyun Sung Kim [82]

proposed a location-based authentication protocol using the location-carousel as a secret credential in CRNs. This protocol was constructed on the assumption that there is no secure channel between entities in a CRN and BS and the home agent (HA) has a key pair based on the public key cryptosystem and a certificate for it. Additionally, it is also assumed that the BS should be fully trusted in the CRN. The protocol has 9 steps as follows and the overview of the protocol is depicted in Figure 2.3:

- step 1 : BS_i sends an identity request to CPE_i.
- step 2 : CPE_i responds back to BS_i for the identity request.
- step 3 : BS_i asks for the carousel of CPE_i to HA
- step 4 : HA responds to BS_i with the encrypted carousel of CPE_i.
- step 5 : BS_i sends a challenge message to CPE_i.
- step 6 : CPE_i answers back to BS_i with a response message.
- step 7 : BS_i responds to the authentication request with either an authentication success message or an authentication fail message.
- step 8 : BS_i notifies the new location-related information of CPE_i to HA by using the previously derived authentication key.
- step 9 : HA resynchronizes the carousel for CPE_i

Zhang et al. [99] proposed a node-to-node authentication scheme based on location-based keys for designing compromise-tolerant security mechanisms for sensor networks. This location-key based authentication scheme has the following properties:

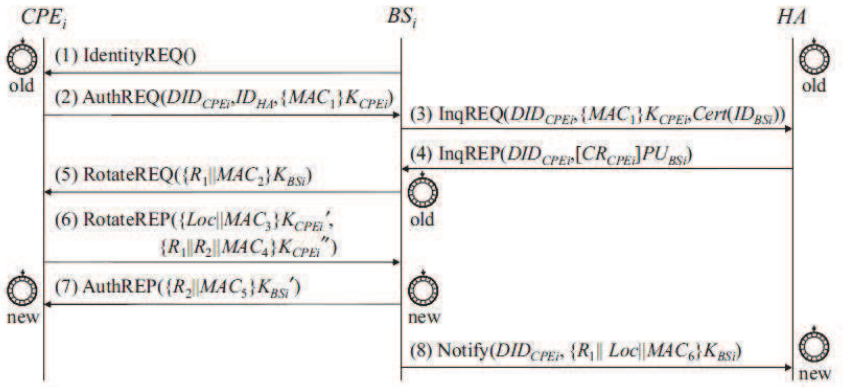

Figure 2.3: Location-based authentication protocol [82]

- First, location-based keys (LBKs), each of which is addressed to a nodes unique location ID deployed in a large geographical area.
- Second, a node-to-node neighborhood authentication scheme using LBKs, which is not only able to localize the impact of compromised nodes within their vicinity, but also to establish pairwise shared keys between neighboring nodes at the same time.
- Third, LBKs's effectiveness to act as efficient countermeasures against different types attacks on sensor network routing protocols.

In a secure location-based authentication scheme [99], one node, A, sends an authentication request, including its location $pos_A =< x_A, y_A >$ and a random nonce n_A, to its neighboring node. Upon receiving A's request, node B with location $pos_B =< x_B, y_B >$ first needs to confirm that the requesting node A's position is in its transmission range by checking equation 2.6

$$(x_A - x_B)^2 + (y_A - y_B)^2 \leq R^2 \tag{2.6}$$

where 'R'is the transmission range.

If the check is successful, node B sends a reply message including its own location $pos_B =< x_B, y_B >$ and a random nonce n_B to node A, otherwise node B ignores node A's request because node A is by no means a neighboring node. This position checking is necessary because otherwise an adversary intentionally might send an authentication request to B, including the location of one compromised node, say D, who is out of the transmission range of B, by boosting the transmission power. In this case, B might be tricked into believing that D is its authentic neighbor as D has the correct LBK corresponding to the claimed location so that it can pass the authentication process [99].

Chen et al. [65] proposed a transmitter verification scheme, called LocDef (localization-based defense), which verifies the PU's signal by utilizing both the signal characteristics and location of the signal transmitter. This scheme is able to detect PUE attacks and defend against PUE attackers. The localization scheme utilizes an underlying wireless sensor network (WSN) to collect snapshots of received signal strength (RSS) measurements across a CR network. By smoothing the collected RSS measurements and identifying the RSS peaks, one can estimate the transmitter locations. LocDef can be integrated into existing spectrum sensing schemes to enhance the trustworthiness of the sensing decisions.

2.6.2 Identity-based authentication schemes

Identity-based authentication is one of the key factors for ensuring secure communications in CRNs. Zhu et al. [53] proposed a new authentication mechanism for CRNs which is based on third-party Certification Authority (CA). The mechanism integrates EAP-SIM and EAP-TTLS, adopts SIM authentication for terminal CR users and secure tunnel +certificates for

servers. CA solves the identity authentication problem of base stations and ensures secure communication between the base station and CA by establishing a security tunnel in core networks. This mechanism consists of 15 steps as shown in Figure 2.4. Zhao et al. [60] proposed an authentication scheme in the physical layer by identifying transmitters in CRNs to differentiate between the PU signal transmitter and the PUE attacker. In their scheme, [60], the verifier extracts the signal from the frequencies of interest by using a band-pass filtering technique and obtains the time domain samples of the transmitted signal. Then, the time domain samples are converted to frequency domain samples, which contain the transmitter location fingerprint information, by implementing the power spectrum density (PSD) estimation technique. These samples are used as the input of the wavelet transform, then the characteristics of the transmitter fingerprints can be extracted.

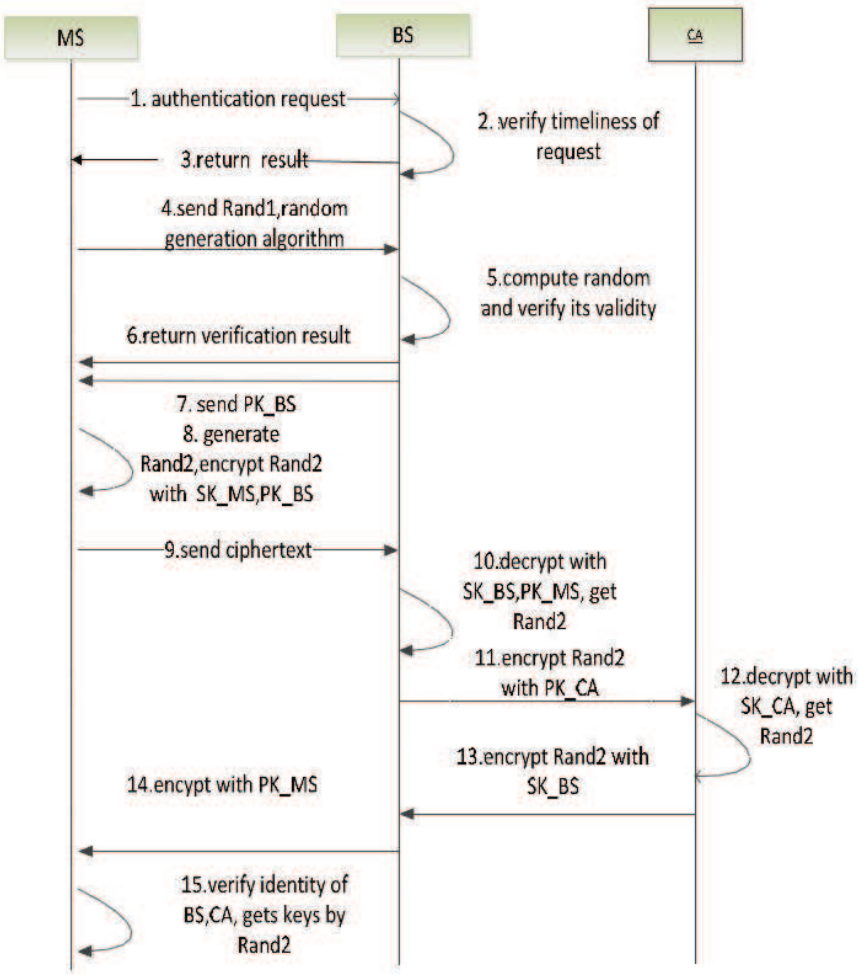

Figure 2.4: Improved identify authentication process [53]

In the proposed authentication schemes, cryptographic techniques have been proposed to ensure security in CRNs, but most of them work in the digital domain and encryption techniques require too much processing power and memory to be used by the cognitive radio nodes. Therefore, it is infeasible to use cryptographic-based authentication schemes to ensure security in CRNs.

2.7 Critical Evaluation of the Existing Approaches to Maintain Secure Communication in CRNs

In this section, a critical evaluation of the approaches discussed in the literature related to trust and security in CRNs is analysed. The aim in this section is to draw an integrative overview in order to discover and identify the main issues in the literature that need to be addressed so as to maintain trustworthy relationships in CRNs to ensure secure communication so that no untrustworthy, misbehaving or selfish node is able to take part in the communication. To ensure trust-based communication for security purposes, there is a need to have a 'complete methodology' which would highlights and represents the various aspects that are required for activities such as trust establishment, spectrum sharing, authentication checking and system availability enhancement which assists the CRN's operation to make an informed decision about its communication.

As can be seen from the discussion in the literature, various researchers have proposed different techniques for determining the level of 'trust' and using it to maintain secure communication between nodes in different areas. For example, trust has been analysed from a security aspect to maintain secure communication in wireless communication such as WSNs etc. But none of them provides a complete methodology which represents and models all the aspects required for establishing trust and using if for secure communication. There are still gaps in the research on approaches which measure and maintain

trust for secure communication in CRNs. For example, Chen et al. [45] defined a mathematical framework to describe trust for CRN communication but this framework does not propose a complete methodology to establish trust to ensure security in CRNs. Qin et al. [46] proposed a novel trust-based spectrum sensing scheme which can identify misbehaving SUs and make an overall sensing decision by filtering out their reported spectrum sensing results, but their approach didn't show how trustworthy nodes could take part in spectrum sharing in CRNs. Jana et al. [96] proposed a trust-based approach for collaborative spectrum sensing in CRNs but they didn't show how this trust-based approach could enhance security in CRNs. Kaligineedi et al. [42] also proposed trust-based methods for secure cooperative spectrum sensing in CRNs but they did not show how security aspects are improved to ensure secure communication in CRNs. Qin et al. [98] proposed a novel trust-aware resource allocation scheme in a centralized CRN in which trustworthiness is measured as a key factor for SUs to gain access to the system resources. The scheme can detect misbehaving SUs and filter out malicious attacks while maximizing the total bit rate of SUs but their approach did not propose a framework for a trustworthiness measurement to ensure secure spectrum sharing in CRNs. Pei et al. [95] proposed a trust management model through the whole cognitive cycle for centralized CRNs to solve the security threats brought by untrustworthy entities, such as selfish, malicious, and faultless nodes, but they didn't show how spectrum decision making takes place in a spectrum sharing mechanism.

Authentication is one of key factors to ensure security. Subsection 2.6 summarizes the different authentication mechanisms in CRNs but most of these approaches [61, 82] use cryptographic techniques which need more processing

power and memory. No approach proposes a light weight cryptographic-based authentication scheme to ensure secure communication in CRNs which requires less processing power and memory.

Hence, the main inadequacy of the approaches, from the literature discussed above, in proposing a complete methodology which represents all the aspects of trust-based security in CRNs for ensuring secure communication, can be summarized as:

- **No guidelines for a security model definition:** Current spectrum management schemes lack a formal security model in CRNs. The existing literature assumes only a hierarchical security model or distributed security model according to the corresponding network topology. There is no quantization in security model and hence the security proof is only a heuristic description.

- **Lack of trust-based authentication scheme:** A variety of techniques have been proposed [53, 61, 82] by which authentication can be achieved. But, all of these approaches are based on cryptographic techniques which require much processing power and memory. However, in the context of CRN, 'trust' is an important concept to consider when authentication has to be achieved on the basis of believing that a new user joining the group will not cause security issues. Trust, in this context, is defined as the belief that the security of a network will not be compromised as a result of a user's action after the user is permitted to join the network. Having such a trust-based authentication mechanism allows only non-malicious SUs to access the licensed spectrum and network resources; thereby playing a complementary role or an

inside-out role in improving overall security and creating a balance in the whole CRN. In the current literature, even though the importance of trust during the process of authentication has been discussed, no trust-based framework in CRNs has been proposed based on which users are authenticated to access the network. To summarize the problem, there is no methodology proposed in the literature by which trust can be established for authentication checking to ensure security in CRNs.

In Chapter 3, the problem associated with trust establishment for authentication in the existing literature is formally identified and defined and in Chapter 4, a solution overview for the defined problem in the existing literature is presented.

- **Lack of a trust-based spectrum sharing mechanism:** Spectrum sharing is one of the major functionalities of CRNs. Several approaches, such as the Game-Theory approach [7] and the auction-based approach [17], have been proposed for spectrum sharing in CRNs but none of them consider security during the spectrum sharing mechanism. The spectrum sharing mechanism between the primary and secondary networks in a CRN requires SUs obey the opportunistic access rules. Selfish and malicious users may send false data or falsify the sensing data, or may want to use a PU's spectrum and fail to vacate the spectrum, even if the PU wants to reclaim its own spectrum. These are termed 'soft security threats' and are addressed by using the notion of trust. So, PUs need to be provided with a trust guarantee from the SUs to allow them to use their free spectrum. However, such a trust-based spectrum sharing mechanism has not been proposed in the literature to overcome

the soft security threats in CRNs. To summarize the problem, there is no methodology proposed in the literature by which spectrum can be shared in a secure way in CRNs.

In Chapter 3, the problem associated with secure spectrum sharing in CRNs in the existing literature is formally identified and defined and in Chapter 4, a solution overview for the defined problem in the existing literature is presented.

- **Deficiencies of the Availability Enhancement Scheme:** According to CRN architecture, the key nodes [53] generate and store all of the important data such as the different keys that are used to communicate in the network and perform the major responsibilities for maintaining the security of the network. There is not much work in the literature which selects a node as the key role to facilitate system security. However, it is possible that malicious nodes may attack the key nodes of the CRN, forcing the whole network to perform at a degraded level or even take it offline. If attackers attack the network with a view to degrading the system performance, the system availability and reliability will fall in a dramatic way and the whole network will collapse. However, there is no methodology currently proposed for availability enhancement in CRNs for smooth and robust communication.

  In Chapter 3, the problem associated with system availability enhancement in CRNs in the existing literature is formally identified and defined and in Chapter 4, a solution overview for the defined problem in the existing literature is presented.

2.8 Conclusion

In this chapter, a survey of the existing literature is carried out. The existing literature is evaluated critically with a view to analyzing and assessing each category to ensure security in CRNs, and found that no proposal in the literature presents a complete method of using trust to ensure secure communication in CRNs, according to its characteristics. In the next chapter, the problems are defined that need to be addressed in this thesis.

Chapter 3

Problem Definition

3.1 Introduction

As discussed in Chapter 1, due to the significant advances in pervasive computing and wireless communication technology, cognitive radio networks (CRNs) have gained wide application. However, some unique features of CRNs make them more vulnerable to security attacks than their wired counterparts. Security countermeasures should be taken to resist these attacks and improve security aspects in CRNs. As discussed in Chapter 1, one of the ways by which this can be achieved is by using an inside-out notion of improving the security; that is by strengthening the notion of trust.

By undertaking a comprehensive critical analysis of the existing technology and approaches, it was found that, despite the significant contributions which have been made over the decades in wireless security, very few practical approaches, especially in terms of trust-based security solutions for CRNs, have been proposed in the literature. In addition, as discussed in Chapter

2, some important auxiliary properties of trust based schemes, such as trust-based authentication, trust-based spectrum sharing and trust-based system availability enhancement have not been addressed in the current approaches to improve the overall performance of CRNs in a secure way.

To address these shortcomings in the literature, in this chapter, the problem that this thesis intends to address is identified and outlined. In Section 3.2, the set of definitions that will be used throughout the thesis is given. In Section 3.3, the motivation for the research and the definition of the problems to be addressed in this thesis are outlined. In Section 3.4, the main problems are broken down into different research issues to propose a solution to the identified problems. In Section 3.5, the research method adopted in this thesis is introduced. Finally, in Section 3.6, the chapter is concluded.

3.2 Key Concepts and Preliminaries

In this section, the key concepts and preliminaries which will be used in this chapter to formulate the problem and subsequently throughout the thesis to propose a solution to the defined problem are explained.

3.2.1 Trust

As explained in Chapter 1, in the literature, there are two understandings of the definition of trust: 1) trusted computing which trust refers to the interacting entity accepting the provided security mechanisms adopted by the other entity by which it feels safe and not vulnerable to the outside forces which might hamper its interaction; 2) the level of belief that the two agents

have in each other for the achievement of desired outcome. In this thesis, the second understanding of trust is considered. Trust is defined in wireless networks as a particular level of subjective probability with which an agent assesses that another agent or group of agents will perform a particular action. Trust is defined as a function "Trust(A, B, F, C)" that node A has in an agent B to perform an action F in a context C [100].

3.2.2 Security

The security of a system is defined as the degree of assurance that a system provides in offering its normal functionality in a correct way with no harmful outside effects which can affect the system. The security of a wireless network is defined by Hu et al. [101] as the protection mechanism of the system which is able to prevent the system from unauthorized modification, destruction, or disclosure.

3.2.3 Trustworthiness

Trustworthiness is defined as the likelihood of an agent completing a certain task. The trustworthiness of an agent is determined from an agent's own past interaction.

3.2.4 Authentication

Authentication is a service related to identification. This function applies to both entities and the information itself. Two parties entering into communication should identify each other. Authentication ensures that the entities with whom one communicates are the expected ones and the received

data is the original data sent by the counterparts.

3.2.5 Availability

Availability is one of the fundamental requirements for any type of network. Network availability is referred to as data availability (user information, routing tables, etc.) of the network. The availability of a system provides assurance that the services of the system are available at all times and are not denied to authorized users [101]. Availability in wireless networks is expressed as the availability of the wireless transmission medium, whereas in the context of cognitive networks, availability refers to the ability of primary and secondary users to access the spectrum to continue its communication [102].

3.2.6 Unavailability

Unavailability refers to the functionality of a system when it fails to perform its normal functionality because of either a planned or an unplanned event.

3.2.7 Reliability

Reliability is defined as the probability that a given demand vector is achieved in order to increase network effectiveness quantitatively, and help network designers tune CR network parameters (for example, the number of channels and radios) for better performance.

3.2.8 Downtime

Downtime refers to a period when a system is unavailable and thus fails to provide or perform its normal functionality. During downtime, the system

introduces an extra system cost which is termed downtime cost.

3.2.9 Trusted Third Party(TTP)

A trusted third party (TTP) is an entity which maintains the interaction record between two parties, both of whom trust the third party. The third party reviews all critical data transactions in the communications between the parties, based on the ease of creating fraudulent digital content.

3.2.10 Trust Repository

The trust repository acts as a mechanism to store and publish trust values that have been provided by the provider to secure communication. The properties of the trust repository are as follows:

- Keeps the trust values secure
- Makes the trust values are available to the appropriate communicating party
- Sends the trust values to the appropriate party based on the request
- Maintains authenticity at a low cost

3.2.11 User/Node

The term *user* refers to a member in a network which is attached to the network and is capable of processing, gathering information and communicating with other connected members in the network. The terms 'user' and 'node' are used interchangeably throughout the thesis.

3.2.12 Deprivation rate

The deprivation rate is the rate at which a secondary user (SU) is forced to vacate the band on the reappearance of the primary user (PU).

3.2.13 Blocking rate

The blocking rate is the rate at which all the sub-bands are occupied by the SUs in the network.

3.2.14 Utilization ratio

The utilization ratio is defined as the ratio of the radio bands that are used by the PUs and SUs to the total number of radio bands that are available in the system.

3.3 Problem Definition

As mentioned in Chapter 1, different security threats in CRNs need to be addressed by enhancing different aspects of security, such as authentication checking by using trustworthiness, mechanisms for secure spectrum sharing, and mechanisms for improving the system availability. Chapters 1 and 2 discussed that one of the ways to improve these aspects of security for secure communication in CRNs is by incorporating trust. By using trust in CRNs, the base station or other nodes can identify and classify malicious and selfish nodes as "untrustworthy" based on their trust label in the network and take the necessary steps to avoid or stop communication with these malicious nodes which intentionally send false data to the network or do not follow the spectrum

usage policies of the network in order to degrade the network performance. As discussed in the previous chapter, the literature shows that significant advancements have been made in the area of trust management for CRN security. But most existing schemes have drawbacks which result in unsolved problems that merit in-depth research. In this section, several problems related to CRN security are discussed in the following three areas :

- Trust-based schemes to authenticate users for improving secure communication in CRNs
- Mechanisms for secure spectrum sharing in CRNs
- Mechanisms for improving system availability in CRNs

In each of these areas, a discussion is presented from two perspectives, namely: existing solutions in the literature, and the research gaps in these solutions which form the key requirements in defining the problems that will be addressed in this thesis.

3.3.1 Trust-based authentication schemes for improving secure communication in CRNs

3.3.1.1 Existing solutions of trust establishment in CRNs

In the literature, trust has been considered as one of the most suitable ways to ensure security in wireless networks [103–105]. As shown in Figure 3.1, a standard trust establishment scheme has four stages, namely: establish communication between nodes, gather experience and recommendations, calculate trust and update trust values.

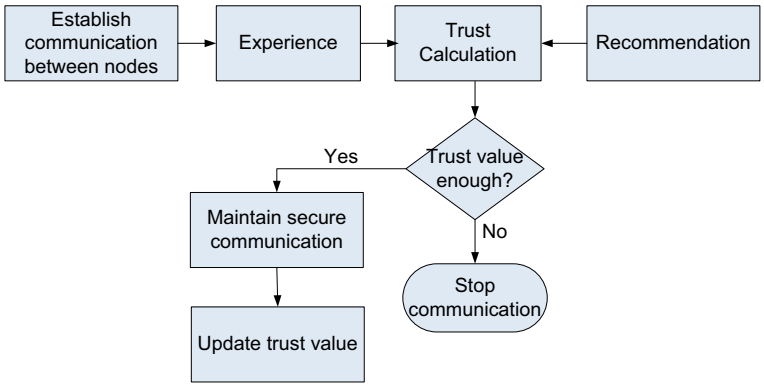

Figure 3.1: The general process of a standard trust establishment paradigm

Using this scheme, when a node A, for example, needs to interact with another node B, they will establish communication link between them. Node B will check its previous experience with node A and the recommendations of the surroundings nodes for node A will be also checked. After receiving those, node B will calculate the total trust value for the communication with node A. If the calculated trust value is enough to set up a secure communication link between the nodes, then node B will interact with node A and update A's trust value after the interaction, otherwise node B will stop communication with node A.

Several approaches have been proposed in the literature that establish trust in CRNs [45]. For example, a trust-based spectrum sensing scheme is proposed to identify misbehaving SUs and make the overall sensing decision by filtering out their reported spectrum sensing results [46]. Trust-based mechanisms have been proposed to: (a) secure cooperative spectrum sensing in CRNs [97]; (b) defend against False Alarm attack and False Alarm Miss Detection attack by detecting untrustworthy malicious nodes, according to their reporting histories [67]; (c) detect suspicious SUs; (d) defend against PUEA attack [106]; and

(e) enable cognitive radios to access the distributed computation, storage, and resources available in the cognitive radio environment by combining the requirements of the trustworthiness and the QoS of the links with the route [107]. Almost all trust establishment schemes for CRNs follow the general trust management paradigm, or a variant. However, as mentioned in the previous chapter, none of the approaches consider the trust establishment process according to specific assessment criteria and the dynamic nature of the interaction when determining the trustworthiness of a CR node for secure communication in CRNs and therfore have the following drawbacks:

3.3.1.2 Research gaps in existing trust establishment schemes in CRNs

- In a CRN, by using Artificial Intelligence (AI) and Dynamic Spectrum Access (DSA) functionalities, PUs share their unused or under-utilized spectrum with SUs for the efficient utilization of the radio spectrum. Although such functionalities provide advanced and flexible communication options, they also render the CRN vulnerable to security attacks, both from local and outside threats. For example, it is quite possible that the SUs could be malicious or selfish at any time due to the unique characteristics of CRNs and spread different security threats in the network which will hinder the network's normal performance. In order to avoid such security threats and the problems, there is a need for a trust establishment framework that is able to detect the malicious or selfish nodes, based on their level of trust, to avoid their selfish behaviour and allow only the trustworthy nodes to access the network resources. Although some research [45], [46], [65], [107] has been conducted on using

trust in CRNs, most have only been used for trusted routing in CRNs, and trust as a mechanism has not been used before for authentication checking during spectrum sharing, spectrum detection or for measuring spectrum availability. The omission of trust establishment for such spectrum management aspects causes CRNs to become more vulnerable to security threats and attacks by malicious nodes.

- One of the main drawbacks of the proposed trust establishment schemes in the literature is "biasing" by other nodes. As a result of this drawback, there is a chance that cognitive radio nodes may be compromised by other surrounding malicious nodes through a biasing technique which always recommend a biased trust value for the candidate node. In other words, if any cognitive radio node is compromised through biasing, this can lead to the assignment of false trust values for the candidate node. This problem calls for the development of a proper trust-based mechanism to check the candidate node's actual trust value and avoid the problem of biasing.

- Approaches have been proposed in the literature that discuss different types of attacks in CRNs but they do not show exactly how a node's trustworthiness level is able to detect and defend against these attacks. For example, in the literature, trustworthiness is used to secure spectrum sensing and decisions by integrating a transmitter verification scheme, called LocDef (localization based defense), into the existing spectrum sensing scheme [65]. But this approach is only able to defend PUEA attacks in CRNs. In other work, trust and reputation are integrated to mitigate the threat of Spectrum Sensing Data Falsification (SSDF)

attacks on CRNs in [38]. However, it does not propose any trust modeling scheme for CRNs. A trust-based malicious user detection algorithm is developed, based on the trust value, to detect suspicious users in CRNs [80], but this method is only able to detect one malicious node. Trust-based approaches [46] are able to defend against different types of attacks but they do not show exactly how a node's trustworthiness level is able to detect these attacks. Therefore, there is a need to develop trust establishment schemes in CRNs in order to identify suspicious nodes based on their level of trust.

3.3.1.3 Existing solutions in authentication mechanisms in CRNs

Once trust is established between different nodes, the next step is to authenticate the node's request based on its level of trust. Authentication is an important tool which is used to distinguish the valid user's signal from an attackers signal in CRNs. It is necessary to have a secure authentication mechanism in CRNs to authenticate the PU's signal and hence ensure overall system security. The current research on authentication mechanisms in CRNs has been examined from various aspects, such as location-based authentication, identity-based authentication, cryptographic-based authentication, filtering false data, PKC-based authentication, and lightweight authentication.

A radio-independent authentication protocol based on user-specific information, such as location information, as a key factor, is used to support EAP (Extensible Authentication Protocol) transport in CRNs [61]. The location-based authentication protocol uses the location-carousel as a secret credential to ensure security in CRNs [82]. An authentication method uses

a location verification scheme, called LocDef (localization-based defense) and received signal strength (RSS) measurements to detect an attacker's signal and identify the PU's signal in secure spectrum sensing in CRNs [65]. A simple but efficient PU identification scheme, based on public key ciphers, uses digital signatures for authentication purposes to enhance CRN security [25]. An authentication scheme provides secure verification of the spectrum by integrating cryptographic signatures and wireless link signatures that enable PUs to detect the presence of PUE attackers and hence improve system security [108]. Another integrated authentication approach is proposed to authenticate the PUs signal by integrating cryptographic and link signatures in CRNs [109]. The PU authentication approach adds a helper node which is placed physically closer to the PU to detect the primary signal [62]. However, most approaches are used only to detect and identify the PU's signal, they are lacking from detecting malicious users in CRNs.

3.3.1.4 Research gaps in authentication mechanisms in CRNs

In the literature, most cryptographic primitives work in the digital domain, it may not be possible to integrate them into analogue TV signals as in the CRN domain. A typical public key infrastructure (PKI) scheme which achieves secure routing and other purposes in typical ad-hoc networks cannot adequately guarantee the security of CRNs, given the limited communication and computation resources. Although several mechanisms [65], [82] have been proposed to defend against specific attacks and authenticate PUs using a location carousel as a secret credential, these approaches are not suitable for ad hoc/distributed scenarios in CRNs, in which the PU and SU have comparable power levels. To avoid these problems, there is a need for a trust-based

authentication framework which authenticates the users in a CRN, based on a trust value, to avoid the adverse impact of malicious and selfish nodes and to enhance the security of communication in CRNs.

3.3.2 Mechanisms for secure spectrum sharing in CRNs

3.3.2.1 Existing solutions in spectrum sharing in CRNs

In the literature, different approaches have been proposed for spectrum sharing in CRNs. Of these, the Game-Theory approach [7] and the Auction-based approach [17] are the most popular and efficient. However, very few work is concerned about secure spectrum sharing in CRNs in which malicious users are identified and excluded from the network so that they cannot access to the PU's free spectrum. A combinatorial auction-based spectrum sharing approach is proposed in [110] where SUs have the flexibility to bid for a bundle of frequencies at different times. The TRuthful doUble Spectrum aucTions (TRUST) framework, which aims to achieve truthfulness and enable spectrum reuse, assists multiple sellers and buyers to trade spectrum dynamically [111]. A new cognitive radio spectrum sharing scheme is developed, based on the trust-based bargaining model which dynamically adjusts bargaining powers and adaptively shares the available spectrum in a real-time online manner [112]. A spectrum sharing scheme in CRNs has been developed based on the Continuous Time Markov Chain (CTMC) model, using the properties of Orthogonal Frequency Division Multiplexing technology [77]. Policy management architecture is used to validate the spectrum sharing approaches in the face of possible security threats on the network behaviour and performance [75]. However, none of the approaches consider security

during spectrum sharing in CRNs.

3.3.2.2 Research gaps in secure spectrum sharing in CRNs

In the literature, there is still some research gaps which are not identified such as follows:

1. The SU needs to vacate the spectrum when the PU needs it, which disrupts its service until it finds another free spectrum. If it cannot find another free spectrum, then its communication is dropped. Therefore, there is a need for a framework which minimizes the problem of the SU's service disruption during spectrum sharing.

2. It is possible that malicious SUs in CRNs search for free spectrum and intentionally hold it without being willing to vacate it, even if a PU later wants to reclaim his own spectrum. This misbehaviour paralyzes the whole network performance. To identify and avoid such threats and misbehaviour, there is a need for a trust-based framework that will assess the trust value for the requesting authenticated SU from both primary and secondary networks in CRNs to assign spectrum based on the trustworthiness label so that no malicious or untrustworthy nodes have access to the spectrum to ensure secure communication through trustworthy spectrum sharing in CRNs.

3. Sometimes, SUs either need to wait a long time to obtain access to another free spectrum or they cannot find another free spectrum band after vacating the spectrum on the reappearance of the PU, as all the spectrum bands are either being used by PUs or SUs. In such scenario, their communication is always blocked. In order to maintain smooth

communication in CRNs and to avoid all dropping and blocking, there is a need for a framework which will balance the number of SUs and PUs in a CRN so that spectrum is always available for the SUs to continue their communication instead of being blocked or dropped.

Although some research [110], [112], [77], [75] has been conducted on spectrum sharing in CRNs, most contain the abovementioned research gaps and no solution to date has addressed the security issues during spectrum sharing in CRNs.

3.3.3 Mechanisms for improving system availability in CRNs

3.3.3.1 Existing solutions in system availability in CRNs

Availability is an important aspect of a secure system. The current research on system availability in CRNs has been examined in terms of channel utilization, deprivation rate, blocking rate, etc. The availability of CRNs depends on the PU's traffic and other attributes. The availability and service of SUs also vary with PU's traffic. The amount of available service that can be achieved from the free bands in a spectrum accessed by PUs is called the capacity of SUs.

Co-operative spectrum sensing is a key function of CRNs to prevent harmful interference with licensed users and identify the spectrum availability to improve the network functionality [113]. The CTMC is used in spectrum access models to increase spectrum utilization in CRNs [114]. The proposed scheme is a non-random access method to remove the forced termination states in CRN system models to reduce the probability of call dropping and blocking.

A distributed cluster agreement algorithm called Spectrum-Opportunity Clustering (SOC) is proposed to increase the availability of common idle channels in cluster-based CRNs [115]. In the proposed approach, the control channel can migrate from the current occupied channel via the PU to another free channel without the need to form a re-cluster. In collaborative spectrum sensing, a number of cognitive radio nodes form a network and the final decision regarding the availability of spectrum opportunity for the CRN is based on the information received from all the cognitive radio nodes [116]. The availability of spectrum for SUs is identified using the Probability Mass Function (PMF) in an OFDMA-based cognitive radio system for different request distributions [117]. The neural network concept is adopted to predict the availability of spectrum for cognitive radio users where the training data is assumed to be available, hence, the accuracy of the spectrum prediction by the SU can be improved significantly [118]. The CTMC-based spectrum access model can increase spectrum utilization in CRNs [114] but the authors did not demonstrate any correlation between system availability and spectrum utilization, nor did they show how the system availability can be increased by reducing the probability of call dropping and blocking. However, most approaches only consider spectrum availability in CRNs, but do not show the system availability.

3.3.3.2 Research gaps in system availability in CRNs

Apart from the solutions discussed above in system availability enhancement, there are still some research gaps such as follows:

- According to CRN architecture, there are several key nodes which are responsible for storing all the important data and performing the major

tasks of the network such as maintaining and updating the trust value of all member nodes in the network. However, if a malicious node is successful in becoming the key node then it can compromise the network and easily obtain the network's data and intentionally change both the data and the network parameters, such as routing information, to degrade the network's performance. There is not much existing work in the literature on a feasible process for selecting a node to perform the key role of facilitating system security. Therefore, there is a need for a framework that is able to select the most reliable and trustworthy nodes as the key nodes which will not be easily compromised by attackers and will undertake the major responsibilities in the event of any attack or error to ensure the smooth continuation of communication in the network.

- Although having a trusted relationship between nodes assists in having an outside-in role for improving the overall performance and security of CRNs, it is quite possible that in the event of a security attack, malicious nodes may attack the key nodes of the CRN and force the whole network to perform at a degraded level or even take it offline, thus decreasing system availability and increasing downtime. Therefore, there is a need for a framework that will increase the system availability and reliability and decrease the downtime cost by performing all the major tasks in cases where the key nodes have been compromised and ensure smooth communication by providing continuous service to all users. Although some research [114, 115] have been conducted on increasing channel availability or utilization in CRNs, no prior work has been done

to enhance system availability.

- In the event of an attack, malicious nodes could join the network by falsifying their identity and use free spectrum to jam the network by continuously sending false data packets and preventing other SUs from using vacant band. As a result, the network performance is degraded in an exponential way by these malicious nodes joining the network. The same thing is possible in the case of a member node leaving the network in a malicious way. If a member node leaves the network abnormally without notifying the other member nodes about its leaving, then the node which has been compromised by the malicious users can reveal all the network information to the malicious users, making the network vulnerable. Furthermore, when nodes are attacked by malicious users, they can also join and leave the network abnormally, without notifying the other nodes in the network and jam the whole network. Several research studies have been conducted on nodes joining and leaving in CRNs. Normal and abnormal node joining and leaving processes are considered as either good manners or bad manners, respectively, in relation to updating the trust value in the model [119]. The Trust-value Updated Model [120] has been proposed to authenticate the nodes when they join and leave the network in ad-hoc network. However, in the existing literature, there is no framework in CRNs that ensures a trust-based joining and leaving process to enhance system security. Therefore, there is a need for a framework that is able to allow the nodes to join and leave the network in a secure way to avoid the security threats brought by malicious nodes and update the trust value depending

on their performance.

Hence, based on the above discussion, the problem that will be addressed in this thesis is defined as follows :

To develop a trust-based framework to maintain secure communication in cognitive radio networks in which a trust relationship can be established between different nodes to authenticate the node's request. The trust value is used to select the key nodes to perform the key responsibilities and to secure spectrum sharing by avoiding malicious users' behavior and to improve the system's availability through the automatic reconfiguration in the network.

In the next section, the research issues that will be addressed to solve the abovementioned problems in CRNs will be discussed.

3.4 Research Issues

In the previous section, three problem areas were defined, with the current solutions and the research gaps arising from each solution. Deliberations on these research gaps have raised several issues which need to be addressed in order to provide a solution to the broadly defined problem. In the following subsections, each issue and its relevance to the research gap addressed in this thesis is discussed.

3.4.1 Issue 1: Propose a trust-based authentication framework which improves the security of communication

As discussed in Chapters 1 and 2, the main focus of using trust in CRNs is to defend against soft security threats, especially when authentication has to be achieved to ensure secure communication. Trust-based approaches [46], [80] are proposed to detect and defend against suspicious users, and different types of attacks in CRNs. However, most trust-based mechanisms have only been used for routing schemes in CRNs. Therefore, a trust establishment framework is proposed to establish trust between different nodes in CRNs to avoid their malicious behaviors, exclude them from accessing the network resources and to authenticate only trustworthy user's request to use the network resources from either the primary or secondary network.

Untrustworthy malicious users can break down the network's normal activities by accessing the network and creating a 'biasing' problem by assigning a false trust value for a node. In order to solve these problems, there is a need for a trust establishment framework that solves the 'biasing' problem to determine the node's actual trust value in the network, thus ensuring secure communication in CRNs.

This thesis aims to highlight the need to have a trust establishment framework for authenticating users and to solve the biasing problem in CRNs. To achieve this, Chapter 4 briefly describes the proposed trust-based authentication framework which is further elaborated in Chapter 5. The

scheme improves the overall security by authenticating only trustworthy user's request to access the network, thereby avoiding the damaging behaviors caused by untrustworthy entities, such as selfish or malicious nodes by preventing their request and access to the network's resources.

3.4.2 Issue 2: Propose a trust-based spectrum sharing scheme for secure communication in CRNs

The objective of this thesis is to propose an approach to ensure secure communication by using the notion of trust in CRNs. Selfish and malicious users always intentionally send false data or falsify sensing data to obtain access to the PU's spectrum and once they have access, they may not be willing to vacate the spectrum on the return of the PUs. Trust-based authentication of the requesting node, as mentioned in research 'Issue 1', only ensures that the request is coming from a valid node. However, this does not ensure the commitment of that node to various CRN policies such as vacating the spectrum when the PU needs it again, ensuring fairness in sensing result etc. Therefore, trust-based solution needs to be proposed in spectrum sharing so that untrustworthy nodes are not given access to share the spectrum which causes the network performance to degrade.

This thesis highlights the need for a trust-based spectrum sharing scheme in CRNs to ensure secure and trustworthy communication. Chapter 4 briefly describes the proposed secure spectrum sharing mechanism which is elaborated further in chapter 6.

3.4.3 Issue 3: Propose a model for minimizing disruption to an SU's service during spectrum sharing in CRNs

According to the CRN working principles, as an SU needs to vacate the spectrum when the PU needs it again, the SU's service is disrupted until it searches or access another free spectrum. Therefore, its service is either dropped or blocked during spectrum sharing and results in the SU's service being disrupted. To solve this problem, there is a need for an approach which can ensure minimum service disruption when it has to vacate a spectrum it has been using.

This thesis highlights the need for such a framework that proposes a state transition diagram showing the states through which an SU should go to minimize the disruption to its service during spectrum sharing. Chapter 4 briefly describes the proposed working states of the diagram which is elaborated further in chapter 6.

3.4.4 Issue 4: Propose a scheme for balancing the number of SUs and PUs during spectrum sharing in CRNs

If there are more SUs in a CNR than PUs, some SU's communication may be dropped or blocked due to spectrum band being unavailable, which may lead to service disruption when all the sub-bands are occupied by either other SUs or PUs. Therefore, to solve this problem, a scheme needs to be proposed to

balance the number of SUs and PUs during spectrum sharing in CRNs. This thesis highlights the need for such a model which balances the number of SUs and PUs in CRNs and ensures spectrum sharing between multiple PUs and SUs. Chapter 4 briefly describes the proposed working states of the diagram which is elaborated further in chapter 6.

3.4.5 Issue 5: Propose a trust-based mechanism for node selection and secure node joining and leaving the network

In order to address the issue of selecting the key nodes from the member nodes in the network to perform the major responsibilities, a trust-based framework needs to be established which selects the key nodes based on the highest level of trustworthiness. The proposed framework provides guidelines for the member nodes to follow in relation to joining and leaving the network securely, so that untrustworthy or malicious users do not degrade the network performance by attacking the key nodes or by joining or leaving the network in a non-secure manner. For the selection of key nodes, the trust values of the member nodes need to be updated depending on their various behaviours.

This thesis aims to highlight the need for a trust-based mechanism to select the key nodes and backup key nodes and ensure that member nodes join and leave the network securely. Chapter 4 briefly describes the proposed processes for node selection and the secure node joining and leaving mechanism which is further elaborated in chapter 7.

3.4.6 Issue 6: Propose a framework for system availability enhancement in CRNs

Although it is possible to ensure the secure use of available spectrum by establishing a trusted platform in CRNs, some malicious nodes always attack the key nodes of the CRNs in order to obtain all the important data and disrupt and degrade network performance in a dramatic way. Therefore, there is a need for a framework that will increase system availability and reliability by proposing a model that will allow backup key nodes to perform all major responsibilities of the main key node in the event of any errors or attacks in the main key node.

This thesis highlights the need to increase system availability and reliability by proposing the model in which the backup key nodes are responsible for performing all the major responsibilities of the main key node when required. Chapter 4 briefly describes the proposed system availability enhancement framework which is elaborated further in chapter 7.

3.5 Research Methodology

3.5.1 The science and engineering-based research method

In addressing the stated technical problem, this thesis focuses on the development of trust-based mechanisms to ensure secure communication in CRNs. In order to propose a solution for the research issues described in the previous section, a systematic scientific approach must be followed to

ensure that the methodology developed is scientifically based. A science and engineering-based research approach is adopted in this thesis. Science and engineering research leads to the development of new techniques, architecture, methodologies, devices or concepts which can be combined to form new theoretical frameworks. This research approach identifies problems and proposes solutions to these problems. Particularly in the engineering field, the spirit of "making something work" is essential [121, 122]. These authors decompose science and engineering based research into three main levels:

- *Conceptual level (level one)*: creating new ideas and new concepts through analysis.
- *Perceptual level (level two)*: formulating new methods and approaches through designing and building the tools, environment or system through implementation.
- *Practical level (level three)*: carrying out testing and validation through experimentation with real world examples. The process of testing and verifying a working system provides unique insights into the benefits of the proposed concepts, frameworks and alternatives.

3.5.2 Research stages

The research stages in this thesis are based on the three levels of the science and engineering research approach.

- *Literature Review:* Firstly, relevant research papers on CRN security are reviewed in order to obtain full understanding of the characteristics and security requirements of CRNs. Secondly, the reviewed security

issues in spectrum sharing in CRNs reviewed as spectrum sharing is a key characteristic in CRNs. Thirdly, trust management is overviewed, including trust establishment and trust maintenance in CRNs which enables open problems related to trust establishment for secure communication in CRNs to be identified. In addition, the following are also reviewed: other lightweight cryptographic primitives; combinatorial mathematics and graph theory; and simulation techniques that will aid in the design and evaluation of frameworks in CRNs.

- *Conceptual Framework for Trust-based Mechanisms for Ensuring Secure Communication in CRNs:* Figure 3.2 shows that trust establishment and maintenance are not separate components of ensuring security in cognitive radio architecture. Secure communication provides a security infrastructure for other security services, while at the same time, relying on other security services. Trust and other security services together make up the trust-based security architecture for secure spectrum sharing to enhance system availability in CRNs. Therefore, a comprehensive consideration of these factors is essential when designing trust-based secure architecture for spectrum usage for CRNs. In this thesis, a conceptual framework for trust-based mechanisms to ensure secure communication in CRNs (Figure 3.2) is proposed. The conceptual framework provides a guidelines to establish secure communication by proposing trust-based mechanisms in the next stage.

    1. As previously mentioned that CRNs are application-specific networks. Except for certain common features, a CRN for a specific application has several unique features and thus security

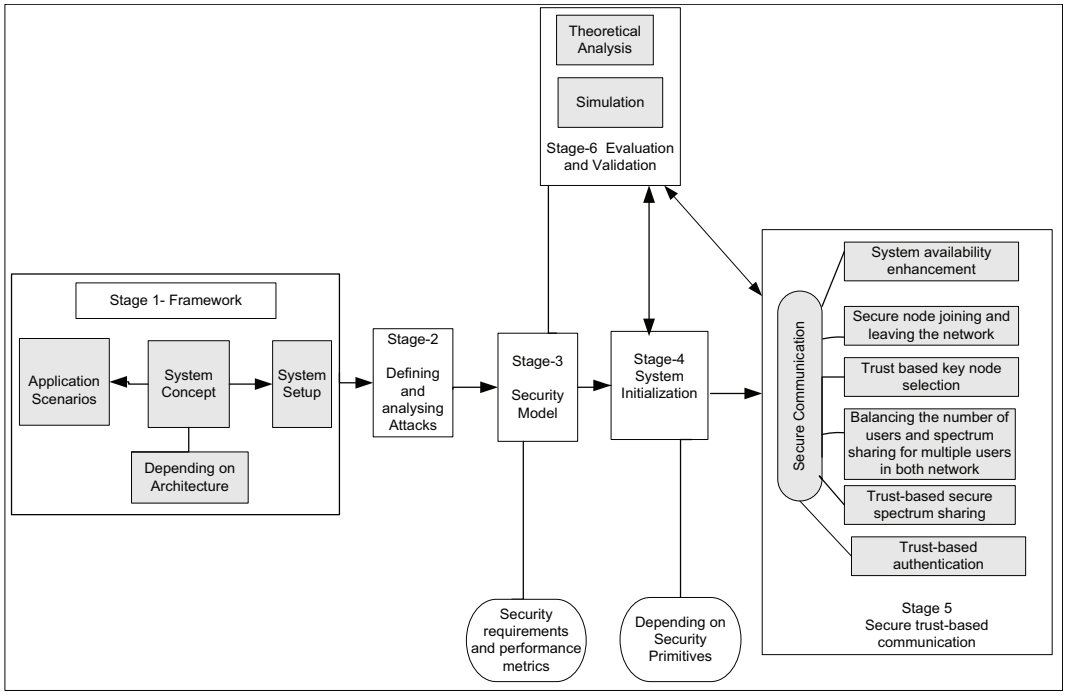

Figure 3.2: A conceptual framework for secure trust-based communication in cognitive radio networks

requirements. Depending on the application and the architecture of CRNs, a framework for the system will be set up. Both primary and secondary networks' security requirements should be different based on the resources that cognitive nodes can use and the risks they face. Therefore, the first step is to fully understand the application's background and extract the network model for the system. The acquired information in this step includes the number of users and the size of the network, the available hardware and software resources, and specific knowledge that can be used in a particular real time scenario, such as location information.

2. This step describes the various possible attacks on CRNs. An attack on CRNs is any activity that results in (a) unacceptable interference

to the licensed PUs; or (b) missed opportunities for SUs. As there is no existing literature which gives a comparatively full taxonomy of attacks for CRNs, this thesis will consider any kind of threat, which, despite involving a minimal number of adversaries performing a minimal number of operations, it may cause maximum damage/loss to either the PUs or SUs in the network.

3. This step describes the techniques available to enhance secure communication in CRNs. These techniques are defined according to security requirements and will work as performance metrics for the proposed trust-based mechanisms for secure communication in CRN. Detecting attackers in CRNs for spectrum management such as during spectrum sharing, spectrum sensing, the development of secure spectrum sharing schemes and the evaluation of various approaches is of great importance in establishing a scientific methodology for the entire CRN security research area. To the best of the researcher's knowledge, this is the first time that a trust-based mechanism has been designed to ensure secure spectrum usage and sharing by detecting untrustworthy users, thereby ensuring secure communication in CRNs.

4. This step initializes the system parameters. The trust-based mechanisms that need to be established in CRNs to ensure secure communication according to different communication requirements, cognitive capabilities and aggregation mechanisms are fixed in this step, including which types of primitives are used for secure communication in CRNs such as for spectrum sharing, or any

predefined policies or recommendations specified for the current network.

5. The outcome of this research is explained in this step 5. Several trust-based schemes have been proposed for securing communication in CRN. Each of these schemes has certain unique characteristic according to the application background. It is not my final goal and it is impossible to design a single protocol that will outperform all others for all possible models. Instead, this thesis concentrates on designing a secure communication scheme in CRNs which matches the abstracted security model in Figure 3.2. The notion of trust between PUs and SUs has been adopted in the development of these components. Trust-based mechanisms for a secure communication suite in CRNs involves 6 modules: (1) establishing trust between different nodes in CRN to check the node's authentication and detect malicious users; (2) trust-based secure spectrum sharing to only authenticated users to avoid untrustworthy users' access to the spectrum; (3) balancing the number of SUs and PUs in CRNs to minimize the disruption to the SUs' service and enhance spectrum sharing when there are multiple PUs and SUs in the network; (4) trust-based node selection to choose the key nodes to enhance the system reliability; (5) trust-based secure node joining and leaving the network to prevent malicious users from accessing the network; (6) system enhancement by having multiple back up CA options in the network. This stage corresponds to perceptual level of the science and engineering research method.

Based on the conceptual framework proposed in the first research stage, the main task in this stage is to design several trust-based mechanisms for ensuring secure communication in CRNs. So, trust is calculated and established between different nodes in CRNs to select the key nodes and authenticity is checked based on the trust value. Then, the free spectrum is detected and allocated to the requesting authenticated SUs for secure spectrum sharing so that untrustworthy entities, such as selfish, malicious, and faulty nodes can not obtain access to the free spectrum. The system's availability is increased by proposing multiple backup key nodes to perform the major functionalities in the even of an error to the key node.

6. Both theoretical analysis and simulation are good tools to test the designed schemes. By using these tools, the validity of the schemes can be proven and at the same time, their deficiencies identied.

Steps 4, 5, and 6 are completed in turn. They form a loop and are performed numerous times before an efficient and secure sharing scheme is obtained. This stage corresponds to the practical level of the science and engineering research method.

- *Evaluation and Verification of the Schemes and Protocols:* In this section, evaluation includes security evaluation and performance depending on the trust level. The theoretical analysis is based on the effectiveness of the security primitives used in the proposed schemes, with the help of the Cognitive Radio Network Simulator, JAVA and MATLAB software and whether or not the schemes satisfy security requirements with reasonable overheads and against different attacks will be verified. It

would be useful to have comprehensive guidelines to evaluate a specific protocol and to compare it with others. However, no previous scheme has been proposed for secure spectrum sharing, spectrum availability checking or system availability enhancement in CRNs. Based on the proposed security model, appropriate performance metrics will be used to evaluate the strengths and weaknesses of the proposed protocol. The framework should evaluate the goodness of the network as a whole and provide metrics to measure the effects of the design on the operation of the network (by evaluating, for example, trustworthiness, availability, reliability etc). In order to quantify the effects of a compromise on security architecture, Tao Qin et al. in [46] investigate the inherent tradeoffs involved in total utility loss, band usage and security robustness in CRNs. The security of the trust-based schemes will be demonstrated by mathematical security proof.

3.6 Conclusion

In this chapter, the set of definitions that will be used throughout the thesis was firstly outlined. Then, the research gaps arising from the literature in terms of key aspects were summarized, and the problem to be addressed in this thesis was defined and decomposed into six research issues, which form the key requirements for the development of an individual new solution. Further, a science and engineering-based research approach which will be utilized in this thesis for the proposed solution development was discussed. Mainly, this chapter identified the problem this thesis aims to address and gave a brief overview of each of the research issues which will enable the research problem

to be solved. The next chapter will give an overview of the proposed solutions for the problem that will be addressed in this thesis.

Chapter 4

Solution Overview

4.1 Introduction

As explained in Chapters 2 and 3, several research studies have been conducted on improving security by using the notion of trust in cognitive radio networks (CRNs). However, as evident from the discussion in these chapters, the literature does not provide a methodology for trust establishment, mechanisms for trust-based network resource sharing such as spectrum sharing or mechanisms for system availability enhancement for maintaining smooth and secure communication in CRNs. In Chapter 3, six research issues that need to be addressed in order to solve these pivotal problems were identified. In this chapter, an overview of the proposed solutions is given, as shown in Figure 4.1. The overview of each solution is further explained in detail in Sections 4.2-4.4 before Section 4.5 concludes the chapter.

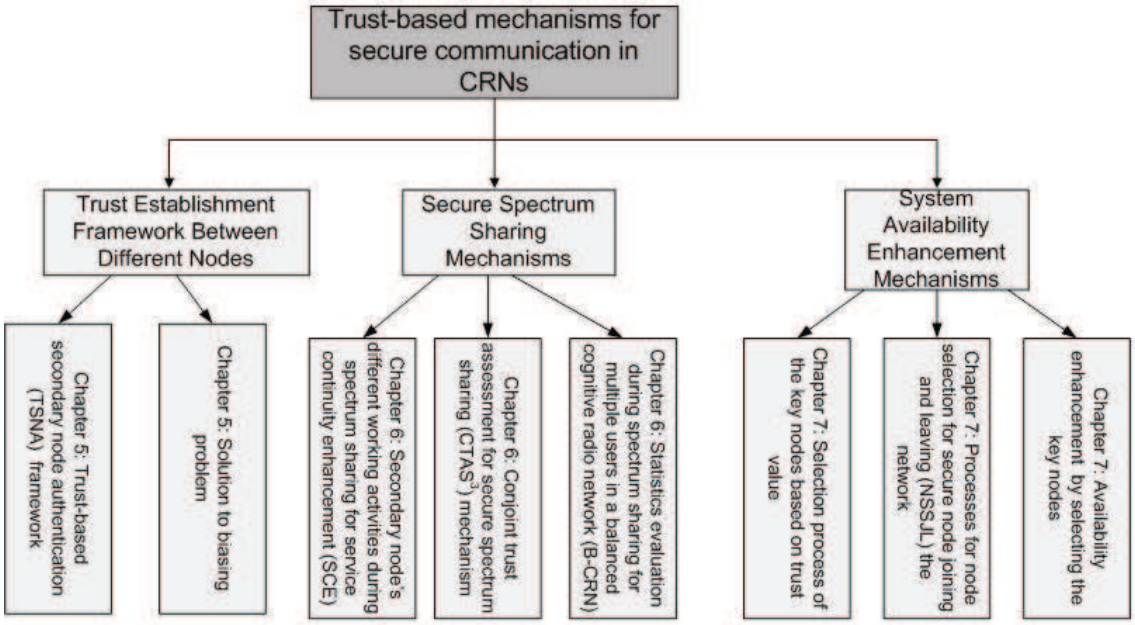

Figure 4.1: Overview of the solutions proposed in this thesis

4.2 Solution Overview for Trust Establishment Between Different Nodes in CRNs

The solution for trust establishment between different nodes in CRNs is divided into two sub-solutions as follows :

- Establishing trust for the authentication of a secondary user's (SU's) request to access network resources.
- Solving the biasing problem to obtain a node's actual trust value.

A detailed overview of these solutions is given in the next subsections.

4.2.1 Overview of the solution for establishing trust-based authentication

To solve this problem, it is proposed that whenever the SU wants to use the network resources, either from the secondary network or the primary network, it is necessary for the corresponding base station to check the SU's trust value to authenticate its request so that no selfish or untrustworthy users has access to the network. The proposed solution for establishing such a trust-based authentication scheme in CRNs is as follows:

- Propose that the two networks (the primary network and the secondary network) in CRNs and their base stations, namely: Secondary User Base Station (SUBS), Primary User Base Station (PUBS) are connected to the CA (Certificate Authority) which has a trust repository that contains the trust value of every cognitive radio node.

- Propose three different ways to calculate the trust values between the different nodes in the network. A *direct trust calculation* is used to compute the trust value if a past interaction experience exists between the nodes. In the absence of any direct past interaction experience between the nodes, *an indirect trust calculation* is used to establish the trust value between the nodes based on recommendations from surrounding nodes. In situations where both direct and indirect trust values exist, the base station can combine both according to the preferences of the nodes to compute the trust value. This is done by the *integrated trust calculation* method.

- The request of the SU will be authenticated based on these trust values

for using free spectrum and other purposes in the network. The SU, who has a trust value above the predefined threshold, will have its request authenticated by the network. If the computed trust value is less than the predefined threshold, then its request is not authenticated.

4.2.2 Overview of the solution for solving the biasing problem

The proposed solution for solving the biasing problem in a secondary network in CRNs is as follows:

- It is proposed that the CA entity which is connected to the base stations and the nodes, performs as the key node in the network. It is also proposed that the CA is also maintains the trust repository to keep a record of all nodes' trust values in the network.

- When an SUBS receives a request from an SU to access the network resources, it calculates its trust value based on the recommendation received from its member nodes and compares it with the trust value of the requesting node stored by the CA.

- If the computed trust value from the SUBS is similar to the received value from the CA, then the SUBS is assured that the recommending node did not bias the trust value of the candidate node.

- On the other hand, if the computed values between the SUBS and CA do not match, then the SUBS is assured that there has been some biasing from the recommending nodes. In such cases, the SUBS identifies the

recommending node who puts the biased value for the candidate node and excludes it from the network.

A pictorial overview of the proposed solution is depicted in Figure 4.2

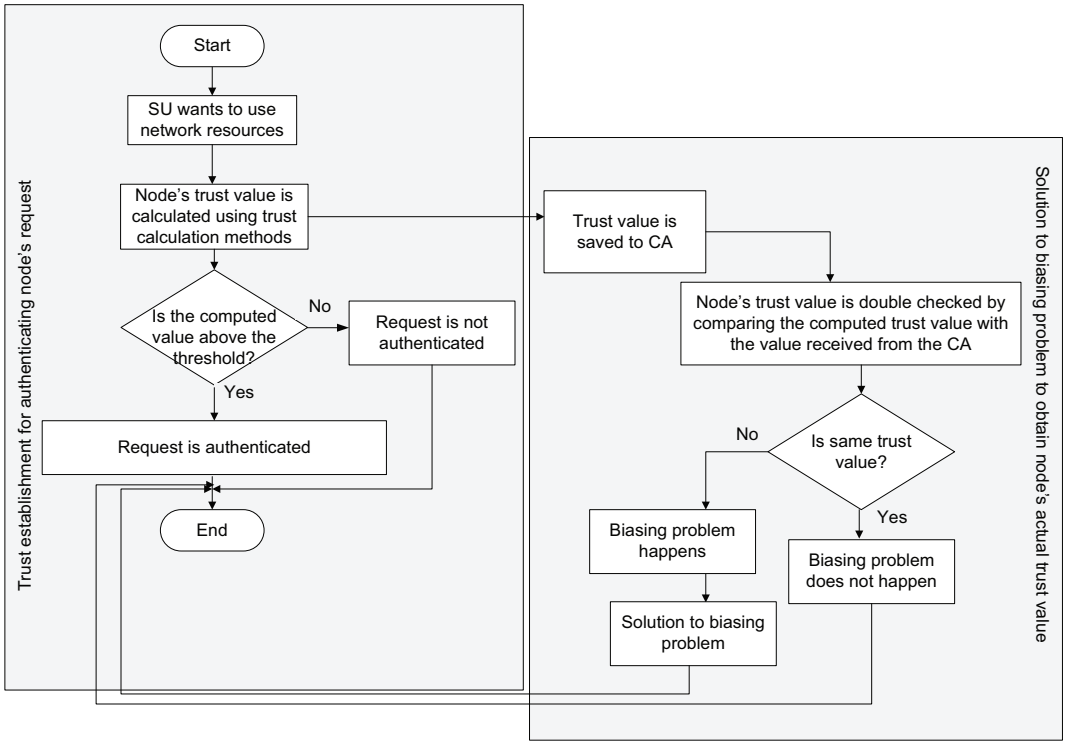

Figure 4.2: Overview of trust establishment scheme

In chapter 5, the proposed methodology by which the trust-based authentication scheme is established for maintaining secure communication in CRNs is explained in detail, with an aim that no selfish or malicious user will have access to the network resources and also to avoid the biasing problem in secondary network in CRNs.

4.3 Solution Overview for Secure Spectrum Sharing Mechanisms in CRNs

The proposed solution for secure spectrum sharing mechanisms in CRNs is divided into three sub-solutions as follows :

- Defining the different working activities of an SU to minimize the disruption in its service when it has to vacate the PU's spectrum and search other free spectrum.
- Proposing a conjoint trust assessment mechanism which allows an SU to use a PU's free spectrum securely.
- Balancing the CRN based on the multiple PUs and SUs and the sub-bands available for spectrum sharing.

A detailed overview of these solutions is given in the next subsections.

4.3.1 Overview of the solution to minimize disruption in the SU's service

An overview of the solution to minimize the disruption of an SU's communication during spectrum sharing in CRNs is as follows:

- During spectrum sharing, it is proposed that an SU needs to go through five different states: search state, access state, interrupt state, vacate state, and dropped state in order to avoid interference with the primary users (PUs).

- At first, the node searches the free spectrum in the search state and when it finds a spectrum, its request to access it is either accepted or rejected based on its trust value. This will be further discussed in Section 4.3.2.

- In the access state, the SU establishes connections with others for communication by using a PU's free spectrum band.

- Whenever the PU returns to the network, the communication of the SU will be interrupted. When this occurs, the SU goes to the interrupt state upon the arrival of the PU.

- As soon as the SU is interrupted by the PU, it will go to the vacate state and will vacate the channel according to the CRNs policies. After vacating the channel, the SU will go to the search state and try to search for another free spectrum. If unsuccessful, then its communication will be dropped and it enters the dropped state.

A pictorial overview of the proposed solution for the different working states in the SU to minimize disruption in its service during spectrum sharing in CRN is depicted in Figure 4.3.

The different working states of an SU are modeled using a state transition diagram shown in Chapter 6 to demonstrate the minimization of the disruption in its service when it goes through the abovementioned defined states, compared to the existing working approach in CRNs.

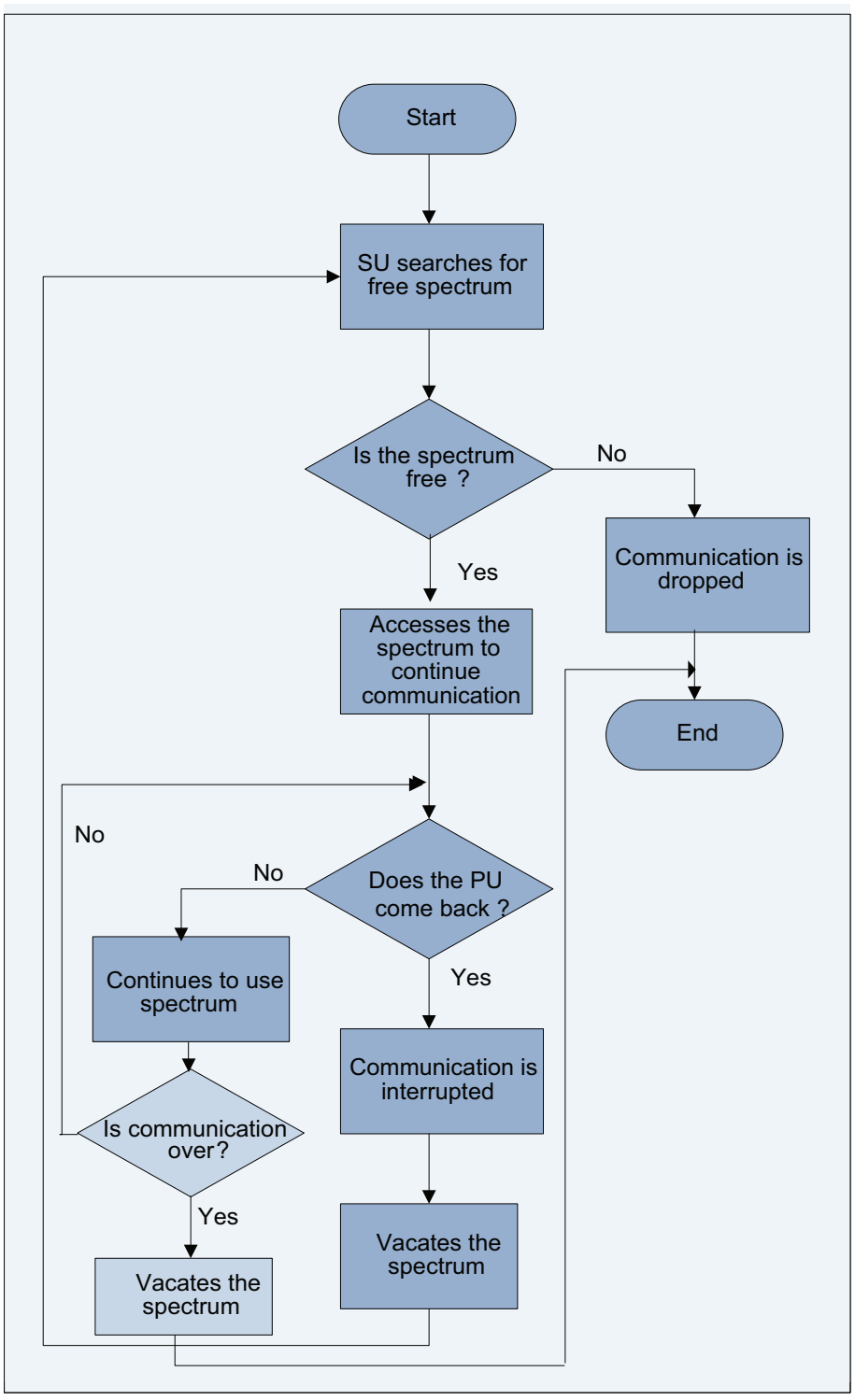

Figure 4.3: Working states of an SU during spectrum sharing

4.3.2 Overview of the solution for a conjoint trust assessment mechanism for secure spectrum sharing

An overview of the solution allowing only the trustworthy users in CRN to securely use the PU's free spectrum is as follows:

- Trust assessment for the spectrum requesting candidate node from the secondary network.
- Trust assessment for the spectrum requesting candidate node from the primary network.
- Conjoint trust assessment of the requesting node from both networks to ascertain its overall trustworthiness to make sure that no untrustworthy malicious or selfish node can access the free spectrum and paralyze the network's normal performance.

A detailed overview of the proposed secure spectrum sharing approach in CRNs is as follows:

- Whenever an SU senses a PU's free spectrum [9], it sends a message to the SUBS requesting access to that spectrum.
- SUBS and PUBS first authenticate its request based on its trust value to ensure that the request is coming from a valid node.
- After this, the SUBS asks its member nodes to send the trust value for the authenticated requesting SU.

- The SUBS accumulates the trust values that it receives from its member nodes and sends it to the PUBS.
- Once the PUBS receives the trust value of the requesting node from the SUBS, it asks its member nodes to assign a trust value for the requesting SU.
- Upon receiving the recommended values from the member nodes, the PUBS accumulates them and combines them with the trust values received from the SUBS.
- If the conjoint trust value of the requesting node is equal to or above a predefined threshold, the requesting SU will be granted permission to use the PU's free spectrum band, otherwise its request to access the spectrum is denied.

A pictorial overview of the proposed solution is depicted in Figure 4.4

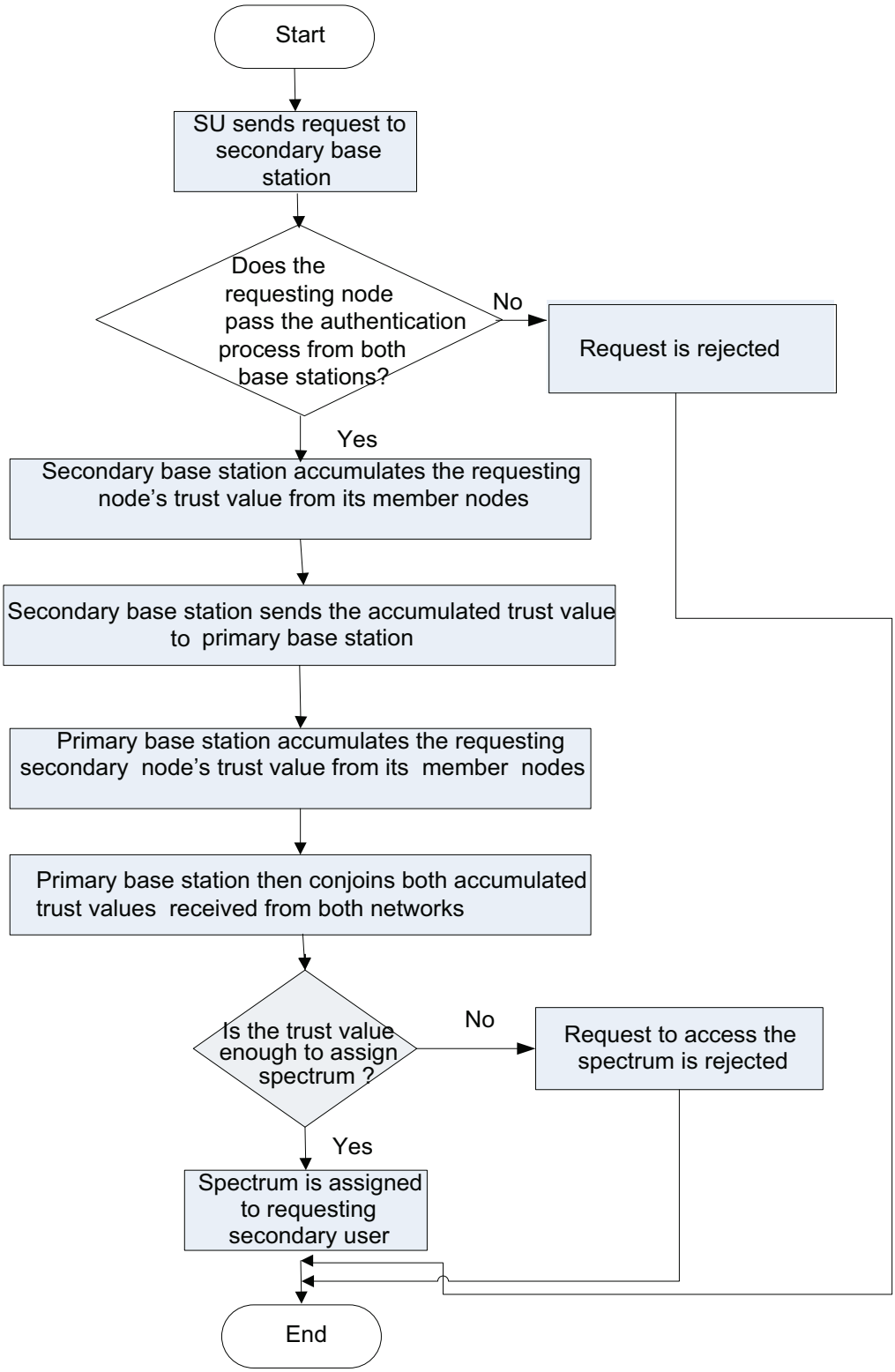

Figure 4.4: Overview of the secure spectrum sharing scheme

4.3.3 Overview of the solution for balancing the CRNs for multiple PUs, SUs and sub-bands

A detailed overview for balancing the CRN and analyzing the system statistics of a balanced network during spectrum sharing is as follows:

- Identify the number of SUs, PUs and the available sub-bands.
- The number of SUs in a balanced CRN depends on either the number of PUs or the number of sub-bands into which each PU's licensed band is divided.
- If the number of PUs or the number of sub-bands in each licensed band is increased, more sub-bands are available. Therefore, more SUs are allowed to use the sub-bands in a balanced network.
- Analyze system statistics by analyzing criteria such as blocking rate, deprivation rate, utilization ratio etc during spectrum sharing while multiple SUs and PUs are used in a CRN to ensure a balance is maintained between them.

A pictorial overview of the proposed solution is depicted in 4.5

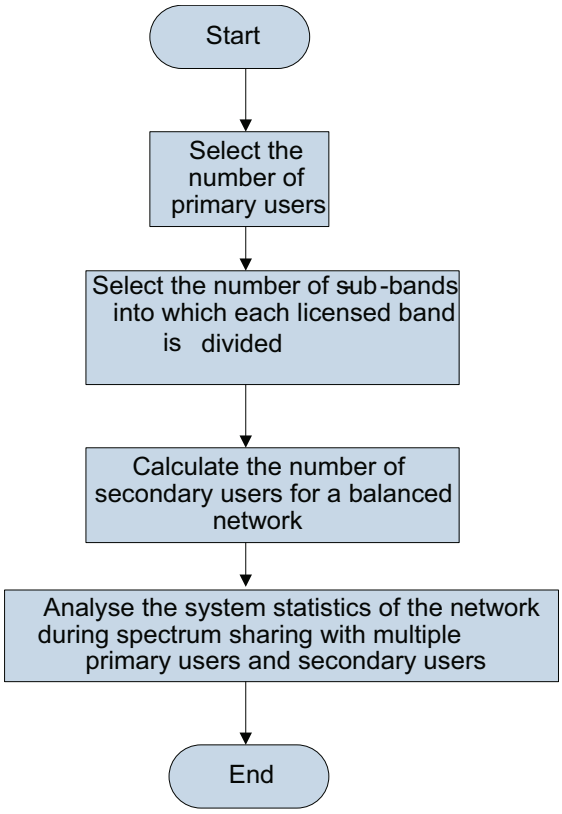

Figure 4.5: Overview of secure spectrum with multiple users in a balanced network

In Chapter 6, the three sub-solutions for secure spectrum sharing in CRN will be described in detail.

4.4 Solution Overview for System Availability Enhancement Mechanisms in CRNs

The proposed solution for enhancing system availability in CRNs, is sub-divided into the following three sub-solutions :

- Selecting the key nodes of CRNs based on their trust value.

- Proposing a process for a secure node joining and leaving process for the network and their effects on the node's trust value.
- Increasing the system's availability and reliability by introducing multiple back up CAs in the network.

A detailed overview of these solutions is given in the next subsections.

4.4.1 Overview of the solution for selecting the key nodes in CRNs based on their trust value

An overview of the solution for selecting the key nodes such as Certificate Authority (CA) and Backup Certificate Authority (BCA) which serve as trusted third parties in the network based on the trust value is as follows:

- Each node's trust value is calculated by other nodes in the CRN depending on the different activities and the trust value given to it for each activity.
- If the node has the highest trust value and its trust value is above the trust threshold, then the node is selected as the CA. If the node has the second highest trust value and its trust value is above the trust threshold, then that node is selected as the first candidate to be the BCA. This process is repeated for each node whose trust value is above the trust threshold.
- If the node has a trust value which is below the trust threshold, then it works as a normal node.

A pictorial overview of the proposed solution for selecting the key nodes based on trust values is depicted in Figure 4.6

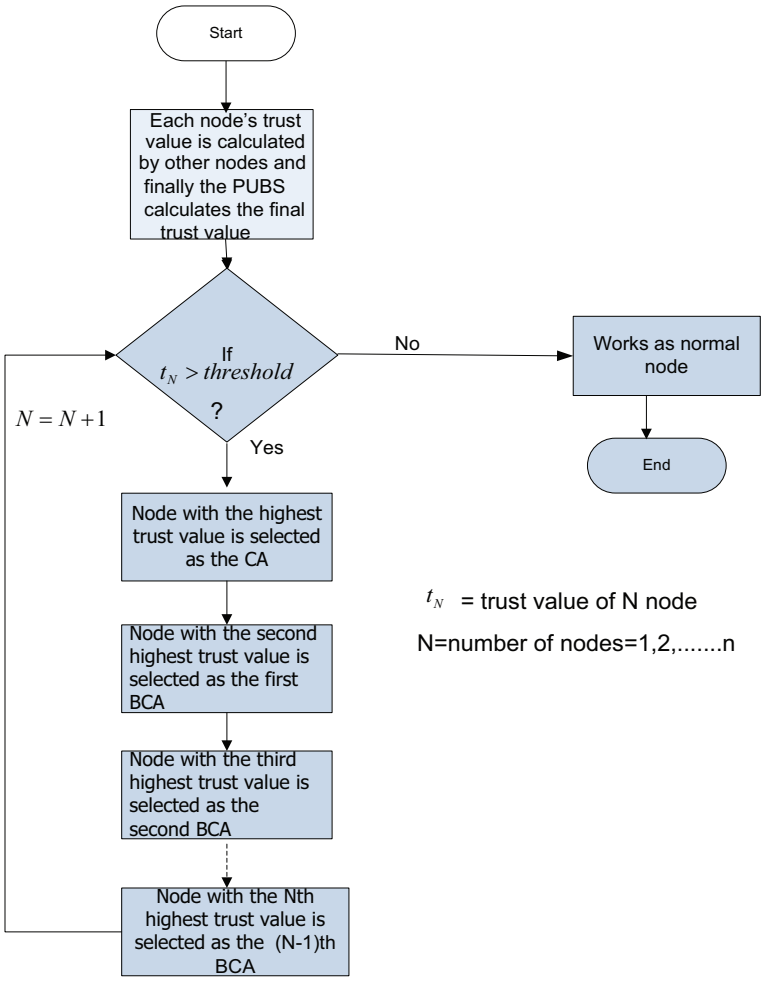

Figure 4.6: Overview of the node selection scheme

4.4.2 Overview of the solution for the process of secure node joining and leaving the network and its effect on the trust value

An overview of the solution for the secure node joining and leaving process in CRNs is as follows:

- In the proposed approach for secure joining the network, the new node broadcasts its certificate and random number to all the member nodes in the network as well as to the base station. The base station and the member nodes verify the validity of the new node's certificate. After verifying the validity, the node is either permitted to join the network or otherwise. If the node successfully passes the joining process, its trust value is incremented by 0.05.

- For secure leaving the network, the node will send the normal leaving message to the base station. This is treated as 'normal leaving', otherwise it is treated as 'abnormal leaving'. For normal leaving, the node's trust value is incremented by 0.05, otherwise its trust value is decremented.

A pictorial overview of the proposed solution for secure node joining and leaving the network is depicted in Figure 4.7

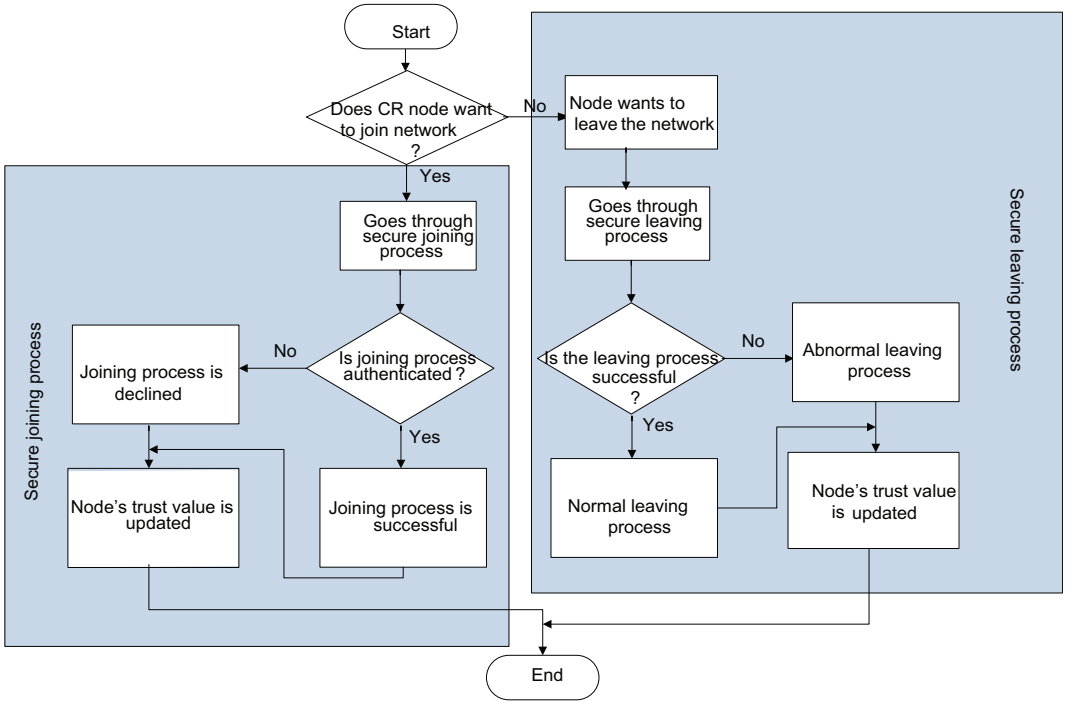

Figure 4.7: Overview of secure node joining and leaving process

4.4.3 Overview of the solution for increasing system availability and reliability by introducing multiple backup CAs in CRN

A detailed overview of the proposed solution to increase system availability and reliability is as follows:

- Propose a system that has multiple BCAs, and which can switch its functionality from a CA to BCA in response to the detection of an error in a CA or in the case of a CA being biased and under attack by other malicious nodes.

- Propose different working states in the working of a CA and BCA in a multiple BCA system through which they need to go according to their present state in order to enhance system availability.
- If the CA is considered a malicious CA due to an attack, then reconfiguration techniques are applied to correct it.
- During the time the reconfiguration techniques are being applied, the first backup CA takes over the role of the CA.
- If the reconfiguration techniques work well for the affected CA, then it is reinstated as the CA from the BCA in the CRN; otherwise, the CA's activities will be taken on by the BCA.
- A similar process is applied when the BCA is under attack by other malicious nodes.
- The effect of the solution to system availability and reliability enhancement is evaluated by using different metrics such as downtime cost, trustworthiness etc.

A pictorial overview of the proposed solution for enhancing availability by introducing multiple BCAs in the system is depicted in 4.8

In Chapter 7, the three sub-solutions to enhance the system's performance by increasing its availability and reliability will be described in detail.

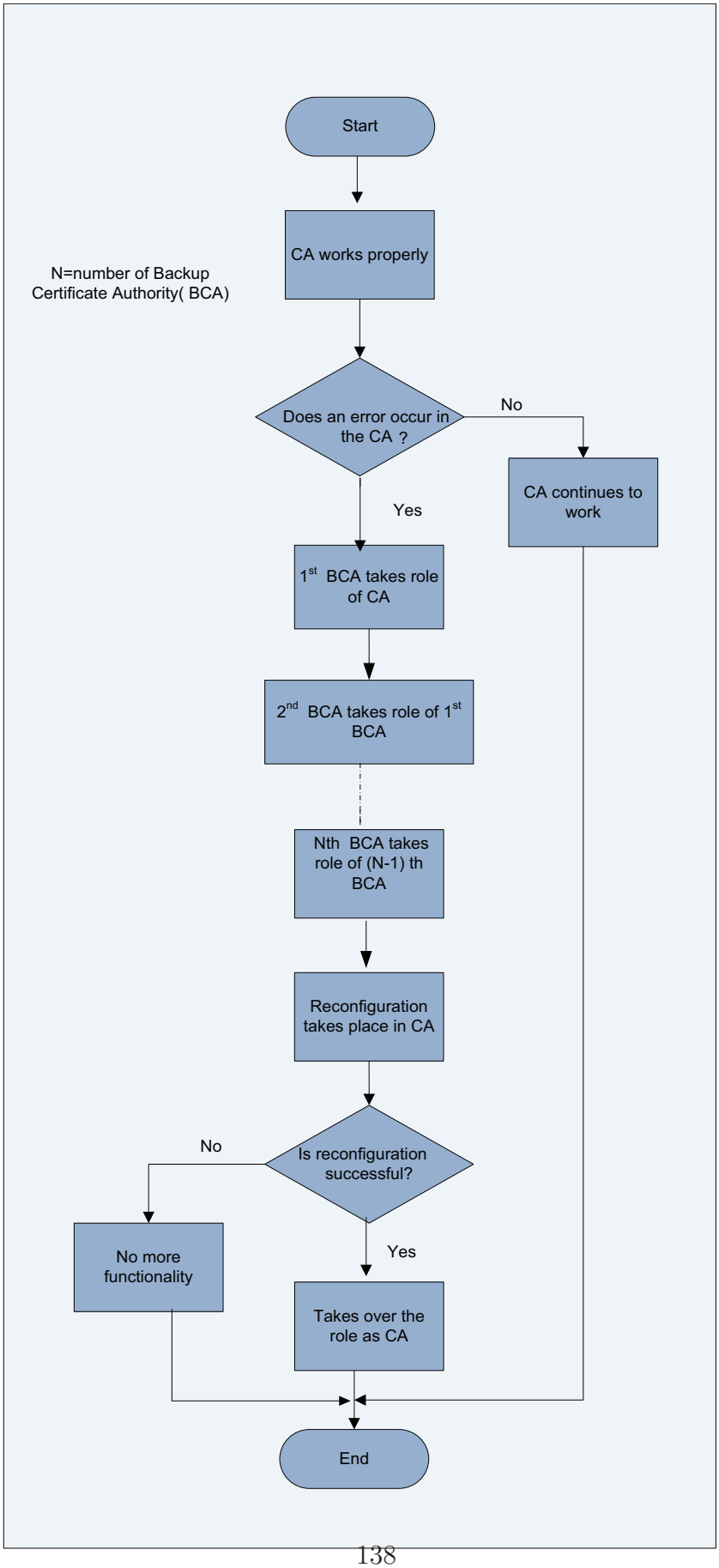

Figure 4.8: System availability enhancement scheme

4.5 Conclusion

In this chapter, a solution for each of the six research issues that were identified in Chapter 3 was proposed. Finally, the solution overview to the problem that is being address in this thesis was presented.

In the next chapter, a framework for trust establishment between different nodes for authentication checking in CRN is proposed, which was identified in this chapter as being the first step of the trust-based methodology to maintain secure communication in CRNs.

Chapter 5

Framework for Trust-based Secondary Node Authentication in Cognitive Radio Networks

5.1 Introduction

In the current literature, even though the importance of trust in cognitive radio networks (CRNs) has been discussed, the proposed approaches using trust are insufficient for a secure system due to the following drawbacks:

- Most trust-based schemes consider trust only for trusted routing in CRNs and not for securing spectrum access from untrustworthy users.
- One of the main problem of establishing trust in CRNs is 'biasing' by other malicious nodes. So, in such scenarios, it is not possible to obtain the actual trust value for authentication purposes. No approach has been proposed to address this.

- No trust-based authentication framework has been proposed in the literature to enhance security in CRNs.

Due to the abovementioned drawbacks, three possible security threats may arise which may disrupt the process of secure communication in CRNs:

1. Any selfish or malicious node could access the network and break down normal network activity by using the network resources in a selfish way.
2. Malicious users may use the primary user's (PU's) free spectrum to jam the network which inhibits secondary users using this spectrum.
3. Any member node can be biased by other malicious users who can increase or decrease any member node's trust value in the network. So, it is not possible to obtain the actual trust value for the member node.

In order to solve these abovementioned security threats, a Trust-based Secondary Node Authentication (TSNA) framework is proposed in this chapter. The proposed framework authenticates a secondary user's (SU's) request for it to be considered to use PU's free spectrum and other network resources based on its trust values to ensure that the request is coming from a valid trustworthy node in the network and no malicious or selfish user can gain access to the network and paralyze the network activity. The proposed framework provides solutions and sufficient proofs for:

- authenticating an SU's request to access PU's free spectrum and other network resources based on their level of trust.
- solving the biasing problem brought by malicious users in the network by checking the requesting node's actual trust value.

This chapter is organized as follows: in Section 5.2, the system architecture and working of the proposed TSNA framework is discussed. In Sections 5.3 to 5.5, each phase of the proposed framework is explained in detail. In Section 5.6, an example is given to calculate the trust value for authenticating an SU's request. Experimental results are shown in Section 5.7. Section 5.8 concludes the chapter.

5.2 Proposed Framework for Trust-based Secondary Node Authentication (TSNA) in CRNs

5.2.1 System model and architecture

The system model of the proposed TSNA framework to ensure secure communication in CRN is shown in Figure 5.1.

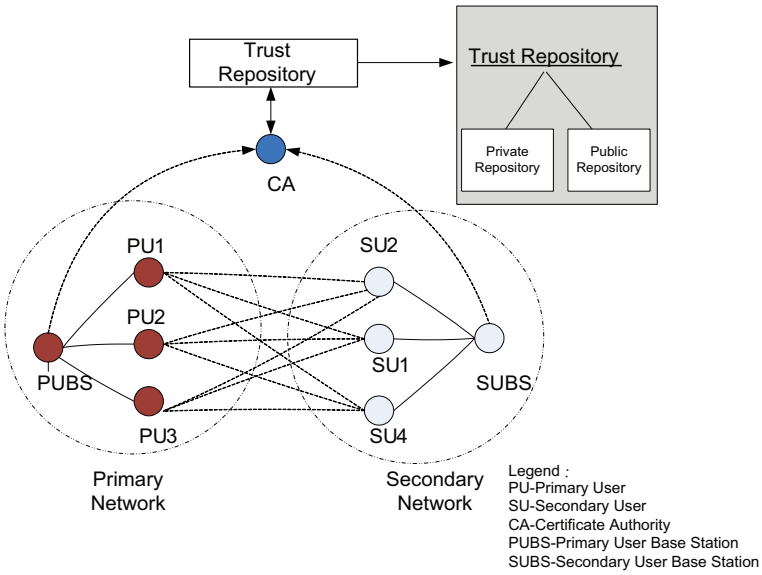

Figure 5.1: System model of the TSNA framework

The key components of the framework are:

- **Base Station**: A base Station is defined as the central point of contact between the two different types of users, namely primary users (PUs) and secondary users (SUs). There are two types of base stations considered in the proposed architecture, namely Primary User Base Station (PUBS) and Secondary User Base Station (SUBS). PUs are connected to the PUBS whereas SUs are connected to the SUBS.

- **Certificate Authority**: A certificate authority (CA) is an entity which is connected to the PUBS and SUBS in the network and is responsible for maintaining the member node's trust values for both networks by managing the trust repository. In the proposed architecture, the CA is an authorized agent which is responsible for providing a node's actual trust value to solve the biasing problem and set up a communication link for authentication purposes in the CRN. The CA is also responsible for updating the trust values of the nodes in the trust repository if they change. The respective base station (SUBS or PUBS) will inform the CA of any change, who will then update the trust value in the trust repository.

- **Trust Repository**: The trust repository stores the trust values of different users. Each user has two types of trust values stored in the repository, the first being the public trust value and the second being the private trust value. Both of these repositories are controlled by the CA. The public trust value of a user is available publicly to other users and is provided to them by the CA, when a request is placed. The private trust value of an user is only visible to the CA and is computed and stored

to ensure the integrity of the public trust value. If any malicious user in the network intentionally alters the public trust value, the CA can check the private trust value and obtain information about which node's trust value has been changed by the malicious users. It then broadcasts a message to the corresponding base station to remove the malicious user from the network.

5.2.2 Working of the proposed TSNA framework in CRNs

In this section, the working of the proposed TSNA framework for authenticating an SU's request to confirm that the request is coming from a valid and trustworthy user to use the spectrum and other network resources based on their trust values in the network is presented. As mentioned in Section 4.2, this framework can prevent a malicious node from accessing the network by authenticating a node's request based on its trust value. It also solves the biasing problem by cross checking the member node's trust value with the trust value stored in the trust repository which plays an important role in spectrum decision making and other purposes in CRNs. Figure 5.2 presents a flowchart diagram of the working of the proposed framework. The sequence of steps in the proposed framework are as follows:

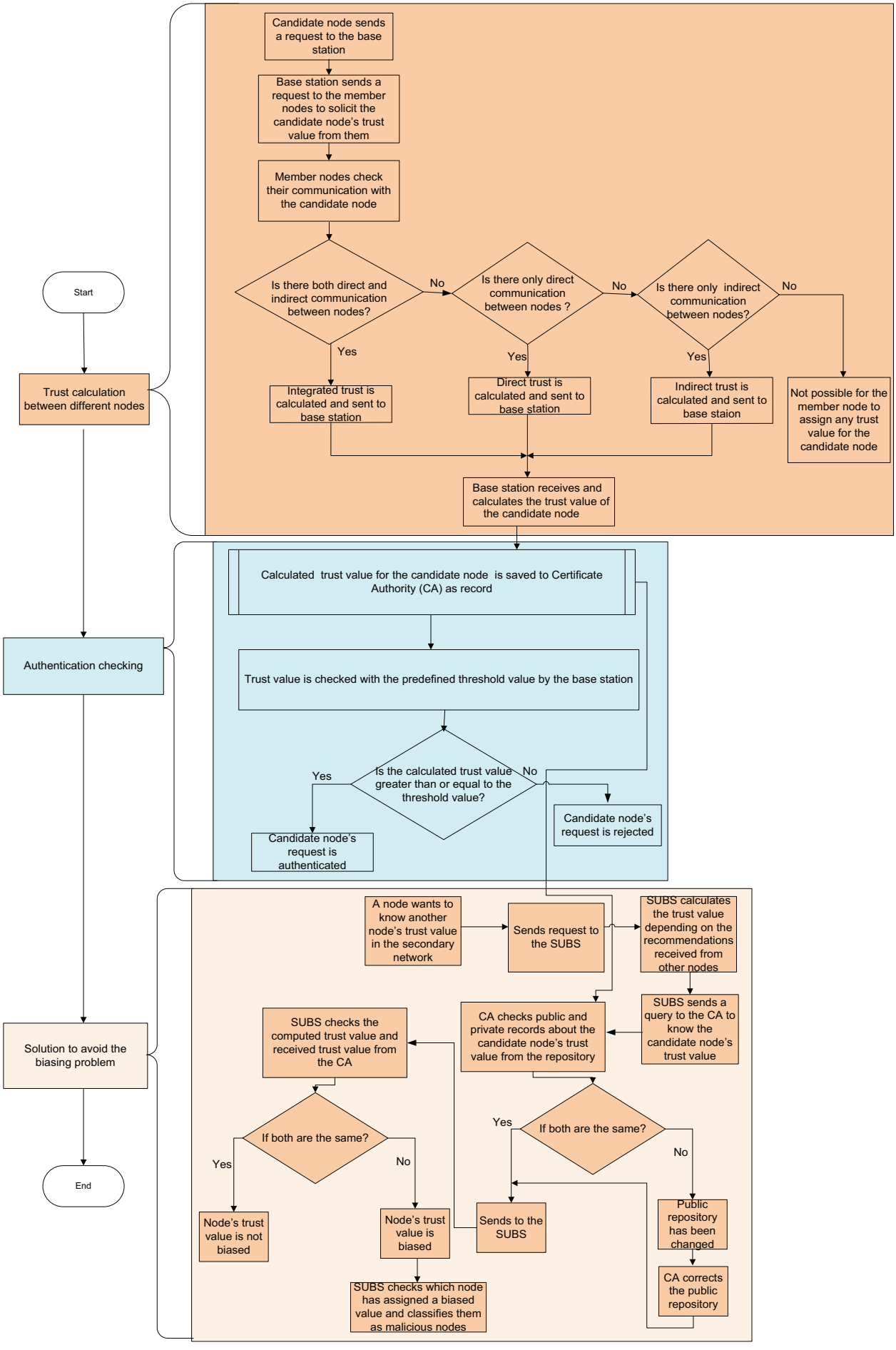

Figure 5.2: Flowchart illustrating steps performed by the TSNA framework

5.2.2.1 Trust calculation between different nodes

The trust calculation phase between different nodes in the proposed TSNA framework is as follows:

1. Whenever an SU wants to use the network resources either from the primary network or secondary network, the requesting or candidate SU's trust value is calculated by the SUBS to decide whether the request is coming from a valid SU or not. Here, the requesting SU is termed either the 'requesting node' or 'candidate node'. During this step, the requesting SU sends a request to the SUBS to use either a PU's free spectrum or network resources from the secondary network.

2. The SUBS then sends a request to all of its member nodes, asking them to assign a trust value to the candidate node.

3. All the member nodes in the secondary network assign or recommend a trust value to the candidate node, based on their previous cooperation with the candidate node, as mentioned in Section 5.3.

4. The SUBS aggregates the received recommendations and calculates the final trust value of the candidate node and, if it is selected as a trustworthy node by the process mentioned in 5.2.2.2, then the SUBS either authenticates the candidate node's request to use its network resources or forwards the candidate node's request to the PUBS to authenticate the candidate node's request to the primary network.

5. In the scenario of the requesting node wanting to access the PU's free spectrum, the request is forwarded to the PUBS by the SUBS. The PUBS

also calculates the candidate node's trust value to decide whether its request is authenticated or not.

6. The process which the PUBS follows is similar to that of the SUBS. The PUBS sends a request to all of its member nodes, asking them to assign or recommend a trust value to the candidate node. All member nodes in the primary network recommend the candidate node using the trust calculation method mentioned in Section 5.3 and sends the trust value to the PUBS.

7. The PUBS calculates the candidate node's final trust value by aggregating the received response and makes a decision as to whether to authenticate its request or not.

8. Both base stations send the calculated trust value of the candidate node to the CA for record keeping purposes.

5.2.2.2 Authenticating an SU's request

The phase for authenticating an SU's request in the proposed TSNA framework is as follows:

1. If the request of the candidate node is to use the secondary network's resources, the SUBS compares the computed trust value against the predefined threshold value to decide whether it is authenticated to use the requesting service or not. If the calculated trust value is greater than the predefined threshold, the requesting SU's request to access the network resources is accepted. Otherwise the SUBS rejects the SU's request.

2. If the request of the candidate node is to use PU's free spectrum, then after passing the authentication process in the secondary network, the SUBS forwards the request to the PUBS who also computes its trust value from the members of its network and then compares its final trust value with the predefined threshold value. If the final trust value is greater than threshold value, the candidate node's request is authenticated, ensuring that its request is from a valid trustworthy node in the secondary network, otherwise its request is not authenticated. After authenticating the candidate node's request, a decision is made as to whether to assign the spectrum to it or not by using the process proposed in Chapter 6.

5.2.2.3 Solution to avoid the biasing problem

The phase for solving the biasing problem that occurs only in the secondary network in the proposed TSNA framework is as follows:

1. Whenever a node wants to obtain other member node's trust value in the secondary network, it sends a request to the SUBS.

2. The SUBS sends a message to the CA as a query to learn the candidate node's trust value. In the meantime, the SUBS also collects the trust value from other member nodes (using the above trust calculation method in 5.2.2.1) and computes the candidate node's final trust value.

3. The CA checks the candidate node's trust value by comparing the trust value from both (public and private) repositories and sends a response to the requesting SUBS.

4. The SUBS compares the computed trust value with the value received from the CA. If both are identical, then the SUBS is sure that the candidate node's trust value is not biased by the member nodes, otherwise the candidate node's trust value is biased in the network.

5. If the trust value of the candidate node is biased, the SUBS then checks the candidate node's trust value received from every individual member node in the network at a period of time before and after the biasing problem happens. If there exists any dissimilarity between these values for any particular member node, the SUBS reports the member node as either a 'malicious user' or 'biased by a malicious user'.

6. The SUBS then broadcasts a message to all of its member nodes not to communicate with the malicious node and excludes this malicious node from the network.

In the next sections, the working of each of these steps defined in the proposed framework is discussed in detail:

5.3 Trust Calculation Methods Between Different Nodes in the TSNA Framework

As discussed in Section 4.2, trust is used to authenticate a SU's request to allow it to use a PU's free spectrum or other network resources and avoid malicious behaviors in the network. There are three different ways by which a node's trust value in the proposed framework is calculated, as shown in Figure 5.3. They are:

Direct trust calculation: Direct trust calculation is used to compute the trust value of a node by other member nodes if a past interaction experience exists between them. This is denoted by $T_{Directtrust}$. Referring to Figure 5.3, node 2 is the candidate node. As both node 1 and node 2 have a direct communication link with the candidate node, they use the direct trust calculation method (using its past communication link) to compute the candidate node's trust value.

Indirect trust calculation: In the absence of any direct past interaction experience between the member nodes and the candidate node, the indirect trust calculation is used to establish the trust value of the candidate node. This method determines the candidate node's trust value based on the recommendations from the other surrounding member nodes. The computed trust value is denoted by $T_{Indirecttrust}$. In other words, if the member node does not have any past behavioral history or any experience with the candidate node, the member node sends a request to other surrounding member nodes, soliciting for recommendations about the candidate node. In this case, trust is calculated indirectly for the candidate node. Referring to Figure 5.3, node 3 has no direct communication link with the candidate node but node 3 has a direct relation with node 1 and node 4 who can make a recommendation about the candidate node. Therefore, node 3 uses the indirect trust calculation method to compute the candidate node's trust value.

Integrated trust calculation: In situations where both direct and the indirect trust values exist between two nodes, the member node combines them to compute the candidate node's trust value. This is denoted by the integrated trust calculation method and the computed trust value is denoted by $T_{Integtrust}$. Referring to Figure 5.3, node 4 has both a direct and an indirect

communication link with the candidate node. Therefore, node 4 uses trust values from both links to compute the candidate node's trust value.

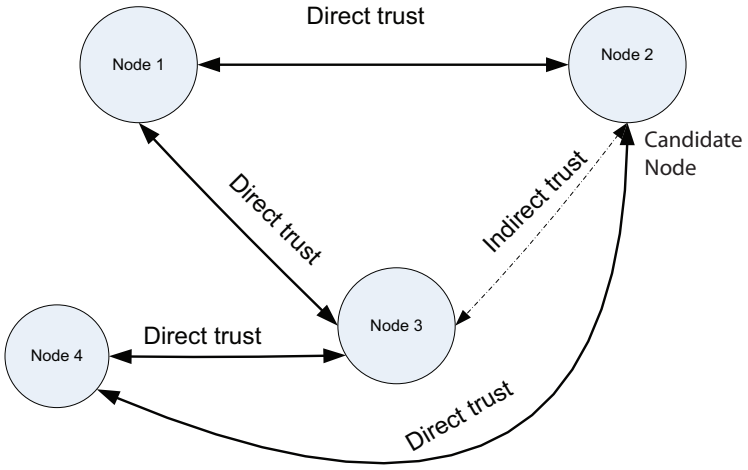

Figure 5.3: Different trust relationships between the candidate node and member nodes

Figure 5.4 illustrates the steps performed by the TSNA framework for the trust calculation between different nodes in the network.

The trust value calculated by each of the abovementioned methods is in the range of 0 and 1, where a value of 0 represents complete distrust and a value of 1 represents complete trust [55]. In the next sub-sections, a detailed explanation of the process by which the trust value of a candidate node is calculated by other member nodes in each scenario is presented.

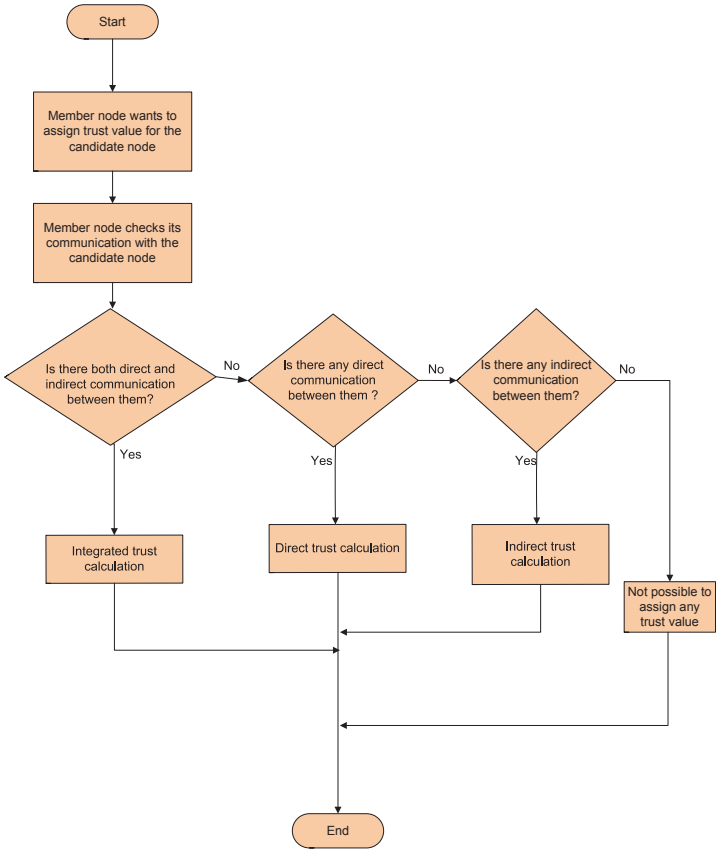

Figure 5.4: Flowchart of trust calculation phase performed by the TSNA framework

5.3.1 Direct trust calculation

The direct trust value of a candidate node is determined by the other member nodes with whom the candidate node's past cooperation exists. Since the conditions of a node are always changing, the base station constantly needs to check the trust values of the member nodes, based on their multi-attribute trust values. Han et al. [123] relate reliability with trust, where reliability

is defined as the capability of a node performing a given task as required and the outcome is based on the number of successes and failures in past cooperation record. Trust can be defined by the reliability that the trusting entity has in the trusted agent [124]. Trust is the subjective probability by which node A depends on node B to fulfil its promises in performing an action; ; after which node A considers node B as a reliable node [125]. In CRNs, a node needs the service provided by other nodes for communication between different nodes. A cognitive radio node can provide some cognitive services to others by cooperating different attributes such as sensing functions, sensing communication, showing sensing result consistency etc. When the cooperation process among the nodes finishes, the trust relationship is set up among the different nodes based on the historical cooperation records which determines them as either reliable or unreliable nodes. The cooperation records include different functionalities such as packet forwarding probability, encryption capability, energy, etc. If a node has a high reliability or trust value in a criterion such as packet forwarding probability then it will be regarded as a trustworthy node and vice versa. The trust value of a node can be calculated based on its reliable or unreliable capability in different functionalities and the trust model establishes the trust relationship during the interaction process by using these values among the nodes. Information about past cooperation is assembled in a table of cooperation records among the users, as shown in Table 5.1. Each member node stores this cooperation record in the network. Whenever a member node wants to assign the candidate node's trust value, it monitors its cooperation record with that candidate node and calculates the trust value for the candidate node. As referred to by Han et al. [123], each attribute has three relevant values: the number

of successes $(S_i, i = 1, 2....n)$ which indicates the reliability of the node, the number of failures $(F_i, i = 1, 2...n)$ which indicates the unreliability of the node and the amount of cooperation $(C_i, i = 1, 2, ...n)$. It is assumed that cooperative/non-cooperative behavior is of equal value during the interaction process between the users.

Table 5.1: Cooperation record table

Attributes	Success	Failure	Cooperation Sum
A_1	S_1	F_1	C_1
A_2	S_2	F_2	C_2
....	....	....	....
A_n	S_n	F_n	C_n

In Table 5.1, the cooperation sum is the summation of the number of failures and the number of successes for an event and is represented by $C_i = S_i + F_i, i = 1, 2, ...n$. The trust value for attribute A_i can be computed based on the values in Table 5.1 as follows:

$$T_{A_i} = \frac{S_i}{C_i} \tag{5.1}$$

Thus, the overall trust value for the candidate node with n attributes $A_i, i = 1, 2, ..n$ (denoted by $T_{Directtrust}$) can be computed using T_{A_i} as follows:

$$T_{Directtrust} = \frac{\prod_{i=1}^{n} T_{A_i}}{\prod_{i=1}^{n} T_{A_i} + \prod_{i=1}^{n} (1 - T_{A_i})} \tag{5.2}$$

5.3.2 Indirect trust calculation

In the absence of member nodes having direct interaction with the candidate node, the member node solicits for recommendations about the candidate node from other surrounding member nodes. It may receive replies from nodes who can be broadly categorized in three different types, namely reliable nodes, unknown nodes and unreliable nodes. Reliable nodes are known to be trustworthy nodes to the member node. In other words, the member nodes have solicited recommendations from these nodes in the past and found them to give trustworthy recommendations. The trust value recommended by such reliable nodes is represented as ($T_{reliable}$). Unknown nodes are those from whom the member node has not solicited recommendations in the past. The trust value recommended from these nodes is represented by ($T_{unknown}$). Unreliable nodes are those from whom the member node has solicited recommendations in the past and has found them to give incorrect recommendations. The trust value recommended from these nodes is represented by ($T_{unreliable}$). While calculating the trust value using the indirect method, it is assumed that the member node considers only the recommendations from reliable and unknown nodes and ignores the recommendations from unreliable nodes. However, to give more weight to the recommendations from the reliable nodes compared to the unknown nodes, the member nodes assign a weight value (utility/importance factor) based on the events that were monitored and quantified.

In order to obtain the indirect trust value of the candidate node, the trust values of $T_{reliable}$ and $T_{unknown}$ need to be calculated. The member node combines all kinds of trust values received from the recommenders to compute

the candidate node's trust value. At first, the member node retrieves the trust values from the reliable nodes, evaluated by themselves, which is stored locally and also receives the trust values of the candidate node from the reliable nodes and computes $T_{reliable}$ using equation 5.3.

$$T_{reliable} = \frac{\sum_{i=1}^{n_{reliable}} T_{MR_i} \times T_{RC_i}}{n_{reliable}} \tag{5.3}$$

where T_{MR_i} denotes the trust value from member node (M) to i th reliable node (R);

T_{RC_i} denotes the trust value from reliable node (R) to candidate node (C) and $n_{reliable}$ denotes the total number of reliable nodes.

Similarly $T_{unknown}$ is calculated using equation 5.4.

$$T_{unknown} = \frac{\sum_{k=1}^{n_{unknown}} T_{UC_k}}{n_{unknown}} \tag{5.4}$$

where T_{UC_k} denotes the trust value from kth unknown node to candidate node and

$n_{unknown}$ denotes the total number of unknown nodes.

Trust value $T_{reliable}$ is assigned a weight $W_{reliable}$ and trust value $T_{unknown}$ is assigned a weight $W_{unknown}$. These weights, $W_{reliable}$ and $W_{unknown}$, can be assigned using different approaches. In the approach used in this thesis, weights were assigned according to the member node's own criteria, based on the events that were monitored and quantified.

Thus, the indirect trust value can be calculated using the traditional

weighted approach [123, 126, 127] as follows:

$$T_{Indirecttrust} = T_{reliable}W_{reliable} + T_{unknown}W_{unknown} \tag{5.5}$$

where $W_{reliable} + W_{unknown} = 1$ and $W_{reliable}, W_{unknown} \in [0, 1]$

5.3.3 Integrated trust calculation

In the proposed framework, integrated trust is calculated in the case where both a direct and indirect communication link exists between the member nodes and the candidate node. In such a scenario, the member nodes can automatically assign different weight values based on the requirements of a certain task. Thus, the integrated trust value can be calculated using the traditional weighted approach [123, 126, 127]. The weight of the direct trust is denoted by $W_{directtrust}$, the weight of the indirect trust is denoted by $W_{indirecttrust}$. The integrated trust value can be calculated by the following equation:

$$T_{integtrust} = W_{directtrust} \times T_{directtrust} + W_{indirecttrust} \times T_{indirecttrust} \tag{5.6}$$

where $W_{directtrust} + W_{indirecttrust} = 1$
and $W_{directtrust}, W_{indirecttrust} \in [0, 1]$

When cooperation between the different nodes has taken place, based on above calculation methods in the network, every member node records and updates the trust value of its cooperation node.

Using the abovementioned trust calculation methods, the SUBS can determine the trust value of an SU and make a decision as to whether its request is authenticated either to use the secondary network's resources or for spectrum sharing (as discussed in detail in Chapter 6) from the primary network. However, in cases where an SU is a new user to the CRN, it may have a certain trust value in the secondary network which it has achieved by the secure joining process (this is discussed in further detail in Chapter 7) but it may not have a trust value with either the PUBS or the other PUs. In such scenarios, the abovementioned trust calculation mechanisms will clearly disadvantage its authentication request to access the free spectrum from the primary network. To address such a scenario, in the next subsection, an approach is proposed to bootstrap the newly joined SU node.

5.3.4 Bootstrapping of a new SU in the primary network

Using the proposed approach, the PUBS can bootstrap a newly joined SU in two ways, namely (a) the triangular trust calculation method and (b) the reference trust calculation method. The steps for bootstrapping a new SU in CRNs are as follows:

1. New SU joins the network and sends a request to the SUBS to use the PU's free spectrum. The SUBS assigns a trust value to this newly joined node based on its joining process to the secondary network and its behaviour is monitored for a certain period. If it passes the authentication process in the secondary network, its request is passed to the PUBS.

2. Once its request is received from the SUBS, the PUBS needs to calculate the SU's trust value to authenticate its request in the primary network.

3. As the SU node does not have any trust value with either the PUBS or the other PUs, the relationship between the PUBS and SUBS is taken into consideration to determine the trust value of the new SU by using either the triangular or reference trust calculation method.

4. If the PUBS and SUBS have a trust relation between them, the PUBS uses the triangular trust calculation method to calculate the SU's trust value. If there is no trust relation between the SUBS and PUBS, but if the PUBS trusts some member nodes in the secondary network, then in this particular case, the PUBS uses reference trust calculation method to calculate the new SU's trust value.

The detailed process of triangular and reference trust calculation are explained next.

5.3.4.1 Triangular trust calculation

The triangular trust calculation method is used to determine the trust value of the newly joined SU when it has a relationship with the SUBS by a certain amount but not with the PUBS. In such cases, the triangular relationship is formed considering the trust relationship between PUBS $\longrightarrow$ SUBS; SUBS $\longrightarrow$ SU1 to calculate the trust value of the SU node, as shown in Figure 5.5.

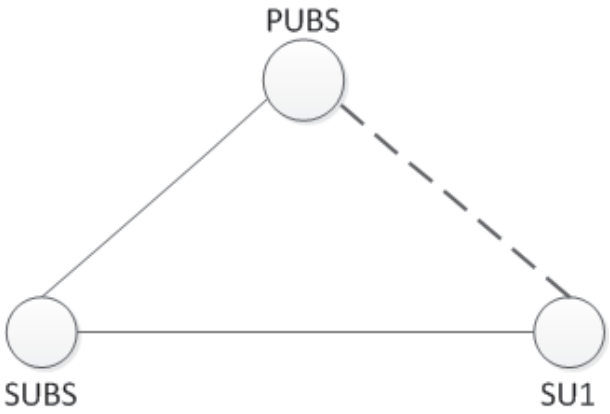

Figure 5.5: Triangular trust calculation to bootstrap a new SU node

The trust value of the PUBS for the SU1 is denoted by $T_{PUBS,SU1}$. Suppose the trust value between the PUBS and SUBS is 0.7, $T_{PUBS,SUBS} = 0.7$ and that between the SUBS and SU1 is 0.6 $T_{SUBS,SU1} = 0.6$, the resultant trust value between the PUBS and SU1 is determined as:

$T_{PUBS,SU1} = T_{PUBS,SUBS} * T_{SUBS,SU1} = 0.7 * 0.6 = 0.42$

However, it is possible that in some cases there may not be a trust value relationship between the PUBS and SUBS. In such cases, the newly joined SU is bootstrapped using the reference trust calculation.

5.3.4.2 Reference trust calculation

The reference trust calculation uses recommendations from other users to calculate the trust value of the new SU. But the solicited recommendations by the PUBS are from the SUs and not from the PUs as occurs in the indirect trust calculation method.

In the reference trust calculation, the average of the recommended trust values received for a newly joined SU is used to determine its trust value. For instance, if the trust relationship between different nodes is as shown in Figure

5.6, it can be seen that the PUBS trusts SU2 and SU3 with a value of 0.5 and 0.6, respectively. But both SU2 and SU3 know the new SU with a trust value of 0.5 and 0.4, respectively.

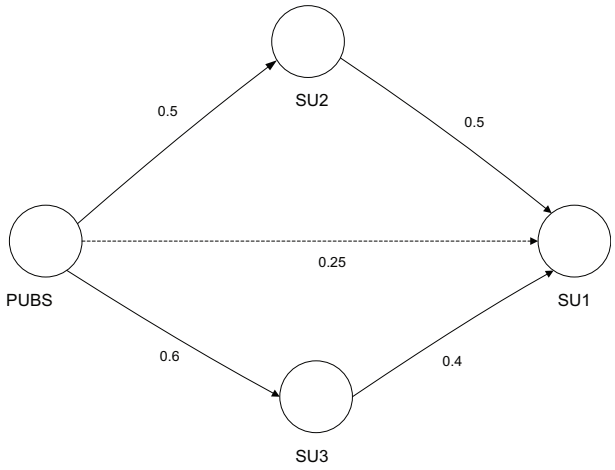

Figure 5.6: Reference trust calculation to bootstrap a new SU node

So, the average trust value between the PUBS and SU1 is determined as:

$T_{PUBS,SU1} = (T_{PUBS,SU2} * T_{SU2,SU1} + T_{PUBS,SU3} * T_{SU3,SU1}))/2 = (0.5 * 0.5 + 0.6 * 0.4)/2 = 0.249 \Longrightarrow 0.25$

For both cases, if the computed trust value of the newly joined SU is greater than the predefined threshold value ($T_{threshold}$), then the PUBS considers that node as a trustworthy node to authenticate its request. On the other hand, if the computed trust value is below the predefined threshold, then the PUBS declines the request of the SU.

5.4 Authenticating an SU's Request in the TSNA Framework

In this phase, the authenticity of the requesting SU is checked based on the trust value in order to accept its request. Figure 5.7 illustrates the flowchart of this phase.

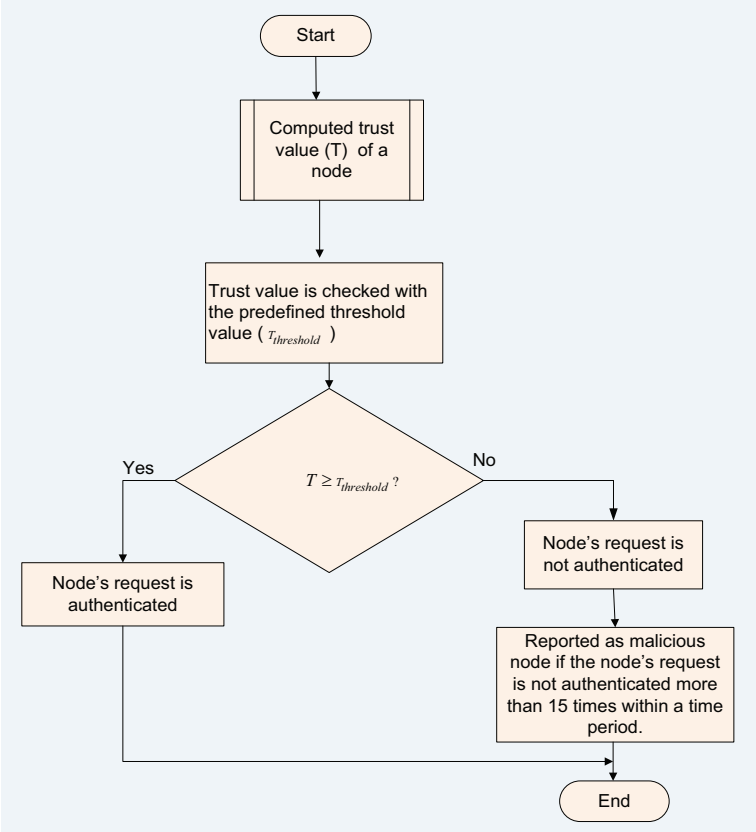

Figure 5.7: Flowchart of the authentication checking step performed by the TSNA framework

The work flow of this step is as follows:

1. The requesting SU's trust value is computed by the trust calculation method described in Section 5.3.

2. The computed trust value T of the requesting node is compared with the system defined threshold value ($T_{threshold}$)

3. If T is greater than or equal to $T_{threshold}$, the requesting node's request is authenticated to be considered as a valid and trustworthy user to use the secondary network's resources or even to use the PU's free spectrum. This then leads to the process of deciding whether to allow the SU's request to use the spectrum. The detailed spectrum sharing process of the primary network after the SU's request is authenticated is described in Chapter 6.

4. If T is less than $T_{threshold}$, then the requesting node's request is declined and it is not considered as an authenticated user in the network.

5. In the proposed approach, if the node's request is declined fifteen times within a time period, then the node is not trustworthy at all and is reported as a malicious node for its suspicious behaviour. This is out of the scope of this thesis.

5.5 Solution to Avoid the Biasing Problem During Trust Recommendation

A malicious node could change the candidate node's trust value as an effect of malicious behaviour, thus the biasing problem arises in the secondary network in CRNs during the trust value recommendation of a node. Another threat is that member nodes in the secondary network, being biased by malicious nodes, can assign a false trust value for the candidate node. As discussed in

Section 4.2.2, to solve this problem, the certificate authority based framework is proposed in this chapter. The working steps of this phase are shown in Figure 5.8.

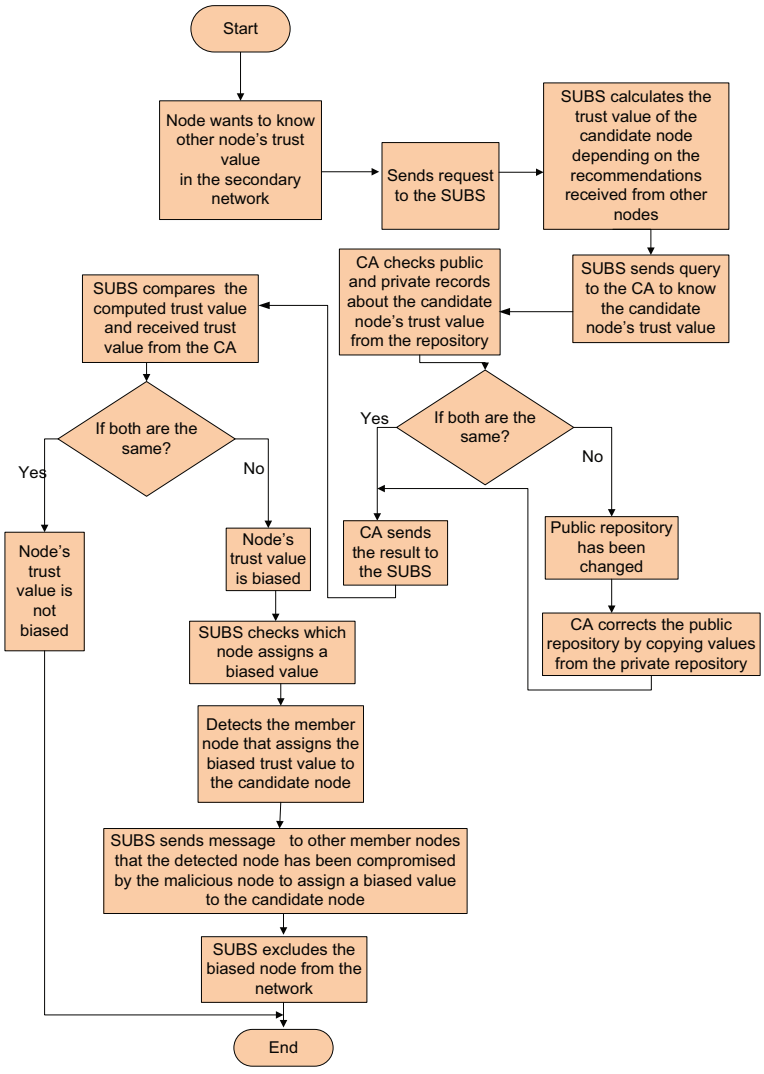

Figure 5.8: Flowchart for the biasing problem solution phase performed by the TSNA framework

The work flow of this step is as follows:

1. Whenever a node wants to obtain another member node's trust value in the secondary network, it sends a request to the SUBS. In some scenarios,

the SUBS may also want to know any other member node's trust value.

2. The SUBS sends a query to the CA node to obtain the candidate node's trust value. The SUBS also collects the trust value from other member nodes and computes the trust value for the candidate node.

3. The CA node checks both repositories for the candidate node's trust value. If both are identical, then CA sends the trust value of the candidate node to the SUBS as a response to the query. If both are not similar, the CA confirms that the public repository has been hacked by some malicious node. To address this problem, the CA corrects the public repository by copying the trust values for all the member nodes in the network from the private repository and replacing them with the values in the public repository. After addressing this issue, the CA sends the trust value of the candidate node to the SUBS.

4. The SUBS receives the result from the CA node. It then compares the trust value that it has computed for the candidate node with the result received from the CA. If both are the same, the SUBS is sure about the candidate node's actual trust value. If both are not same, the SUBS is sure that the candidate node's trust value has been biased by malicious users in its network. The SUBS checks and compares the trust values assigned by every individual member node before and after the biasing problem occurs in the network. If there is any dissimilarity between these values, the SUBS reports these nodes as either being 'biased by malicious nodes' or as 'malicious nodes'. Member nodes biased by malicious nodes always assign a biased trust value for the candidate node. To solve this malicious behaviour, the SUBS excludes these member nodes from the

network and broadcasts a message to the network not to communicate with such biased nodes.

5.6 Example of Trust Calculation to Authenticate an SU's Request in CRNs

In this subsection, an example is given as to how the trust value is calculated to authenticate an SU's request. In the example, there are two networks in the CRN, namely the primary network and the secondary network, and all the member nodes of each network have direct communication with one another as well as with their base stations.

5.6.1 Example of direct trust calculation

In this example, there is direct communication between the member node and the candidate node. The member node has a history of cooperation with the candidate node, as shown in Table 5.2. In this example, there are three criteria against which a candidate node's trust value is determined by the member nodes. Table 5.2 represents the cooperation records of the past behaviour of the candidate node in each of these three criteria in different time periods (T_n).

(a) Cooperation records for criteria C1			(b) Cooperation records for criteria C2			(c) Cooperation records for criteria C3		
	Success	Failure		Success	Failure		Success	Failure
Time T1	1	0	T1	1	0	T1	1	0
T2	1	0	T2	1	0	T2	0	1
T3	0	1	T3	0	1	T3	0	1
T4	0	1	T4	1	0	T4	1	0
T5	1	0	T5	1	0	T5	1	0
T6	1	0	T6	1	0	T6	0	1
T7	0	1	T7	0	1	T7	0	1

Table 5.2: Cooperation record table for direct trust calculation

Using equation 5.1, the trust value between the candidate node and the member node for criterion C_1 is determined as follows:

$$T_{A_i} = \frac{S_i}{C_i} = \frac{4}{7} = 0.57 \tag{5.7}$$

Similarly, the trust values for criteria C_2 and C_3 are 0.71 and 0.42, respectively. Using equation 5.8, the overall trust value of the candidate node is calculated as follows:

$$\begin{aligned} T_{Directtrust} &= \frac{\prod_{i=1}^{n} T_{A_i}}{\prod_{i=1}^{n} T_{A_i} + \prod_{i=1}^{n} (1 - T_{A_i})} \\ &= \frac{0.57 + 0.71 + 0.42}{(0.57 + 0.71 + 0.42) + (1 - 0.57) + (1 - 0.71) + (1 - 0.42)} \\ &= \frac{1.7}{3} = 0.56 \end{aligned} \tag{5.8}$$

Therefore, the member node computes the candidate node's trust value $T_{Directtrust}$ using the direct trust calculation and its value is 0.56.

5.6.2 Example of indirect trust calculation

As mentioned in Section 5.3.2, it is possible that a member node and a candidate node do not have a direct communication link, as shown in Figure 5.9. In this particular case, the member node uses the indirect trust calculation method to compute the candidate node's trust value.

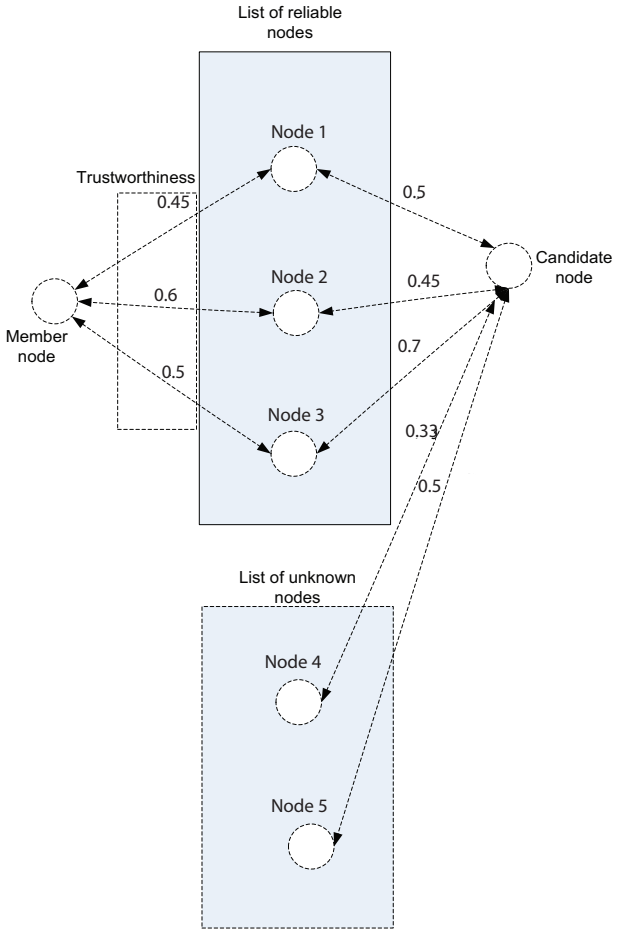

Figure 5.9: Example of indirect trust calculation

Firstly, the member node receives the recommendations for the candidate node from the reliable nodes and computes the candidate node's trust value using equation 5.9.

$$T_{reliable} = \frac{\sum_{i=1}^{n_{reliable}} T_{MR_i} \times T_{RC_i}}{n_{reliable}} = \frac{0.45 * 0.5 + 0.6 * 0.45 + 0.5 * 0.7}{3} = \frac{0.22 + 0.27 + 0.35}{3} = 0.28 \quad (5.9)$$

Then, the member node receives the recommendations for the candidate node from the unknown nodes and computes the candidate node's trust value using equation 5.10.

$$T_{unknown} = \frac{\sum_{k=1}^{n_{unknown}} T_{UC_k}}{n_{unknown}} = \frac{0.33 + 0.5}{2} = 0.41 \quad (5.10)$$

Therefore, the member node computes the candidate node's trust value using the indirect trust calculation as follows:

$$T_{Indirecttrust} = 0.7 * 0.28 + 0.3 * 0.41 = 0.196 + 0.123 = 0.319 \quad (5.11)$$

where 0.7 and 0.3 is assigned a weight value for reliable trust and unknown trust, respectively.

5.6.3 Example of integrated trust calculation

As discussed in Section 5.3.3, where the member node has both the direct and indirect communications with the candidate node as shown in Figure 5.10, the member node uses the integrated trust calculation method to determine the candidate node's trust value.

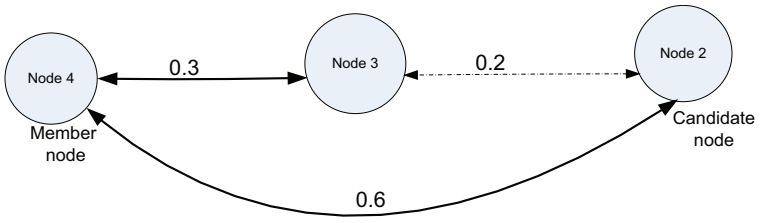

Figure 5.10: Example of integrated trust calculation

As shown in Figure 5.10, the member node wants to know the candidate node's trust value. The member node has a direct relationship with the candidate node by a trust value of 0.6 and it also has a direct relationship with node 3 by a trust value of 0.3 who can recommend the candidate node by a value of 0.2. Therefore, the trust value of the candidate node from the member node can be calculated using equation 5.6 as follows:

$$T_{integtrust} = 0.8 * 0.6 + 0.2 * (0.2 * 0.3) = 0.72 \tag{5.12}$$

where 0.8 and 0.2 are the assigned weight values for the direct trust and indirect trust, respectively.

5.7 Verification of the TSNA Framework

A system is designed to verify the proposed TSNA framework, using the JAVA programming language version 1.5 and the standard JAVA SDK libraries and third party graphing libraries. JAVA is an object-orientated programming language and the use of objects is ideal in representing a real-world problem such as this. JAVA is also able to be run OS independent using a virtual machine, so it is a good candidate for implementation. The platform used for coding, compilation, debugging and execution is NetBeans IDE (Integrated

Development Environment) version 5.5. NetBeans was used in the engineering because of the ease with which it can build the Graphical User Interface (GUI). The aim of using a networking tool in Java is to simulate the implementation and operation of the proposed methodology for establishing trust in the network and then utilizing it for making a decision as to whether the requesting node's request will be authorized to use network resources or not.

5.7.1 Phases in the trust-based SU authentication framework verification

Verification for the TSNA framework to authenticate an SU's request consists of 3 phases. They are:

1. Initialization Phase: In this phase, the network is set up according to the system's parameters. In this phase, it is assumed that initially, all the nodes in the network are well behaved and fair. The parameters which are input for each network in this phase are: the candidate node number whose trust value is to be calculated, the number of nodes in the network, the criteria number by which the candidate node's behaviour is observed for a certain period and trust is calculated depending on the monitored behaviour. In this phase, two networks (secondary network as 'Network 1' and primary network as 'Network 2') are set up. 'Network 1' has 5 member nodes including the candidate node and one base station, whereas 'Network 2' has 4 member nodes and one base station.

2. Calculation Phase: In this phase, the candidate node's trust value is calculated using the different types of calculation methods described in Section 5.3. The member nodes in both 'Network 1' and 'Network 2' use

the direct calculation method to assign trust values to the candidate node to authenticate its request. Each member node calculates the candidate node's trust value for different criteria and sends these to the corresponding base station. The corresponding base station calculates the final trust value of the candidate node and sends the result to the CA for record keeping purposes and the CA uses this value to solve the biasing problem. The aim of this phase is to determine the candidate node's trust value according to the different criteria in the system.

3. Decision Phase: During this phase, the computed trust value of the candidate node is compared with the system's predefined threshold value. In this simulation, the predefined threshold value is set to 0.6. If the computed trust value is greater than the threshold value, the candidate node's request is authenticated, otherwise not. During this phase, the biasing problem is solved by checking the candidate node's trust value and comparing it with the value received from the CA node.

5.7.2 Scenario 1: Authenticating the SU's request based on the trust value

In this scenario, the candidate node's trust value is computed to determine whether its request to use either the network resources from 'Network 1' or to consider its request to use the PU's spectrum from 'Network 2' is authenticated by the corresponding base station and to avoid a malicious node's behaviour in the network. As mentioned earlier, if a candidate node sends a request to use the PU's free spectrum, the SUBS first calculates the candidate node's trust value and checks its authenticity. If the candidate node is selected as an

authenticated user, the SUBS forwards its request to the PUBS. PUBS also needs to check its authenticity to ensure that the request is coming from a valid and trustworthy user. Verification results for different cases are shown as follows:

5.7.2.1 *Case 1: Candidate node's request authentication process in the secondary network ('Network 1')*

For this case, the following steps are verified and the results are shown accordingly.

1. Initialization Phase : The network environment is set up as shown in Figure 5.11. Node 2 is selected as a 'candidate node' in 'Network 1'. There are another four nodes and one base station (SUBS) in the network.

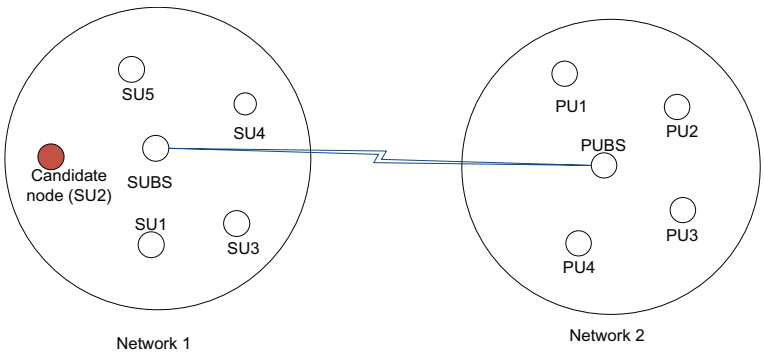

Figure 5.11: Snapshot Network Set-up

During this phase, it is assumed that all nodes in 'Network 1' are well behaved nodes (fair nodes) and have not been biased by malicious users, as shown in Table 5.3.

Candidate Node	Node number in 'Network 1'	Type
Node 2 in 'Network 1'	1	Fair
	3	Fair
	4	Fair
	5	Fair

Table 5.3: Node initialization from 'Network 1'

Figure 5.12 shows the network window for calculating the trust value of the candidate node in 'Network 1'.

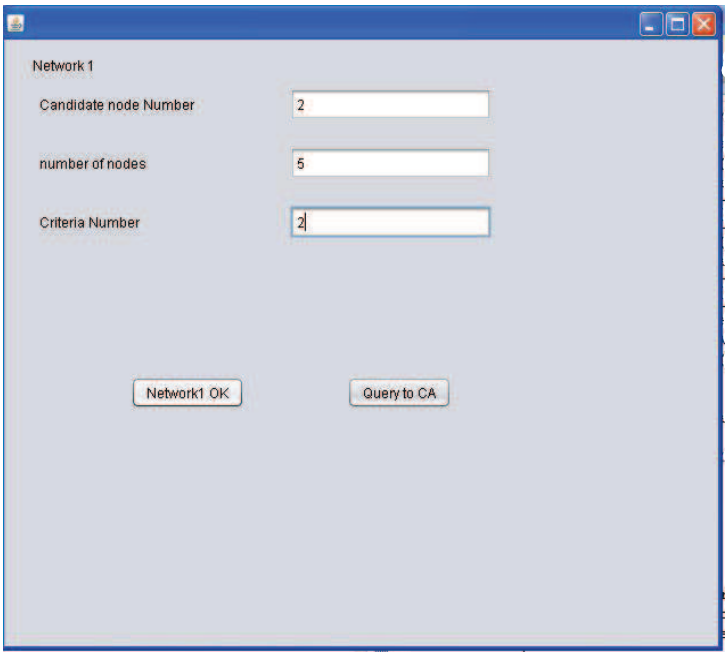

Figure 5.12: Input for 'Network 1'

2. Calculation Phase:

   The member nodes in 'Network 1' assign a trust value to the candidate node in different time periods using equation 5.1 for three different criteria and sends it to the SUBS. So, four member nodes (SU1, SU3,

SU4, and SU5) in 'Network 1' assign different trust values for each criteria at different timed. The system runs 100 times and generates random values for the success and failure for each time period for each criteria and gives the trust value for the candidate node using equations 5.1 and 5.8.

The trust value of the candidate node from four nodes for different time periods for criteria 1 in 'Network 1' is shown in Figure 5.13.

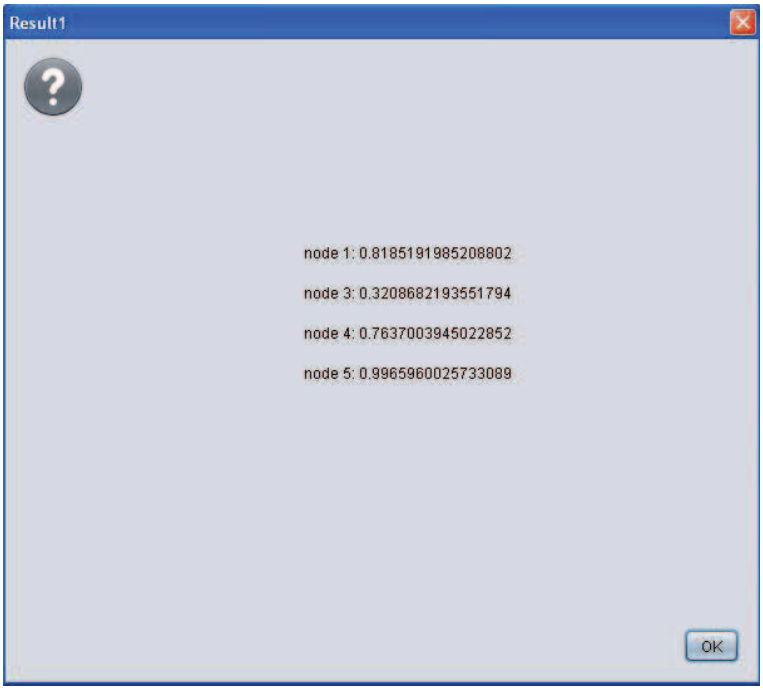

Figure 5.13: Trustworthiness of the candidate node from four nodes in 'Network 1' for criteria 1

Therefore, the average trust value of the candidate node for criteria 1 in 'Network 1' is : $\frac{0.81+0.32+0.76+0.99}{4} = 0.72$

Similarly, the trust values of the candidate node from four nodes for different time periods for criteria 2 and 3 in 'Network 1' are shown in Figure 5.14 and 5.15, respectively. Therefore, the average trust value of

the candidate node for criteria 2 and 3 in 'Network 1' is 0.67 and 0.45, respectively. The SUBS then computes the final trust value and sends it to the CA for record keeping. The final trust value of the candidate node calculated from the SUBS for three different criteria in 'Network 1' using equation 5.8 is :$\frac{0.72+0.67+0.45}{3} = 0.61$, as shown in Figure 5.16.

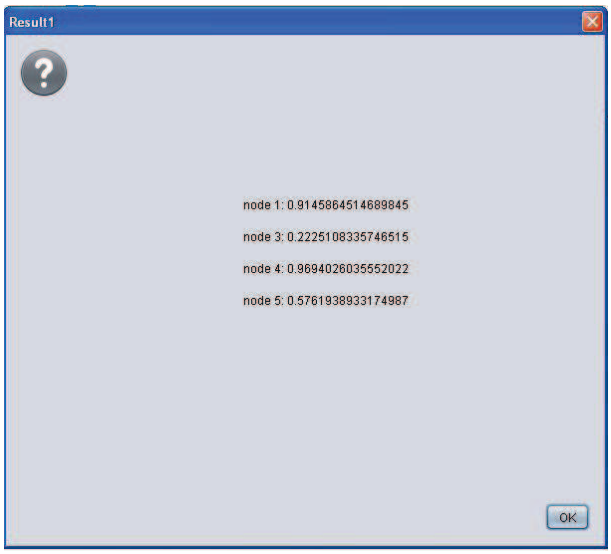

Figure 5.14: Trustworthiness of the candidate node from four nodes in 'Network 1' for criteria 2

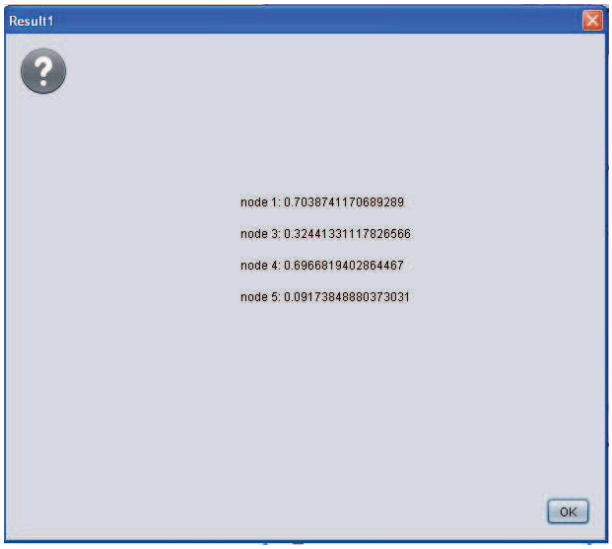

Figure 5.15: Trustworthiness of the candidate node from four nodes in 'Network 1' for criteria 3

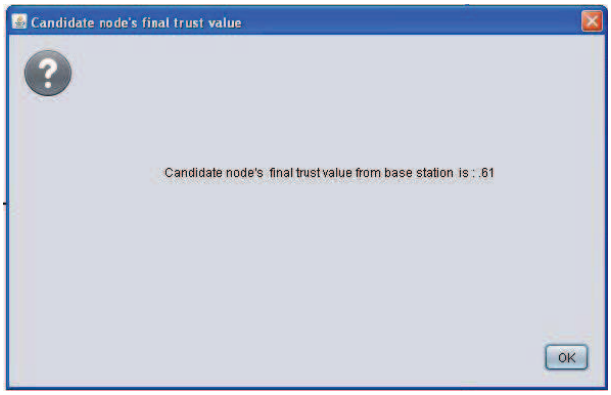

Figure 5.16: Candidate node's final trust value computed by the SUBS in 'Network 1'

3. Decision Phase: In this phase, the computed trust value from the above step is compared with the trust threshold and the decision is made based on this comparison, as shown in Table 5.4. In this verification, it is assumed that the predefined threshold value is 0.6. Therefore, the computed final trust value (0.61) is above the threshold (0.6) and as a result, the SUBS authenticates the candidate node to accept its request

to use the network resources or forwards its request to the 'Network 2', as shown in Table 5.4.

Candidate node	Trust Value of Candidate node			Final trust value	Threshold value	Trust value ≥ threshold value ?	Decision
	Criteria 1	Criteria 2	Criteria 3		0.6		Request is authenticated or request is forwarded to 'Network 2'
Node 2 'Network 1'	0.72	0.67	0.45	0.61		Yes	

Table 5.4: Trustworthiness comparison to decide to authenticate the candidate node's request in 'Network 1'

5.7.2.2 *Case 2: Candidate node's request authentication process in the primary network ('Network 2')*

The candidate node's request also needs to be authenticated for accessing the resources in the primary network. Firstly, the candidate node's trust value is calculated from 'Network 1' and if it is above the threshold, only then is its request to access the primary network resources forwarded to 'Network 2'. For this purpose, 'Network 2' calculates the candidate node's final trust value for further consideration and decides whether its request is authenticated to be considered as a trustworthy user to use the primary network's resources (which is described in detail in Chapter 6). The steps to authenticate the SU's request in the primary network are as follows:

1. Initialization Phase : The candidate node's trust value from 'Network 1' is calculated and checked from Table 5.4 and it shows that 'Decision' is

'Accepted', so the candidate node's request is forwarded to 'Network 2'. During this phase, it is assumed that all nodes in 'Network 2' are fair and not biased by malicious users, as shown in Table 5.5.

Candidate Node	Node number in 'Network 2'	Type
Node 2 in 'Network 1'	1	Fair
	2	Fair
	3	Fair
	4	Fair

Table 5.5: Nodes initialization from 'Network 2'

Figure 5.17 shows the network window for calculating the trust value of the candidate node in 'Network 2'.

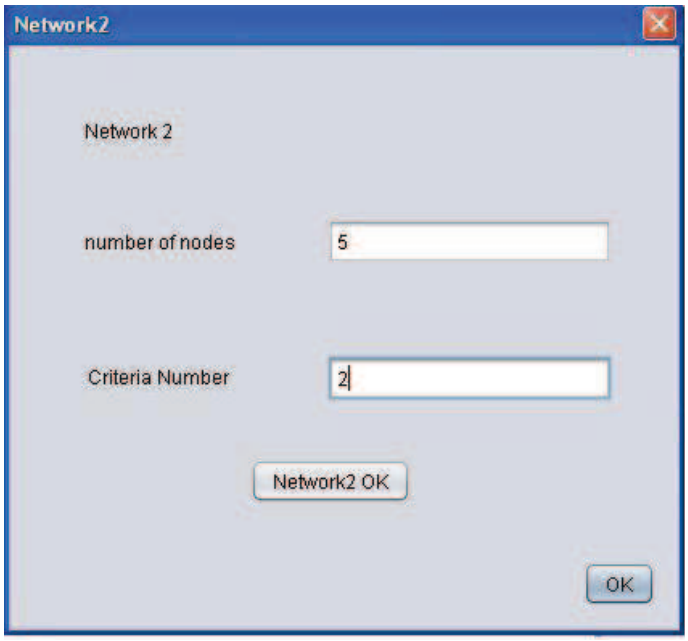

Figure 5.17: Input for 'Network 2'

2. Calculation Phase:

The member nodes of 'Network 2' calculate the candidate node's trust value using the direct trust calculation.

The trust values of the candidate node from four nodes from different time periods for criteria 1 in 'Network 2' is shown in Figure 5.18

Therefore, the average trust value of the candidate node for criteria 1 in 'Network 2' is : $\frac{0.59+0.95+0.76+0.93}{4} = 0.81$ Similarly, the trust values of the candidate node from four nodes from different time periods for criteria 2 and 3 in 'Network 2' are shown in Figures 5.19 and 5.20, respectively. Therefore, the average trust values for the candidate node for criteria 2 and 3 in 'Network 2' is 0.55 and 0.77, respectively. The base station (PUBS) then computes the final trust value and sends it to the CA for record keeping. The final trust value of the candidate node computed by the PUBS from 'Network 2' is : $\frac{0.81+0.55+0.77}{3} = 0.71$ as shown in Figure 5.21.

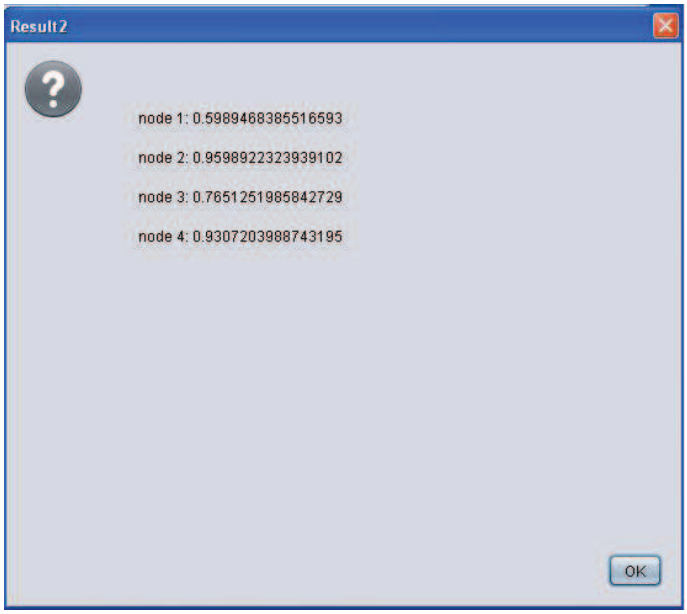

Figure 5.18: Trustworthiness of the candidate node from different nodes in 'Network 2' for criteria 1

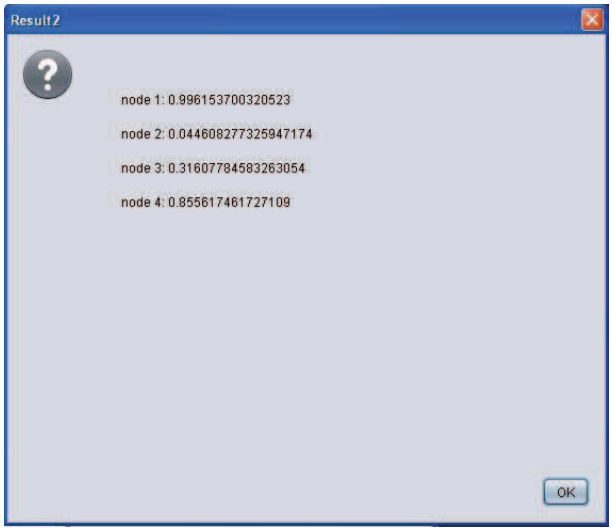

Figure 5.19: Trustworthiness of the candidate node from different nodes in 'Network 2' for criteria 2

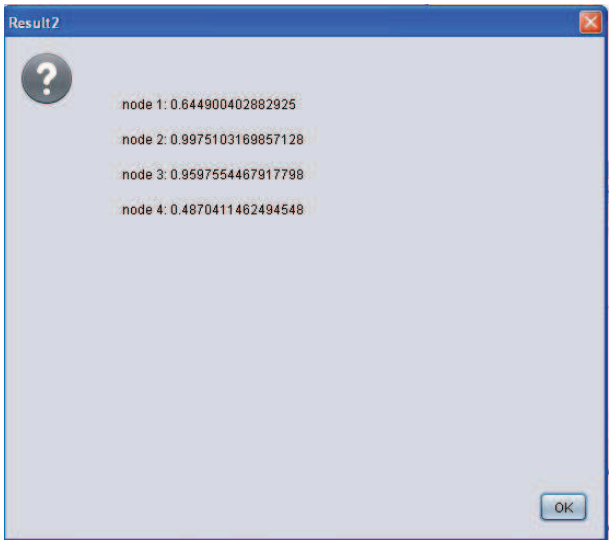

Figure 5.20: Trustworthiness of the candidate node from different nodes in 'Network 2' for criteria 3

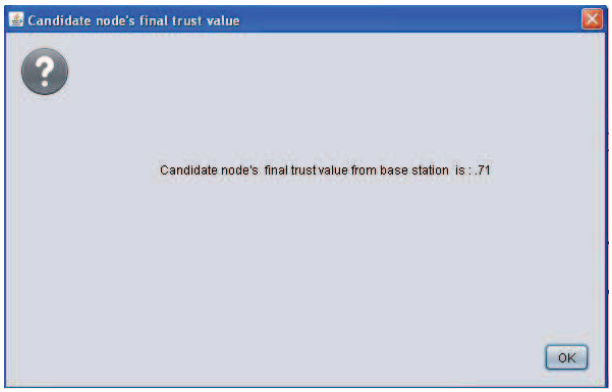

Figure 5.21: Candidate node's final trust value computed by the PUBS in 'Network 2'

3. Decision Phase: In this phase, the computed trust value from the above step is compared with the trust threshold and a decision is made based on this comparison, as shown in Table 5.4. The computed final trust value (0.71) is above the threshold (0.6) and as a result, the candidate node's request is authenticated in the primary network ('Network 2'), as shown in Table 5.6.

Candidate node	Trust Value of Candidate node			Final trust value	Threshold value	Trust value ≥ threshold value ?	Decision
	Criteria 1	Criteria 2	Criteria 3				
Node 2 in 'Network 1'	0.81	0.55	0.77	0.71	0.6	Yes	Request is authenticated

Table 5.6: Trustworthiness comparison to decide to authenticate the candidate node's request in 'Network 2'

5.7.2.3 *Case 3: Candidate node's request is not authenticated either in the 'Network 1' or in the 'Network 2'*

For this case, the same working phases are executed in a simulation environment considering node number 4 in 'Network 1' is a candidate node. After executing all the steps as above in 'Case 1', the decision table is shown is Table 5.7 as follows:

Candidate node	Trust Value of Candidate node			Final trust value	Threshold value	Trust value ≥ threshold value ?	Decision
	Criteria 1	Criteria 2	Criteria 3				
Node 4 in 'Network 1'	0.21	0.33	0.47	0.33	0.6	No	Declined to authenticate its request

Table 5.7: Trustworthiness comparison to decide to authenticate 'node 4' in 'Network 1'

From Table 5.7, it is noticeable that the final trust value of the candidate node is below the threshold value, so its request is not authenticated in the 'Network 1'. In other words, the candidate node is not considered a valid and trustworthy user in its own network, therefore, the SUBS does not forward the candidate node's request to access the primary network resources to 'Network 2' for further authentication checking.

5.7.3 Scenario 2: Member nodes are biased by malicious users to assign a biased trust value for the candidate node and its solution

In this scenario, it is assumed that some member nodes are biased either by malicious users or other member nodes to assign a biased trust value to the candidate node. This scenario will be examined and solved by the SUBS by comparing the computed trust value of the candidate node with the trust value received from the CA node.

1. Initialization Phase: This phase is similar to the 'initialization phase' in scenario 1, as discussed in Section 5.7.2.1. The network environment is set up according to Figure 5.11. Here, node 3 in 'Network 1' is selected as a candidate node. There are four other nodes and one base station in every network. For this scenario, three different criteria are considered to evaluate the trust value for the candidate node. Firstly, it is assumed that all the nodes are fair in 'Network 1'. After the candidate node's final trust evaluation and after being saved to the CA, some malicious nodes intentionally bias the member nodes in 'Network 1' to assign a biased trust value to the candidate node. Therefore, there is a need to calculate the candidate node's trust value twice: (1) before the biasing problem happens in the network; and (2) after the biasing problem happens in the network.

2. Calculation Phase:

   - ***Before Biasing*** : Firstly, the candidate node's trust value is calculated by the member nodes in 'Network 1' and all member

nodes are fair. For criteria 1, four nodes in 'Network 1' assign a trust value to the candidate node accordingly, as shown in Figure 5.22

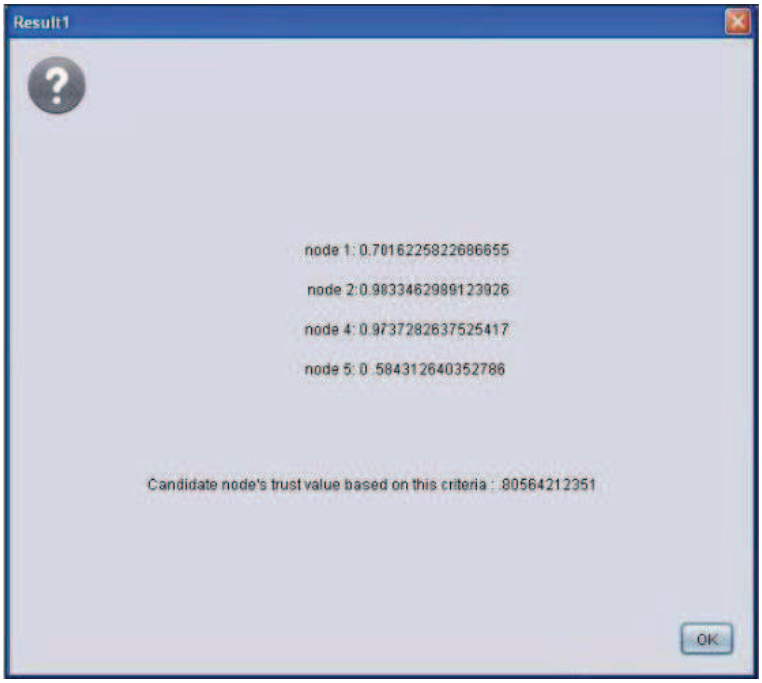

Figure 5.22: Trust value for the candidate node in 'Network 1' for criteria 1

Therefore, the average trust value of the candidate node for criteria 1 in 'Network 1' is : 0.8056

For criteria 2 and 3, four nodes in 'Network 1' assign trust value to the candidate node accordingly, as shown in Figures 5.23 and 5.24, respectively. Therefore, the average trust value of the candidate node for criteria 2 and 3 in 'Network 1' is 0.7842 and 0.5032, respectively. The final trust value for the candidate node computed by the SUBS in 'Network 1' is $\frac{0.8056+0.7842+0.5032}{3} = 0.6976$

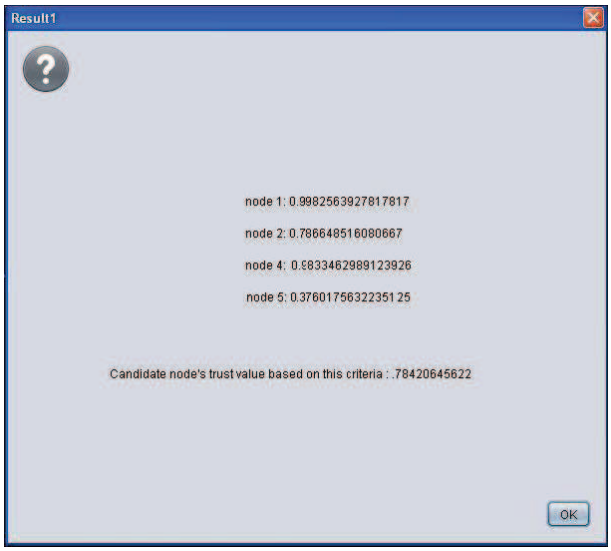

Figure 5.23: Trust value for the candidate node in 'Network 1' for criteria 2

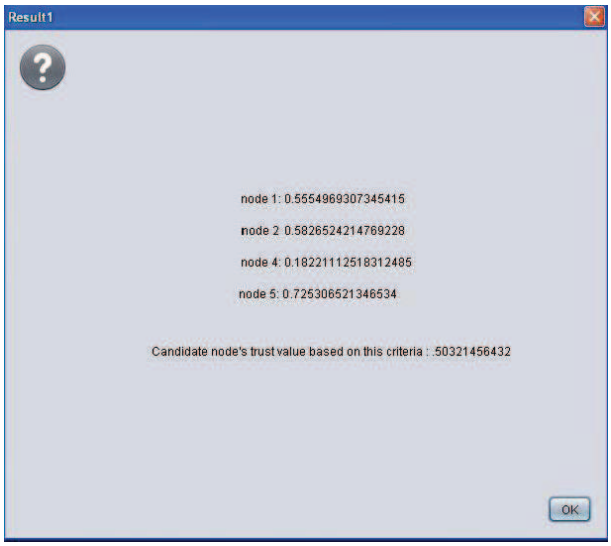

Figure 5.24: Trust value for the candidate node in 'Network 1' for criteria 3

The SUBS in 'Network 1' sends the computed results to the CA. The CA stores this value in both repositories, as shown in Table 5.8.

Node Number in 'Network 1'	Private Value	Public Value
3	0.6976	0.6976
....	....	....
.....	....	.....

Table 5.8: Saving trust value of candidate node in CA repository

- ***After Biasing:***

  After being biased by malicious nodes, the types of nodes in 'Network 1' are shown in Table 5.9.

Candidate node number in 'Network 1'	Node number in 'Network 1'	Type
3	1	Fair
	2	Fair
	4	Fair
	5	Biased

Table 5.9: Nodes initialization in 'Network1'

The member nodes which are biased by the malicious nodes assign a false trust value to the candidate node. Following the same steps of calculation in 'Before Biasing' step, the SUBS computes the candidate node's final trust value using the biased trust value received from the biased member nodes. After the biasing problem, the candidate node's trust value computed by the SUBS is shown in Table 5.10, which is different from the trust value computed before the biasing problem happens.

Candidate node	Criteria 1	Criteria 2	Criteria 3	Final Trust vale
Node 3 in 'Network 1'	0.69	0.93	0.57	0.80

Table 5.10: The candidate node's trust value computed by the SUBS in 'Network 1' after the biasing problem

After receiving the query from the SUBS about the candidate node's trust value, the CA checks both repositories. If the trust values in both repositories are the same as shown in Table 5.8, the CA forwards this result to the SUBS in 'Network 1', as shown in Figure 5.25. If the trust value in both repositories is not the same, the CA can be sure that public repository has been hacked by some malicious users who have intentionally changed the trust value in the public repository. To solve this problem, the CA copies all the trust values for all member nodes in both networks in the private repository and replaces them with the values in the public repository. After solving this issue, the CA forwards the query result to the SUBS in 'Network 1'.

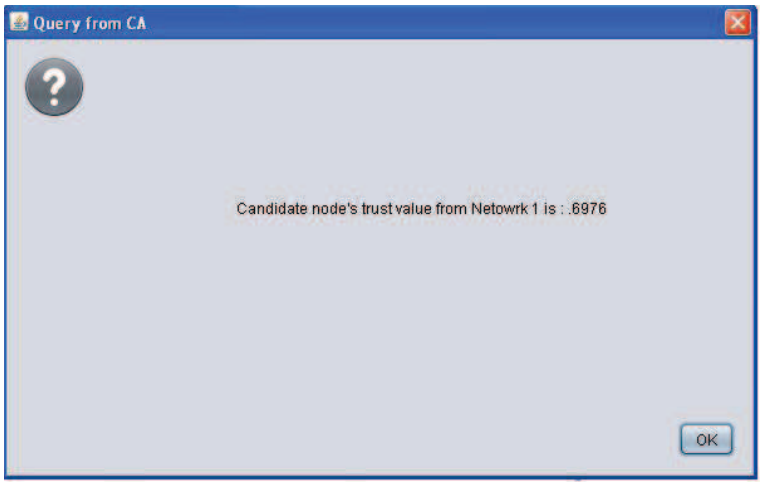

Figure 5.25: Query response for the candidate node's trust value in 'Network 1'

After receiving the candidate node's trust value from the CA, the SUBS compares it with the computed result, as shown in Table 5.11.

Candidate node	Trust value received from CA	Trust value computed by the SUBS after biasing	Are they similar?
Node 3 in 'Network 1'	0.69	0.80	No

Table 5.11: Comparison of candidate node's trust value

If the received result from the CA and the computed result from the SUBS is the same, the SUBS sends the result to the requesting node who places a query to know the candidate node's trust value. Whenever the SUBS observes that it is not the same as shown in Table 5.11, it checks the candidate node's trust value assigned by every individual member node for different criteria in 'Network 1', as shown in Table 5.12.

Criteria	Node number	Trust value of the candidate node before biasing	Trust value of the candidate node after biasing	Similar	Decision
	Node 1	0.7016	0.7016	Yes	Not biased
1	Node 2	0.9833	0.9833	Yes	Not biased
	Node 4	0.9737	0.9737	Yes	Not biased
	Node 5	0.5843	0.9999	No	Biased
2	Node 1	0.9982	0.9982	Yes	Not biased
	Node 2	0.7866	0.7866	Yes	Not biased
	Node 4	0.9833	0.9833	Yes	Not biased
	Node 5	0.3760	0.9999	No	Biased
3	Node 1	0.5554	0.5554	Yes	Not biased
	Node 2	0.5826	0.5826	Yes	Not biased
	Node 4	0.1822	0.1822	Yes	Not biased
	Node 5	0.7253	0.9999	No	Biased

Table 5.12: Trust value comparison from every individual node for different criteria in 'Network 1'

Based on the data from Table 5.12, the SUBS observes that the trust value of the candidate node from node 5 is not similar. Moreover, it observes that node 5, being biased, always assigns a high trust value for the candidate node as shown in Figure 5.26.

3. Decision Phase : After checking and comparing, the SUBS confirms that *node 5 in the 'Network 1'* has been biased by either other member nodes or malicious nodes to assign a biased trust value for the candidate node, as shown in Table 5.13. So, the SUBS spreads the message to the other member nodes in 'Network 1' about the biased node and advises them not to communicate with the biased node as it is comprised. The SUBS exclude the biased node from the network so that it cannot take part further in any network communication.

Biased node number in 'Network 1'	Decision
5	Exclude from the network

Table 5.13: Decision by the SUBS based on the biasing value

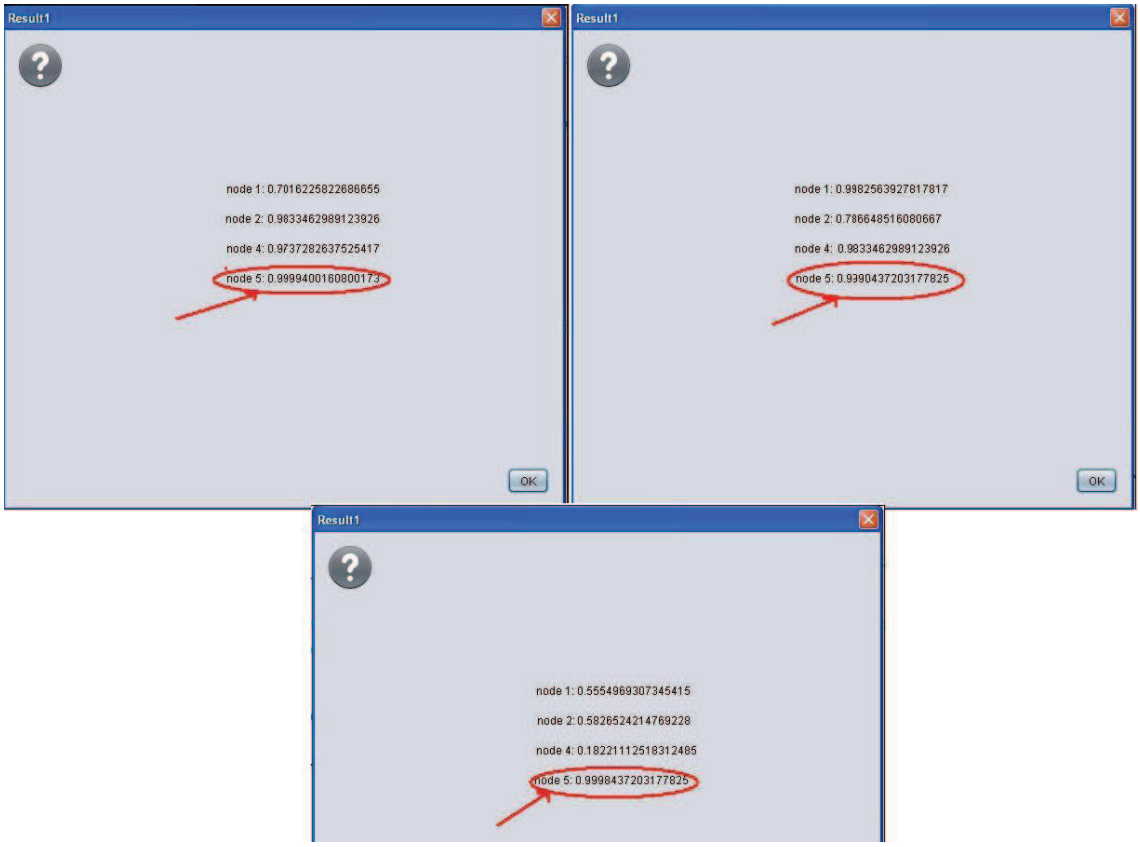

Figure 5.26: Checking of the candidate node's trust value assigned by each individual member node in 'Network 1'

5.8 Conclusion

In CRNs, some non-compliant cognitive radio users may create interference and break down the normal network activity by unauthorized access to the network resources. Such malicious users can seriously damage the whole network performance, possibly resulting in the collapse of the CRN. Hence,

the issue of secure communication in CRNs becomes more important than for other conventional wireless networks. Therefore, in this chapter, a trust-based framework is proposed for calculating trust between CR nodes that authenticates the candidate node's request to the CRN to make sure that the request is coming from a valid, trustworthy node in the network to ensure that the security of the network will not be compromised as a result of that candidate node's request authentication to access the network resources. The CA is proposed in the framework for managing and maintaining a trust repository in the proposed framework to solve the biasing problem in CRNs.

Chapter 6

Mechanisms for Secure Spectrum sharing in CRNs

6.1 Introduction

As discussed in Chapter 5, whenever a secondary user (SU) wants to use a primary user's (PU's) free spectrum, it sends a request to the secondary user base station (SUBS). The SUBS authenticates the SU's request, based on its trust value by using the approach mentioned in Chapter 5 and sends it to the PUBS, which also authenticates it. After passing the authentication process, the next step is for the primary base station (PUBS) to calculate the trustworthiness of the requesting SU and make a decision to assign the spectrum to the SU. As mentioned in Chapter 3, it is important for the PUBS to make this decision based on trust apart from authenticating its request, because authentication at best checks whether the request is coming from a valid node in the network or not; but this does not confirm the past behaviours or the adherence of the SU node to the cognitive radio network (CRN) policies,

such as vacating the spectrum when the PU needs it, releasing the spectrum whenever it does not need it, giving actual spectrum sensing results to the other users when asked etc. This is done based on the level of the SU in adhering to these tasks and thus, this should be the main criteria for the PUBS on which it can make a decision. In order to assist the PUBS in ascertaining the level of trust to allow an SU to access the spectrum, in this chapter, a Conjoint Trust Assessment approach for Secure Spectrum Sharing (CTAS^3) is proposed. The proposed approach allows only the trustworthy authenticated SUs who will behave properly according to CRN policies during spectrum sharing to use the PU's spectrum.

Once the spectrum is assigned to the requesting SU, according to the working principles of CRN, it can use the spectrum for its communication with other nodes in the network but must vacate it as soon as the PU needs it back. In such scenarios, it is possible that an SU's service is disrupted until it is able to search and access another free spectrum from the PU. To minimize such disruption in its service, a Service Continuity Enhancement (SCE) approach is presented in this chapter. The SCE approach is a multi-state working approach of an SU that ensures it experiences minimum service disruption when it needs to vacate the spectrum for the PU during spectrum sharing in CRNs.

During the process when the SU has to vacate the PU's spectrum, there may also arise a worst case scenario in which SUs cannot find other users free spectrum due to an imbalance in the number of SUs and PUs in the network. Therefore, SUs are blocked and are not be able to continue their communication due to the unavailability of PU's free spectrum. To solve this problem, in this chapter, an approach is proposed to balance the number of

PUs and SUs in the CRN (B-CRN), so that SUs can gain access to use any other PU's spectrum in the CRN to continue their communication when they have to vacate a PU's spectrum.

The approaches proposed in this chapter for secure spectrum sharing in CRNs are as follows:

- Approach 1: A stochastic model that defines the different states through which an SU needs to go during spectrum sharing to minimize the disruption to its service in the event of vacating a PU's spectrum which it was using.
- Approach 2: A conjoint trust assessment approach that assists the PUBS for secure spectrum sharing, based on SU's trust value calculated from both primary and secondary networks in CRNs. This will solve the security threats brought about by untrustworthy, selfish, and malicious SUs.
- Approach 3: Balancing the number of PUs and SUs in the CRN so that SUs can continue to engage in smooth communication without having their service interrupted or blocked in the event of vacating a spectrum to the PU when it needs it.

The rest of this chapter is organized as follows: In Section 6.2, the stochastic model that shows the different working states through which an SU needs to go to minimize its service disruption during spectrum sharing in the CRN is presented. Section 6.3 describes the secure spectrum sharing scheme, based on the conjoint level of trust so that no untrustworthy user can have access to the spectrum. Section 6.4 proposes the algorithms for balancing the number of SUs

according to the number of PUs and the sub-bands available in them in the CRN to minimize the disruption in the SU's service during spectrum sharing. Section 6.5 shows the numerical results by verifying the three approaches proposed in this chapter. Finally, Section 6.6 concludes the chapter.

6.2 Service Continuity Enhancement (SCE) Approach for Authenticated SUs During Spectrum Sharing

In this section, the SCE model with a state transition diagram is proposed that shows the different states through which an SU should go while accessing and vacating the spectrum when needed. By following this model, each SU can reduce the disruption in its service by further searching and accessing the spectrum while it needs to vacate the spectrum to the returning PU. The different states in the proposed model are explained in the next subsection.

6.2.1 Defining different working states to enhance an SU's service continuity

The five different states through which an SU needs to go to enhance its service continuity during spectrum sharing are as follows:

Search state (S)***:*** The search state is the state in which an SU searches for the free spectrum.

Access state (A)***:*** The access state is the state in which the spectrum is assigned to the authenticated SUs. This is done after its trust value is assessed by the PUBS through the conjoint trust assessment approach. The

detailed working of conjoint trust assessment approach for spectrum sharing is described in Section 6.3.

Interrupt state (I)***:*** The interrupt state is the state in which an SU detects a PU's reappearance and needs to vacate the spectrum for the PU.

Vacate state (V)***:*** The vacate state is the state when an SU vacates the spectrum on the PU's reappearance.

Dropped state (D)***:*** The dropped state is the state where no spectrum band is available for the SU to continue the communication.

The transition and working process between these states is as follows: at first, the SU searches for the free spectrum through the *Search (S)* state. Whenever it finds a free spectrum, it accesses it through the *Access (A)* state and establishes connections with others for its communication. On the PU's appearance back to the network, the SU's communication is interrupted. When this occurs, the SU goes to the *Interrupt (I)* state and then to the *Vacate (V)* state where it vacates the channel for the PU according to the CRNs policies. After vacating the channel, the SU will go to the *Search (S)* state and tries to search for that PU's other free spectrum or any other free spectrum from other PUs. If it is successful, then it will go to the *Access* state. On the other hand, if it is unsuccessful, then its communication will be dropped and it enters the *Dropped (D)* state. The flow of control between the different working states for an SU during spectrum sharing is shown in Figure 6.1.

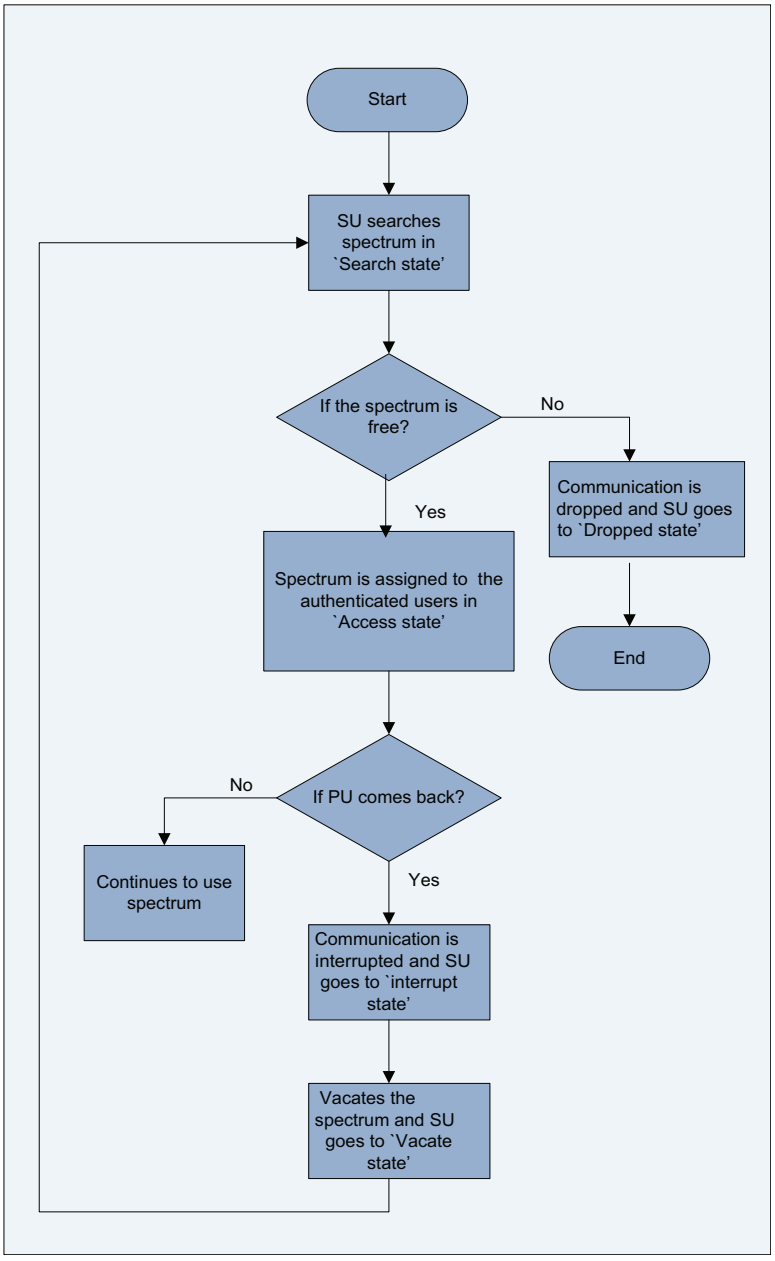

Figure 6.1: Transition between different working states of an SU during spectrum sharing

The main aim of defining these states and making sure that the SU goes through them is to ensure minimum disruption to its service when it has to vacate a spectrum to the PU and search for another spectrum. According to

this model, the SU may not be able to continue with its service when it is in *Search*, *Vacate* and *Dropped* states due to spectrum unavailability. By using this model to reduce disruption in the SU's service, the probability of an SU being in each state can be determined and the different transition rates that need to be across the defined states to minimize such level of disruption to its service can be ascertained.

To determine the probability of an SU being in each state, in the proposed transition diagram model, it is considered that an SU goes from one state to another in the event of a transition. This transition shows the rate by which the SU switches from one state to another during spectrum sharing which will result in it having minimum service disruption. In the next sub-section, the transition rates from one state to another are defined to calculate the probability of an SU being in each working state in order to measure the disruption in its service during spectrum sharing.

6.2.2 Defining the transition rates and probabilities of an SU being in different states during spectrum sharing

Transition rates are used to describe how quickly the transition happens from one state to another in the state transition diagram of the proposed model during spectrum sharing. The notation of transition rates used for this approach is as follows:

Spectrum access rate: λ_A;

Interruption rate: λ_I ;

Vacate rate: λ_V;

Repair rate of Vacate state: μ_V;

Dropping rate : λ_D;

Recovery rate of Dropped state: μ_D.

The Search state may change to the Access state with rate λ_A. In the Access state, the SU establishes normal communication through the PU's free spectrum band. If the SU is interrupted by the PU, the state can change to the Interrupt state (I) with rate λ_I. After interruption, the SU will go to the Vacate state (V) with λ_V. After vacating the spectrum, the SU will go to the Search state (S) with rate μ_V again and keeps on searching for the free spectrum. If no PU's free spectrum is available to access, then the SU will go to the Dropped state (D) with a rate λ_D . The SU will keep trying to search for free spectrum, so it goes to the Search state (S) again from the Dropped state (D) with a rate μ_D. The state transition diagram with different transition rates is depicted in Figure 6.2.

To calculate the probability of an SU being in each working state during spectrum sharing, the transition rate from one state to the next state is used. The probability of each state is assumed as follows:

Probability of Search State : π_S;

Probability of Active State : π_A ;

Probability of Interrupt State : π_I;

Probability of Vacate State : π_V;

Probability of Dropped State : π_D.

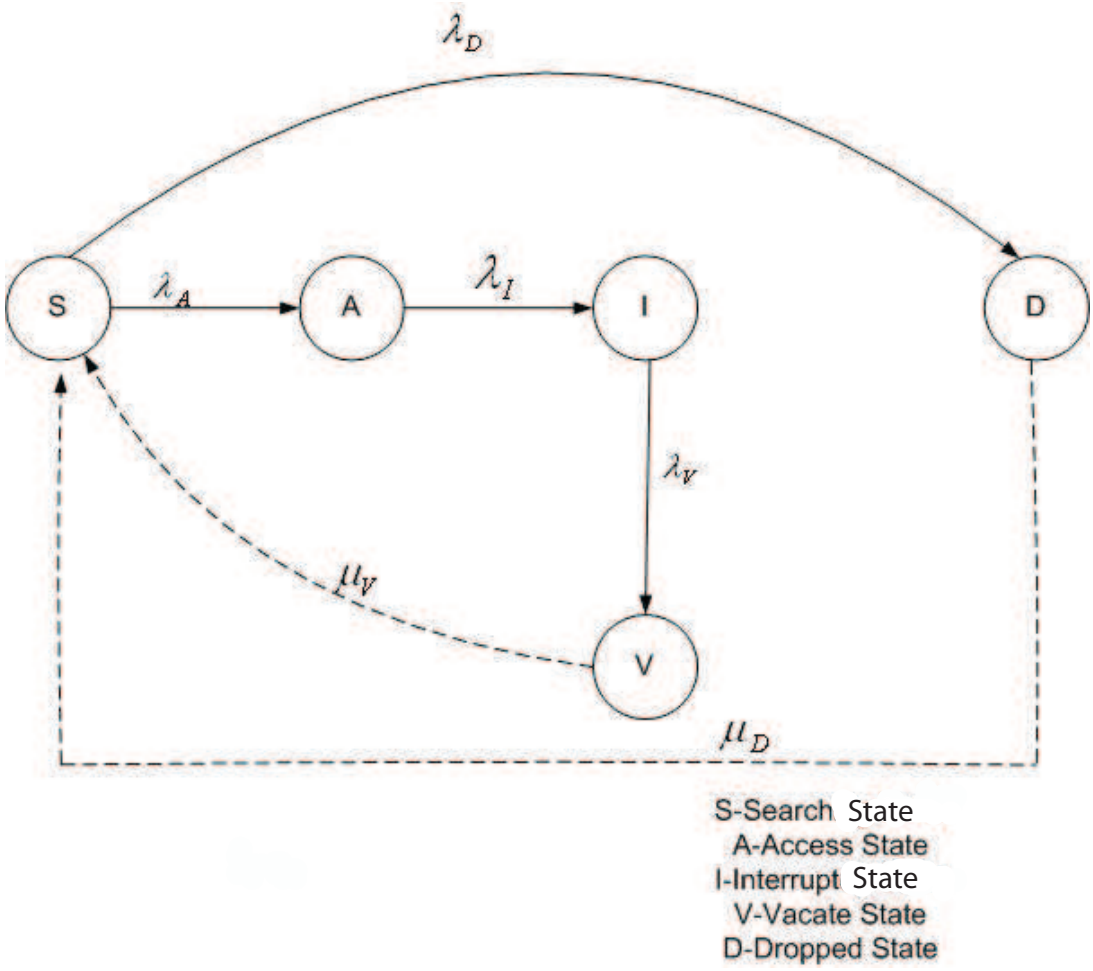

Figure 6.2: Stochastic model for an SU's activity.

Next the probability of an SU being in each working state at a point of time is calculated. According to the Markov Chain mode in every state, the incoming rate is equal to the outgoing rate [128]. Using this principle, the steady state balance equation for each state during spectrum sharing is used

in order to compute the probability of the SU being in each state as follows:

$$S : \pi_S \lambda_A + \pi_S \lambda_D = \pi_V \mu_V + \pi_D \mu_D \tag{6.1}$$

$$A : \pi_S \lambda_A = \pi_A \lambda_I \tag{6.2}$$

$$I : \pi_A \lambda_I = \pi_I \lambda_V \tag{6.3}$$

$$V : \pi_I \lambda_V = \pi_V \mu_V \tag{6.4}$$

$$D : \pi_S \lambda_D = \pi_D \mu_D \tag{6.5}$$

According to probability theory, the summation of all probabilities is equal to 1. So

$$\pi_S + \pi_A + \pi_I + \pi_V + \pi_D = 1 \tag{6.6}$$

By solving the steady-state balance equations in 6.1-6.6, the following expressions for the steady-state probabilities of an SU being in each state are obtained.

$$\pi_A = \frac{\lambda_A}{\lambda_I} \pi_S \tag{6.7}$$

$$\pi_I = \frac{\lambda_A}{\lambda_V}\pi_S \tag{6.8}$$

$$\pi_V = \frac{\lambda_A}{\mu_V}\pi_S \tag{6.9}$$

$$\pi_D = \frac{\lambda_D}{\mu_D}\pi_S \tag{6.10}$$

$$\pi_S = (1 + \frac{\lambda_A}{\lambda_I} + \frac{\lambda_A}{\lambda_V} + \frac{\lambda_A}{\mu_V} + \frac{\lambda_D}{\mu_D})^{-1} \tag{6.11}$$

The continuity of a service refers to the continual functionality of the expected service requested from an SU. As mentioned earlier, the spectrum is not available for an SU's usage when it is in the *Vacate* and *Search* states and the continuity of its service is affected. Though in the *Search* state, the spectrum is not available to continue its functionality, it is not considered to measure the service continuity level as it is the non-functional and intermediate state to go the *Access* state. Also, the continuity in the SU's service is affected when the SU is not successful in accessing another free spectrum after searching, then it goes to the Dropped state and its service becomes non-functional in this state. So, the continuity of the SU's service during the spectrum sharing mechanism in CRN is defined as follows:

$$\begin{aligned} Service\ continuity &= 1 - Non - availability\ of\ service \\ &= 1 - (\pi_V + \pi_D) \end{aligned} \tag{6.12}$$

Substituting the value of π_V and π_V in equation 6.12, the service continuity of an SU is defined as:

$$Service\ continuity = 1 - (\frac{\lambda_A}{\mu_V} + \frac{\lambda_D}{\mu_D})\pi_S \tag{6.13}$$

Using equation 6.13, the service continuity level of an SU is evaluated depending on different transition rates across the different states. As discussed earlier, in the proposed approach, the service continuity of an SU is improved by further searching and accessing the spectrum while it needs to give back the spectrum to the PU. In the verification part in Section 6.5, it is shown how the continuity of the SU's service is improved by choosing different transition rates across the different states during spectrum sharing. Having such a framework improves the service of an SU while spectrum sharing over the normal working principles of CRN.

In the next section, the CTAS^3 framework is described in detail to allow SUs to use PU's free spectrum based on its trust value so that no untrustworthy users can have access to the free spectrum. As pointed out in Section 6.1, this process is done by the PUBS in the *Access* state.

6.3 Conjoint Trust Assessment for Secure Spectrum Sharing (CTAS^3) Framework in CRNs

The system architecture of the proposed CTAS^3 model is as same as described in Section 5.2.1 where there are two different networks, namely primary user network (PUN) and secondary user network (SUN). Each network consists of different member nodes and base stations, as shown in Figure 6.3.

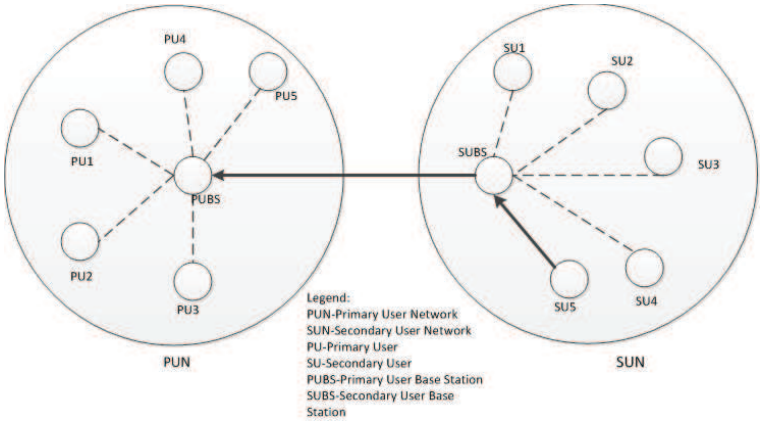

Figure 6.3: System architecture

Whenever an SU wants to gain access to a PU's free spectrum in CRNs, at first its request needs to be authenticated by both base stations, based on its trust value, which indicates the validity of the requesting node. The authentication process is described in detail in Chapter 5. After an SU's request has being authenticated by both networks, the next process is for both networks to calculate the requesting SU node's trust value. In this process, the SUBS calculates the trust value of the requesting SU and sends it to the PUBS. The PUBS also calculates the trust value from its network and then

conjoins the trust value from both networks to calculate the requesting SU's final trust value to check its trustworthiness in order to make a decision as to whether the SU can have access to the spectrum. As there are two networks in CRNs and the requesting SU which is a member of secondary network, makes a request to use the free spectrum from the primary network, it is important to assess the requesting node's trust value from both networks for the following reasons:

1. Trust is assessed from the secondary network to obtain an overall recommendation about the node and to have an idea about this node's behaviour in its own network.

2. Trust is assessed from the primary network to obtain the recommendations from all the primary member nodes and to have an idea about past interactions with the node.

3. After the level of trust from both the networks has been assessed, it is conjoined to determine the overall recommendation about the requesting node. As mentioned earlier, this level of trust is important for the PUBS to ensure that the requesting SU is trustworthy enough to use its free spectrum band and vacate the spectrum when the PU needs it and will not hold the spectrum for a long time in order to break the network's performance.

6.3.1 Working of the proposed CTAS^3 framework

In this section, the working of the proposed framework for secure spectrum sharing in CRNs which solves the security threats brought about by

untrustworthy entities is presented. Figure 6.4 presents a flowchart diagram of the working of the proposed CTAS^{3}framework.

The sequence of the working steps in the proposed CTAS^3 framework are as follows:

- Trust calculation by the secondary network: Whenever an SU wants to use a PU's free spectrum, its request needs to be authenticated by both networks (SUN and PUN) to confirm its validity in the network. This is done by using the proposed approach in Chapter 5. If the level of trust is above the defined threshold, the SUBS sends a request to all of its member nodes to give a recommendation for the requesting node. All member nodes give feedback to the base station which then calculates the average trust value for the requesting user and forwards the requesting node's trust value to the PUBS.

- Trust calculation and aggregation in a primary network: The PUBS receives the requesting node's trust value from the SUBS. The PUBS also sends a request to all its member nodes to give a recommendation for the requesting node. All member nodes send the recommendations to the PUBS. The PUBS then calculates the average trust value of the requesting node received from its member nodes and then aggregates it with the trust value received from the SUBS to calculate the requesting node's final trust value. If needed, a weighting value is used to justify the importance of the trust value from each network

- Trust value checking in the primary network: The PUBS now compares the aggregated final trust value of the requesting node with the system's predefined threshold value. If the aggregated value is higher than the

threshold, then the requesting is permitted to use the PU's free spectrum, otherwise its request is rejected.

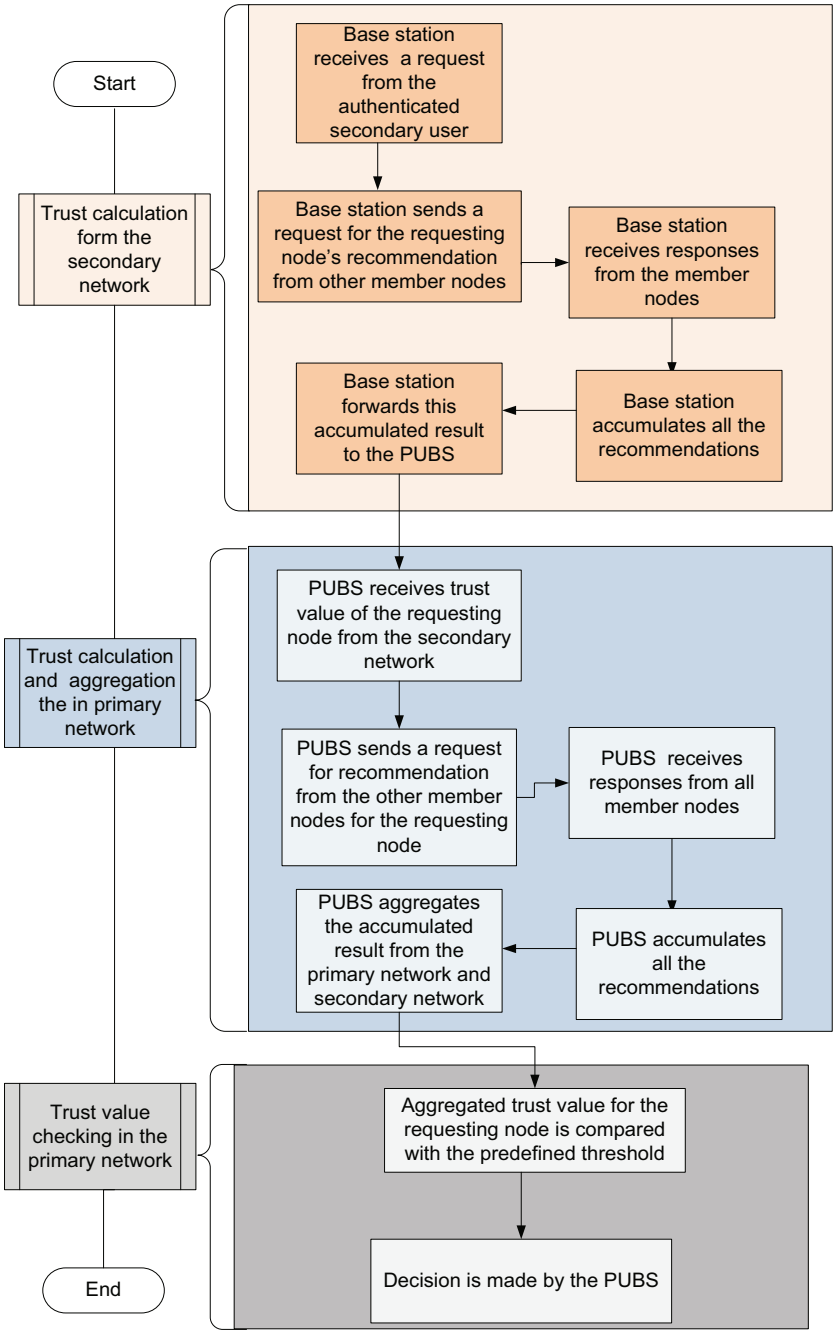

Figure 6.4: Flowchart illustrating the steps performed by the CTAS^3 framework

The flowchart of the proposed model between the four different entities (SU, SUBS, PU, PUBS) is depicted in Figure 6.5.

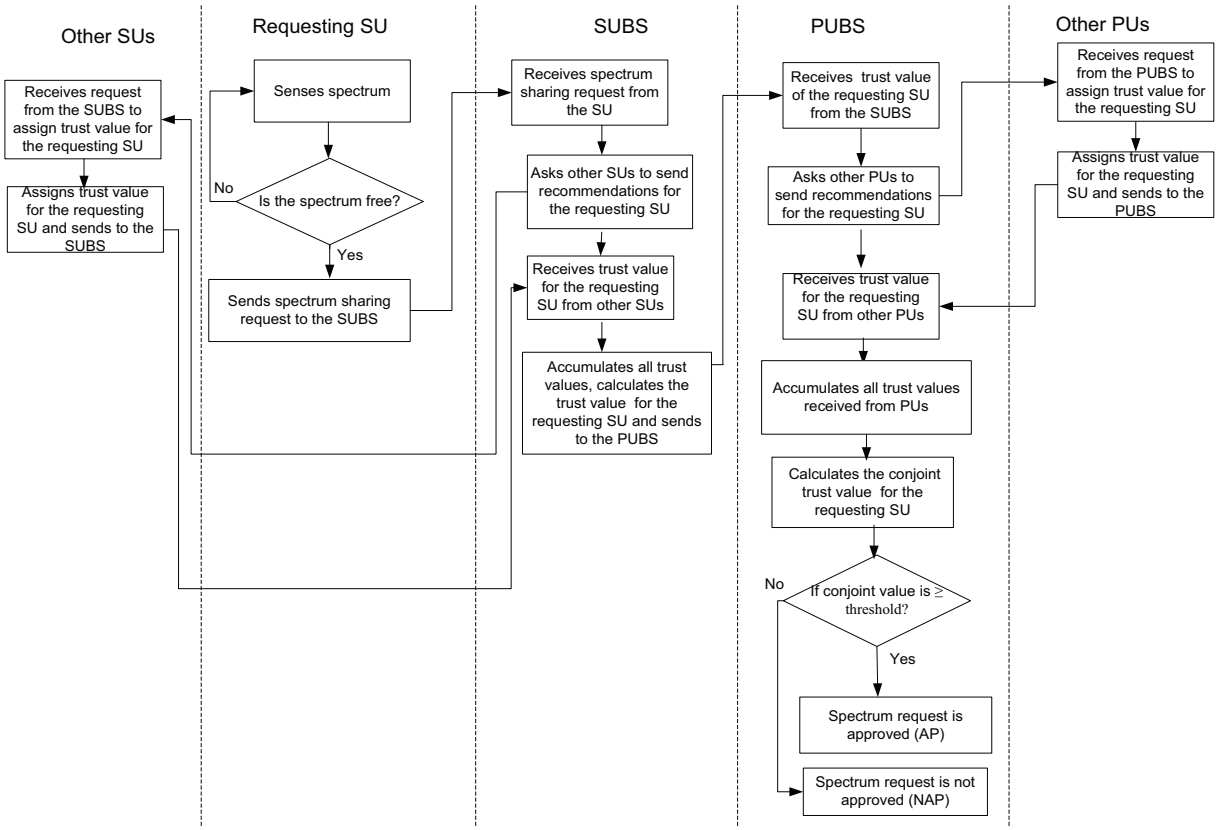

Figure 6.5: Flow of controls between different nodes in the CTAS^3 framework

In the next section, the working of each phase defined in the proposed framework is discussed in detail.

6.3.2 Trust calculation of the requesting node from the secondary network

The working steps of this phase as shown in Figure 6.4 are as follows:

1. After a requesting SU's request has been authenticated by both networks, the SUBS asks all member nodes to send it the trust value for the

requesting SU.

2. Each member node checks its cooperation record table with the requesting node. This cooperation record table is different from the table discussed in Chapter 5 although both record tables show the outcome by success and failure. The record table for this purpose stores the different past behaviours related to spectrum sharing such as vacating the spectrum on the PU's arrival, release the spectrum when it does not need it etc. Each member node calculates the trust value of the requesting node for the different services using equation 6.14 and sends it to the SUBS.

$$T_{s_i} = \frac{\sum_{j=1}^{T}(T_{value}(SU_{requesting\ node}, S_j, t, n_j))}{T} \tag{6.14}$$

where T_{s_i} denotes the trust value of the requesting secondary node from ith member node in the secondary network,
$T_{value}(SU_{requesting\ node}, S_j, t, n_j)$ denotes the trust value of the secondary requesting node ($SU_{requestingnode}$) of service j at t time period having n interactions for the service and
T is total number of services that the recommender node has with the requesting node.

For example, if a member node $SU2$ in Figure 6.3 has a cooperation record for the requesting node ($SU1$) as shown in Table 6.1, then its trust value is calculated as follows:

Service 1				Service 2				Service 3			
Time	Interactions	Outcome	Value	Time	Interactions	Outcome	Value	Time	Interactions	Outcome	Value
T1	1	Success	1	T2	1	Success	1	T3	1	Failure	0
	2	Success	1		2	Success	1		2	Failure	1
	3	Failure	0		3	Success	1		3	Failure	0
	4	Success	1		4	Failure	0		4	Success	1
	5	Failure	0		5	Success	1		5	Success	1

Table 6.1: Cooperation record table of node 2 with requesting node

From the Table 6.1, it shows that $SU1$ has 3 services and 5 interactions for each service with node $SU2$. Here, $SU1$ is the requesting node ($SU_{requesting\ node}$).

Therefore, the trust value of $SU_{requesting\ node}$ from node $SU2$ for service 1 at time period $T1$ for 5 interactions is :

$$T_{value}(SU_{requesting\ node}, 1, T1, 5)) = \frac{number\ of\ success}{number\ of\ success\ +\ number\ of\ failure} = \frac{3}{5} = 0.6 \tag{6.15}$$

The trust value of $SU_{requesting\ node}$ from node $SU2$ for service 2 at time period $T2$ for 5 interactions is :

$$T_{value}(SU_{requesting\ node}, 1, T2, 5)) = \frac{number\ of\ success}{number\ of\ success\ +\ number\ of\ failure} = \frac{4}{5} = 0.8 \tag{6.16}$$

The trust value of $SU_{requesting\ node}$ from node $SU2$ for service 3 at time period $T3$ for 5 interactions is :

$$T_{value}(SU_{requesting\ node}, 1, T3, 5)) = \frac{number\ of\ success}{number\ of\ success\ +\ number\ of\ failure} = \frac{3}{5} = 0.6 \tag{6.17}$$

Therefore, the trust value of $SU1$ from node $SU2$ by using equation 6.14

is :

$$T_{1_2} = \frac{0.6 + 0.8 + 0.6}{3} = 0.66 \tag{6.18}$$

Following the same process, it is assumed that the trust value of $SU_{requesting\ node}(SU1)$ from node $SU3$ for service 1, 2 and 3 is 0.4, 0.6, and 0.4, respectively. Therefore, the trust value of node $SU1$ from node $SU3$ using equation 6.14 is as follows:

$$T_{1_3} = \frac{0.4 + 0.6 + 0.4}{3} = 0.46 \tag{6.19}$$

3. SUBS receives trust values from each member node and calculates the average trust value of the requesting node using equation 6.20.

$$T_S = \frac{\sum_{i=1}^{N} T_{s_i}}{N} \tag{6.20}$$

where T_S is the trust average value of the requesting node and
N is the total number of member nodes.

Therefore, by using equation 6.20, the average trust value of node $SU_{requesting\ node}(SU1)$ from the secondary network computed by the SUBS, based on the trust values received from node $SU2$ and node $SU3$ in Figure 6.3 is as follows:

$$T_S = \frac{0.66 + 0.46}{2} = 0.56 \tag{6.21}$$

4. The SUBS forwards this average trust value of the requesting node (T_S)

to the PUBS.

6.3.3 Trust calculation of the requesting node from the primary network

The working steps of this phase are as follows:

1. The PUBS receives the average trust value of the requesting node from the SUBS as described in section 6.3.2 and asks all member nodes to send it the trust value for the requesting SU.

2. Each member node in the primary network searches its cooperation record table and calculates the trust value of the requesting node using equation 6.22 and sends it to the PUBS.

$$T_{p_i} = \frac{\sum_{j=1}^{T} (T_{value}(SU_{requesting\ node}, S_j, t, n_j))}{T} \tag{6.22}$$

   where T_{p_i} denotes the trust value of the requesting node from ith member node in the primary network

   $T_{value}(SU_{requesting\ node}, S_j, t, n_j))$ denotes the trust value of the requesting node ($SU_{requesting\ node}$) of service j at t time period having n interactions for the service and

   T is the total number of services.

3. PUBS receives trust values from each member node and calculates the

average trust value of the requesting node using equation 6.23.

$$T_P = \frac{\sum_{i=1}^{N} T_{p_i}}{N} \tag{6.23}$$

where T_P is the average trust value of the requesting node and
N is the total number of member nodes.

Following the examples in Section 6.3.2 and using equations 6.22 and 6.23, the PUBS calculates the average trust value of the requesting node T_P in the primary network as 0.65.

4. The PUBS accumulates the received T_S and T_P from the secondary network and primary network, respectively and aggregates them to obtain the final recommended conjoint trust value (T_R) for the requesting SU, using equation 6.24. Therefore, the recommended final conjoint trust value of the requesting node is:

$$T_R = \alpha T_S + \beta T_P \tag{6.24}$$

where α and β is the weight used for the secondary network and the primary network, respectively and $\alpha + \beta = 1$,
T_R is the recommended conjoint trust value of the requesting node,
T_S is the trust value of the requesting node from the secondary network and
T_P is the trust value of the requesting node from the primary network.

Continuing with the abovementioned example, the PUBS calculates the

conjoint recommended trust value of the requesting node ($SU1$) using equation 6.24 as follows:

$$T_R = 0.5 * 0.56 + 0.5 * 0.65 = 0.60 \tag{6.25}$$

6.3.4 Checking the trust value of the requesting node for spectrum access

The PUBS compares the computed T_R with a specific trust threshold T (0.7)and makes a decision D_p using equation 6.26. If the T_R is greater than T, the requesting SU's request is approved (AP) and is permitted to use the PU's free spectrum band, otherwise its request is not approved (NAP).

$$D_p = \begin{cases} AP & \text{if } T_R \geq T \\ NAP & \text{if } T_R < T \end{cases} \tag{6.26}$$

Continuing the example mentioned in Section 6.3.2 and 6.3.3, the PUBS calculates the conjoint average trust value of the requesting node ($SU1$) as 0.60 which is lower than the threshold value (0.7). So, the requesting SU's request is not approved in this scenario. In other words, in this scenario, the requesting node is not trustworthy enough to use the PU's free spectrum and the PUBS does not have enough confidence that this node will vacate the PU's spectrum when the PU needs it and will not display any untrustworthy behaviours in the network.

The algorithm 1 for the PUBS to calculate the recommended conjoint trust value from both networks and make a decision to give access to the requesting SU to use the PU's spectrum is as follows:

Algorithm 1 Conjoint Trust Calculation Algorithm

Input: number of SUs (N), number of PUs (M), trust value of the requesting secondary node ($T_{requesting\ node}$) and initially set to zero, the trust value of the requesting node from each secondary member node and primary member node ($T_{S_{member\ node}}$), ($T_{P_{member\ node}}$), respectively, total trust value of the requesting node in secondary network and primary network ($T_{S_{total}}$), ($T_{P_{total}}$), respectively and initially set to zero, number of services (l), the average trust value from the secondary network and primary network (T_S), (T_P), respectively, threshold value ($T_{threshold}$), requesting node (SU).

Output: Spectrum sharing request approved(AP) or not approved (NAP)

The SUBS sends a request for the recommendation of the SU to the other SUs in the CRNs and the PUBS sends the request for the recommendation of the SU to the other PUs in the CRNs with which the requesting SU has previously interacted.

The SUBS will receive $T_{value(s)}$ for every node in the secondary network.

for $i \leftarrow 0$ to $i \leq N$ **do**

    for $j \leftarrow 0$ to $j \leq l$ **do**

        $T_{requesting\ node} = T_{requesting\ node}(SU, S_j, t, n_j) + T_{requesting\ node}$

    end for

    $T_{S_{member\ node}} = \frac{T_{requesting\ node}}{l}$

    $T_{S_{total}} = T_{S_{total}} + T_{S_{member\ node}}$

end for

The SUBS will calculate the total trust value received from all the SUs

$T_S = \frac{T_{S_{total}}}{N}$;

The PUBS will receive $T_{requesting\ node}$ from every member node in the primary network.

for $i \leftarrow 0$ to $i \leq M$ **do**

    for $j \leftarrow 0$ to $j \leq l$ **do**

        $T_{requesting\ node} = T_{requesting\ node}(SU, S_j, t, n_j) + T_{requesting\ node}$

    end for

    $T_{P_{member\ node}} = \frac{T_{requesting\ node}}{l}$

    $T_{P_{total}} = T_{P_{total}} + T_{P_{member\ node}}$

end for

The PUBS will calculate the total trust value received from all the PUs

$T_P = \frac{T_{P_{total}}}{M}$;

The PUBS will calculate the recommended conjoint trust value (T_R):

$T_R = T_P + T_S/2$;

The PUBS will compare $T_{conjoint}$ with $T_{threshold}$

if $T_R \geq T_{threshold}$ **then**

    The requesting SU's spectrum request will be approved(AP);

else

    The requesting SU's spectrum request will not be approved(NAP);

end if

By using the proposed approach, the requested authenticated trustworthy SU can have access to the PU's free spectrum. But a problem arises in situations where there are many SUs in the CRN in comparison to PUs. In such scenarios, some SUs, even though trustworthy, may not have any chance to use the PU's free spectrum due to the unavailability of the spectrum. Therefore, in the next section, the B-CRN framework is proposed which aims to balance the number of PUs and SUs for efficient spectrum sharing in the CRN.

6.4 B-CRN Framework for Multiple Users for Efficient Spectrum Sharing in CRNs

As described in Section 6.2, an SU should vacate the spectrum by detecting the reappearance of the PUs and searches for other free spectrum to maintain smooth communication. To increase the chance of gaining access to another free spectrum, one of the main factors is to ensure that there is a balance in the number of PUs and SUs in CRNs, so that an SU can search and use another free spectrum band instead of going to the Dropped state during spectrum usage due to absence of available spectrum. In this section, a relation between the number of PUs and SUs in a CRN for multiple PUs and SUs is proposed during the basic spectrum sharing scheme so that network statistics, such as the utilization ratio, blocking rate, deprivation rate etc. are at a standard level in order to maintain smooth communication in CRNs.

6.4.1 B-CRN system model and architecture

In the proposed B-CRN model, there are n number of PUs in the network such as PU1 , PU2, PU3.....PU_n. Each PU has its licensed spectrum. Therefore, PU1 has licensed frequency bands of f_1, PU2 has licensed bands of f_2, ...and PU_n has licensed band of f_n. Each band is divided into N sub-bands, as shown in Figure 6.6 by means of Orthogonal Frequency Division Multiplexing technology. Therefore, in the proposed model, there are $n \times N = nN$ sub-bands available to use for the SUs in parallel when the spectrum is not used by the PUs. Therefore, nN SUs can use these sub-bands in parallel. If more than nN SUs are allowed into the network, some SU's communication will be always blocked or dropped when all the sub-bands are occupied by either SUs or PUs. By using these statistics, in the next subsection, a relation in the number of the PUs and allowed SUs in CRN is proposed, for efficient spectrum sharing between them.

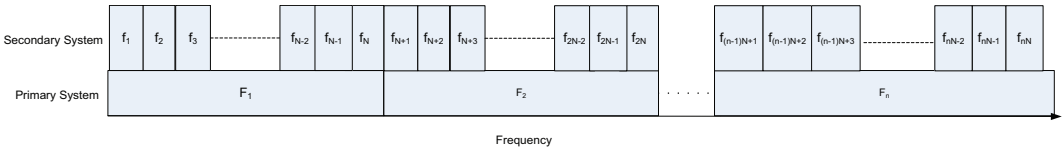

Figure 6.6: Frequency band sharing in CRNs

6.4.2 Balancing the number of PUs and PUs in CRNs

By using the network values mentioned in the earlier subsection, the number of SUs, PUs and the sub-bands in them is as follows:

$$S = n \times N \Longrightarrow \frac{S}{n} = N \tag{6.27}$$

From equation 6.27, it can be seen that if either the number of PUs or

number of sub-bands in each licensed band increases, the number of SUs increases to use the free spectrum. Therefore, the established relation between PUs and SUs is as follows:

$$S \propto n \tag{6.28}$$

and

$$S \propto N \tag{6.29}$$

6.4.2.1 For a fixed sub-band network

The relation between the number of SUs and PUs where each PU's spectrum band is divided into a fixed number of sub-bands is expressed using equation 6.30.

$$S \propto n \Longrightarrow S = K.n \Longrightarrow \frac{S}{n} = K \tag{6.30}$$

where K is a positive constant and represents the number of sub-bands in each licensed band.

If $\frac{S}{n} \leq K$; therefore, the network is in a balanced mode. This means, all SUs can have access to the PU's spectrum and continue their communication while no PU is using it. Even when a PU comes back and needs its own spectrum, they are successful in finding a band from another PU.

On the other hand, if $\frac{S}{n} > K$; the network is not in a balanced mode, as not all of the SUs can not gain access to the PU's free spectrum. Some SUs will be always deprived of accessing the free spectrum as the number of available sub-bands is lower than the number of SUs.

Therefore, for a fixed sub-band network, the number of SUs depends on

the number of PUs. If the number of PUs is increased, more SUs are allowed to use the PU's spectrum, based on the ratio in equation 6.30. Therefore, for a fixed band PU, the network status is shown by

$$Network\ status = \begin{cases} Balanced & \text{if } \frac{S}{n} \leq K \\ Imbalanced & \text{if } \frac{S}{n} > K \end{cases} \tag{6.31}$$

6.4.2.2 For a fixed number of PUs in a network

The relation between the number of SUs and the sub-bands where each network has a fixed number of PUs is expressed using equation 6.32.

$$S \propto N \Longrightarrow S = K.N \Longrightarrow \frac{S}{N} = K \tag{6.32}$$

where K is a positive constant and represents the number of PUs in the network.

If $\frac{S}{N} \leq K$; therefore, the network is a balanced one. This means all the SUs can have access to the PU's spectrum and can continue with their communication while no PU is using it.

On the other hand, if $\frac{S}{N} > K$; the network is not a balanced one, as not all of the SUs can gain access to the PU's free spectrum. Therefore, the number of SUs in a fixed PU network depends on the number of sub-bands in which each band is divided. If the number of sub-bands is increased, the number of SUs can also be increased in a balanced network. Therefore, for a fixed number of

PUs, the network status is shown by

$$Network\ status = \begin{cases} Balanced & \frac{S}{N} \leq K \\ Imbalanced & \text{if } \frac{S}{N} > K \end{cases} \tag{6.33}$$

Therefore, the network balance depends on either the number of sub-bands or the number of PUs. For example, if each PU's licensed spectrum is fixed into 2 sub-bands, then the ratio of the number of SUs and PUs for a balanced network must be always 2. If the number of PUs is fixed to 2 in a network, then the ratio of the number of SUs and the number of sub-bands for a balanced network must be always 2.

The formed relationships between PUs, SUs and sub-bands in CRNs enables the determination of the ideal maximum number of SUs that could be in the CRN to ensure there is less call dropping and blocking for SUs. Therefore, any CRN should follow the above relationship between PUs and SUs to improve the network performance during spectrum sharing. In the literature, a basic spectrum sharing scheme is proposed considering only one and two PUs [76, 77] and multiple SUs in both cases. However, it is possible that there are more than two PUs in the CRNs. For such scenarios, in the next subsection, a basic spectrum sharing mechanism is demonstrated between multiple PUs and SUs to improve network performance. The proposed approach for spectrum sharing follows the following steps:

1. Determine the different states of the spectrum sharing mechanism

2. Determine the transition rates between the different states

3. Determine the probability of the model being in each state during

spectrum sharing

6.4.3 Efficient spectrum sharing in the presence of multiple PUs and SUs in CRNs

In this section, a basic spectrum sharing mechanism is described for multiple PUs and SUs. The proposed spectrum sharing mechanism is extended with n number of PUs and nN number of SUs. For this multi-user model, the network parameters such as utilization ratio, blocking rate etc. are derived to determine their effect on this model during spectrum sharing. Figure 6.7 shows the state transition diagram during spectrum sharing between multiple PUs and SUs.

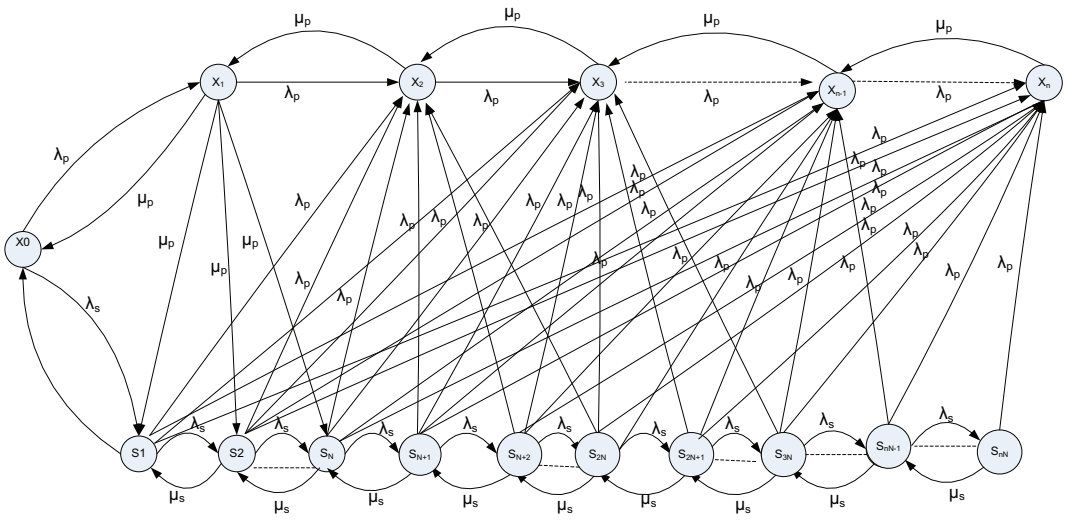

Figure 6.7: State transition diagram of spectrum sharing for multiple users in CRNs

To describe the basic spectrum sharing for multiple PUs and SUs model, Continuous Time Markov Chain (CTMC) is used. The random variables used to represent the inter-arrival times and services in the proposed model are

easily represented by using the negative-exponential distribution of memory less property of CTMC. In the next subsection, different states are defined to describe the model.

6.4.3.1 Defining states during spectrum sharing for multiple SUs and PUs

To describe the model using CTMC, the following different states are assumed:

1. X_0 stands for the state when the spectrum is used by neither PU nor the SU.
2. X_1 is the state when one PU is exclusively uses one of n spectral bands.
3. X_2 is the state when two PUs use two spectrum bands.
4. X_3 is the state when three PUs use three spectrum bands.
5. X_n is the state n when PUs use all n spectrum bands.
6. S_j it the state when jth SU uses any of the spectrum band from the PUs. Here, $(j = 1, 2, 3, ...nN)$.
7. Z denotes the set of all states used in the model, i.e., $Z = X_0, X_1, X_2, X_3.....X_n, S_1, S_2, ...S_{nN}$.

The proposed approach uses the same statistics in [77] and [76] to evaluate different matrices for multiple PUs and SUs during spectrum sharing in a balanced CRN. In the next subsection, the different transition rates are defined to calculate the probability of the model being in each state.

6.4.3.2 Defining transition rates during spectrum sharing for multiple SUs and PUs

The following transition rates to calculate the probability of the model being in each state during spectrum sharing are as follows:

1. The arrival rate of the PU to access the spectrum is λ_p. This rate is used using the Poisson process. In other words, the inter accessing time is negative-exponentially distributed with mean time $\frac{1}{\lambda_p}$ (ms);

2. The time of the PU to occupy the spectrum is a random variable that uses a negative exponential distribution with mean $\frac{1}{\mu_p}$(ms);

3. The arrival rate of the SU to access the spectrum is λ_s. The inter-arrival time of SUs accessing the spectrum is a random variable that obeys a negative-exponentially distributed with mean time $\frac{1}{\lambda_s}$(ms);

4. The time of each SU using a radio band is a random variable obeying negative-exponential distribution with mean $\frac{1}{\mu_s}$ (ms).

Apart from these assumptions, it is considered that one SU is able to use any of the nN bands but is allowed to use only one band at each time. The time for an SU to vacate the spectrum band on the detection of reappearance of PU is ignored here as the time of SU's using a band remains negative-exponentially distributed having no impact whether the SUs are forced to stop by the PU or not.

From Figure 6.7, it is clearly predictable that no more than nN number of SUs can use the spectrum in the model as there are nN number of spectrum sub-bands available for SUs. According to [77], the basic queueing theory

is applied to CTMC to derive the balance equations using transition rates from the model by which the probability of the model being in each state is calculated. In the next subsection, the probability of the model being in each state is calculated using the different transition rates in order to derive the network statistics.

6.4.3.3 Probability of the model being in each state during spectrum sharing for multiple SUs and PUs

The probability of the model being in each state is assumed as follows:

1. Π_j represents the steady state probability of the state of SUs using the spectrum in a state S_i where $j = 1, 2, 3.....nN$.

2. Π_{X_i} represents the steady state probability of PUs using the spectrum in a state X_i where $i = 0, 1, 2, 3.....n$

The balance equations for every state are as follows:

For state X_n:

$$\Pi_{x_n}\mu_p = \Pi_{x_{n-1}}\lambda_p + \sum_{n=1}^{nN} \Pi_n\lambda_p \tag{6.34}$$

For state X_{n-1}:

$$\Pi_{x_{n-1}}\mu_p = \Pi_{x_{n-2}}\lambda_p + \Pi_{x_n}\mu_p + \sum_{n=1}^{nN-1} \Pi_n\lambda_p \tag{6.35}$$

For state X_{n-1}:

$$\Pi_{x_{n-2}}\mu_p = \Pi_{x_{n-3}}\lambda_p + \Pi_{x_{n-1}}\mu_p + \sum_{n=1}^{nN-2} \Pi_n\lambda_p \tag{6.36}$$

For state X_3:

$$\Pi_{x_3}\mu_p = \Pi_{x_2}\lambda_p + \sum_{n=1}^{nN} \Pi_n \lambda_p \tag{6.37}$$

For state X_2:

$$\Pi_{x_2}\mu_p = \Pi_{x_1}\lambda_p + \sum_{n=1}^{nN} \Pi_n \lambda_p \tag{6.38}$$

For state X_1:

$$\Pi_{x_1}(\lambda_p + (N+1)\mu_p) = \Pi_{x_0}\lambda_p + \Pi_{x_2}\mu_p \tag{6.39}$$

For state X_0:

$$\Pi_{x_0}(\lambda_p + \lambda_s) = \Pi_1\mu_s + \Pi_{x_1}\mu_p \tag{6.40}$$

For state S_1

$$\Pi_1(\mu_s + \lambda_s + \lambda_p) = \Pi_2\mu_s + \Pi_{x_0}\lambda_s + \Pi_{x_1}\mu_p \tag{6.41}$$

For state S_2

$$\Pi_2(\mu_s + \lambda_s + \lambda_p) = \Pi_3\mu_s + \Pi_1\lambda_s + \Pi_{x_1}\mu_p \tag{6.42}$$

Therefore, the probability of the multi-user model being in state S_j during spectrum sharing is expressed by the following equation for $j = 1$ to N.

$$\Pi_j(\mu_s + \lambda_s + \lambda_p) = \Pi_{j+1}\mu_s + \Pi_{j-1}\lambda_s + \Pi_{x_1}\mu_p \tag{6.43}$$

The probability of the multi-user model being in state S_j is expressed by the following equation for $j = N + 1$ to $nN - 1$.

$$\Pi_j(\mu_s + \lambda_s + \lambda_p) = \Pi_{j+1}\mu_s + \Pi_{j-1}\lambda_s \tag{6.44}$$

For state S_{nN}

$$\Pi_{nN}(\mu_s + \lambda_p) = \Pi_{nN-1}\lambda_s \tag{6.45}$$

It is known that the summation of all the probabilities in the model is equal to 1, according to the probability property. Therefore,

$$\sum_{j=1}^{nN} \Pi_j + \Pi_{x_0} + \sum_{i=1}^{n} \Pi_{x_i} = 1 \tag{6.46}$$

Combining equations 6.44 and 6.46, it is obtained $A\Pi = B$ where $\Pi = (\Pi_1, \Pi_2, \Pi_3 \ldots\ldots \Pi_{nN}, \Pi_{x_0}, \Pi_{x_1} \ldots\ldots \Pi_{x_{n-1}}, \Pi_{x_n},)^T$ and $B = (1, 0, 0, 0 \ldots\ldots)^T$ and A is a matrix as shown in equation 6.48. Thus, it is obtained from the model,

$$\Pi = A^{-1}B \tag{6.47}$$

Combining the probability of the model being in each state from the matrix, in the next subsection, the different criteria to evaluate the performance characteristics of the network are presented, consisting of multiple PUs and SUs during spectrum sharing.

$$A = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & \lambda_p & \lambda_p & \lambda_p & .... & \lambda_p & \lambda_p & .... & \lambda_p & \lambda_p & \lambda_p & 0 & 0 & 0 & .... & 0 & 0 & \lambda_p & -\mu_p \\
0 & \lambda_p & \lambda_p & \lambda_p & .... & \lambda_p & \lambda_p & .... & \lambda_p & \lambda_p & 0 & 0 & 0 & 0 & .... & 0 & \lambda_p & -\mu_p & \mu_p \\
0 & \lambda_p & \lambda_p & \lambda_p & .... & \lambda_p & \lambda_p & .... & \lambda_p & 0 & 0 & 0 & 0 & 0 & .... & \lambda_p & -\mu_p & \mu_p & 0 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
-(\lambda_p + \lambda_s) & \mu_s & 0 & 0 & .... & 0 & 0 & .... & 0 & 0 & 0 & \mu_s & 0 & 0 & .... & 0 & 0 & 0 & 0 \\
\lambda_s & -(\lambda_p + \lambda_s + \mu_s) & \mu_s & 0 & .... & 0 & 0 & .... & 0 & 0 & 0 & \mu_p & 0 & 0 & .... & 0 & 0 & 0 & 0 \\
0 & \lambda_s & -(\lambda_p + \lambda_s + \mu_s) & \mu_s & .... & 0 & 0 & .... & 0 & 0 & 0 & \mu_p & 0 & 0 & .... & 0 & 0 & 0 & 0 \\
0 & 0 & \lambda_s & -(\lambda_p + \lambda_s + \mu_s) & .... & 0 & 0 & .... & 0 & 0 & 0 & \mu_p & 0 & 0 & .... & 0 & 0 & 0 & 0 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
0 & 0 & 0 & 0 & .... & \lambda_s & -(\lambda_p + \lambda_s + \mu_s) & ..... & 0 & 0 & 0 & \mu_p & 0 & 0 & .... & 0 & 0 & 0 & 0 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
0 & 0 & 0 & 0 & .... & 0 & 0 & .... & \lambda_s & -(\lambda_p + \lambda_s + \mu_s) & \mu_s & 0 & 0 & 0 & .... & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & .... & 0 & 0 & .... & 0 & \lambda_s & -(\lambda_p + \mu_s) & 0 & 0 & 0 & .... & 0 & 0 & 0 & 0
\end{pmatrix} \tag{6.48}$$

6.4.4 Criteria to evaluate system performance for a balanced multi-user network during spectrum sharing

6.4.4.1 The mean number of SUs

The mean number of SUs refers to the available spectrum bands which are used by the SUs to continue their service. For a balanced CRN, the mean number of SUs should be lower or equal to the total sub-bands available in the network. Therefore, the mean number of radio bands used by the SUs, i.e the mean number of SUs accessing the spectrum, is expressed by the following equation.

$$Mean\ number\ of\ SUs = \sum_{j=1}^{nN} j\Pi_j \tag{6.49}$$

6.4.4.2 Deprivation rate

For a balanced network, the deprivation rate is the rate at which an SU is forced to vacate the band on the reappearance of the PU. Therefore, the deprivation rate is related to the arrival rate of the PU (λ_p) to access the spectrum. The deprivation rate of an SU for a system of one PU whose licensed band is divided into N sub-bands is as follows.

$$Deprivation\ rate = \lambda_p \sum_{j=1}^{N} j\Pi_j \tag{6.50}$$

Therefore, the total deprivation rate of an SU for the proposed model of n

PUs whose licensed band is divided into N sub-bands is as follows.

$$Deprivation\ rate = \lambda_p \sum_{j=1}^{nN} j\Pi_j \tag{6.51}$$

6.4.4.3 Blocking rate

When all the bands are occupied by either PUs or SUs, then the communication of the SU is blocked. nN th SU have chance to be blocked on the arrival of PUs while all the bands are used. Therefore, the blocking rate for the proposed multi-user system is as follows:

$$Blocking\ rate = \lambda_s \Pi_{nN} \tag{6.52}$$

6.4.4.4 Utilization ratio

The utilization ratio is defined as the ratio of the radio bands that are used by the PUs and SUs to the total number of radio bands that are available in the system. In the proposed multi-user system, the utilization ratio is defined as follows:

$$\begin{aligned} Utilization\ ratio = \frac{Number\ of\ radio\ bands\ used\ by\ users}{Total\ number\ of\ radio\ bands} &= \frac{n * \sum_{j=1}^{n} \Pi_{x_n} * N + \sum_{j=1}^{nN} j\Pi_j}{nN} \\ &= \sum_{j=1}^{n} \Pi_{x_n} + \frac{1}{nN} \sum_{j=1}^{nN} j\Pi_j \end{aligned} \tag{6.53}$$

In the next section, the verified numerical results are shown for the

approaches for spectrum sharing.

6.5 Verification and Numerical Results

In this section, the proposed three approaches in this chapter are verified and the numerical results are shown accordingly.

6.5.1 Enhancing the SU's service continuity through the SCE framework

In order to demonstrate how the disruption to an SU's service is minimized when it needs to return the spectrum to the PU during spectrum sharing, a simulation is performed using the random system-operation parameters defined in [129] and shown in Table 6.2.

System operation parameter	Values
λ_A	0, 1/15, 1/10, 1/5, 1/3 (per minute) Or
	0, 0.0011, 0.0017, 0.0033, 0.0056 (per seconds)
λ_I	1 time/second
λ_V	1 time/second
μ_V	0.2, 0.4, 0.6, 0.8, 1 (per second)
μ_D	0.2, 0.4, 0.6, 0.8, 1 (per second)
λ_D	1 time/minute

Table 6.2: System operation oarameters.

The aim is now to choose different transition rates from the Table 6.2 to determine its effect on SU's service continuity.

Here, $\lambda_A = 1/15$ means an SU accesses the spectrum once per 900 seconds;
$\lambda_A = 1/10$ means an SU accesses the spectrum once per 600 seconds;
$\lambda_A = 1/5$ means an SU accesses the spectrum once per 300 seconds;
$\lambda_A = 1/3$ means an SU accesses the spectrum once per 180 seconds.

The service continuity level of an SU varies depending on different access, recovery and repair rates as follows. According to equation 6.13, the probability of the SU being in the Search state (π_S) needs to be calculated for every case.

For $\lambda_A = 0$; μ_V and $\mu_D = 0.2$, then

$$\pi_S = (1 + 0 + 0 + 0 + \frac{0.016}{0.2})^{-1} = (1 + 0.08)^{-1} = 0.925 \tag{6.54}$$

and

$$Service\ Continuity = 1 - (\frac{0.016}{0.2}) * 0.925 = 1 - 0.074 = 0.926 \tag{6.55}$$

For $\lambda_A = 1/15$; μ_V and $\mu_D = 0.4$, then

$$\pi_S = (1 + 0.0011 + .0011 + \frac{0.0011}{0.4} + \frac{0.016}{0.4})^{-1} = (1.04)^{-1} = 0.961 \tag{6.56}$$

and

$$Service\ Continuity = 1 - (\frac{0.0011}{0.4} + \frac{0.0016}{0.4}) * 0.961 = 0.958 \tag{6.57}$$

For $\lambda_A = 1/10$; μ_V and $\mu_D = 0.6$, then

$$\pi_S = (1 + 0.0017 + .0017 + \frac{0.0017}{0.6} + \frac{0.016}{0.6})^{-1} = (1.032)^{-1} = 0.968 \tag{6.58}$$

and

$$Service\ Continuity = 1 - (\frac{0.0017}{0.6} + \frac{0.0016}{0.6}) * 0.968 = 0.972 \tag{6.59}$$

For $\lambda_A = 1/5$; μ_V and $\mu_D = 0.8$, then

$$\pi_S = (1 + 0.0033 + .0033 + \frac{0.0033}{0.8} + \frac{0.016}{0.8})^{-1} = (1.027)^{-1} = 0.973 \tag{6.60}$$

and

$$Service\ Continuity = 1 - (\frac{0.0033}{0.8} + \frac{0.0016}{0.8}) * 0.973 = 0.976 \tag{6.61}$$

For $\lambda_A = 1/3$; μ_V and $\mu_D = 1$ then

$$\pi_S = (1 + 0.0055 + .0055 + 0.0055 + 0.016)^{-1} = (1.032)^{-1} = 0.968 \tag{6.62}$$

and

$$Service\ Continuity = 1 - (0.0055 + 0.0016) * 0.973 = 0.979 \tag{6.63}$$

The abovementioned results are shown in Table 6.3.

Access rate (λ_A)	Repair rate (μ_V)	Recovery rate (μ_D)	Service Continuity level
0	0.2	0.2	0.926
0.0011	0.4	0.4	0.958
0.0017	0.6	0.6	0.972
0.0033	0.8	0.8	0.976
0.0056	1	1	0.979

Table 6.3: Service continuity level of the SU depending on various transition rates

In this section, the effect of different transition rates on an SU's service continuity is discussed. The first state is the *Access* state. From Table 6.3, it is shown that the service continuity level of an SU varies according to different access rates, that is, how frequently the SU needs to access the free spectrum to continue its service. In other words, Figure 6.8 shows that the service continuity levels of the SU are enhanced by increasing the spectrum access rate. The results indicate that an increase of access rate has a positive impact on the increment of the service continuity of an SU. Therefore, an SU can minimize the disruption in its service by increasing the access rate in the model when it has to vacate the spectrum for the PU.

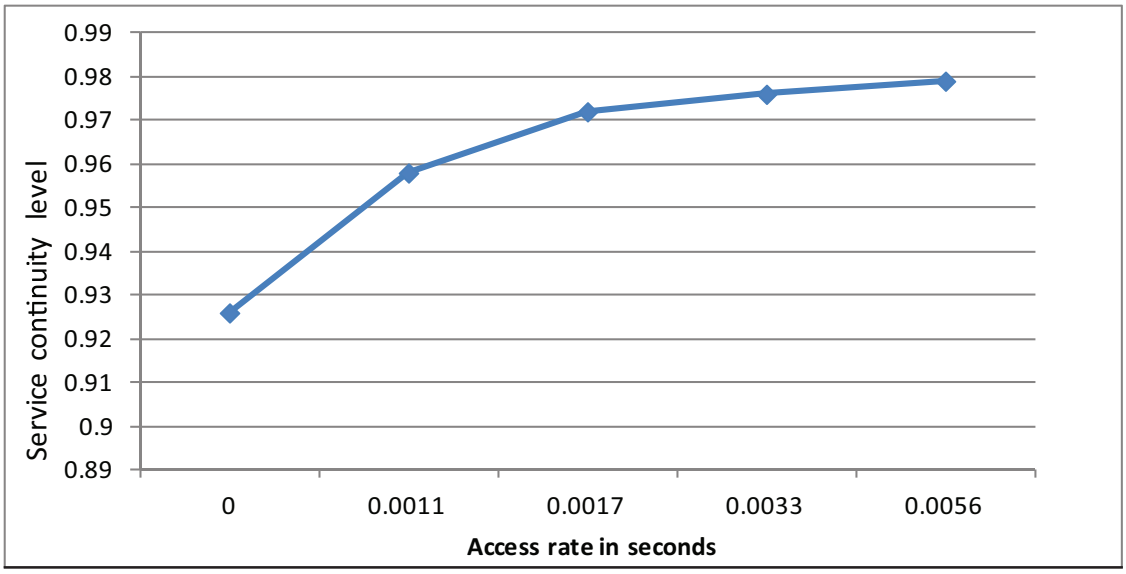

Figure 6.8: Service continuity vs access rate

For the *Vacate* state, from Table 6.3, it is also seen that the service continuity level of an SU depends on different repair rates. An increase in the repair rate has a positive impact on the increase of service continuity. An SU can minimize the disruption in its service by increasing its repair rate from the vacate state. Therefore, the minimization of an SU's service disruption depends on how frequently the SU can search and access the other free spectrum after vacating the spectrum for the PU.

For the *Dropped* state, from Table 6.3, it is also seen that the service continuity level of an SU depends on different recovery rates. An increase in the recovery rate has a positive impact on the increase of service continuity. An SU can minimize the disruption in its service by increasing its recovery rate from the Dropped state. Therefore, the minimization of an SU's service disruption depends on how frequently the SU can search and access the other free spectrum from the Vacate state. It is clearly identified that the

minimization of service continuity of an SU depends on the increment of access rate, repair rate and recovery rate across the states during the spectrum sharing mechanism in CRNs.

To summarize the observations, Table 6.3 shows that the service continuity for SUs varies with the different variations in the state transition rates. If the SU accesses the PU's spectrum very frequently, its service continuity will increase. This means that if the SU continues to search to obtain the free spectrum instead of going to the Dropped state after vacating the spectrum for the PU in the CRNs, the chance of obtaining the free spectrum is increased. Whenever the SU cannot obtain any free spectrum, then its communication is dropped and it goes to the Dropped state. If the SU searches for another free spectrum as soon as possible after it goes to the Vacate state and the Dropped state and obtains access to the spectrum, then it can repair and recover from the Vacate state and Dropped state, respectively. If both the repair rate and recovery rate increase, then the service continuity level also increases. So in this section, it is shown that the service continuity of SUs depends on various state transition rates for the different states throgh which it needs to go during the spectrum sharing mechanism. Therefore, by controlling the different transition rates in the SU's working states, it is possible to minimize the disruption in its service by continuously searching and accessing the spectrum in CRNs.

6.5.2 Secure spectrum sharing through CTAS^3 framework

A system is made and programmed using the programming environment described in Section 5.7 in order to verify the proposed CTAS^3 framework.

After achieving the trust values using the trust calculation method in Sections 6.3.2 and 6.3.3, the values are plotted using MATLAB programming environment. The system is verified using two networks in CRNs. There are 5 nodes in the primary network and 6 nodes in the secondary network. Node 2 in the secondary network is used as a requesting node. Using the proposed conjoint trust calculation approach in CRNs, firstly, 5 nodes from the secondary network recommend the requesting node, then 5 different nodes from the primary network recommend the requesting node.

6.5.2.1 Trust calculation from the secondary network

Every node in the secondary network assigns a trust value for 1000 services to the requesting node. Therefore, 1000 trust values are obtained for the requesting secondary node using equation 6.14. Figure 6.9 shows these 1000 trust values of the requesting node from 5 member nodes in the secondary network.

Therefore, the trust value of the requesting node from each member node in the secondary network is shown in Figure 6.10.

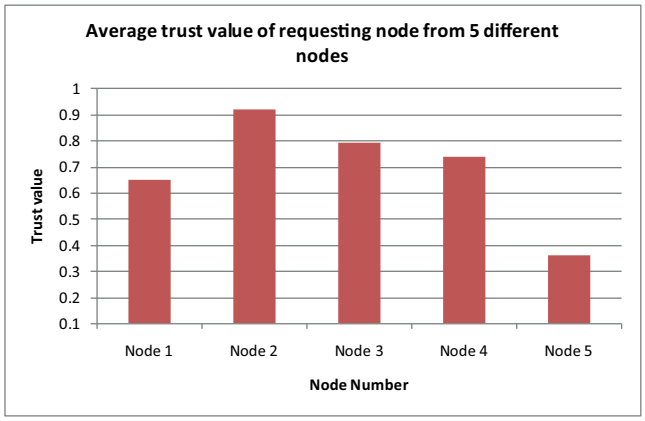

Figure 6.10: Average trust value of the requesting node from the other 5 nodes in the secondary network

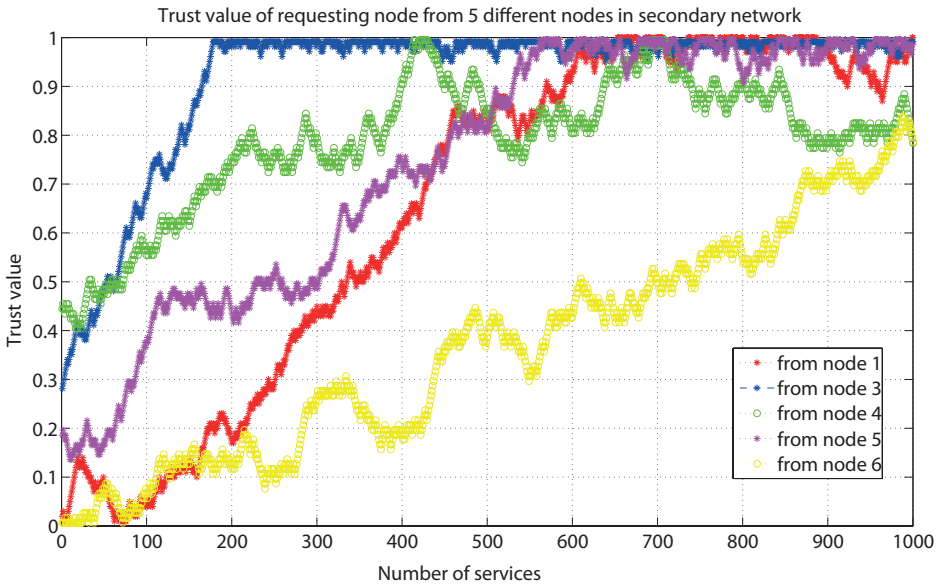

Figure 6.9: Trust value of the requesting node from each member node in the secondary network for 1000 services

Each member node in the secondary network sends the computed trust value of the requesting node to the SUBS. The SUBS calculates the requesting node's trust value using Table 6.4.

Trust value of the requesting node		
From node	Value	Trust value computed by the SUBS
Node 1	0.6531	0.6934
Node 3	0.9213	
Node 4	0.7913	
Node 5	0.7401	
Node 6	0.3619	

Table 6.4: Trust value of the requesting node from the secondary network

The SUBS sends this trust value (0.6934) to the PUBS.

6.5.2.2 Trust calculation from the primary network

The PUBS receives the 1000 trust values of the requesting node from each member node in the primary network using equation 6.22. Figure 6.11 shows the 1000 trust values of the requesting node from each member node.

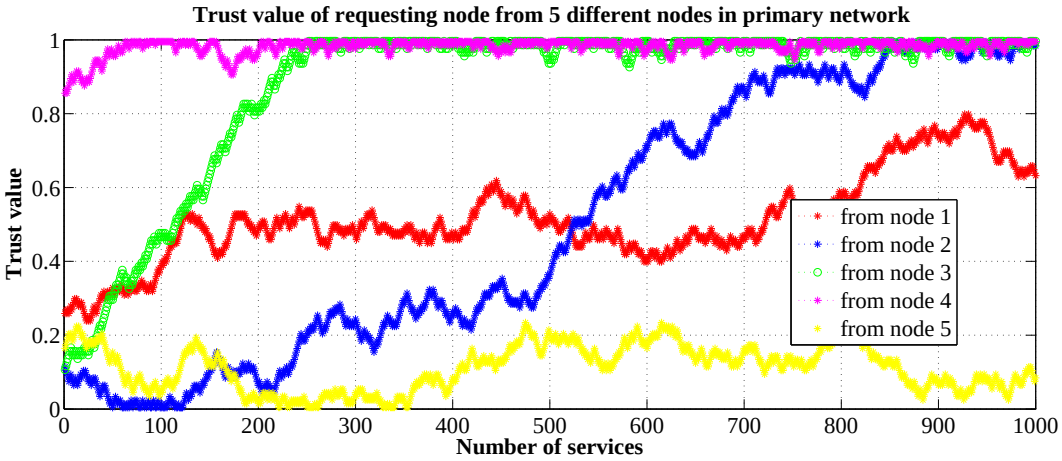

Figure 6.11: Trust value of the requesting SU from each member node for the 1000 services in the primary network

The PUBS averages these trust values received from each member node in the primary network. The average trust value of the requesting node in the primary network is shown in Figure 6.12.

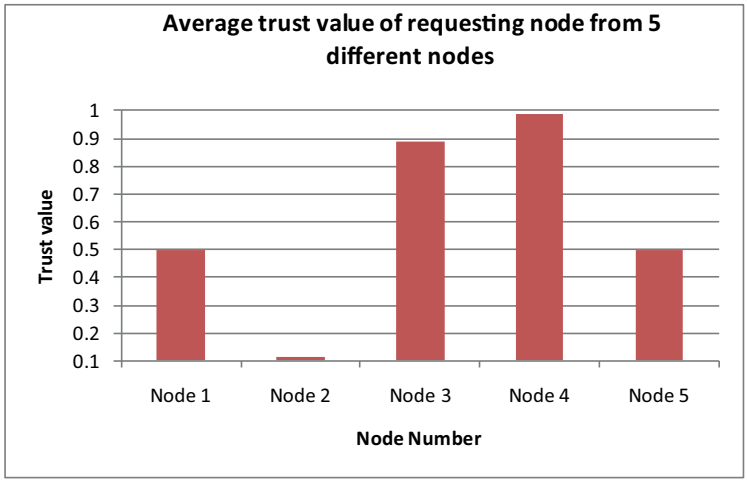

Figure 6.12: Average trust value of the requesting node from the primary network

Each member node in the primary network sends the computed trust value of the requesting node to the PUBS. At first, the PUBS calculates the average trust value of the requesting node based on the values received from each member node and then the PUBS calculates the recommended conjoint trust value using 6.24, as shown in Table 6.5.

Trust Value of the requesting node			
From node	Value	Trust value received from the SUBS	Conjoint trust value computed by the PUBS
Node 1	0.501	0.6934	0.64
Node 2	0.113		
Node 3	0.891		
Node 4	0.989		
Node 5	0.501		

Table 6.5: Trust value of the requesting node from the PUBS

The PUBS checks the conjoint trust values of the requesting node and it observes that the trust value of the requesting node (0.64) is lower than the trust threshold (0.7). In this case, the requesting node is not considered a trustworthy node to assign spectrums and its request to use the spectrum is

not approved (NAP).

6.5.3 Evaluation of network statistics for a B-CRN framework

In this subsection, channel utilization and other important statistics are evaluated during the spectrum sharing scheme for a balanced network. Numerical results are shown using the parameters in [77], as mentioned in the next subsection. In the numeric experiments for testing the feasibility of the model, three cases are considered as follows:

- 1 PU with a total of 3 sub-bands
- 2 PUs with a total of 6 sub-bands
- 3 PUs with a total of 9 sub-bands

For one and two PUs in the system, a maximum of three and six SUs are allowed to use the spectrum in the network, respectively. Similarly, for three PUs in the system, a total of 9 sub-bands are available. Therefore, a maximum of 9 SUs are allowed to use the spectrum in the network using equation 6.28.

6.5.3.1 Mean number of SUs analysis

For the mean number of SU analysis, the parameters are assumed as in Table 6.6.

System Operation Parameter	Values
λ_p	1, 2, 3, 4, 5, 6, 7, 8, 9 times per 10 minutes
μ_p	0.4
λ_s	0.6
μ_s	0.2, 0.4, 0.6, 0.8

Table 6.6: System operation parameters for mean number of SU analysis for multiple users during spectrum sharing

The mean number of SUs for different arrival rates of PU (λ_p) for different number of PUs is shown in Figure 6.13.

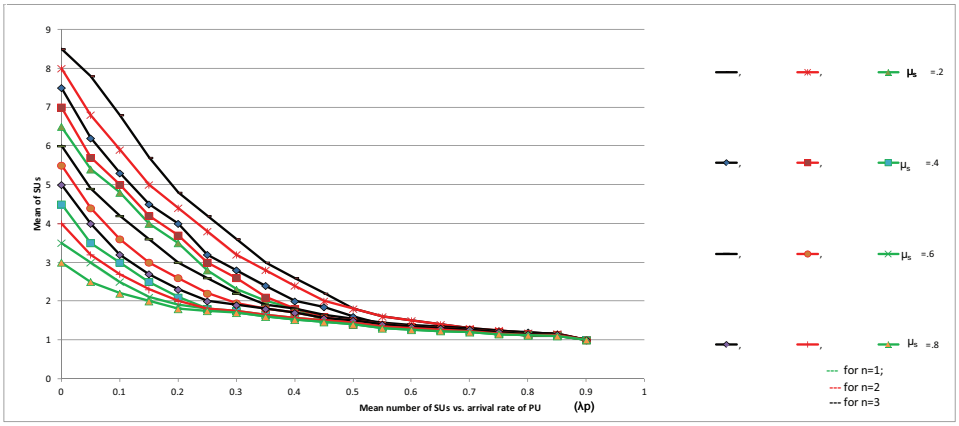

Figure 6.13: Mean number of SUs vs. arrival rate of PUs (λ_p)

From Figure 6.13, it can be seen that the mean number of SUs using the spectrum decreases with an increase of λ_p. Three case studies have been used to show the numerical results, for $n = 1, 2, 3$. For one PU (n=1), the mean number of SUs decreases from 3 to 1, 3.5 to 1, 4.5 to 1, and 6.5 to 1 for $\mu_s = 0.8, 0.6, 0.4$ and 0.2, respectively. This shows that if the arrival rate

of the PU increases, the mean number of SUs decreases. Similar results are obtained for $n = 2$ and $n = 3$. Therefore, if PUs access their own spectrum very frequently, the mean number of SUs who are able to use the free spectrum decreases as the PUs use their own spectrum. Therefore, if the PU's arrival rate to access their own spectrum increases, the mean number of SUs who are able to access the spectrum decreases. All of these three cases show the same results.

6.5.3.2 Deprivation rate analysis

For deprivation rate analysis, the parameters are assumed as shown in Table 6.7.

System Operation Parameter	Values
λ_p	1, 2, 3, 4, 5, 6, 7, 8, 9 times per 10 minutes
μ_p	0.4
λ_s	0.6
μ_s	0.2, 0.4, 0.6, 0.8

Table 6.7: System operation parameters for deprivation rate analysis for multiple users during spectrum sharing

The deprivation rate for different arrival rates of PUs (λ_p) for a different number of PUs is shown in Figure 6.14.

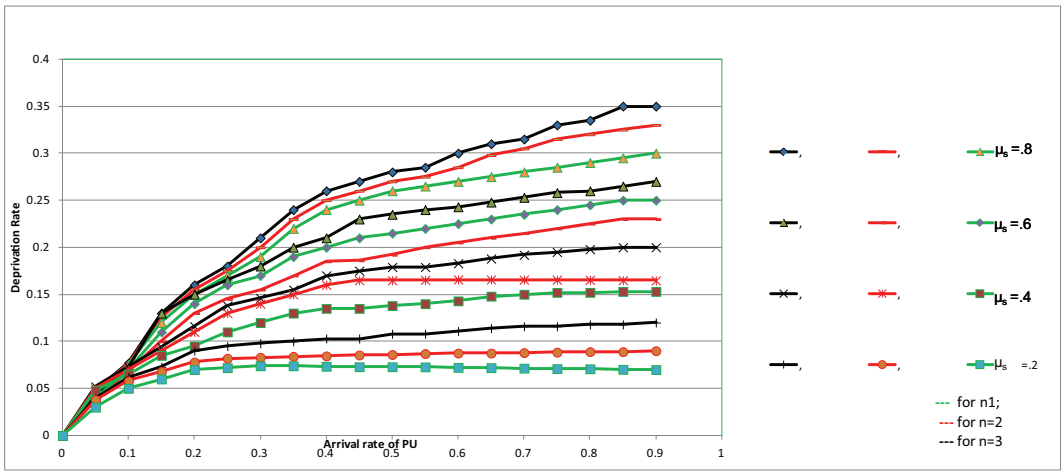

Figure 6.14: Deprivation rate vs. arrival rate of PUs (λ_p)

From Figure 6.14, it can be seen that for each arrival rate of the PU, the deprivation rate increases with an increase of λ_p. Three case studies were considered, for $n = 1, 2, 3$ to show the numerical results. For one PU ($n = 1$), the deprivation rate is increased from 0 to 0.07, 0 to 0.15, 0 to 0.25 and 0 to 0.3 for $\mu_s = 0.2, 0.4, 0.6$, and 0.8, respectively. This shows that if the rate of PU's arrival increases, the deprivation rate of the SU also increases. Similar results are observed for $n = 2$ and $n = 3$. Therefore, if the arrival rate of PUs increases in the system, the deprivation rate of SUs increases in CRNs. Thais means that if the PUs come to use their own spectrum very frequently, the SU's call deprivation rate increases as they are forced to vacate the spectrum band. The three cases show the same results.

6.5.3.3 Blocking rate analysis

For the blocking rate analysis, the parameters are assumed as shown in Table 6.8.

System Operation Parameter	Values
λ_s	1, 2, 3, 4, 5, 6, 7, 8, 9 times per 10 minutes
μ_p	0.4
λ_s	0.6
μ_s	0.2, 0.4, 0.6, 0.8

Table 6.8: System operation parameters for blocking rate analysis for multiple users during spectrum sharing

The blocking rate for different arrival rates of SUs (λ_s) for a different number of PUs is shown in 6.15.

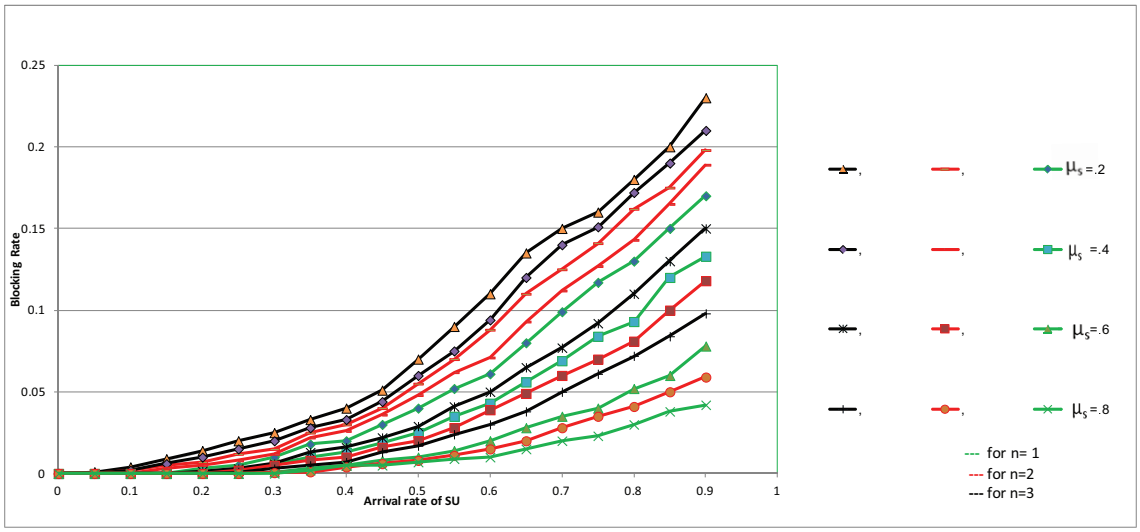

Figure 6.15: Blocking rate vs. arrival rate of SUs (λ_s)

From Figure 6.15, it is observed that for one PU (n=1), the blocking rate is increased from 0 to 0.03, 0 to 0.07, 0 to 0.14 and 0 to 0.17 for $\mu_s = 0.8, 0.6, 0.4$ and 0.2, respectively. This shows that if the rate of SU's arrival increases, other SU's blocking rate increases. Similar result are observed for $n = 2$ and $n = 3$. Therefore, if the arrival rate of SUs increases in the system, the blocking rate of SUs increases in CRNs due to the unavailability of the sub-bands. This

means, if SUs come to use the PU's free spectrum frequently, other SU's call blocking rate increases as all the available sub-bands are occupied by other PUs. The three cases show the same results.

6.5.3.4 Utilization ratio analysis

For blocking rate analysis, the parameters are assumed as shown in Table 6.9.

System Operation Parameter	Values
λ_s	1, 2, 3, 4, 5, 6, 7, 8, 9 times per 10 minutes
μ_p	0.4
λ_s	0.6
μ_s	0.2, 0.4, 0.6, 0.8

Table 6.9: System operation parameters for utilization rate analysis for multiple users during spectrum sharing

The blocking rate for different arrival rate of SU (λ_s) for different number of PUs is shown in 6.16.

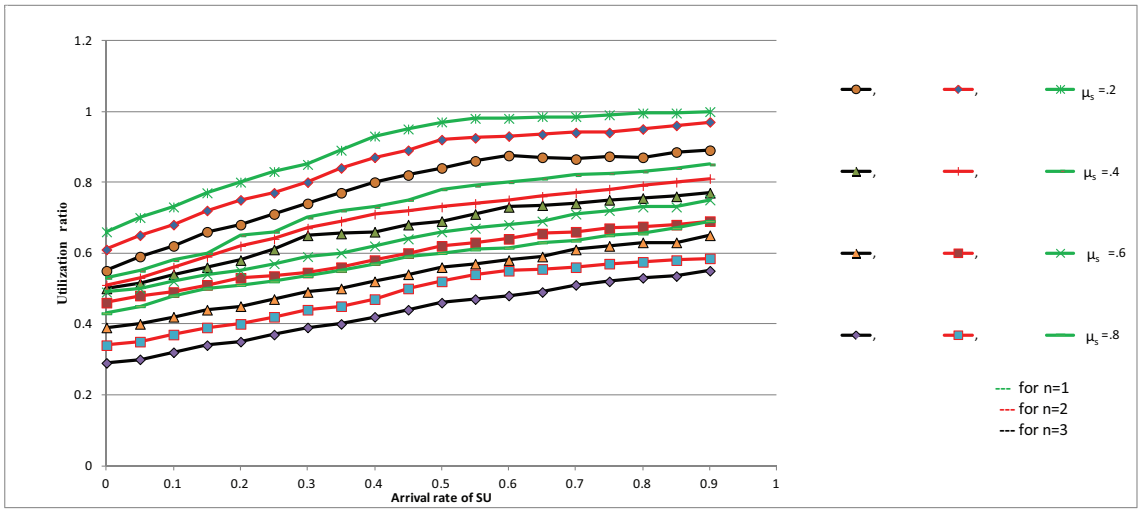

Figure 6.16: Utilization ratio vs. arrival rate of SUs (λ_s)

From 6.16, it is observed that for $n = 1$, the utilization ratio is increased from 0.62 to 1, 0.55 to 0.83,0.45 to 0.73 and 0.42 to 0.65 for $\mu_s = 0.2, 0.4, 0.6$ and 0.8, respectively. This shows that if the rate of SU's arrival increases according to the channel availability, the utilization ratio increases. Similar results are observed for $n = 2$ and $n = 3$. Therefore, if the arrival rate of SUs increases in the system, the utilization ratio of the system increases. The three cases show the same result.

6.6 Conclusion

Spectrum should be shared in a secure way in CRNs to avoid untrustworthy user behavior in the network. Therefore, in this chapter, the conjoint trust assessment approach is proposed to share the spectrum in a secure way. During spectrum sharing, if a PU comes back to the network, the SU needs to vacate the spectrum. In this case, the SU's service is discontinued until it searches and accesses other free spectrum. To minimize this service disruption of the SU, a state transition diagram of the working states of SUs is proposed. By controlling different transition rates in the state transition diagram, it is possible to minimize SU's service disruption during spectrum sharing. For efficient spectrum sharing, there should be a balance in the number of SUs and PUs so that the SUs' communication is not blocked, nor are their calls dropped when all SUs use the spectrum. Therefore, an approach is proposed to balance the number of SUs and PUs in the network and a basic spectrum sharing mechanism is also proposed for this multiple SUs and PUs model. Different network statistics are derived to see the network performance during spectrum sharing for multiple users in CRNs.

Chapter 7

Mechanisms for Enhancing System Availability of CRNs

7.1 Introduction

In Chapter 5, a Certificate Authority (CA)-oriented trust-based framework was proposed to authenticate a secondary user's (SU's) request to either use network resources or access primary user's (PU's) free spectrum so that malicious users cannot gain access to the network. The CA in the proposed framework serves as the key node which is responsible for performing the primary functions of the CRN and storing the trust values of all member nodes in the network. However, as pointed out in Section 3.3.3, the aim of a malicious node is to disrupt the security of the cognitive radio network (CRN), and one of the ways by which it can do this is by becoming the CA to break all the normal network activities. This, in turn, leads to the collapse of the whole network. To address this limitation, in this chapter, a framework for selecting the node as the CA is proposed that establishes a procedure for selecting the

most trustworthy node as the CA and other trustworthy nodes as the backup CAs (BCAs). The BCA is selected in the framework so that in the case of a malicious attack on the CA, the responsibility of the CA can be transferred to the BCA which can then act as the main CA to ensure the normal working process of CRNs. Having such a framework enhances the availability and reliability of the CRN.

Another way by which malicious users can disrupt the working of CRNs is by joining the network by falsifying their identity with a target to inject different security threats and jam the network. Another security threat occurs in the network when a member node behaves maliciously by leaving the network abnormally without informing any other member node in the network and revealing all the data to the malicious user after leaving the network. Thus, this abnormal leaving renders the whole network vulnerable to different threats. In order to address this limitation, in this chapter, a framework for secure node joining and leaving the network is proposed.

The proposed framework for the Node Selection as a CA and BCAs and Secure node Joining and Leaving (NSSJL) aims to increase the system availability of CRNs and maintains smooth and secure communication. Therefore, the proposed framework provides solutions and sufficient proofs for:

- selecting the most trustworthy node as the CA, and other nodes as the BCA to provide continuous service to maintain smooth communication in CRNs in case an error occurs in the CA.

- proposing the node *joining* and *leaving* procedure in the CRN in a secure way so that no malicious user can join the network and member nodes cannot leave the network abnormally. These schemes update a node's trust value depending on their joining and leaving activities which, in turn, cause the nodes to be selected as the CA and BCA in CRNs.

- demonstrating the increase in system availability and reliability by using the proposed NSSJL framework in CRNs.

The rest of this chapter is organized as follows: In Section 7.2, the architecture and working of the proposed NSSJL framework for increasing system availability is described. In Section 7.3, a detailed explanation of the process of selecting a node as a CA and BCA is given with an example. The process of secure node joining and leaving the network is described in Section 7.4 along with a description of how the successful joining and leaving processes impact on the node's trust update in the network. In Section 7.5, the proposed NSSJL framework is modeled to show how it can improve the availability and reliability of the CRN. The verification of the proposed framework is shown in Section 7.6. Finally, Section 7.7 concludes the chapter.

7.2 Proposed Framework for Node Selection and Secure Node Joining and Leaving (NSSJL) the Network to Increase the System Availability

In this section, the proposed framework for selecting the most trustworthy node and secure node joining and leaving the network to increase the system availability is presented.

7.2.1 System model and architecture

The architecture of the proposed NSSJL framework, presented in Figure 7.1, consists of four major components as follows:

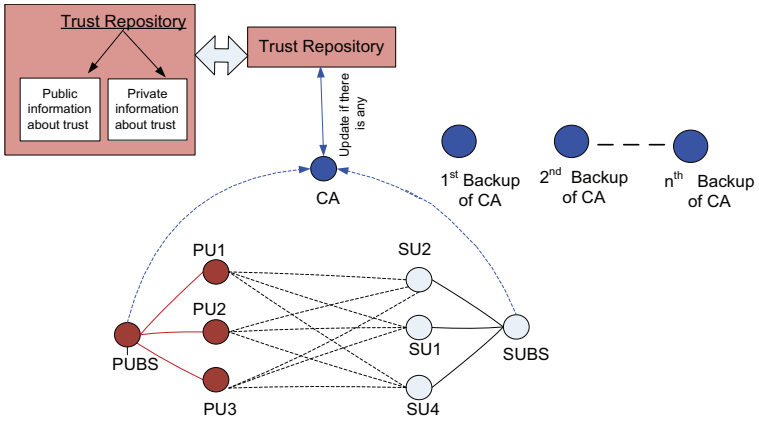

Figure 7.1: Proposed model using multiple BCAs in the NSSJL framework

- **Base Station**: As mentioned in Section 5.2, the base station is the central point of contact between different nodes in the network.
- **Certificate Authority (CA)**: As mentioned in Section 5.2, a CA is

an authorized entity connected to both networks to perform the main functions in the CRN.

- **Back-up Certificate Authority (BCA)**: BCAs are those nodes which have the capability to control the CRN when the CA is attacked by malicious users.

- **Trust Repository**: As mentioned in Section 5.2, the trust repository in a CA serves as the storage to store all the nodes' trust values in CRNs.

7.2.2 Working steps of the NSSJL framework

In this section, the working of the proposed NSSJL framework to increase the system availability is proposed. To increase availability, the proposed framework aims to (a) select the most trustworthy nodes to work as the CA and the BCA and (b) establish a secure node joining and leaving process in the network. Figure 7.2 presents a flowchart diagram of the working of the proposed framework, which is as follows:

1. Node Selection: In the proposed CRN architecture, the CA is responsible for performing all the major functionalities and storing the trust values of all the member nodes in the network. Therefore, after comparing the trust values against the trust threshold value, the most trustworthy node is selected as the CA so that it will not be easily compromised by the malicious nodes. Then, after comparing the trust values with the trust threshold, the second most trustworthy node is selected as the first BCA to work as the main CA in the event of any error or attacks to the main CA to ensure the system's continuous service as expected. This process

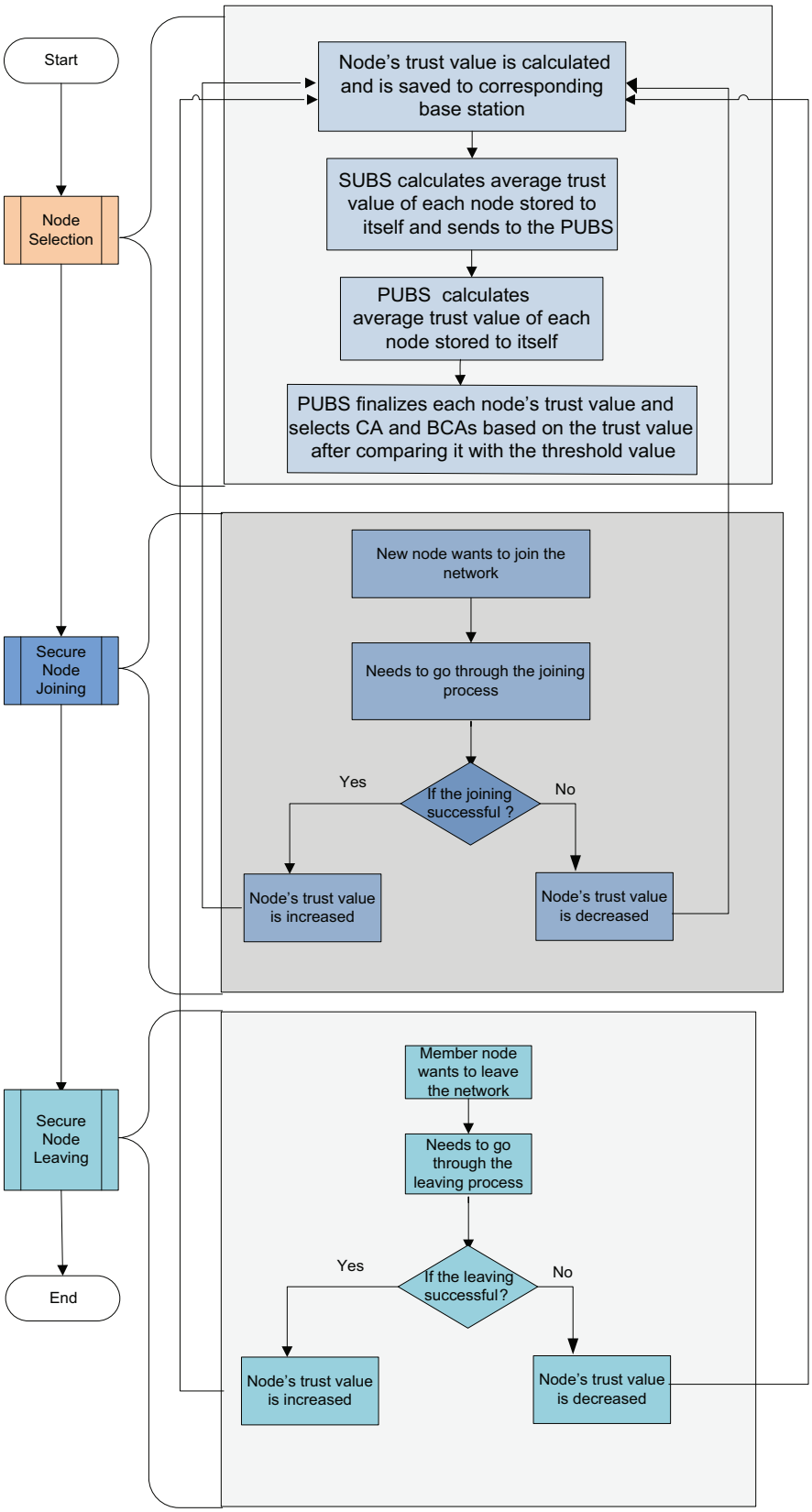

Figure 7.2: Flowchart illustrating the steps performed by the NSSJL framework

is repeated for all nodes whose trustworthiness value is above the trust threshold and they are selected as the nth BCA, where n is the number of BCAs.

2. Secure Node Joining the Network: If a new node wants to join the CRN, then it broadcasts a message to the network and goes through the secure joining process. If the process it follows to join the network is successful, then the node is considered a trustworthy node and its trust value is increased for its good behaviour which, in turn, results in the joined node to be selected as a CA.

3. Secure Node Leaving the Network: If a member wants to leave the network, it sends a message to the respective base station before leaving the network according to the secure leaving process policy. The node should go through the secure leaving process. If the process it follows to leave the network is normal, then the node's trust value is increased for its good behaviour which, in turn, helps the leaving node to join another network.

In the next section, the working of each of these steps is defined in the proposed NSSJL framework which will be discussed in detail.

7.3 Trustworthy Node Selection to Work as a CA and BCA

In this section, the process of selecting a node as the CA and BCA is presented. As all member nodes may always have a high opinion of their respective base

stations, the base stations may always receive the highest trust value. To avoid this, in the proposed framework, base stations do not take part in CA and BCA selection. As a result, the CA and BCAs are selected from the member nodes in the CRNs. Figure 7.3 illustrates the steps in the node selection phase in the proposed framework. The steps are as follows:

- The trust calculation process is carried out at the secondary network and the primary network
- At first, the available node's trust value from both networks in CRNs is calculated, depending on its trust relationship between the different nodes in CRNs. Every node in the network finds its 1-hop neighbors and calculates their trust values depending on various activities and sends these to their corresponding base stations. Both base stations also assign trust values for its 1-hop member nodes.

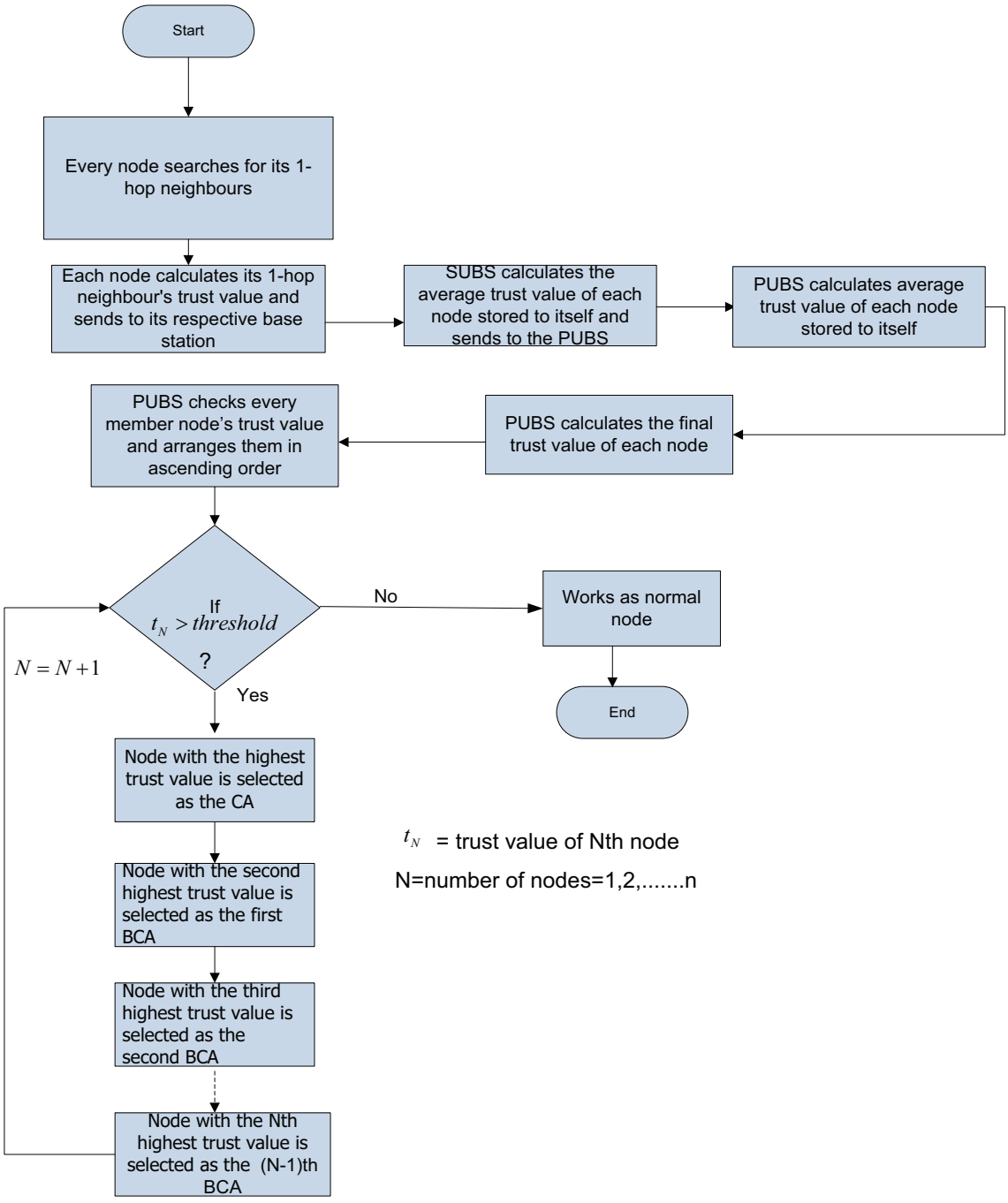

Figure 7.3: Working steps for the node selection phase in the NSSJL framework

Following Chang et al. [119] it is assumed that each CR node is aware of its 1-hop neighbor nodes and assigns a trust value for it, using the trust

calculation method 7.3.1. The 1-hop neighbor of node i is denoted by $N^1(i)$. For instance, from Figure 7.4, it can be seen that the CR node PU1's 1-hop neighbors, $N^1(PU1)$, are SU2, SU3 and SU1.

$$N^1(PU1) \xrightarrow{one\ hop\ neighbour} > \ SU2, SU3, SU1 \tag{7.1}$$

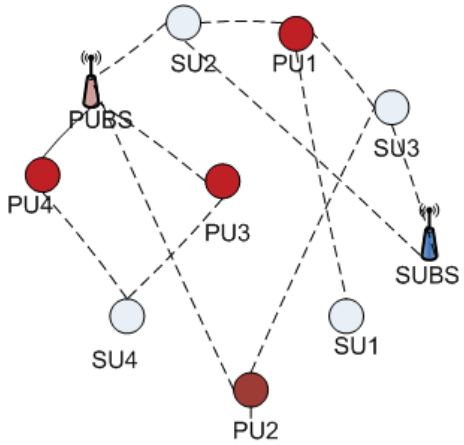

Figure 7.4: Communication between CR Nodes

After receiving each member node's 1-hop neighbor's trust value, both base stations store these trust values and calculate the average trust value of each node. First, SUBS calculates the average trust value of all the nodes for which it receives a recommendation from its member nodes. PUBS also calculates the average trust value of each node for which it receives a recommendation from its member nodes. SUBS then forwards all nodes' trust values to the PUBS.

- After receiving the trust values from SUBS, PUBS calculates every node's final trust value in the CRN. If there is more than one trust value for a node calculated from SUBS and PUBS, then its average value is

considered as the final trust value.

- If a node has the highest trust value and its trust value is above or equal to the trust threshold, PUBS selects this node as the CA. If a node has the second highest trust value and its trust value is above or equal to the trust threshold, PUBS selects this node as the first candidate for the BCA and so on. If the node has a trust value which is below the trust threshold, then it works as a normal node.

- The first candidate for the BCA takes charge as the CA if any error occurs in the CA and the second candidate for the BCA takes the role of the first BCA and so on.

From the above working steps, node selection has two sub-processes as follows:

- Trust calculation method for each node

- Selection of the CA and BCA based on the trust values

In the next subsection, the node's trust calculation method is described in detail.

7.3.1 Trust calculation method

A node has a trust relationship with other nodes in the CRN depending on its performance in complying with various activities such as vacating the PU's spectrum band on its arrival, normal joining or leaving the CRN, and appropriate spectrum sensing. A node that has high compliance in all these

activities will have a high trust value. The trust value of a node is evaluated by other nodes and is represented by $TV_i(j)$, where $TV_i(j)$ represents the trust value of node j evaluated by node i. The range for representing one node's trust value is from 0 to 1.

$$TV_i(j) = \frac{\sum_{k=1}^{n} TV_i^k(j)}{n} \tag{7.2}$$

where k is an activity that node i has with node j and
n is the total number of activities.

When there is more than one node that evaluates the trust value of a cognitive radio node, then the cumulative trust value is represented by:

$$\overline{TV}(j) = \frac{\sum_{i=1}^{|R_R|} TV_i(j)}{|R_R|} \tag{7.3}$$

where $|R_R|$ denotes the number of nodes of the network region R. An example is illustrated in Figure 7.5 to explain this calculation method using equations 7.2 and 7.3.

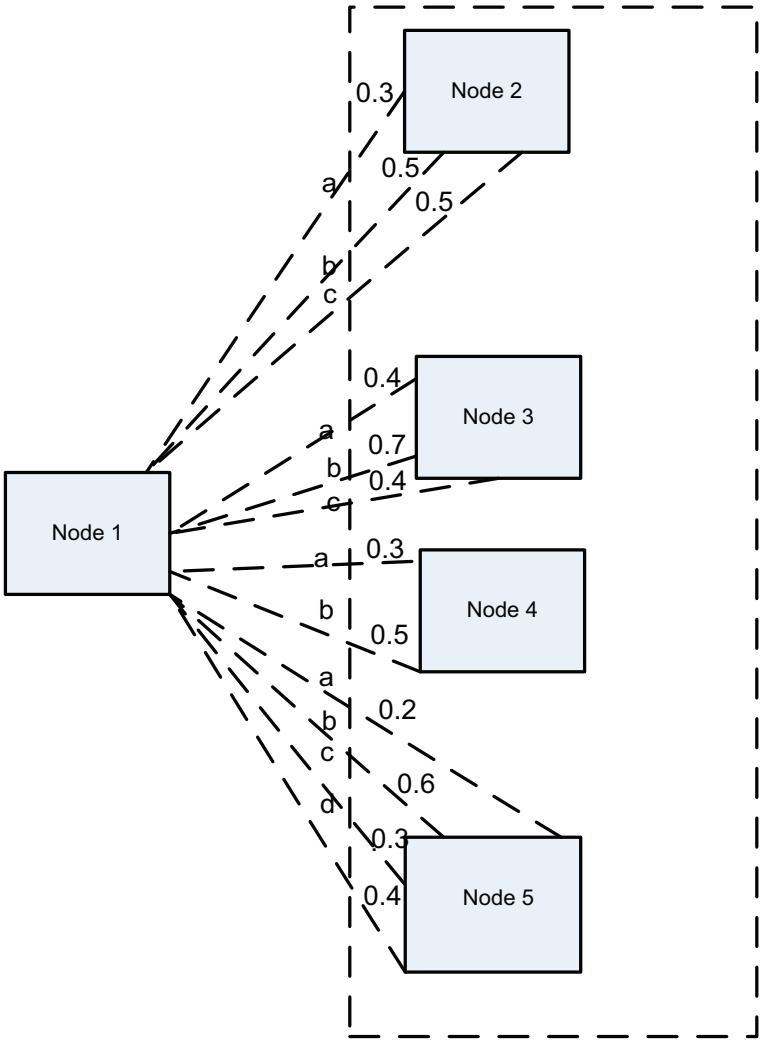

Figure 7.5: Example to illustrate the trust calculation method

Node 1 has three past activities (activity numbers: a, b, c) with node 2, and for each of these activities, node 1 is assigned a certain trust value by node

2. Therefore, node 1's trust value is evaluated by node 2 using equation 7.2 :

$$TV_2(1) = \frac{TV_2^a(1) + TV_2^b(1) + TV_2^c(1)}{3} = \frac{0.3 + 0.5 + 0.5}{3} = 0.43 \qquad (7.4)$$

Accordingly, node 1's trust values as evaluated by node 3, node 4 and node 5 are 0.5, 0.4 and 0.37, respectively.

There are four nodes which evaluate node 1's trust value. Therefore, node 1's final trust value is calculated using equation 7.3.

$$\overline{TV}(1) = \frac{TV_2 1 + TV_3 1 + TV_4 1 + TV_5 1}{4} = \frac{0.43 + 0.5 + 0.4 + 0.37}{4} = 0.42 \qquad (7.5)$$

Using this trust calculation method, every node in Figure 7.4 calculates its 1-hop neighbor's trust value and sends this to the corresponding base station. For instance, node SU3's trust value evaluated by PU1 is denoted by $TV_{PU1}^{SU3} = 0.6$ and PU1 sends the evaluated trust value of SU3 to the PUBS. Different nodes evaluate the same node's trust value and may have different results because of their findings and experiences. Each secondary node calculates its 1-hop neighbor's trust value and sends it to the SUBS, as shown in Table 7.1.

The trust value received by the SUBS		
From node	For node	Value
SU1	PU1	0.7
SU2	PUBS	0.9
	SUBS	0.8
	PU1	0.7
SU3	SUBS	0.9
	PU1	0.6
	PU2	0.6
SU4	PU3	0.5
	PU4	0.6
SUBS	SU2	0.3
	SU3	0.5

Table 7.1: The trust value received by the SUBS for the CR node

Each primary node calculates its 1-hop neighbor's trust value and sends it to the PUBS, as shown in Table 7.2. SUBS forwards each node's average trust value to the PUBS. Finally, PUBS calculates each node's final trust value.

Trust value received by the PUBS		
From node	For node	Value
PU1	SU2	0.5
	SU3	0.6
	SU1	0.3
PU2	PUBS	0.9
	SU3	0.6
PU3	SU4	0.3
	PUBS	0.8
PU4	PUBS	0.9
	SU4	0.5
PUBS	PU4	0.3
	PU3	0.4
	SU2	0.2
	PU2	0.4

Table 7.2: The trust value received by the PUBS for the CR node

SUBS calculates the average trust value of each node for which it receives a trust value from its member node, as shown in Table 7.3 and sends these trust values to PUBS.

The average trust value calculated by the SUBS	
Node	Value
PU1	0.66
PU2	0.6
PU3	0.5
PU4	0.6
SU2	0.3
SU3	0.5

Table 7.3: The average trust value of nodes calculated by the SUBS

PUBS calculates the average trust value of each node for which it receives a trust value from its member node, as shown in Table 7.4.

The average trust value calculated by the PUBS	
Node	Value
SU2	0.35
SU3	0.6
SU1	0.3
SU4	0.4
PU4	0.3
PU2	0.4
PU3	0.4

Table 7.4: The average trust value of nodes calculated by the PUBS

After receiving the trust values from the SUBS, the PUBS calculates the

final trust value of each node using equation 7.3 and stores this in itself, as shown in Table 7.5.

Node Number	Node name, j	$TV(j)$
1	PU1	0.66
2	PU2	0.5
3	PU3	0.45
4	PU4	0.45
5	SU4	0.4
6	SU3	0.56
7	SU1	0.3
8	SU2	0.33

Table 7.5: Local trust relationship table stored in the PUBS

7.3.2 Selection of CA and BCA based on the trust value

Each node's final trust value is calculated and stored in PUBS using the trust calculation method described in Section 7.3.1 as shown in Table 7.5. From Table 7.5, the possible CA and BCA candidates will be selected by the PUBS, depending on their trust value. The PUBS checks each member node's trust value. If a node has the highest trust value and it is above or equal to the trust threshold (0.5, in this approach), it is selected as the CA. If a node has the second highest trust value and it is above or equal to the trust threshold, then the node is selected as the first candidate of the BCA and takes the role of the CA if any errors occur in the main CA. If a node has the third highest trust value and it is above or equal to the trust threshold, then the node is selected as the second candidate of the BCA. The node whose trust value is

lower than the threshold, works as a normal node in the network. Table 7.6 shows the candidate list for the CA and BCAs. Using the flowchart in Figure 7.3, from Table 7.6, the PU1 node is selected to act as the CA as it achieves the highest trust value of all the nodes and its trust value is above 0.5. SU3 is selected as the first BCA as it achieves the second highest trust value in the network and its trust value is above 0.5. PU2 is selected as second BCA as it has third highest trust value and its trust value is equal to 0.5. Nodes PU4, PU3, SU4 work as normal nodes in the network.

	Node Number	Trust value
CA candidate	PU1	0.66 (highest trust value and is above the threshold)
First BCA candidate	SU3	0.56 (second highest trust value and is above the threshold)
Second BCA candidate	PU2	0.5 (third highest trust value and is equal to the threshold)
Normal node	PU4, PU3	0.45 (trust value is lower than the threshold)
Normal node	SU4	0.4 (trust value is lower than the threshold)

Table 7.6: Candidate list for CA and BCA selection

It is possible that there may be more than one node with the same trust value and which is above the trust threshold and is therefore eligible to be selected as either the CA or the BCAs. In such scenarios, these member nodes of CRNs will compete to be selected as either a CA or BCA as explained in the next sub-section.

7.3.3 Selection of CA and BCA node when there is more than one possible node

When there is more than one possible node which can be selected as either a CA or BCA, then an election process is held. During the election process, the selection of the nodes is done according to the following priorities:

1. Priority 1: The node is a current CA or BCA.

2. Priority 2: The node is from the primary network.

7.3.3.1 *CA Selection Process*

In the selection process, if a potential CA candidate either currently works as a CA of the network or is from the primary network and its trust value is greater than all the potential CA nodes, then it is selected as the CA. Otherwise, the CA is chosen from the potential candidates. The selection procedure is described through Algorithm 2.

Algorithm 2 CA Competition Algorithm

Input: Trust table in primary user base station (PUBS), number of CA competitors (n), system defined trust threshold ($T_{threshold}$)

Output: CA selection

PUBS will search the trust table for the list of CA competitors and see the current trust value of each competitor ($T_{current}$).
for $j \leftarrow 1$ to $j \leq n$ **do**
  if $T_{current} \geq T_{threshold}$ **then**
    if the CA competitor is current the CA **then**
      this node will be selected as the jth CA
    else
      if the CA competitor is from the primary node **then**
        this node will be selected as the jth CA
        $T_{current} = T_{current} + 0.05$
      else
        Not selected as a CA and will take part in the next election procedure.
      end if
    end if
  end if
end for

As the CA node should be more trustworthy than the BCA, if a node successfully wins the competition as the CA, its trust value will be incremented

by 0.05 as a reward for winning the competition. Specifically, the CA node is responsible for managing the authority and authentication processes within the CRN group.

7.3.3.2 *BCA Selection Process*

As in the CA selection process, if a potential BCA node is currently a BCA of the network and its trust value is greater than all the potential BCA nodes, then it is given a higher priority and is selected as the BCA. Otherwise, the BCA is chosen from the potential candidates. The selection process is described through Algorithm 3.

Algorithm 3 BCA Competition Algorithm

Input: Trust table in primary user base station (PUBS), number of BCA competitors (n), system defined trust threshold ($T_{threshold}$)

Output: BCA selection winner

PUBS will search the trust table for the list of BCA competitors and see the current trust ($T_{current}$) of each competitor.
for $j \leftarrow 1$ to $j \leq n$ **do**
  if $T_{current} \geq T_{threshold}$ **then**
    if the BCA competitor is the current BCA **then**
      this node will be selected as the jth CA
    else
      if the BCA competitor is from the primary node **then**
        this node will be selected as the jth CA
        $T_{current} = T_{current} + 0.05$
      else
        Not selected as BCA and will take part in the next election procedure.
      end if
    end if
  end if
end for

If a node wins the BCA competition, its trust value will be incremented by 0.05 as a reward for winning the competition. From Table 7.7, an example is

demonstrated to select the CA/BCA when there is more than one candidate.

Node	Current status	Trust value stored to the PUBS
PU1	CA candidate	0.68
PU2	1st BCA candidate	0.6
SU1	CA candidate and works as CA	0.68
SU2	2nd BCA candidate and works as BCA	0.5
SU3	2nd BCA candidate	0.5
SU4	Works as normal node	0.4

Table 7.7: Example when both nodes have the same trust value

From Table 7.7, it can be clearly seen that SU1 and PU1 both have the highest trust value of 0.68 which is higher than the threshold value (0.5). Therefore, both are selected as a CA candidate. But currently, SU1 is working as the CA. Therefore, SU1 is selected as the CA according to Algorithm 2 and PU1 takes part in the next CA selection process, which by this time, it may have received a trust increment for its good behaviour in the network which, in turn, makes its trust value the highest which means it is selected as the CA. If SU1 was not working as the current CA, then PU1 is selected as the CA as it is a node from the primary network. On the other hand, SU2 and SU3 have the same trust value of 0.5 which is equal to the threshold. In this particular case, SU2 is selected as the second BCA as it is currently working as a BCA and SU3 takes part in the next BCA competition. In the next competition, there is a chance of a new updated trust value for SU3.

In the next section, the secure node joining and leaving process in the network is described which has an effect on the node's trust value update and,

in turn, results in the nodes taking part in the CA/BCA selection process.

7.4 Process of Secure Node Joining and Leaving the CRN and its Effect on Trust Value

In this section, the steps involved in the process of node joining and leaving the network in a secure way are described.

7.4.1 Secure joining the network and its effect on a node's trust value

The working steps in the secure process of joining the network and its effect on a node's trust value is as follows:

1. If a new node wants to join the CRN, it broadcasts a message to the network and waits until it receives a response, which is considered to be a normal joining event.

2. The new node produces its certificate using cryptography techniques and generates a random number and sends them to all member nodes in the network.

3. The new node's certificate is verified by all member nodes and the base station in order to give authorization for it to join the network.

4. After obtaining authorization from all the trusted member nodes and the base station, the new node joins the network, otherwise it cannot join

the network.

5. After successful joining the network, the joining node achieves some trust increment for its good and normal behaviour in the joining process.

6. If the new node sends many messages within a short period in order to join the network, this is an abnormal joining event as the broadcasting of numerous messages might result in the breakdown of normal network activity. If one node wants to join abnormally without following the policies of the joining process, the node's trust value is decreased by a certain amount.

The working steps of the joining process, including its effect on a node's trust value update is shown in Figure 7.6.

In order to explain the authentication process to join the network, the framework uses the following symbols:

New node's Certificate: C_N

Random Number generated by new node: R_N

Base Station's Certificate: C_{BS}

Random Number generated by new node: R_N

Numerical signature of Base Station to 'JOIN' message: $S_{BS}(JOIN)$

Numerical signature of New Node to message: $S_N(JOIN)$

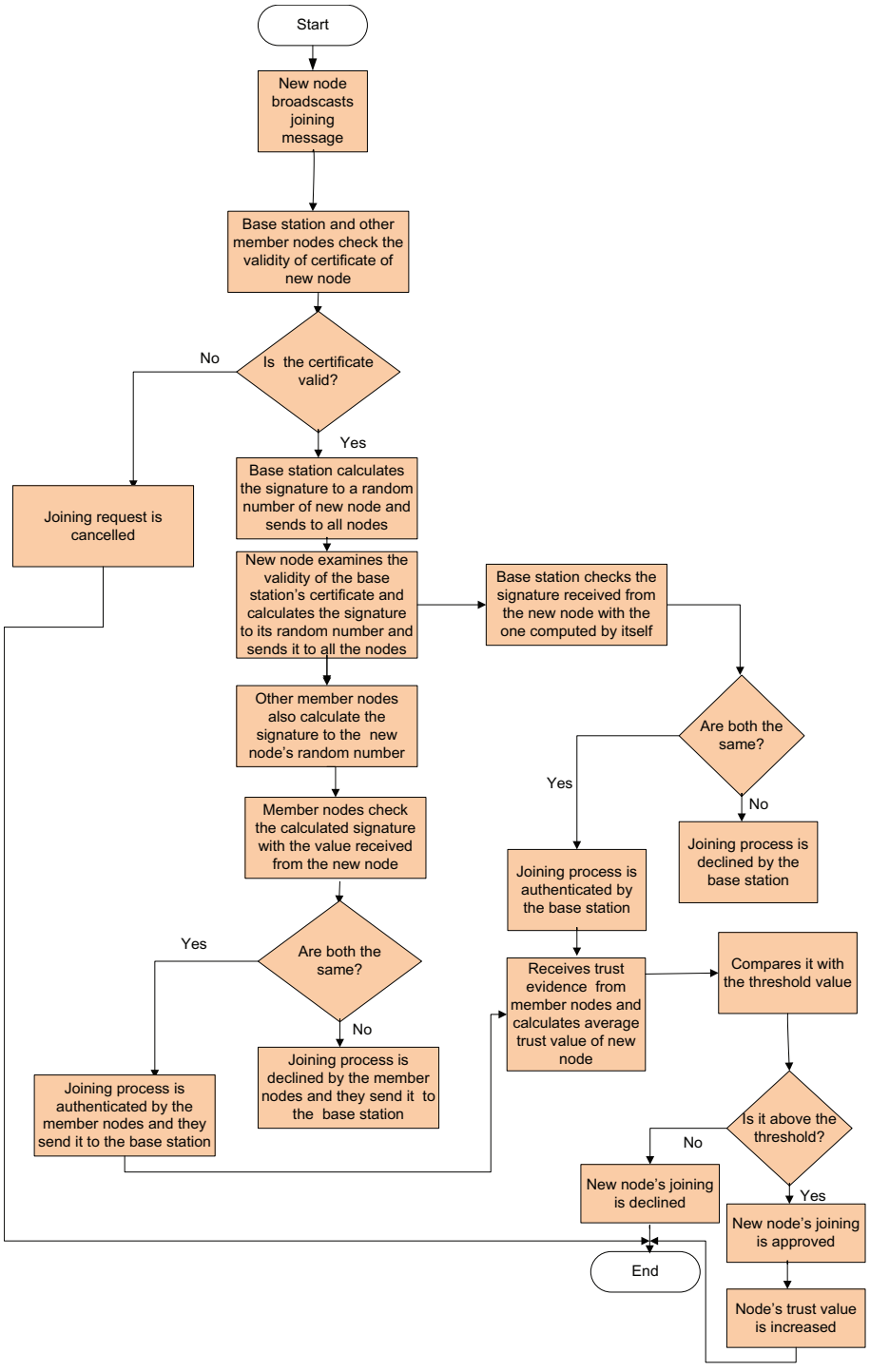

Figure 7.6: Working steps of the secure joining process in the NSSJL framework

In order to pass the authentication procedure for joining the CRNs, the following steps are followed by the new node:

1. The new node broadcasts its certificate and random number to all member nodes in the network as well as to its base station.

   $New\ Node \xrightarrow{Broadcast} > Node_{[All]} : C_N \parallel R_N$

2. The base station and the member nodes verify the validity of the new node's certificate.

3. The base station then produces random number R_{BS}, calculates the signature to R_N and sends it to all nodes.

   $BaseStation \xrightarrow{Broadcast} > Node_{[All]} : C_{BS} \parallel R_{BS} \parallel S_{BS}(R_N)$

4. A new node examines the validity of the base station's certificate C_{BS} and calculates the numerical signature $S_{BS}(R_N)$ for R_N and sends this to all member nodes.

   $NewNode \xrightarrow{Broadcast} > Node_{[All]} : S_N(R_{BS})$

5. The base station and other member nodes verify the numerical signature to R_N and broadcast the result to each other.

6. If the result from the base station node and the member nodes is same, each member node sends the message to the base station which informs the trust evidence of the new node as a trust value of 0.01.

7. The trust evidence indicates that the node is authenticated by the member nodes and the base station to join the network. The base station then calculates the trust value of the new node, depending on the trust

evidence assigned by each member node. In this way, the new node passes the authentication process to join the network. The joining node joins the network with an initial trust value using the following equation 7.6.

$$T_{new\ node}(p) = \left\{ \frac{1}{u} \sum_{i=1}^{u} T_i\,(p) \right\} \tag{7.6}$$

where u is the total number of member nodes in the network.

After successfully joining the network, the node's trust value is incremented by 0.05 according to the following equation 7.7 by the base station for its good behaviour, as shown in Table 7.8. This trust increment for successful joining will work for five consecutive joining process. Therefore, after that this particular node is considered as a highly trustworthy node to join the network securely and hence no further trust increment is required.

$$T_{node}(p) = T_{new\ node}(p) + 0.05 \tag{7.7}$$

Complying behaviour	Trust increment value	Uncomplying behaviour	Trust decrement value
Normal Joining	0.05	Abnormal Joining	0.05
Normal Leaving	0.05	Abnormal Leaving	0.05

Table 7.8: Behaviour-based event table

8. If the verification result of the numerical signature to R_N is not same

from the member nodes and the base station, then the member node and the base station relay the message to each other which informs that the total trust evidence of the new node is not authenticated enough to join the network.

The flow of the secure joining process between different nodes in the network is shown in Figure 7.7

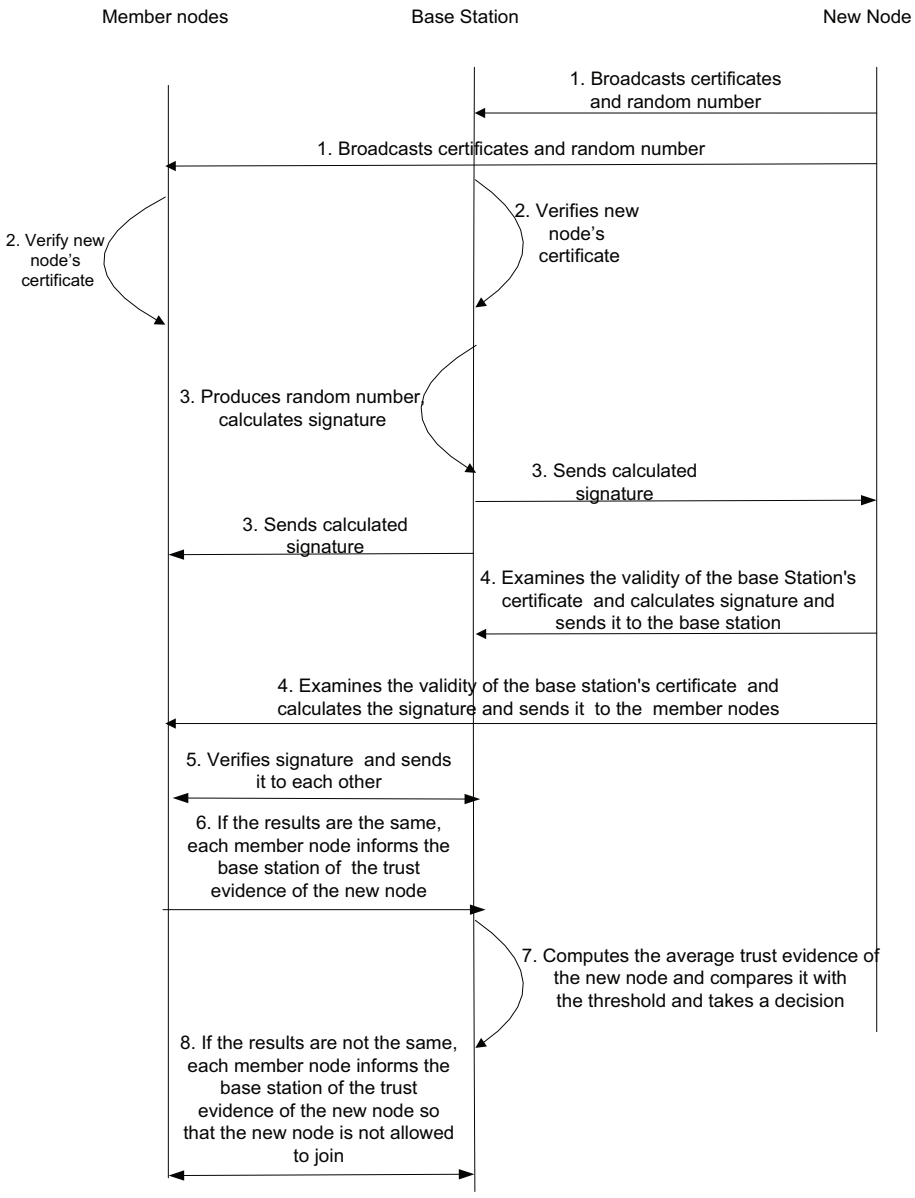

Figure 7.7: Flow of the secure joining process between different nodes in the network in the NSSJL framework

7.4.2 Secure leaving process from the network and its effect on the node's trust value

The working steps of the secure leaving process from the network and its effect on the node's trust value is as follows:

1. If a member sends a message to the base station before leaving the network, this is marked as a normal leaving event.

2. After verifying the leaving node's message, the leaving node is allowed to leave the network by the base station.

3. The base station sends a message to all of its member nodes not to communicate with the leaving node so that the leaving node cannot obtain any network information after it leaves the network.

4. The leaving node is given a trust increment for its good behaviour during the normal leaving process.

5. If the member node leaves the network without sending a prior message, this is an abnormal leaving event. If the node leaves the network abnormally, its trust value is decreased by a certain amount.

The working steps of the leaving process are shown in Figure 7.8.

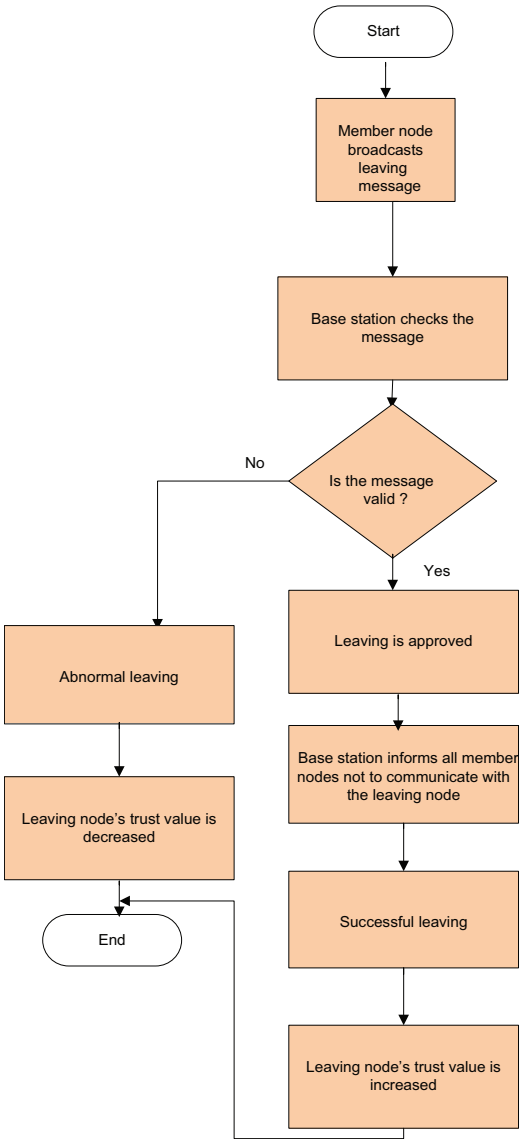

Figure 7.8: Working steps of the secure leaving process in the NSSJL framework

In order to explain the secure leaving process from the network to avoid any malicious behaviour, the framework uses the following steps:

1. The leaving member node signs its departing message and broadcasts the leaving information to all other member nodes and the base station.

2. The base station verifies the departing message from the leaving node and

if it is a valid departing message, the base station broadcasts a message to all other member nodes to revoke all the certificates issued to it and to stop communication with the leaving node.

3. The broadcast message from the base station will be authenticated by each member node.

4. The base station produces a new group key by using a key distribution algorithm and distributes it to all members. All member nodes use this new group key to communicate between themselves so that the leaving node cannot obtain any information later. After a node leaves the network, no valid certificate is attached to it any more. Hence, backward security is guaranteed.

   $Node_{[All]} \xrightarrow{Stop\ sharing\ keys} > Leaving\ Node$

   $Base\ Station \xrightarrow{new\ group\ key} > Node_{[All]}$

5. If the CA is a departing node, then the BCA will take on the role of the CA and sends about this new role to all member nodes. Then the new CA produces a new group shared key which is distributed to all base stations and other member nodes.

   $BCA \xrightarrow{Take\ Charge\ of\ CA} > Node_{[All]}$

   $New\ CA \xrightarrow{Shared\ New\ Group\ Key} > Node_{[All]}\ and\ Base\ Stations$

6. If these steps are followed by the leaving node, then the leaving node successfully leaves the network and is rewarded for its good behaviour. Therefore, its trust value is incremented by 0.05 by the base station for its complying behaviour; otherwise, its trust value is decremented by 0.05. The corresponding base station stores and informs the other member

nodes about this updated trust value of the leaving node. As a result of the trust increment for good behaviour, the leaving node can join other networks after leaving and can take part in the CA and BCA selection procedure. This trust increment for successful leaving will work for five consecutive leaving process. Therefore, after that this particular node is considered as a highly trustworthy node to leave the network securely and hence no further trust increment is required.

The flow of the secure node leaving process from the network is shown in Figure 7.9

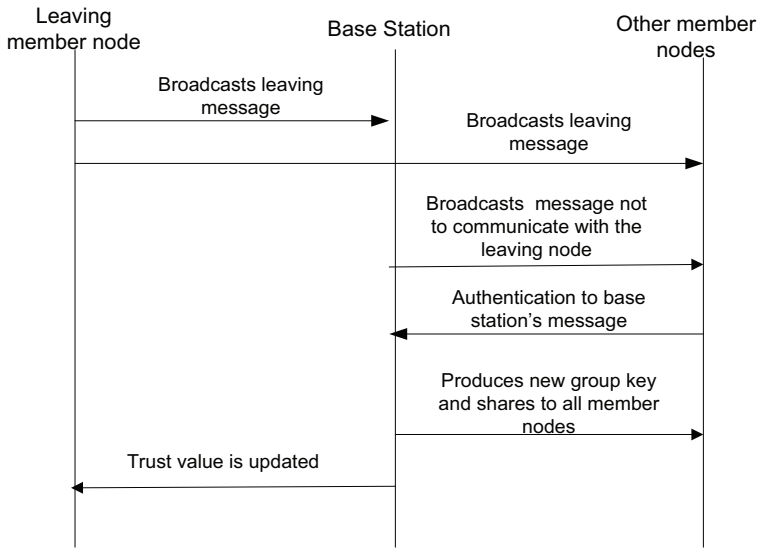

Figure 7.9: Flow of the secure node leaving process in the NSSJL framework

7.5 Enhancing the Availability of the CRN System using the NSSJL Framework

In this section, how the proposed NSSJL framework can enhance the availability and reliability of the system is explained. As described in Section

7.3, the system with a CA and multiple BCAs switches from the CA to the first BCA in response to the detection of an error to the CA or if the CA is biased by any other malicious nodes or is under attack, which thereby ensures continuous service for smooth communication in CRNs. Whenever a CA is under attack and its functionality is handed over to the BCA, the CA is considered a malicious CA and some reconfiguration techniques are applied to correct it. If the reconfiguration techniques work well for the CA, then the CA is reinstated from the BCA; otherwise, the CA has no more functionality in the network. This scenario is depicted in Figure 7.10. In this model, the multiple BCA system has one CA and a multiple BCA option.

To assist in the transition process from one CA to another BCA, it is assumed that each CA contains two extra functionalities: one for monitoring and the other for software reconfiguration. Furthermore, each CA has multi-states which facilitate the transition of the main CA to the BCA, once an error in the main CA has been detected. In order to enhance the availability of the system, each CA goes through different working states to hand over its functionality to another CA (BCA). In the next subsection, the different states in the framework of the proposed model are described.

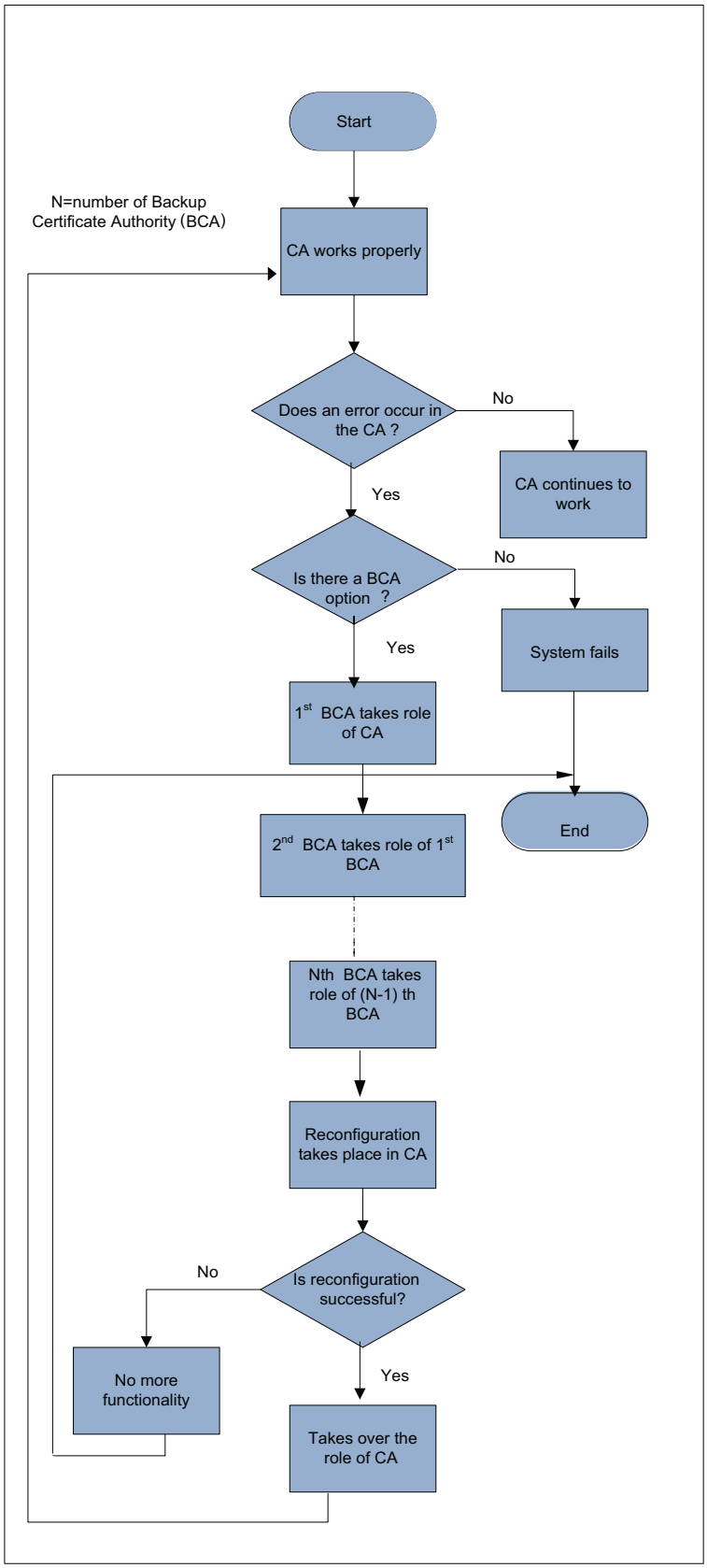

Figure 7.10: CA and BCA's cooperation to maintain smooth communication in CRNs

7.5.1 Defining multi-states in a CA and the transition between them

The five different states that a CA goes through in a multiple BCA framework are as follows:

Healthy state (H_i)***:*** A healthy state is one in which a CA is working as expected.

Unstable state (U_i)***:*** An unstable state is one in which a degradation in the performance of the CA has been detected.

Switchover state (S_i)***:*** The switchover state is one that exists before the reconfiguration process of the affected CA takes place.

Reconfiguration state (R_i)***:*** The reconfiguration state is one in which an attempt is made to restore the operation of the affected CA to its normal working state.

Failure state (H_0)***:*** If the reconfiguration process of the affected CA is unsuccessful, it enters the failure state.

It is assumed that at first, the main CA and the BCAs in the system are in the healthy state. If any error is detected in the main CA by the IDS (Intrusion Detection System), then its state will shift to the unstable state. The CA that has been affected and is under-performing is treated as a malicious CA. From the unstable state, the malicious CA will go to the switchover state to hand over the current functionalities to the first backup CA as shown in Figure 7.11. From the switchover state, the malicious CA will go to the reconfiguration state where an attempt is made to reconfigure it. If the reconfiguration techniques work well for the malicious CA, it will

take over from the BCA as the main CA; otherwise, the CA's activities will be performed by the BCA which now becomes the main CA and the malicious CA goes to the failure state. Algorithm 4 shows the transition process of the main CA from one state to another in the face of an error occurs in the CA for a multi-BCA-based framework.

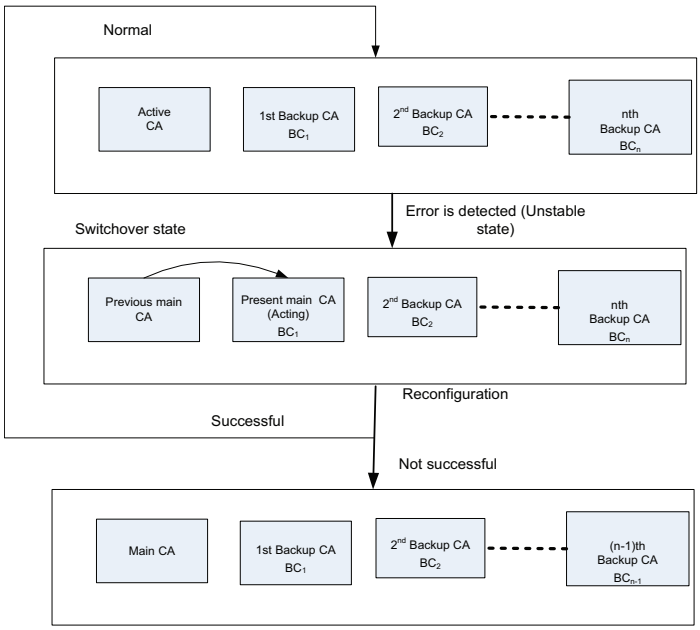

Figure 7.11: Multiple BCAs framework

In the proposed approach, it is assumed that the CA goes from one state to another when an event occurs. In the next subsection, to demonstrate the improvement in availability and reliability of CRN, the transition rates are defined to show how quickly the transition happens from one state to another which will cause the CA to change its state from the current one to another, accordingly.

Algorithm 4 State Transition Algorithm for the multiple BCA System
Input: Number of BCAs (n)
Output: Stable and secure system

The system counts the number of CAs.
if $n = 1$ **then**
if CA functions properly **then**
the system is secured and available
Go to 'Healthy state'
else
Go to 'Failure state'
end if
end if
if $n => 2$ **then**
for $j \leftarrow 2$ to $j \leq n$ **do**
if the jth backup functions properly **then**
the system is available
else
Go to 'Unstable state'
end if
Unstable state:
if $n \neq 1$ **then**
Go to 'Switchover state'
else
Go to step 'Reconfigure state'
end if
Switchover state:
$j = j + 1$
All active functions are transferred to jth BCA and
the system performs properly
Failure state:
The system does not perform any function
Reconfigure state:
if the system is reconfigured **then**
Go to 'Healthy state'
else
Go to 'Failure state'
end if
Healthy state:
The system performs properly
end for
end if

7.5.2 Defining the transition rates and probabilities of CAs being in different states

The transition rates that will change the state of the CA in the proposed model from the current one to another are: failure rate (λ), repair rate (μ), unstable rate (λ_u), and reconfiguration rate (λ_r). As the proposed model goes through many transitions from one state to another, it follows the Markov Chain model. The Markov chain model is a memoryless system with different possible states in which the future state of the system depends only on its present state and behaves accordingly. The change of a CA/BCA's state in the proposed model from one to another is clearly suitable to follow the Markov model. The Markov Chain state transition diagram with the multi-BCA framework is shown in Figure 7.12. In this model, it is assumed that there are n number BCAs and the system will transit from nth BCA to $n-1$th BCA and so on until to the first BCA.

According to the Markov Chain, the sojourn time in a state is always distributed exponentially. In the proposed multi-BCA framework, it is assumed that the main CA and all BCAs at first are in a healthy state (H_i), but the main CA could become malicious. At that time, the main CA's state may change from the healthy state to the unstable state at a rate of ($i * \lambda_u$). In the unstable state, the main CA performance is degraded and it has to be reconfigured. When the CA is about to be reconfigured, the state of the malicious CA may change from the unstable state to the switchover state at a rate of ($i \times \lambda_s$). In this state, the first BCA will take on the role of the main CA and continue to perform the required computations of the system. The malicious CA may change from the unstable state to the reconfiguration state

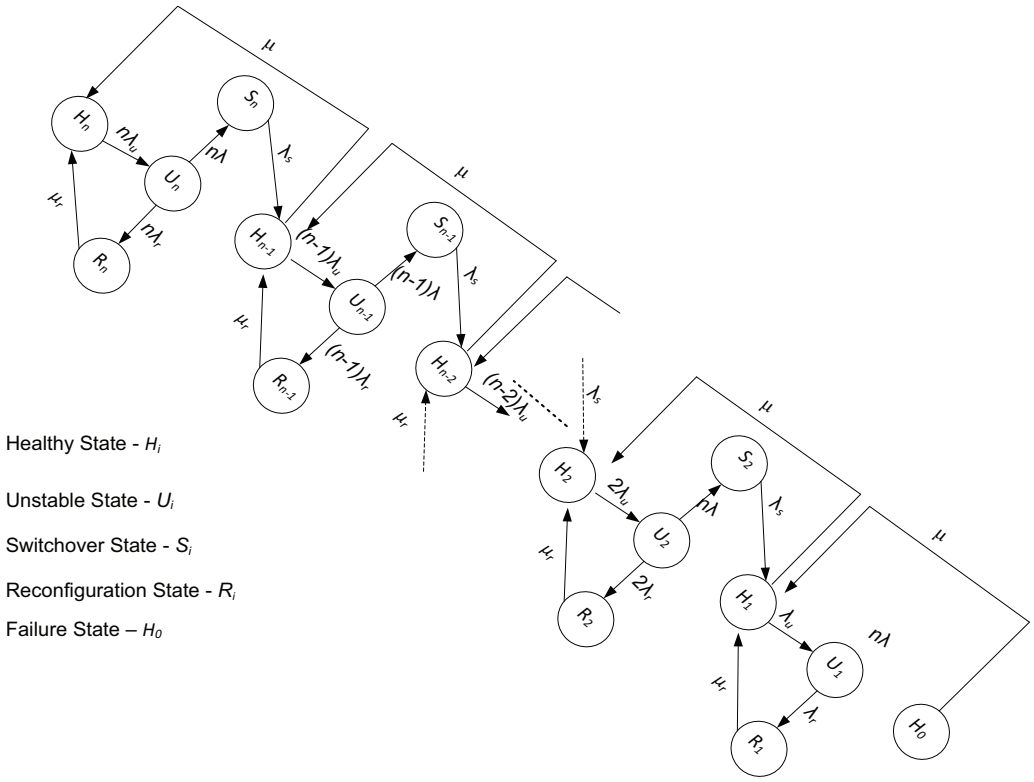

Figure 7.12: Multi-BCA model using Markov Chain

at a rate of $(i \times \lambda_r)$.

The steady-state probability which shows the probability of the proposed model being in each state is as follows:

Probability of being in the healthy state (H_i): $\sum_{i=1}^{n} P_{H_i}$

Probability of being in the unstable state (U_i):$\sum_{i=1}^{n} P_{U_i}$

Probability of being in the reconfiguration state (R_i):$\sum_{i=1}^{n} P_{R_i}$

Probability of being in the switchover state (S_i):$\sum_{i=2}^{n} P_{S_i}$

Probability of being in the failure state (H_0): P_{H_0}

where n is the number of BCAs.

Based on the steady-state probabilities, it is possible to determine the probability of being in each state for the model with the CA and multiple

BCAs. The probability of being in each state is measured by using the transition rates from one state to another state in the proposed multiple BCAs framework. For every state, the incoming rate is equal to the outgoing rate according to the Markov chain model. The steady state balance equation for the CA and each BCA of the proposed model being in a healthy state is as follows:

For state H_0, the incoming rate equals the outgoing rate as follows:

$$\mu P_{H_o} = \lambda P_{U_1} \tag{7.8}$$

For state H_1, the incoming rate is equal to the outgoing rate as follows:

$$(\mu + \lambda_U) P_{H_1} = \lambda_s P_{s_2} + \mu_r P_{R_1} + \mu P_{H_o} \tag{7.9}$$

For state H_2, the incoming rate is equal to the outgoing rate as follows:

$$(\mu + 2\lambda_U)\, P_{H_2} = \lambda_s P_{s_4} + \mu_r P_{R_2} + \mu P_{H_1} \tag{7.10}$$

For state H_3, the incoming rate is equal to the outgoing rate as follows:

$$(\mu + 3\lambda_U)\, P_{H_3} = \lambda_s P_{s_4} + \mu_r P_{R_3} + \mu P_{H_2} \tag{7.11}$$

For state H_i $(i = 2, 3, \ldots\ldots..n-1)(n \geq 3)$, the incoming rate is equal to the outgoing rate as follows:

$$(\mu + i\lambda_U) P_{H_i} = \lambda_s P_{s_{i+1}} + \mu_r P_{R_i} + \mu P_{i-1} \tag{7.12}$$

The steady state balance equation for the CA and each BCA of the proposed

model being in an unstable state is as follows:

For state U_i $(i = 1, 2, 3, ...n)$, the incoming rate is equal to the outgoing rate as follows:

$$i\lambda_U P_{H_i} = (i\lambda + i\lambda_r)P_{U_i} = (\lambda + \lambda_r)P_{U_i} \tag{7.13}$$

The steady state balance equation for the CA and each BCA of the proposed model being in a switchover state is as follows:

For state S_i $(i = 2, 3, ..n)$, the incoming rate is equal to the outgoing rate as follows:

$$\lambda_s P_{s_i} = i\lambda P_{U_i} \tag{7.14}$$

The steady state balance equation for the CA and each BCA of the proposed model being in a reconfiguration state is as follows:

For state R_i $(i = 1, 2, 3, ..n)$, the incoming rate is equal to the outgoing rate as follows:

$$\mu_r P_{R_i} = i\lambda_r P_{U_i} \tag{7.15}$$

The conservation equation is obtained by summing all the probabilities of every state in the system and the summation is equal to 1.

$$\sum_{i=0}^{n} P_{H_i} + \sum_{i=0}^{n} P_{U_i} + \sum_{i=0}^{n} P_{R_i} + \sum_{i=0}^{n} P_{S_i} = 1 \tag{7.16}$$

Combining this conservation equation with the balanced equations above, and solving them, the closed-form solutions are obtained being in a healthy state in one-CA and multi-BCA models. In the next subsection, using the Markov Chain transition diagram, the probability of the proposed model

being in a healthy state when there are multiple BCAs compared to when there is one CA is determined.

7.5.3 Determining the probability of the system being in a healthy state

7.5.3.1 Probability of the system being in a healthy state in a single-CA system ($n = 1$)

In this system, only one CA exists and performs the system's required functionalities as shown in Figure 7.13. As there are no backup CAs, the switchover state is not represented.

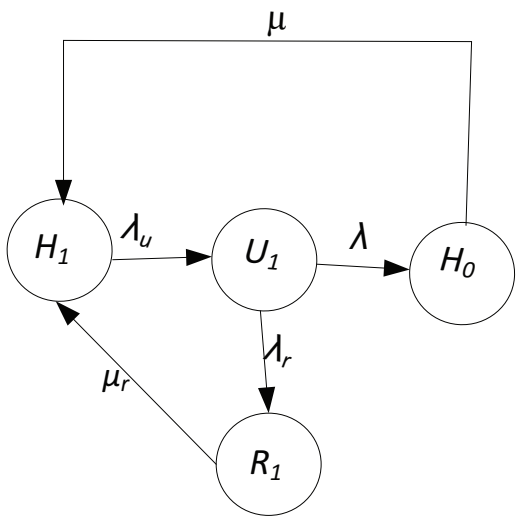

Figure 7.13: Single-CA system

The probability of a single-CA system entering a healthy state is:

$$P_{H_1} = \left[1 + \frac{\lambda_u}{\lambda + \lambda_r}(1 + \frac{\lambda_r}{\mu_r} + \frac{\lambda}{\mu})\right]^{-1} \tag{7.17}$$

7.5.3.2 Probability of the system being in a healthy state in a multi-BCA System ($n >= 2$)

The multi-BCA system consists of the active CA and the (n-1) backup CAs.

$$P_{H_n} = [A + B + C + D + E]^{-1} \tag{7.18}$$

where

$$A = n!\{\sum_{i=1}^{n} \frac{1}{i!}\left(\frac{\lambda}{\mu}\frac{\lambda_u}{\lambda + \lambda_r}\right)^{n-i}$$

$$B = \frac{\lambda_u}{\lambda + \lambda_r}\sum_{i=1}^{n} \frac{1}{i!}\left(\frac{\lambda}{\mu}\frac{\lambda_u}{\lambda + \lambda_r}\right)^{n-i}$$

$$C = \frac{\lambda_r}{\mu_r}\frac{\lambda_u}{\lambda + \lambda_r}\sum_{i=1}^{n} \frac{1}{(i-1)!}\left(\frac{\lambda}{\mu}\frac{\lambda_u}{\lambda + \lambda_r}\right)^{n-i}$$

$$D = \frac{\lambda}{\lambda_s}\frac{\lambda_u}{\lambda + \lambda_r}\sum_{i=1}^{n} \frac{1}{(i-1)!}\left(\frac{\lambda}{\mu}\frac{\lambda_u}{\lambda + \lambda_r}\right)^{n-i}$$

$$E = \left(\frac{\lambda}{\mu}\frac{\lambda_u}{\lambda + \lambda_r}\right)^{n}$$

The probability of a multi-BCA system entering a healthy state is:

$$P_{H_i} = \frac{n!}{i!}\left(\frac{\lambda}{\mu}\frac{\lambda_u}{\lambda + \lambda_r}\right)^{n-i} P_{H_n}, (i = 0, 1, 2, \ldots..n)\,, \tag{7.19}$$

The probability of a multi-BCA system entering an unstable state is:

$$P_{U_i} = \left(\frac{\lambda_u}{\lambda + \lambda_r} \right) P_{H_n} \left(i = 1, 2, \ldots..n \right), \tag{7.20}$$

The probability of a multi-BCA system entering a reconfiguration state is:

$$P_{R_i} = \frac{i\lambda_r}{\mu_r} \frac{\lambda_u}{\lambda + \lambda_r} P_{H_n} \left(i = 1, 2, \ldots..n \right), \tag{7.21}$$

The probability of a multi-BCA system entering a switchover state is:

$$P_{S_i} = \frac{i\lambda}{\lambda_s} \frac{\lambda_u}{\lambda + \lambda_r} P_{H_n} \left(i = 2, 3, \ldots..n \right), \tag{7.22}$$

The probability of being in a healthy state is much higher in a multi-BCA system than a single CA system. Therefore, the system with multi-BCAs is more available than a system with a single CA. The different metrics which are utilized for measuring the improvement in the performance of the system using the multi-BCA framework is described in the next subsection.

7.5.4 Criteria to evaluate the availability of the CRN

7.5.4.1 Availability

Availability refers to the system's continual functionality. With the proposed approach, availability is ensured by having multiple BCAs. Whenever the main CA is not performing as required, the first BCA will take on the role of the main CA. In this way, the whole system is available even though the main CA is not functioning. In the proposed model, service from the system is not available in the reconfiguration state (R_1) or the failure state (H_0). Therefore,

system availability in the steady-state is determined as follows:

$$Availability(A) = 1 - Unavailability = 1 - (P_{H_o} + P_{R_1}) \tag{7.23}$$

7.5.4.2 Downtime and downtime cost

When the system goes down, no service is provided and no output is received; this situation is termed 'downtime'. With the proposed multi-BCA model depicted in Figure 7.1, whenever a CA is not performing as expected, there will inevitably be some business costs due to the service being unavailable during downtime and during the reconfiguration of the system. If the main CA is suddenly turned off due to service failure, there will be a cost which is higher than the anticipated shutdown cost. (C_f) is the unit cost of CA for an unexpected shutdown and (C_r) is the cost due to reconfiguration when the CA is not available to provide the service. Therefore, the expected downtime and downtime cost are determined as follows:

$$Downtime = (P_{H_o} + P_{R_1}) \times T \tag{7.24}$$

$$Downtime\ Cost = (P_{H_o} \times C_f + P_{R_1} \times C_r) \times T \tag{7.25}$$

where T is the operational time.

7.5.4.3 Reliability

Reliability is defined as the probability that a system can perform its task at a given point of time. According to the proposed approach, reliability is maintained by using multiple BCAs because it can then provide continuous

service by having multiple BCA options. In the proposed model depicted in Figure 7.1, the system is able to provide continuous service until it enters the failure state, so reliability is defined as :

$$Reliability = (1 - P_{H_0}) \tag{7.26}$$

7.5.4.4 Trustworthiness

Trustworthiness is defined as a function of reliability and availability of a system. If a system has high reliability and high availability, then it is called a trustworthy system. According to the proposed approach, high reliability and high availability is maintained by using multiple BCAs because it can then provide continuous service by having multiple BCA options. Therefore, the trustworthiness of a system is defined as :

$$Trustworthiness \ \ of \ \ a \ system, T = f(A, R) = A * R \tag{7.27}$$

where A represents the availability and
R represents the reliability.

In the next section, first the verification of the NSSJL framework is demonstrated to select the CA and BCA nodes and then different criteria are evaluated to show how the proposed NSSJL framework can enhance system availability and reliability and decrease the downtime cost.

7.6 Verification Results and Discussion

In this section, the verification results are categorized into three sections:

1. Firstly, the proposed NSSJL framework is verified to select the CA and BCA nodes in the CRN.

2. Secondly, the proposed NSSJL framework is verified to show the effect of secure node joining and leaving the network which, in turn, causes the nodes to be selected as the CA and the BCA as a result of their trust increment depending on their good behaviour.

3. Thirdly, different criteria are verified to show how the NSSJL framework can enhance system availability and reliability.

For verification purposes, a system is made using the NSSJL framework and is programmed using the same programming environment as discussed in Section 5.7. Later on, the MATLAB programming tool is used to evaluate the results using the trust data generated from the JAVA environment. For verification purposes, two networks (the primary network and the secondary network) have been considered in CRNs and each network has three member nodes and their corresponding base station. Therefore, there are six member nodes (SU1, SU2, SU3, PU1, PU2, PU3) and two base stations in the network. It is assumed that all the member nodes are distributed according to the 1-hop fashion. Each node calculates its 1-hop neighbor node's trust value and sends it to the PUBS. Thus, the process of trust calculation is computed only by the PUBS. The verification steps are as follows:

7.6.1 Selection of the CA and BCA from the member nodes in CRNs

Each node has different activities with other nodes. First, the trust value of each member node from the other five member nodes is calculated using the trust calculation method described in Section 7.3.1 for 100 different activities. Suppose node 1 has 100 activities with node 2, node 3, node 4, node 5 and node 6. Therefore, node 2 assigns 100 trust values for node 1. In the same way, node 2, node 3, node 4, node 5, and node 6 assign 100 trust values for node 1. So, 100 trust values are produced for one node for 100 activities from the five other nodes. Figure 7.14 shows 100 different trust values of node 1 for 100 different activities with the other five nodes in the network.

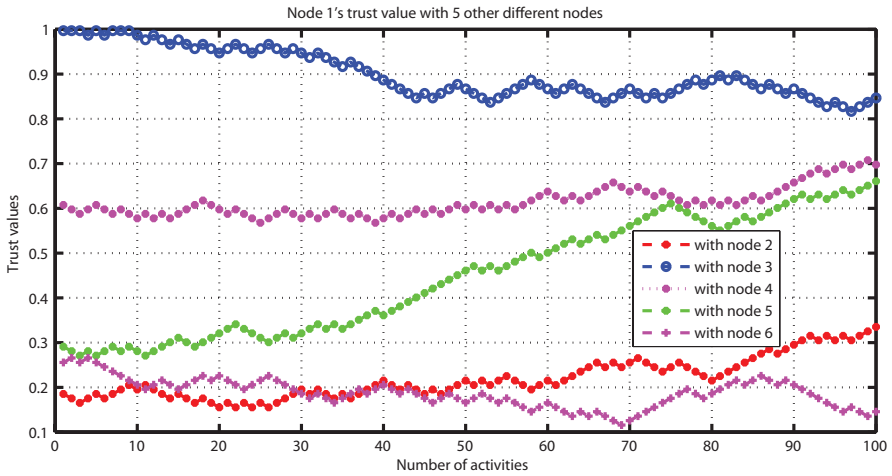

Figure 7.14: Node 1's trust value with the other five nodes in the NSSJL framework

Figure 7.15 shows 100 different trust values of node 2 for 100 different activities with the other five nodes in the network.

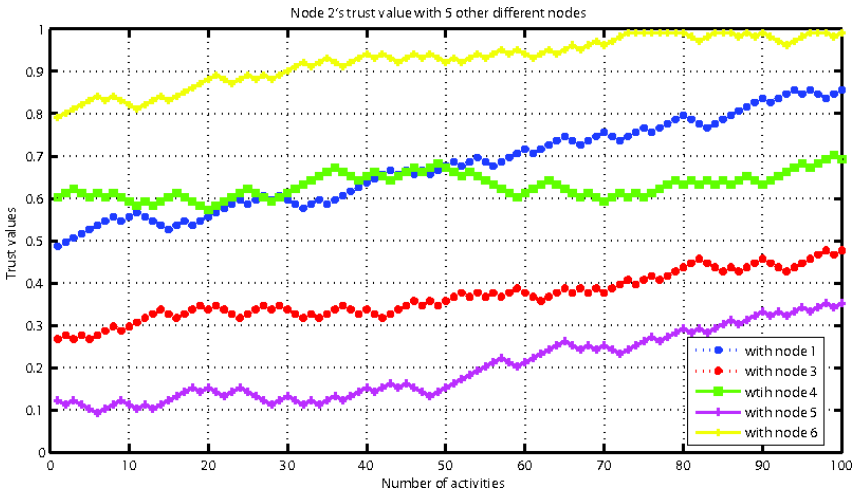

Figure 7.15: Node 2's trust value with the other five nodes in the NSSJL framework

Figure 7.16 shows 100 different trust values of node 3 for 100 different activities with the other five nodes in the network.

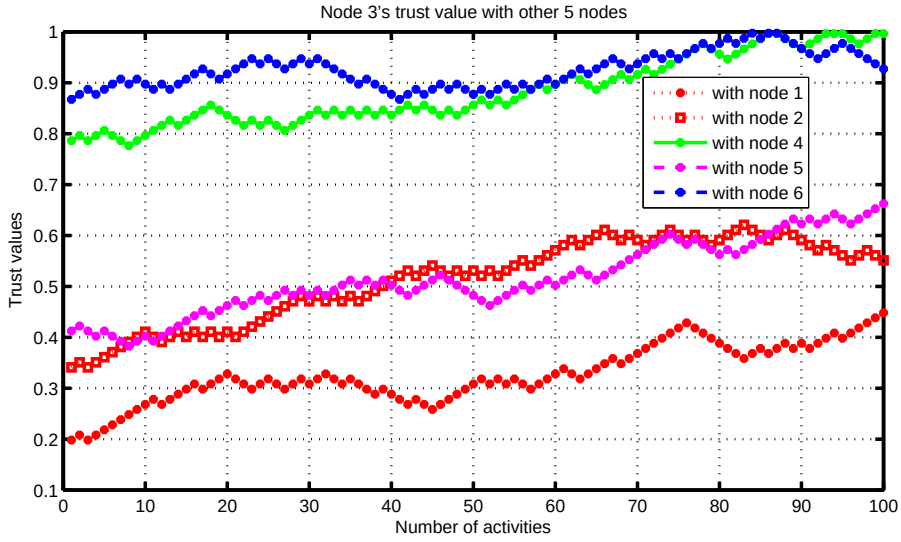

Figure 7.16: Node 3's trust value with the other five nodes in the NSSJL framework

Figure 7.17 shows 100 different trust values of node 4 for 100 different activities with the other five nodes in the network.

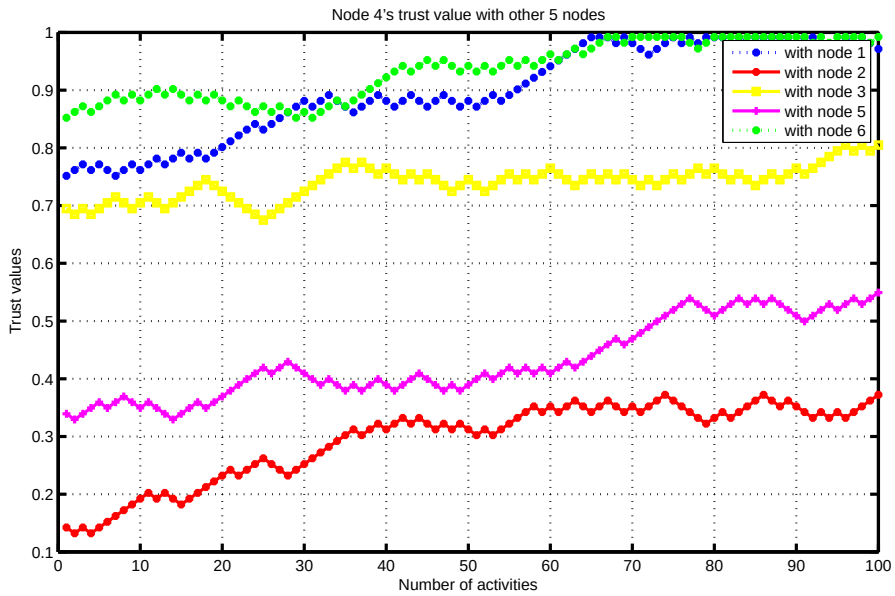

Figure 7.17: Node 4's trust value with the other five nodes in the NSSJL framework

Figure 7.18 shows 100 different trust values of node 5 for 100 different activities with the other five nodes in the network.

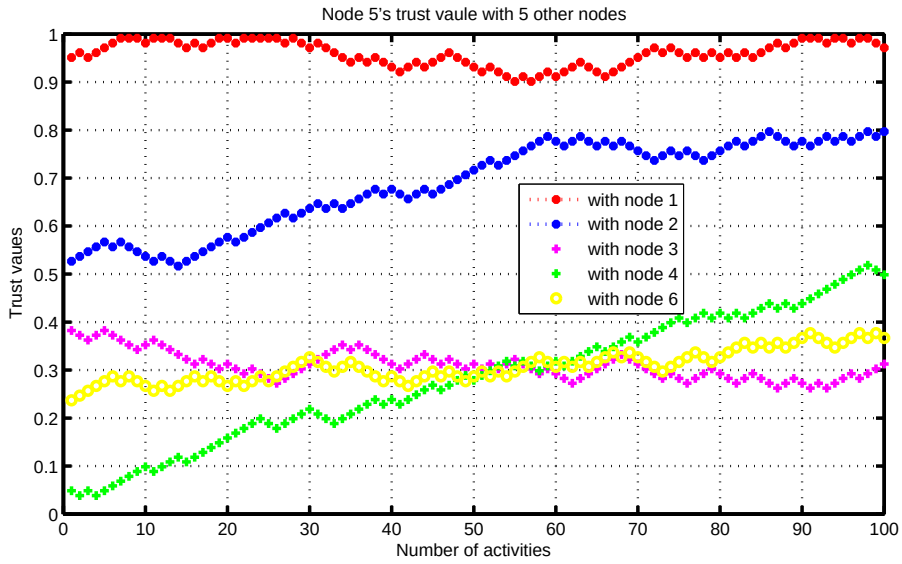

Figure 7.18: Node 5's trust value with the other five nodes in the NSSJL framework

Figure 7.19 shows 100 different trust values of node 6 for 100 different activities with the other five nodes in the network.

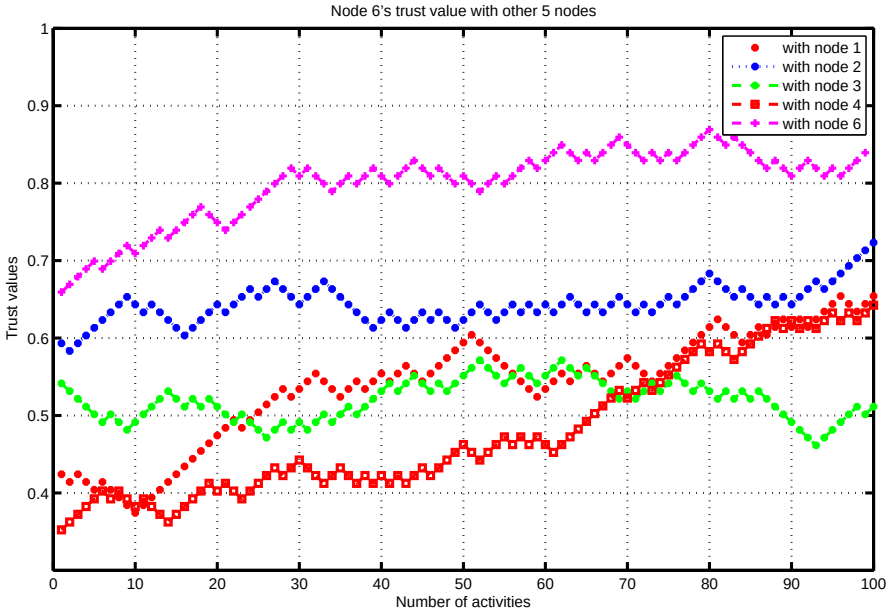

Figure 7.19: Node 6's trust value with the other five nodes in the NSSJL framework

Each node's trust value is evaluated by the other five member nodes depending on these 100 activities and the node's final trust value in the framework using equations 7.2 and 7.3, respectively, is summarized in Table 7.9. In this table, '0' represents the node's trust value computed by itself as a node cannot compute its own trust value.

Node Number	Evaluated by						Final trust value	Decision from PUBS
	Node 1 (SU1)	Node 2 (SU2)	Node 3 (SU3)	Node 4 (PU1)	Node 5 (PU2)	Node 6 (PU3)		
Node 1 (SU1)	0	0.2187	0.89932	0.6135	0.44821	0.1875	0.473	Normal node
Node 2 (SU2)	0.6759	0	0.3671	0.630116	0.1994	0.9255	0.55	3rd BCA
Node 3 (SU3)	0.3267	0.5130	0	0.8824	0.5155	0.9250	0.63	1st BCA
Node 4 (PU1)	0.8986	0.2945	0.7403	0	0.4331	0.9351	0.66	CA
Node 5 (PU2)	0.9722	0.5266	0.3824	0.2813	0	0.3071	0.38	Normal node
Node 6(PU3)	0.5387	0.6412	0.5202	0.4782	0.7928	0	0.59	2nd BCA

Table 7.9: Each member node's trust value

From Table 7.9, it can be seen that node 4's final trust value in the network is 0.66 and it is above the threshold (0.5), therefore this node is selected as the CA by the PUBS. For node 3 and node 6, their trust values are 0.63 (the second highest trust value) and 0.59 (the third highest trust value), respectively and both are above the threshold value, so node 3 is selected as the first BCA and node 6 is selected as the second BCA. For the case of node 1 and node 5, both of their trust value is below the threshold value, so they work as normal nodes in the network.

7.6.2 Secure node joining and leaving process which affects the node's trust value

It is assumed that one joins the network after successfully passing the authentication process described in Section 7.4. In this verification, only the node's trust value updates after secure node joining is shown. In other words, it is shown how the trust value of a new joining node is updated for its normal behaviour. It is assumed that node 7 wants to join the network as an SU. The trust evidence calculated by the SUBS from the successful joining process is

0.03, as there are three member nodes in the secondary network and each node assigns 0.01 as a trust evidence to the new node for passing the authentication to join the network. So, the new node is authenticated from the base station and member nodes to join the network as an initial trust value of 0.03 as shown in Figure 7.20 and after joining its trust value is incremented by 0.05 for its good complying behaviour as shown in Figure 7.21. Therefore, after joining, the new node's trust value is 0.08 (0.03+0.05=0.08).

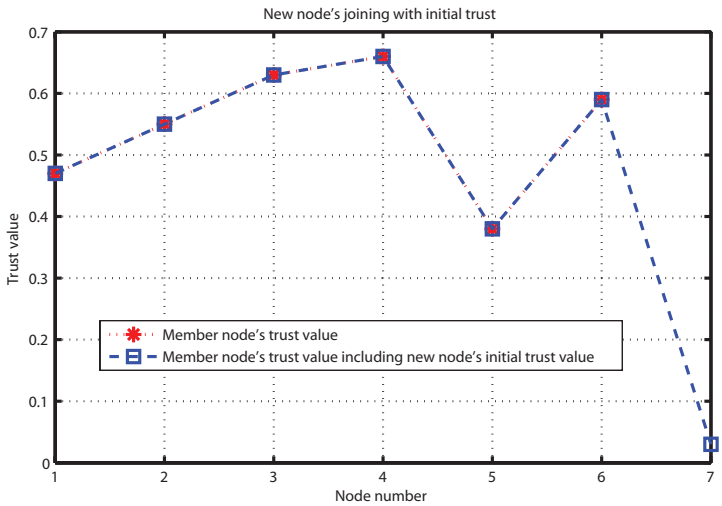

Figure 7.20: Trust value of member nodes during the joining process to the network

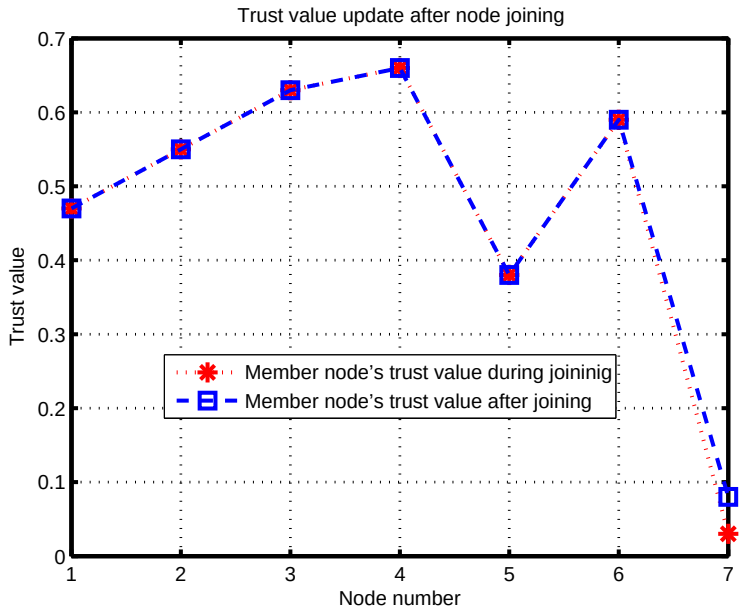

Figure 7.21: Trust value of member nodes after new node's trust value is updated for the successful joining of the NSSJL framework

In relation to secure leaving process verification, it is shown that the trust value of the leaving node is updated according to its normal or abnormal behaviour. It is assumed that node 4 wants to leave the network using the abovementioned leaving process. So, after leaving the network, its trust value is incremented as shown in Figure 7.22. From this figure, it can seen that node 4's trust value is increased from 0.66 to 0.71 as it receives a trust increment of 0.05 after successfully leaving, due to its good behaviour.

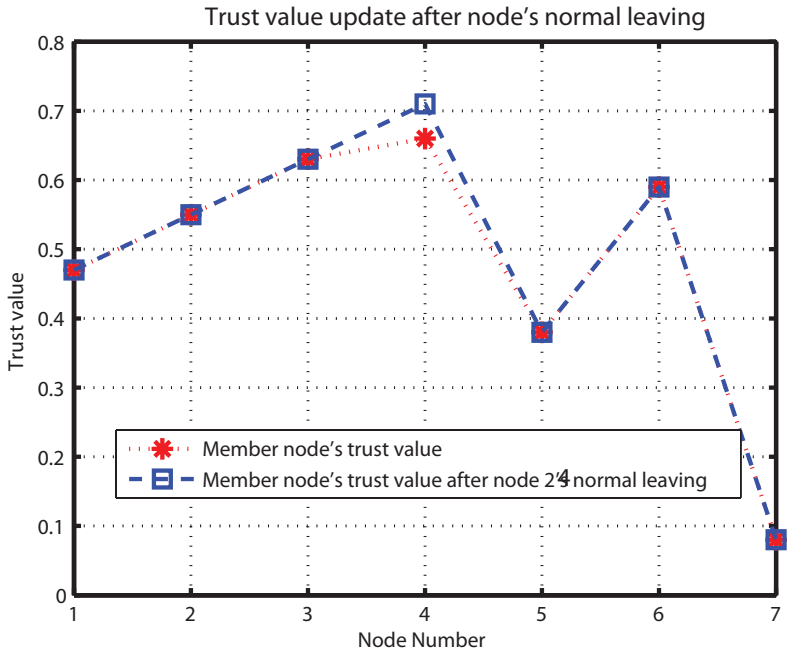

Figure 7.22: Trust value increased after normal leaving in the NSSJL framework

Node 2 wants to leave the network but it did not send any message. Rather, it simply left the network without informing to any other member node. Therefore, its trust value is decreased from 0.55 to 0.50 as it receives a trust decrement of 0.05 for its abnormal behaviour as shown in Figure 7.23.

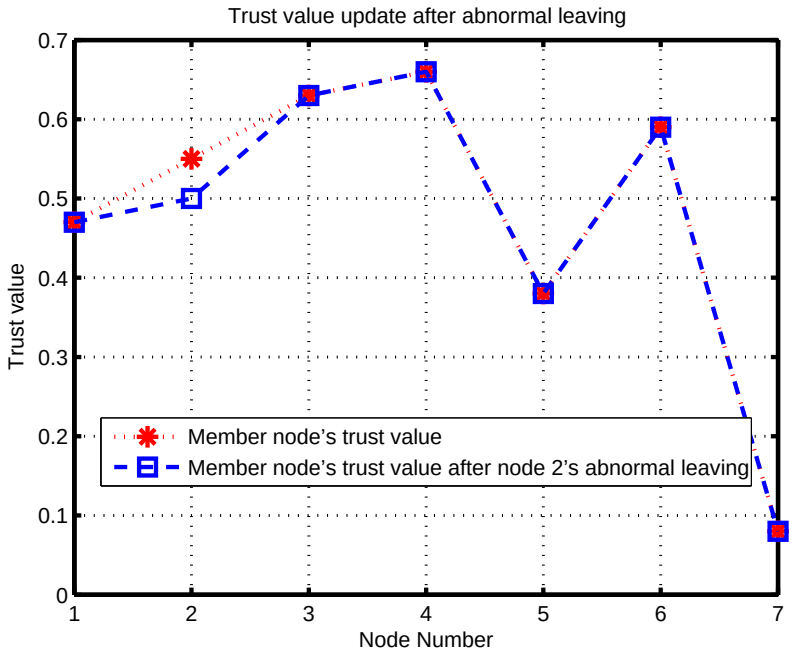

Figure 7.23: Trust value decreased after abnormal leaving in the NSSJL framework

7.6.3 System availability and reliability enhancement in CRNs using the NSSJL framework

In this subsection, examples are given to show the applicability of the NSSJL framework for enhancing system availability, reliability and other parameters. A good estimate value for a range of model parameters is used from [46], [130] to demonstrate the framework. It is assumed that the system using the NSSJL framework is operated for two months, continuously. The mean time between two consecutive failures is two months and the repair rate is two hours. A healthy CA becomes unstable once every seven days. The reconfiguration time and switchover time are 2 minutes and 1 minute, respectively. The number of operational CAs varies from simplex (n=1) to multiplex (n=4). In a single-CA system, there is one active CA. In a system with more than one CA, there is

one active CA and the others are backup CAs and it is called a multi-BCA system. One CA in the system means that there is only one CA in the system and no BCA option. Two CAs in the system means that there is one CA and 1 BCA in the system. Three CAs in the system means that there is one CA and two BCAs. Four CAs in the system means that there is 1 CA and 3 BCAs. Furthermore, it is assumed that the unexpected downtime cost per unit is 100 times greater than the anticipated reconfiguration cost.

7.6.3.1 Availability analysis

The change in the availability of the system with different numbers of CAs and the number of times it has been reconfigured (reconfiguration rate) when the main CA goes to the unstable state, is plotted in Figure 7.24.

As mentioned earlier, it is assumed that a healthy CA becomes unstable once a week and reconfiguration techniques are applied to it as soon as it enters the unstable state. However, it is possible that even after the reconfiguration process is applied, the availability of the system may not increase to the required level. So, reconfiguration is repeated to the malicious CA to see the effect on the system's availability.

It is observed that for a single-CA system, whenever the system enters the unstable state once a week, it is necessary to reconfigure the system four times to obtain high availability. As there is only one active CA, during the reconfiguration state, the system's service may be unavailable, so a low level of availability (zero availability) of the system is achieved at first as shown in 7.24. By performing repeated reconfiguration, it is observed that system availability increases if the malicious CA is not forced offline and is performing in a degraded mode.

For a multi-BCA system, whenever the main CA goes to an unstable state and reconfiguration takes place within the main CA, the system's operation is performed by the first BCA. So, the system availability is always higher compared to that of a single-CA model. It is also observed that in a multi-BCA system, the availability of the system increases with an increase in the number of reconfigurations.

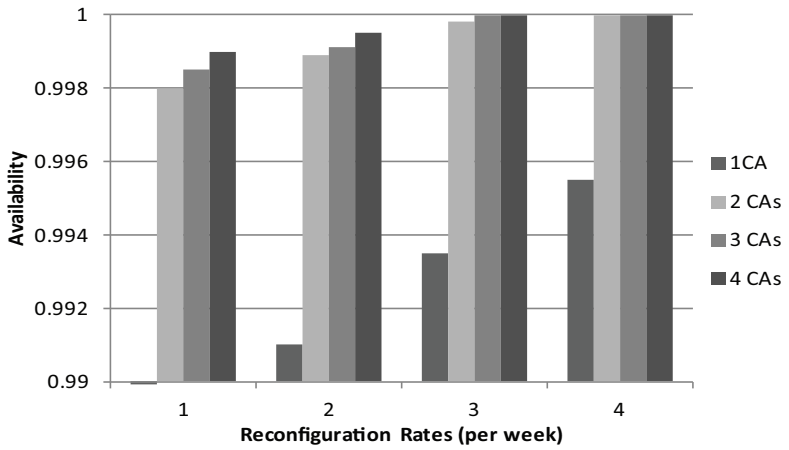

Figure 7.24: Availability vs. different reconfiguration rates for different numbers of CAs

Reconfiguration time (i.e. the time it takes to reconfigure) also has an effect on the availability of the system, as shown in Figure 7.25. The figure shows that if the system is removed from an unstable state with a short reconfiguration time, the availability of the system is increased. For a single-CA system, the system's service is temporarily unavailable whenever the CA is reconfigured, and if it takes a long time to reconfigure, the system's service is unavailable until reconfiguration is completed. It can be clearly seen that if the reconfiguration time for a single CA system is increased, the system's availability is decreased. By contrast, when the main CA in a multi-BCA system is reconfigured, the system's functionalities are transferred to the BCA.

The system's service is always available in a multi-BCA system even when the reconfiguration of a CA takes a long time, because the service is performed by the BCA.

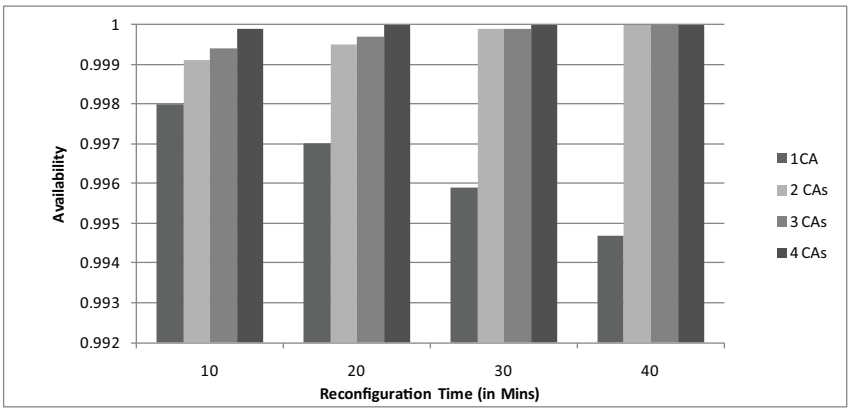

Figure 7.25: Availability vs. different reconfiguration time for different numbers of CAs

From Figures 7.24 and 7.25, it is noticeable that the increment in the level of availability from one CA to two CAs is significant, compared to having two CAs to three CAs. Clearly, if more than one CA is as BCA, the availability of the system increases sharply. In Figure 7.26, the steady-state availability of the system, based on the number of failures and the reconfiguration applied to it per week is plotted. The parameters that are used are λ (failure rate)= 2 time/week and λ = 3 time/week, and note that with an increased number of reconfigurations with rate λ_r=0 (no reconfiguration) to λ_r=5 in a week, the availability of the system increased. The result shows that, if the failure rate is high, reconfiguration should be performed frequently so that the system remains in a healthy state.

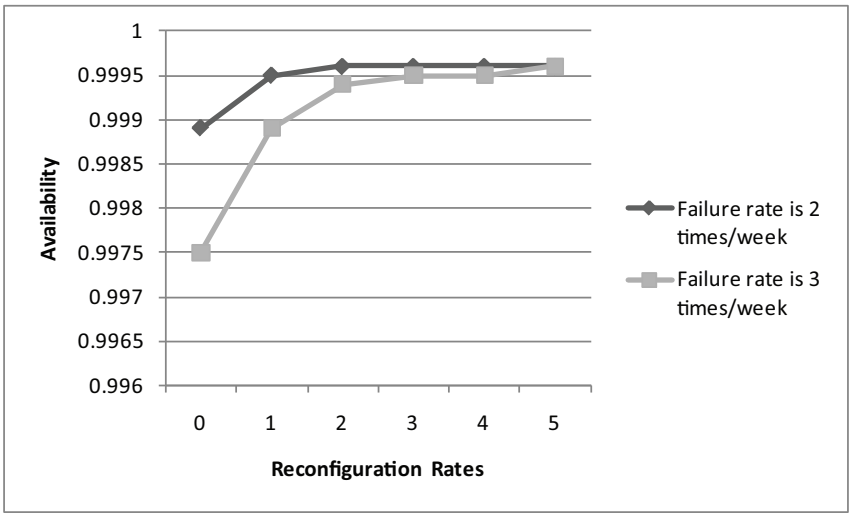

Figure 7.26: Availability vs. different reconfiguration times and different failure rates

7.6.3.2 Downtime cost analysis

Figure 7.27 shows the plot of downtime cost versus different reconfiguration rates and the different numbers of CAs. Here, it is assumed that the average cost of downtime due to failure (C_f) and reconfiguration (C_r) are 100 units and 50 units, respectively. If the main CA is suddenly offline due to service failure or an attack, the cost will be higher than the planned shutdown cost. The downtime cost is calculated using equation 7.25 for an operation time of 1 month = (30*24*60) mins= 43200 mins. This figure demonstrates that if only one CA is used for the proposed system, the downtime cost is high because if the CA is suddenly turned off, the whole system will fail and a high level of reconfiguration cost will be incurred. If there is more more than one CA in the system like the multiple BCA system, however, and a malfunction is detected, all operations will be shifted to the BCA and the main CA will be shut down. In this case, the affected CA can be taken offline according to a plan whereby the cost will be much less than if it were to unexpectedly go offline with no

backup.

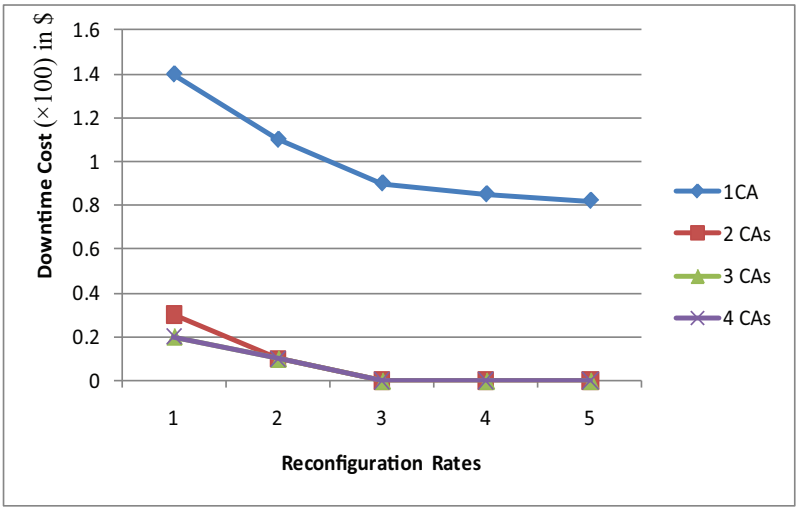

Figure 7.27: Downtime cost vs. different reconfiguration rates for different numbers of CAs

7.6.3.3 Reliability analysis

From Figure 7.28, it can be seen that if more than one CA is used, the system's reliability increases. If there is only one CA in the system, the system is not available while the reconfiguration takes place. Moreover, if there is a sudden computing failure in the main CA before reconfiguration takes place, the whole system will collapse and the system's reliability will decrease. In contrast, if there is more than one CA in the system like the multiple BCA system, the BCAs always provide service to the system though the main CA goes for reconfiguration. So, the system with multiple BCAs is always available because if malfunction is detected in the main CA, the system's operation is transferred to the BCA and the system is able to give continuous service without any interruption. In this case, the system is more reliable.

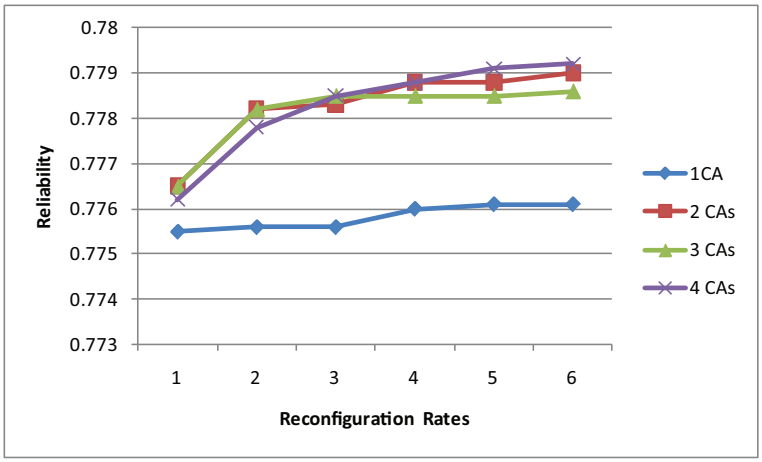

Figure 7.28: Reliability vs. different reconfiguration rates

7.6.3.4 Trustworthiness analysis

From Figure 7.29, it can be seen that if more than one CA is used, the system's trustworthiness increases. If there is only one CA in the system and there is a sudden computing failure in the main CA before reconfiguration takes place, the whole system will be unavailable and the system's reliability will be low. Therefore, the system's trustworthiness will be low. In contrast, if there is more than one CA in the system like the multiple BCA system, the system is more trustworthy because if a malfunction is detected in the main CA, the system's operation is transferred to the BCA to provide continuous service. In this case, the system is always available. Similarly, if a system has more than one CA, it is more reliable. Eventually, the system with multiple BCAs always achieves a high level of trustworthiness.

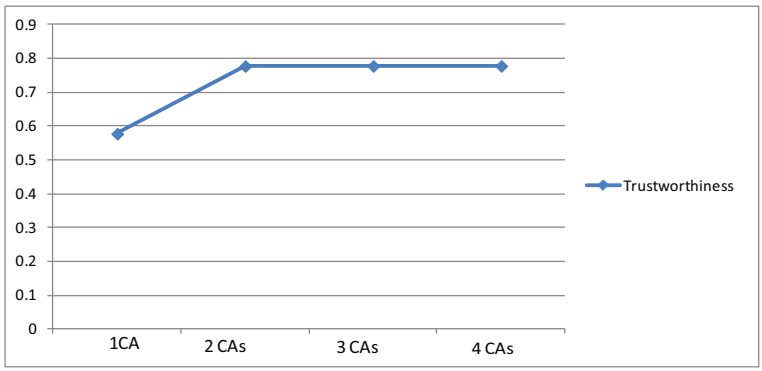

Figure 7.29: Trustworthiness for different CA options

From the numerical results, it can be concluded that if more than one CA is used as BCAs in the system, the system will be more available and reliable, thereby reducing downtime costs.

7.7 Conclusion

According to CRN architecture, there are certain key nodes which are responsible for performing the major tasks in the network, such as maintaining and updating the trust values of all member nodes. However, if a malicious node is successful in becoming the key node, it can easily break down normal network performance by exposing it to different threats. Furthermore, if a malicious node joins the network and injects different threats, the whole network will be vulnerable. Also, if a member node leaves the network abnormally, it reveals the key and other information on the network to the malicious users after becoming compromised by them. To avoid these unwanted situations, in this chapter, a framework for node selection and secure node joining and leaving (NSSJL) the network is proposed to select the most trustworthy node to work as the CA to perform the key functionalities and

will not be compromised easily by the malicious users and the BCA takes the role of the CA if an error occurs in the CA. Having such a framework increases the whole CRN system's availability and reliability by providing continuous service to the network. This framework also proposed a secure node joining process so that no malicious users can join the network abnormally in order to paralyze the network. At the same time, this framework ensures the member node's normal leaving process in order to protect the network from exposing its data outside the network.

Chapter 8

Recapitulation and Future Work

8.1 Introduction

In the existing literature, cryptographic-based solutions have been proposed in secure routing and for authenticating the primary user's (PU's) signal in cognitive radio networks (CRNs). However, such approaches fail to provide a complete solution for detecting security threats brought about by untrustworthy entities, such as selfish, malicious and faulty nodes and to ensure secure communication in CRNs. This is particularly important where untrustworthy, malicious nodes may join and access the free spectrum to inhibit CR nodes to continue their communication using the PU's free spectrum and break down the normal network functionality. In such situations, 'trust' is an important concept to defend against soft security threats in CRNs, especially when authentication has to be achieved to ensure secure communication on the basis of believing that a secondary user (SU), using the PU's spectrum, will not cause interference to the PU.

In order to overcome these problems and ensure secure communication in CRNs by using the notion of trust, six major research issues have been identified and addressed in this thesis. Section 8.2 recapitulates these research issues and in Section 8.3, the contributions made by this thesis to the literature by successfully addressing these research issues are highlighted. In Section 8.4, areas for future work are identified and in Section 8.5 the chapter is concluded.

8.2 Recapitulation of Research Issues

CRNs are more flexible and exposed to wireless networks compared to other traditional radio networks. Hence, there are many security threats to CRNs because of their special characteristics, such as intelligence functionality and dynamic spectrum access application etc. more so than other traditional radio environments. These security issues in CRNs threaten the security of communication and deprive the CRN users of being able to utilize the spectrum in an opportunistic way. Although some cryptographic-based techniques have been proposed to ensure security in CRNs, most only detect if the signal is coming from the primary user (PU) and do not focus on the issue of detecting and stopping malicious users from affecting the performance of the CRNs. Moreover, they require a large amount of processing power and memory for computation.

One way by which the abovementioned problem has been addressed in the area of security in CRNs is by using the notion of 'trust'. However, most of the trust-based approaches proposed in the literature focus on ensuring secure routing in CRNs. There is no complete methodology in the existing literature

to establish trust between different nodes in CRNs so that untrustworthy users can be stopped from accessing the spectrum and paralyzing network functionality. So, in the course of the research documented in this thesis, a broad issue was addressed i.e. *the design and development of a generic framework for trust establishment in CRNs*. Such a trust-based framework can be used to authenticate only valid users to access and share the network resources, such as spectrum, in a secure way, select the key nodes of the CRNs based on the label of trust and perform the major responsibilities for enhanced system availability. Several sub-problems were identified to solve the broad issue as follows:

1. to propose a methodology to establish trust between different CR nodes in the network for authentication purposes so that it can effectively prevent malicious and selfish users from interacting in the network.

2. to propose a methodology to detect and solve the problem of biasing when a node's actual trust value is being solicited by other users. This will help the requesting node to gain the candidate node's actual trust value in CRNs.

3. to propose a methodology to minimize disruption to the SUs' service when they need to vacate the spectrum for the PUs.

4. to propose a secure spectrum sharing mechanism to solve the security threats brought about by untrustworthy entities during spectrum sharing in CRNs and ensure secure communication.

5. to propose a methodology to balance the number of SUs and PUs for efficient spectrum sharing when an SU has to vacate a PU's spectrum.

6. to propose a methodology to select the key nodes in CRNs to perform the major system functionalities.

7. to propose a methodology for secure node joining and leaving the network.

8. to propose a methodology to enhance system availability and reliability in CRNs in the case of an attack on the key nodes of the network.

9. To validate the proposed approaches to improve security in CRNs by using simulation experiments.

8.3 Contributions of the Thesis

The major contribution of this thesis to the literature is the proposal of a trust-based framework in CRNs which establishes trust between different CR nodes to authenticate only valid users to share spectrum in CRN and selects the most trustworthy nodes as the key nodes (main and backup) to enhance system availability and reliability in CRNs. The contributions of this thesis are as follows:

1. to propose a methodology to establish trust between different CR nodes in the network by three different ways of trust calculation namely: direct, indirect and integrated trust calculation. This computed trust value is used to authenticate a node's request to check whether it is coming from a valid node or from an unknown/malicious node.

2. to propose a methodology to detect and solve the biasing problem while soliciting the recommendations of a node by introducing a Certificate

Authority (CA) node in the CRN architecture which maintains the trust repository.

3. to propose an approach with a state transition diagram of the different working states through which an SU needs to go to minimize the disruption to its service when it needs to vacate the spectrum for the PU during spectrum sharing.

4. to propose a methodology that ascertains the trust value of a requesting node conjointly from the secondary network and primary network to share the spectrum securely in a CRN and solves the security threats brought about by untrustworthy entities.

5. to propose a methodology to balance the number of PUs and SUs in a CRN. The proposed approach considers the number of PUs, SUs and the sub-bands into which each licensed band of PU is divided and determines the relationship between them to ascertain the maximum number of SUs which are allowed for efficient spectrum sharing. This is to ensure that the SUs do not need to wait for a long time to access the spectrum.

6. to propose a methodology to select the key nodes of the CRN to perform the major functionalities based on their level of trust.

7. to propose a secure node joining and leaving process in CRNs so that malicious users cannot join and leave the network abnormally and break down the network functionality.

8. to propose a methodology to enhance the availability and reliability of the CRNs by having multiple backup key nodes which can take charge of the network in the event of an error or attack on the current key node.

9. to demonstrate the application of each proposed methodology to ensure secure communication in CRNs.

In the following, a brief explanation of the contributions which this thesis has made to the existing literature is given.

8.3.1 Contribution 1: Methodology to establish trust between different CR nodes to authenticate the node's request

The first contribution of this thesis to the existing literature is that it proposes a methodology to establish trust between different nodes in CRNs to make a decision to authenticate a node's request. The main features of the proposed methodology which are discussed in Chapter 5 are as follows:

- When an SU node sends a request to access either the network resources or the free spectrum from the primary network, its trust value is calculated based on any of the three different trust calculation methods namely: direct, indirect and integrated trust calculation.

- After the calculation process, the decision is made by the corresponding base station to authenticate the request by comparing the computed trust value of the requesting node with the defined trust threshold.

To the best of my knowledge, trust has been discussed in the CRN literature for security such as secure routing, detecting attacks etc., but it has not been used to authenticate a user's request to share network resources, as is discussed in this thesis.

8.3.2 Contribution 2: Methodology to solve the biasing problem to obtain the node's actual trust value

The second contribution of this thesis to the existing literature is that it proposes a methodology to solve the biasing problem brought by either biased nodes or malicious nodes in CRNs. The main features of the proposed methodology which are discussed in Chapter 5 are as follows:

- Whenever a node wants to know another member node's trust value in the network, it sends a request to the SUBS.
- The SUBS calculates the candidate node's trust value and compares it to the value stored by the CA.
- If both results are not similar, the SUBS is assured that the member node's trust value is being compromised by a selfish node who assigns a biased trust value to the candidate node. The SUBS detects the biased node and excludes it from the network for further communication. If both results are similar, the SUBS is assured that no biasing problem has occured in the network.

To the best of my knowledge, there is no methodological approach in the literature where the biasing problem is addressed by using trust in CRNs to obtain the node's actual trust value.

8.3.3 Contribution 3: Methodology to propose different working states of an SU to minimize the disruption to its service when it needs to vacate the spectrum for the PU in CRNs

The third contribution of this thesis to the existing literature is that it proposes an approach regarding the different working states through which an SU needs to go during spectrum sharing to minimize disruption to its service when it needs to return the spectrum to the PU. The main features of the proposed methodology which are discussed in Chapter 6 are as follows:

- A state transition diagram with the five working states through which an SU should go during spectrum sharing, namely: Search State, Access State, Interrupt State, Vacate State and Dropped State is modelled.
- The disruption to an SU's service is measured when it goes to the Vacate state to return the spectrum to the PU and also when it goes to the Dropped state in the absence of free available spectrum surrounding it. It can minimize the disruption to its service while being in these states by again searching and accessing other free spectrum.

To the best of my knowledge, there is no methodological approach in the literature which defines the working states through which an SU in a CRN needs to go to minimize the disruption to its service.

8.3.4 Contribution 4: Methodology for a conjoint trust assessment to share the spectrum securely in CRNs

The fourth contribution of this thesis to the existing literature is that it proposes a conjoint trust assessment approach to share the spectrum only to authenticated trustworthy SUs to avoid the selfish threats brought by untrustworthy users in CRNs. The main features of the proposed methodology which are discussed in Chapter 6 are as follows:

- Whenever an SU sends a request to the SUBS to share the spectrum from the primary network, at first its request is authenticated by both networks as discussed in the first contribution in Section 8.3.1 to check whether the request is coming from a valid node.

- The requesting node's trustworthiness is calculated by both networks and then finally the PUBS makes a decision as to whether the spectrum should be shared with the requesting node or not.

To the best of my knowledge, there is no methodological approach in the literature where a conjoint trust assessment approach is used for secure spectrum sharing in CRNs to avoid untrustworthy user's behaviour in the network.

8.3.5 Contribution 5: Methodology for balancing the number of PUs and SUs for efficient spectrum sharing in CRNs

The fifth contribution of this thesis to the existing literature is that it proposes an approach to balance the number of secondary users and PUs to avoid the blocking probability of SUs in CRNs. The main features of the proposed methodology which are discussed in Chapter 6 are as follows:

- By taking the number of SUs, PUs and the sub-bands into which each licensed band is divided, the proposed methodology allows the maximum identified number of SUs for spectrum sharing in CRNs to avoid the call blocking probability when all the sub-bands are occupied by the SUs.

- Proposing a state transition diagram for spectrum sharing which cater for multiple PUs and SUs in a balanced network and analyzes the different network statistics such as call dropping, call blocking, mean number of SUs and utilization ratio.

To the best of my knowledge, there is no methodological approach in the existing literature which establishes the relation between the number of PUs and SUs in CRNs for efficient spectrum sharing and no basic spectrum sharing scheme has been proposed between multiple PUs and SUs, although a methodological approach in the literature for spectrum sharing is used for only one and two PUs. This is the first attempt to share spectrum for multiple PUs and SUs considering the balanced network properties.

8.3.6 Contribution 6: Methodology for selecting the key nodes to perform the major functionalities

The sixth contribution of this thesis to the existing literature is that it proposes an approach to select the key nodes as a certificate authority (CA) and back up certificate authority (BCA) based on trust so that it can perform the major functionalities and will not be compromised easily in CRNs. The main features of the proposed methodology which are discussed in Chapter 7 are as follows:

- To calculate the trust value of each node in the network. The most trustworthy node whose trust value is above or equal to the trust threshold is selected as the CA to perform the major functionalities in CRNs.

- The second most trustworthy node whose trust value is above or equal to the trust threshold is selected as the first BCA and this process is repeated for each node whose trust value is above or equal to the trust threshold.

- In the case where more than one node has the same trust value which is above or equal to the trust threshold, an election process is required to select the key nodes.

Several approaches have been proposed to select the CA in wireless networks but no methodological approach has been proposed to select the key nodes as the CA and BCA in CRNs to perform the major functionalities which cannot be compromised easily by malicious users.

8.3.7 Contribution 7: Methodology for proposing a secure node joining and leaving process in CRNs

The seventh contribution of this thesis to the existing literature is that it proposes a process for secure node joining and leaving in the network so that malicious nodes which want to either join or leave the network abnormally are identified and denied from doing so. The main features of the proposed methodology which are discussed in Chapter 7 are as follows:

- to propose a secure node joining process through which a node should go whenever it wants to join the network. The node's trust value is incremented by a certain range as a reward after it successfully joins the network.

- to propose a secure leaving process through which a node should go whenever it wants to leave the network so that it cannot reveal network keys to the malicious user after leaving the network. The node's trust value is incremented by a certain range as a reward after it successfully leaves the network.

In the literature, different cryptographic-based approaches have been proposed for node joining and leaving, however none showed the effect on the trust value in CRNs which helps the nodes to be selected as the key nodes.

8.3.8 Contribution 8: Methodology for system availability and reliability enhancement in CRNs

The eighth contribution of this thesis to the existing literature is that it proposes a methodology for enhancing the system's availability and reliability

by introducing the multiple BCA framework in the system. The main features of the proposed methodology which are discussed in Chapter 7 are as follows:

- to propose a system that has multiple BCAs, and can switch from a CA to a BCA in response to the detection of an error in a CA or in the case where a CA is biased and under attack by other malicious nodes. In this scenario, the first BCA takes charge of the CA and the second BCA takes charge of the first BCA and so on.

- to propose different working states in the working of a CA and BCA in a multiple BCA through which they need to go according to their present state in order to enhance system availability.

- to evaluate the effect of the solution on system availability and reliability enhancement using different metrics such as downtime cost, trustworthiness etc.

To the best of my knowledge, there is no proposed generic framework in the literature on key node selection which enhances system availability and reliability by reducing downtime and failure.

8.4 Future Work

This thesis has demonstrated that it has sufficiently achieved the research objectives for secure communication by using the notion of trust in CRNs. However, there is some suggested future work for further investigation in order to strengthen the proposed framework to provide more intuitive results to support trust-based secure communication in CRNs. The possible areas which could be explored further in this area are as follows:

- Consider the dynamic behaviours of CR nodes to obtain the most updated trust value
- Extend the proposed framework for multi-hop CRNs
- Consider soft encryption-based techniques during message transmission in CRNs
- Establish certificate-based trust to ensure the integrity and authenticity of information for the candidate node in CRNs
- Consider communication overheads for cryptography techniques and huge data in the co-operation record table

8.4.1 Consider the dynamic behaviours of CR nodes to obtain the most recent trust value

As discussed in Chapters 5, 6 and 7, the proposed framework for trust establishment between different nodes in CRNs uses a reputation-based model where trust management depends on the behavior of each node in the network. In this methodology, a co-operation record of past behaviours is used to calculate the node's trust value. In the co-operation record, there is no consideration of the dynamic behavior of a node such as delay through a path, number of packets dropped during transmission etc. In such scenarios, it is possible that the most recent trust value of a node is not determined. Moreover, the proposed methodology works well for the specification of a small network with a low number of nodes, however, if the number of nodes increases, the amount of information of past behaviours in the record increases which requires more processing power for computation and memory for storage.

This triggers the need to consider the dynamic behaviours of nodes in CRNs and to introduce the *helper node* in the network for storing and updating the record table for a large network. Each member node can access the record table from the helper node and process the information. The strength of considering dynamic behaviours and introducing a helper node can then be used to compute one node's current updated trust value by the member node which only needs a small amount of processing power to compute.

8.4.2 Extend the proposed framework for multi-hop CRNs

As discussed in Chapter 7, the proposed framework for key node selection considers only a one-hop network infrastructure during trust calculation between different nodes in CRNs. However, the proposed framework is inadequate for a large network where a multi-hop CRN infrastructure exists. Therefore, the proposed trust-based framework can be extended to the theory and design of multi-hop CRNs. One of the ways to measure a trusted relationship in a multi-hop CRN is by using graph theory where connections and hyper connections are used for a node's behaviour in the network.

This triggers the need to consider the trust relationship based on graph theory for multi-hop CRNs. The strength of considering the trust relationship for multi-hop CRNs makes the framework more applicable.

8.4.3 Consider soft encryption-based techniques during message transmission in CRNs

As discussed in Chapters 5, 6, and 7, the proposed framework did not consider security during message transmission for communicating between different nodes, for example, in the scenario where the trust value of a node needs to be transmitted to other nodes as a message. Though the proposed frameworks are able to ensure security by trust-based authentication checking, secure spectrum sharing and enhancement of system availability through trusted key node selection, soft encryption techniques can be applied on top of it during message transmission through which the trust value of a node is transmitted to other nodes in the network, which can reduce the computational overhead over conventional encryption techniques.

This triggers the need to consider soft encryption techniques during the trust value as a message transmission between different nodes through multipath techniques which are more trustworthy [131] in the CRNs. The strength of considering these soft encryption techniques in the proposed frameworks will enhance the security of communication in CRNs.

8.4.4 Establish certificate-based trust to ensure the integrity and authenticity of the trust value for the candidate node in CRNs

As discussed in Chapter 5, 6 and 7, the proposed frameworks establish trust for different nodes in the CRNs based on past behaviours stored in the co-operation record. Malicious users attempt to access the co-operation record

and change the behavior status which ascertains a candidate node's false trust value. Therefore, digital certificate-based schemes can be applied to establish trust to ensure the integrity and authenticity of the computed trust value through the assistance of a trusted third party between different nodes in CRNs.

This triggers the need to consider a certificate-based trust establishment between different nodes in CRNs to ensure the integrity and authenticity of the candidate node's trust value. The strength of considering this certificate-based trust establishment makes communication in CRNs more secure and reliable.

8.4.5 Consider communication overheads for cryptography techniques and huge data in the co-operation record table

As mentioned in Section 1.7, the proposed methodologies are lightweight as there is no extra overhead on the resources while computing the trust value for small CRNs to ensure secure communication. For large network, the node needs more processing power and memory to store and also the case for certificate-based trust calculation to ensure more secure communication as cryptography techniques such as key management requires computational cost.

This triggers the need to consider communication overhead such as computational, time complexity and memory overhead for considering such large network to make trust-based secure communication in CRNs more practical.

8.5 Conclusion

In this chapter, the work that has been undertaken and documented in this thesis has been recapitulated and the issues addressed in the literature which prompted the work in this thesis have been highlighted. The different contributions to the literature as the result of the outcome of the work done in this thesis have also been highlighted. A brief description of the further work that is intended to be undertaken in order to extend the approaches developed in this thesis were then provided.

The work that was undertaken in this thesis has been published extensively as a part of the proceedings in peer-reviewed international journals and conferences. Selected publications are provided in Appendix A. A complete list of all the publications arising as a result of the work and related to this work documented in this thesis is given at the beginning of the thesis.

References

[1] G. M. D. R. Peter Steenkiste, Douglas Si cker, "Future directions in cognitive radio network research," NSF Workshop Report, Tech. Rep., 2009.

[2] *Federal Communications Commission. Facilitating opportunities for flexible, efficient, and reliable spectrum use employing spectrum agile radio technologies. ET Docket, (03-108), Dec. 2003.*, Federal Communications Commission. Std.

[3] J. Mitola, "Cognitive radio: an integrated agent architecture for software defined radio," *Doctor of Technology, Royal Inst. Technol.(KTH), Stockholm, Sweden*, 2000. [Online]. Available: http://web.it.kth.se/~{}maguire/jmitola/Mitola_Dissertation8_Integrated.pdf

[4] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *Selected Areas in Communications, IEEE Journal on*, vol. 23, no. 2, pp. 201 – 220, feb. 2005.

[5] P. P. Bhattacharya, R. Khandelwal, R. Gera, and A. Agarwal, "Smart radio spectrum management for cognitive

radio," *CoRR*, vol. abs/1109.0257, 2011. [Online]. Available: http://dblp.uni-trier.de/db/journals/corr/corr1109.html#abs-1109-0257

[6] K.-C. Chen, Y.-J. Peng, N. Prasad, Y.-C. Liang, and S. Sun, "Cognitive radio network architecture: part i – general structure," in *Proceedings of the 2nd international conference on Ubiquitous information management and communication*, ser. ICUIMC '08. New York, NY, USA: ACM, 2008, pp. 114–119. [Online]. Available: http://doi.acm.org.dbgw.lis.curtin.edu.au/10.1145/1352793.1352817

[7] B. Wang, Y. Wu, and K. R. Liu, "Game theory for cognitive radio networks: An overview," *Comput. Netw.*, vol. 54, no. 14, pp. 2537–2561, Oct. 2010. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2010.04.004

[8] D. S. Vernekar, "An investigation of security challenges in cognitive radio networks," Master's thesis, Telecommunications Engineering; University of Nebraska, 2012.

[9] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *Communications Surveys Tutorials, IEEE*, vol. 11, no. 1, pp. 116 –130, quarter 2009.

[10] ——, "Spectrum characterization for opportunistic cognitive radio systems," in *Military Communications Conference, 2006. MILCOM 2006. IEEE*, 2006, pp. 1–6.

[11] J. Unnikrishnan and V. Veeravalli, "Cooperative sensing for primary detection in cognitive radio," *Selected Topics in Signal Processing, IEEE Journal of*, vol. 2, no. 1, pp. 18 –27, feb. 2008.

[12] Z. Chair and P. Varshney, "Optimal data fusion in multiple sensor detection systems," *Aerospace and Electronic Systems, IEEE Transactions on*, vol. AES-22, no. 1, pp. 98 –101, jan. 1986.

[13] Z. Quan, S. Cui, and A. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio networks," *Selected Topics in Signal Processing, IEEE Journal of*, vol. 2, no. 1, pp. 28 –40, feb. 2008.

[14] E. Peh, Y.-C. Liang, Y. L. Guan, and Y. Zeng, "Optimization of cooperative sensing in cognitive radio networks: A sensing-throughput tradeoff view," *Vehicular Technology, IEEE Transactions on*, vol. 58, no. 9, pp. 5294 –5299, nov. 2009.

[15] M. Bin Shahid and J. Kamruzzaman, "Weighted soft decision for cooperative sensing in cognitive radio networks," in *Networks, 2008. ICON 2008. 16th IEEE International Conference on*, dec. 2008, pp. 1 –6.

[16] M. Xie, S. Han, B. Tian, and S. Parvin, "Anomaly detection in wireless sensor networks: A survey," *J. Netw. Comput. Appl.*, vol. 34, no. 4, pp. 1302–1325, Jul. 2011. [Online]. Available: http://dx.doi.org/10.1016/j.jnca.2011.03.004

[17] X. Wang, Z. Li, P. Xu, Y. Xu, X. Gao, and H.-H. Chen, "Spectrum sharing in cognitive radio networks-an auction-based approach," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 40, no. 3, pp. 587 –596, june 2010.

[18] N. Radhi and H. Al-Raweshidy, "Primary signal transmitter localization using cognitive radio networks," in *Next Generation*

Mobile Applications, Services and Technologies (NGMAST), 2011 5th International Conference on, 2011, pp. 137–141.

[19] X. Sheng and Y.-H. Hu, "Maximum likelihood multiple-source localization using acoustic energy measurements with wireless sensor networks," *Signal Processing, IEEE Transactions on*, vol. 53, no. 1, pp. 44–53, 2005.

[20] R. C. Miller, W. Xu, P. Kamat, and W. Trappe, "Service Discovery and Device Identification in Cognitive Radio Networks," in *Sensor and Ad Hoc Communications and Networks*, 2007, pp. 670–677.

[21] S. Misra and A. Jain, "Policy controlled self-configuration in unattended wireless sensor networks." *J. Network and Computer Applications*, vol. 34, no. 5, pp. 1530–1544, 2011. [Online]. Available: http://dblp.uni-trier.de/db/journals/jnca/jnca34.html#MisraJ11

[22] M. Abdullah and S. Mahmood, *Priority Queuing Based Spectrum Sensing in Cognitive Radio Network: Priority Queuing Based Spectrum Sensing Methodology in Cognitive Radio Network*. VDM Publishing, 2011. [Online]. Available: http://books.google.com.au/books?id=qVfeXwAACAAJ

[23] H. Zheng and L. Cao, "Device-centric spectrum management," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*, nov. 2005, pp. 56 –65.

[24] S. Bahramian and B. Khalaj, "A novel low-complexity dynamic frequency selection algorithm for cognitive radios," in *Wireless*

Communication Systems, 2007. ISWCS 2007. 4th International Symposium on, oct. 2007, pp. 558 –562.

[25] C. N. Mathur and K. P. Subbalakshmi, "Digital signatures for centralized dsa networks," in *Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE*, jan. 2007, pp. 1037 –1041.

[26] L. W.-Y. C. K. Akyildiz, I.F., "Crahns: Cognitive radio ad hoc networks," *Ad Hoc Networks*, vol. 7, no. 5, pp. 810–836, 2009, cited By (since 1996) 182.

[27] M.-T. Zhou and H. Harada, "Cognitive maritime wireless mesh/ad hoc networks," *J. Netw. Comput. Appl.*, vol. 35, no. 2, pp. 518–526, Mar. 2012. [Online]. Available: http://dx.doi.org/10.1016/j.jnca.2010.12.018

[28] D. Sarkar and H. Narayan, "Transport layer protocols for cognitive networks," in *INFOCOM IEEE Conference on Computer Communications Workshops , 2010*, 2010, pp. 1–6.

[29] I. Akyildiz, W.-Y. Lee, M. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *Communications Magazine, IEEE*, vol. 46, no. 4, pp. 40 –48, april 2008.

[30] Y.-C. Liang, K.-C. Chen, G. Li, and P. Mahonen, "Cognitive radio networking and communications: An overview," *Vehicular Technology, IEEE Transactions on*, vol. 60, no. 7, pp. 3386–3407, 2011.

[31] H. Arslan, *Cognitive Radio, Software Defined Radio, and Adaptive Wireless Systems*, ser. Signals and Communication

Technology. Springer, 2007. [Online]. Available: http://books.google.com.au/books?id=yMgGGe-z7mYC

[32] M. Rehmani, A. Viana, H. Khalife, and S. Fdida, "A cognitive radio based internet access framework for disaster response network deployment," in *Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on*, 2010, pp. 1–5.

[33] A. Khattab, D. Perkins, and M. Bayoumi, *Cognitive Radio Networks: From Theory to Practice*, ser. Analog Circuits and Signal Processing Series. Springer-Verlag GmbH, 2012. [Online]. Available: http://books.google.com.au/books?id=aclBLgEACAAJ

[34] D. Maldonado, B. Le, A. Hugine, T. Rondeau, and C. Bostian, "Cognitive radio applications to dynamic spectrum allocation: a discussion and an illustrative example," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*, nov. 2005, pp. 597 –600.

[35] A. Gorcin and H. Arslan, "Public safety and emergency case communications: Opportunities from the aspect of cognitive radio," in *New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on*, 2008, pp. 1–10.

[36] T. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in *Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on*, may 2008, pp. 1 –8.

[37] J. Burbank, "Security in cognitive radio networks: The required evolution in approaches to wireless network security," in *Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on*, may 2008, pp. 1 –7.

[38] R. Chen, J.-M. Park, Y. Hou, and J. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *Communications Magazine, IEEE*, vol. 46, no. 4, pp. 50 –55, april 2008.

[39] S. K. Mathur, C.N., *Security Issues in Cognitive Radio Networks , In Cognitive Networks: Towards Self-Aware Networks*, ser. Signals and Communication Technology. John Wiley and Sons, Ltd, 2007. [Online]. Available: http://books.google.com.au/books/about/Cognitive_Networks.html?id=8cGYuZK66YwC

[40] A. Fragkiadakis, E. Tragos, and I. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *Communications Surveys Tutorials, IEEE*, vol. PP, no. 99, pp. 1 –18, 2012.

[41] A. Naveed and S. S. Kanhere, "Security vulnerabilities in channel assignment of multi-radio multi-channel wireless mesh networks." in *GLOBECOM*. IEEE, 2006.

[42] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in *Communications, 2008. ICC '08. IEEE International Conference on*, may 2008, pp. 3406 –3410.

[43] Y. Zhang, G. Xu, and X. Geng, "Security threats in cognitive radio networks," in *High Performance Computing and Communications, 2008. HPCC '08. 10th IEEE International Conference on*, sept. 2008, pp. 1036 –1041.

[44] X. Zhang and C. Li, "The security in cognitive radio networks: a survey," in *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, ser. IWCMC '09. New York, NY, USA: ACM, 2009, pp. 309–313. [Online]. Available: http://doi.acm.org.dbgw.lis.curtin.edu.au/10.1145/1582379.1582447

[45] K.-C. Chen, Y.-J. Peng, N. Prasad, Y.-C. Liang, and S. Sun, "Cognitive radio network architecture: part ii – trusted network layer structure," in *Proceedings of the 2nd international conference on Ubiquitous information management and communication*, ser. ICUIMC '08. New York, NY, USA: ACM, 2008, pp. 120–124. [Online]. Available: http://doi.acm.org/10.1145/1352793.1352818

[46] T. Qin, H. Yu, C. Leung, Z. Shen, and C. Miao, "Towards a trust aware cognitive radio architecture," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 13, no. 2, pp. 86–95, Sep. 2009. [Online]. Available: http://doi.acm.org/10.1145/1621076.1621085

[47] S. J. H. S. M. Leon, O., "A new cross-layer attack to tcp in cognitive radio networks," in *Second International Workshop on Cross Layer Design*, 2009, pp. 1–5.

[48] J. Xiang, Y. Zhang, and T. Skeie, "Medium access control

protocols in cognitive radio networks," *Wirel. Commun. Mob. Comput.*, vol. 10, no. 1, pp. 31–49, Jan. 2010. [Online]. Available: http://dx.doi.org/10.1002/wcm.v10:1

[49] N. Cam-Winget, R. Housley, D. Wagner, and J. Walker, "Security flaws in 802.11 data link protocols," *Commun. ACM*, vol. 46, no. 5, pp. 35–39, May 2003. [Online]. Available: http://doi.acm.org/10.1145/769800.769823

[50] "Fips, specification of the advanced encryption standard (aes)." Federal Information Processing Standards Publication, 1987.

[51] B. Schneier, *Applied cryptography : protocols, algorithms, and source code in C*. New York, NY, USA: John Wiley & Sons, Inc., 1995.

[52] X. Tan, K. Borle, W. Du, and B. Chen, "Cryptographic link signatures for spectrum usage authentication in cognitive radio," in *Proceedings of the fourth ACM conference on Wireless network security*, ser. WiSec '11. New York, NY, USA: ACM, 2011, pp. 79–90. [Online]. Available: http://doi.acm.org/10.1145/1998412.1998428

[53] L. Zhu and H. Mao, "An efficient authentication mechanism for cognitive radio networks," in *Proceedings of the 2011 Asia-Pacific Power and Energy Engineering Conference*, ser. APPEEC '11. Washington, DC, USA: IEEE Computer Society, 2011, pp. 1–5. [Online]. Available: http://dx.doi.org/10.1109/APPEEC.2011.5748783

[54] D. Zhou, "The handbook of ad hoc wireless networks," M. Ilyas and R. C. Dorf, Eds. Boca Raton, FL, USA: CRC Press, Inc., 2003, ch.

Security issues in ad hoc networks, pp. 569–582. [Online]. Available: http://dl.acm.org/citation.cfm?id=989711.989744

[55] O. León, J. Hernández-Serrano, and M. Soriano, "Securing cognitive radio networks," *Int. J. Commun. Syst.*, vol. 23, no. 5, pp. 633–652, May 2010. [Online]. Available: http://dx.doi.org/10.1002/dac.v23:5

[56] R. Anderson, "'trusted computing' frequently asked questions," Tech. Rep., August 2003.

[57] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *Communications Surveys Tutorials, IEEE*, vol. 13, no. 4, pp. 562 –583, quarter 2011.

[58] B. Wang and K. Liu, "Advances in cognitive radio networks: A survey," *Selected Topics in Signal Processing, IEEE Journal of*, vol. 5, no. 1, pp. 5 –23, feb. 2011.

[59] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," 1996. [Online]. Available: http://citeseer.ist.psu.edu/blaze96decentralized.html

[60] C. Zhao, L. Xie, X. Jiang, L. Huang, and Y. Yao, "A phy-layer authentication approach for transmitter identification in cognitive radio networks," in *Proceedings of the 2010 International Conference on Communications and Mobile Computing - Volume 02*, ser. CMC '10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 154–158. [Online]. Available: http://dx.doi.org/10.1109/CMC.2010.36

[61] M. Kuroda, R. Nomura, and W. Trappe, "A radio-independent

authentication protocol (eap-crp) for networks of cognitive radios," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON '07. 4th Annual IEEE Communications Society Conference on*, june 2007, pp. 70 –79.

[62] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *Security and Privacy (SP), 2010 IEEE Symposium on*, may 2010, pp. 286 –301.

[63] M. G. Wassim El-Hajj, Haidar Safa, "Survey of security issues in cognitive radio networks," *Journal of Internet Technology*, vol. 12, 2011.

[64] Q. Zhu, J. B. Song, and T. Basar, "Dynamic secure routing game in distributed cognitive radio networks." in *GLOBECOM*. IEEE, 2011, pp. 1–6. [Online]. Available: http://dblp.uni-trier.de/db/conf/globecom/globecom2011.html#ZhuSB11

[65] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J.Sel. A. Commun.*, vol. 26, no. 1, pp. 25–37, Jan. 2008. [Online]. Available: http://dx.doi.org/10.1109/JSAC.2008.080104

[66] H. Li and Z. Han, "Dogfight in spectrum: Jamming and anti-jamming in multichannel cognitive radio systems," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, 30 2009-dec. 4 2009, pp. 1 –6.

[67] W. Wang, H. Li, Y. Sun, and Z. Han, "Securing collaborative spectrum sensing against untrustworthy secondary users in cognitive radio

networks," *EURASIP J. Adv. Signal Process*, vol. 2010, pp. 4:4–4:4, Jan. 2010. [Online]. Available: http://dx.doi.org/10.1155/2010/695750

[68] G. Jakimoski and K. Subbalakshmi, "Denial-of-service attacks on dynamic spectrum access networks," in *Communications Workshops, 2008. ICC Workshops '08. IEEE International Conference on*, may 2008, pp. 524 –528.

[69] E. Hossain, D. Niyato, and Z. Han, *Dynamic Spectrum Access and Management in Cognitive Radio Networks*, 1st ed. New York, NY, USA: Cambridge University Press, 2009.

[70] W.-Y. Lee and I. Akyildiz, "Optimal spectrum sensing framework for cognitive radio networks," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 10, pp. 3845 –3857, october 2008.

[71] S. Mangold and Z. Zhong, "Spectrum agile radio: Detecting spectrum opportunities," in *International Symposium on Advanced Radio Technologies ISART*, Boulder CO, USA, Mar 2004, p. 5. [Online]. Available: http://www.comnets.rwth-aachen.de

[72] M. Olivieri, G. Barnett, A. Lackpour, A. Davis, and P. Ngo, "A scalable dynamic spectrum allocation system with interference mitigation for teams of spectrally agile software defined radios," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*, nov. 2005, pp. 170 –179.

[73] R. Chen and J.-M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in *Networking Technologies for Software*

Defined Radio Networks, 2006. SDR '06.1st IEEE Workshop on, sept. 2006, pp. 110 –119.

[74] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Comput. Netw.*, vol. 50, no. 13, pp. 2127–2159, Sep. 2006. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2006.05.001

[75] G. Baldini, V. Rakovic, V. Atanasovski, and L. Gavrilovska, "Security aspects of policy controlled cognitive radio," in *New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on*, may 2012, pp. 1 –5.

[76] L. ke Wang and Y.-H. Zhu, "A spectrum sharing scheme for cognitive radio networks," in *Communications and Networking in China, 2009. ChinaCOM 2009. Fourth International Conference on*, aug. 2009, pp. 1 –4.

[77] K. Patil, M. Deshmukh, and H. Cornean, "Ctmc based spectrum sharing scheme for cognitive radio networks," in *Communications (COMM), 2010 8th International Conference on*, june 2010, pp. 509 –512.

[78] S. E. S. Ghasemi, A., "Opportunistic spectrum access in fading channels through collaborative sensing," *JOURNAL OF COMMUNICATIONS*, vol. 2(2), pp. 71–82, 2007.

[79] M. Bin Shahid and J. Kamruzzaman, "Agile spectrum evacuation in cognitive radio networks," in *Communications (ICC), 2010 IEEE International Conference on*, may 2010, pp. 1 –6.

[80] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Information Sciences and Systems, 2009. CISS 2009. 43rd Annual Conference on*, march 2009, pp. 130 –134.

[81] 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, pp. 1876 –1884.

[82] H. S. Kim, "Location-based authentication protocol for first cognitive radio networking standard," *J. Netw. Comput. Appl.*, vol. 34, no. 4, pp. 1160–1167, Jul. 2011. [Online]. Available: http://dx.doi.org/10.1016/j.jnca.2010.12.017

[83] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, ser. MobiCom '00. New York, NY, USA: ACM, 2000, pp. 275–283. [Online]. Available: http://doi.acm.org/10.1145/345910.345958

[84] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," *Wireless Communications, IEEE*, vol. 11, no. 1, pp. 48 – 60, feb 2004.

[85] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," *J. High Speed Netw.*, vol. 15, no. 1, pp. 33–51, Jan. 2006. [Online]. Available: http://dl.acm.org/citation.cfm?id=1140563.1140567

[86] C. L. F. R. C. M. R.-P. L. Filho, J.G., "Ids-cog - intrusion detection system for cognitive radio network," *International Journal of Computer Science and Network Security*, vol. 12(3), 2012.

[87] O. León, R. Román, and J. Hernández-Serrano, "Towards a cooperative intrusion detection system for cognitive radio networks," in *Proceedings of the IFIP TC 6th international conference on Networking*, ser. NETWORKING'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 231–242. [Online]. Available: http://dl.acm.org/citation.cfm?id=2039912.2039937

[88] J. Toonstra and W. Kinsner, "A radio transmitter fingerprinting system odo-1," in *Electrical and Computer Engineering, 1996. Canadian Conference on*, vol. 1, may 1996, pp. 60 –63 vol.1.

[89] A. Al Hanbali, E. Altman, and P. Nain, "A survey of tcp over ad hoc networks," *Communications Surveys Tutorials, IEEE*, vol. 7, no. 3, pp. 22 – 36, quarter 2005.

[90] S. Mishra, A. Sahai, and R. Brodersen, "Cooperative sensing among cognitive radios," in *Communications, 2006. ICC '06. IEEE International Conference on*, vol. 4, june 2006, pp. 1658 –1663.

[91] N.-T. Nhan and I. Koo, "A secure distributed spectrum sensing scheme in cognitive radio," in *Proceedings of the Intelligent computing 5th international conference on Emerging intelligent computing technology and applications*, ser. ICIC'09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 698–707. [Online]. Available: http://dl.acm.org/citation.cfm?id=1788154.1788247

[92] T. R. Newman and T. C. Clancy, "Security threats to cognitive radio signal classifiers," Proc. of the Virginia Tech Wireless Personal Communications Symposium.

[93] G. Jakimoski and K. Subbalakshmi, "Towards secure spectrum decision," in *Communications, 2009. ICC '09. IEEE International Conference on*, june 2009, pp. 1 –5.

[94] Y.-S. Chen, C.-H. Cho, I. You, and H.-C. Chao, "A cross-layer protocol of spectrum mobility and handover in cognitive lte networks," *Simulation Modelling Practice and Theory*, vol. 19, no. 8, pp. 1723–1744, 2011.

[95] Q. Pei, R. Liang, and H. Li, "A trust management model in centralized cognitive radio networks," in *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2011 International Conference on*, oct. 2011, pp. 491 –496.

[96] S. Jana, K. Zeng, and P. Mohapatra, "Trusted collaborative spectrum sensing for mobile cognitive radio networks." in *INFOCOM*, A. G. Greenberg and K. Sohraby, Eds. IEEE, 2012, pp. 2621–2625. [Online]. Available: http://dblp.uni-trier.de/db/conf/infocom/infocom2012.html#JanaZM12

[97] M. X. Deming Pang, Gang Hu, "Trust model-based secure cooperative sensing techniques for cognitive radio networks," in *The Tenth International Conference on Networks*, 2011.

[98] T. Qin, C. Leung, C. Miao, and Y. Chen, "Trust-aware resource allocation in a cognitive radio system," in *Computer Science and*

Automation Engineering (CSAE), 2012 IEEE International Conference on, vol. 3, may 2012, pp. 797 –801.

[99] W. L. Y. F. Yanchao Zhang, Wei Liu, "Securing sensor networks with location-based keys," in *IEEE Wireless Commun. and Networking Conf.*, 2005.

[100] H. L. Vincent Toubiana, "Asma : Towards adaptive secured multipath in manets," in *IFIP International Federation For Information Processing, Mobile and Wireless Communication Networks*, 2006.

[101] J. Hu, W. Hawkes, D. Lois, W. Hawkes, D. A. Yasinsac, D. D. Schwartz, D. Z. Duan, I. Dr, M. Burmester, D. Robert, A. Engelen, and D. Stephen, "Trust management in mobile wireless networks: Security and survivability by," 2007.

[102] C. N. Mathur and K. P. Subbalakshmi, *Security Issues in Cognitive Radio Networks*. John Wiley & Sons, Ltd, 2007, pp. 271–291. [Online]. Available: http://dx.doi.org/10.1002/9780470515143.ch11

[103] Y. Yussoff and H. Hashim, "Ibe-trust: A security framework for wireless sensor networks," in *Internet Security (WorldCIS), 2011 World Congress on*, 2011, pp. 171–176.

[104] R. A. Shaikh, "Intrusion tolerant trust-based privacy-assured security solution for wireless sensor networks," Ph.D. dissertation, Department of Computer Engineering, August, 2009.

[105] V. Oleshchuk, "Trust-based framework for security enhancement of wireless sensor networks," in *Intelligent Data Acquisition and Advanced*

Computing Systems: Technology and Applications, 2007. IDAACS 2007. 4th IEEE Workshop on, 2007, pp. 623–627.

[106] 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 *Wireless Communications and Networking Conference (WCNC), 2011 IEEE*, 2011, pp. 599–604.

[107] R. Dubey, S. Sharma, and L. Chouhan, "Secure and trusted algorithm for cognitive radio network," in *Wireless and Optical Communications Networks (WOCN), 2012 Ninth International Conference on*, 2012, pp. 1–7.

[108] I. A. E.-w. A. Fatty Mustafa Salem, Maged Hamada Ibrahim, "Secure authentication scheme preventing wormhole attacks in cognitive radio networks," *Asian Journal of Computer Science and Information Technology*, vol. Vol 2, No 04 (2012), pp. 52–55, 2012.

[109] S. Chandrashekar and L. Lazos, "A primary user authentication system for mobile cognitive radio networks," in *Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on*, 2010, pp. 1–5.

[110] M. Dong, G. Sun, X. Wang, and Q. Zhang, "Combinatorial auction with time-frequency flexibility in cognitive radio networks," in *INFOCOM, 2012 Proceedings IEEE*, 2012, pp. 2282–2290.

[111] X. Zhou and H. Zheng, "Trust: A general framework for truthful double spectrum auctions," in *INFOCOM 2009, IEEE*, 2009, pp. 999–1007.

[112] S. Kim, "Trust-based bargaining game model for cognitive radio spectrum sharing scheme," *IEICE Transactions*, vol. 95-B, no. 12, pp. 3925–3928, 2012.

[113] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical Communication*, vol. 4, no. 1, pp. 40 – 62, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S187449071000039X

[114] Y. Kondareddy, N. Andrews, and P. Agrawal, "On the capacity of secondary users in a cognitive radio network," in *Sarnoff Symposium, 2009. SARNOFF '09. IEEE*, 30 2009-april 1 2009, pp. 1 –5.

[115] L. Lazos, S. Liu, and M. Krunz, "Spectrum opportunity-based control channel assignment in cognitive radio networks," in *Proceedings of the 6th Annual IEEE communications society conference on Sensor, Mesh and Ad Hoc Communications and Networks*, ser. SECON'09. Piscataway, NJ, USA: IEEE Press, 2009, pp. 135–143. [Online]. Available: http://dl.acm.org/citation.cfm?id=1687299.1687315

[116] A. Rawat, P. Anand, H. Chen, and P. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *Trans. Sig. Proc.*, vol. 59, no. 2, pp. 774–786, Feb. 2011. [Online]. Available: http://dx.doi.org/10.1109/TSP.2010.2091277

[117] N. Rahimian, C. Georghiades, H. Celebi, and K. Qaraqe, "Spectrum availability model of secondary users in cognitive radio networks," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International*, 2012, pp. 360–365.

[118] V. Tumuluru, P. Wang, and D. Niyato, "A neural network based spectrum prediction scheme for cognitive radio," in *Communications (ICC), 2010 IEEE International Conference on*, 2010, pp. 1–5.

[119] B.-J. Chang, S.-L. Kuo, Y.-H. Liang, and D.-Y. Wang, "Markov chain-based trust model for analyzing trust value in distributed multicasting mobile ad hoc networks," in *Asia-Pacific Services Computing Conference, 2008. APSCC '08. IEEE*, dec. 2008, pp. 156 –161.

[120] Y. tao Yang, Z. Yuan, Y. Fang, and P. Zeng, "A novel authentication scheme based on trust-value updated model in adhoc network." in *COMPSAC (1)*. IEEE Computer Society, 2007, pp. 643–645.

[121] J. F. Nunamaker, Jr., M. Chen, and T. D. M. Purdin, "Systems development in information systems research," *J. Manage. Inf. Syst.*, vol. 7, no. 3, pp. 89–106, Oct. 1990. [Online]. Available: http://dl.acm.org/citation.cfm?id=116927.116932

[122] F. Burstein and S. Gregor, "The systems development or engineering approach to research in information systems: An action research perspective," in *Proceedings of ACIS99*, Wellington, NZ, 1999, pp. 122–134.

[123] G. Han, D. Choi, and W. Lim, "A reliable approach of establishing trust for wireless sensor networks," in *Proceedings of the 2007 IFIP International Conference on Network and Parallel Computing Workshops*, ser. NPC '07. Washington, DC, USA:

IEEE Computer Society, 2007, pp. 232–237. [Online]. Available: http://dl.acm.org/citation.cfm?id=1306873.1307066

[124] T. D. Elizabeth Chang, Farookh Hussain, *Trust and Repuration for Service-Oriented Environment*. Wiley, 2006.

[125] M. Momani, S. Challa, and K. Aboura, "Modelling trust in wireless sensor networks from the sensor reliability prospective," in *Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications*, T. Sobh, K. Elleithy, A. Mahmood, and M. Karim, Eds. Springer Netherlands, 2007, pp. 317–321. [Online]. Available: http://dx.doi.org/10.1007/978-1-4020-6266-7_57

[126] A. A. Pirzada and C. McDonald, "Establishing trust in pure ad-hoc networks," in *Proceedings of the 27th Australasian conference on Computer science - Volume 26*, ser. ACSC '04. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2004, pp. 47–54. [Online]. Available: http://dl.acm.org/citation.cfm?id=979922.979929

[127] Y. Wang and V. Varadharajan, "Trust2: Developing trust in peer-to-peer environments," in *Proceedings of the 2005 IEEE International Conference on Services Computing - Volume 01*, ser. SCC '05. Washington, DC, USA: IEEE Computer Society, 2005, pp. 24–34. [Online]. Available: http://dx.doi.org/10.1109/SCC.2005.104

[128] W. K. Ching and M. K. Ng, *Markov chains models, algorithms and applications*. New York: Springer, 2006. [Online]. Available: http://dx.doi.org/10.1007/0-387-29337-X

[129] T. Theinn, J. S. Park, and S. D. Chi, *Increasing Availability and Survivability of Cluster Head in WSN.* ACM, 2008.

[130] T. Thein and J. S. Park, "Availability analysis of application servers using software rejuvenation and virtualization," *J. Comput. Sci. Technol.*, vol. 24, no. 2, pp. 339–346, Mar. 2009. [Online]. Available: http://dx.doi.org/10.1007/s11390-009-9228-1

[131] Q. Niu, "A trust-based message encryption scheme for mobile ad hoc networks," *Computer Science and Engineering, International Workshop on*, vol. 1, pp. 172–176, 2009.

Appendix A

The Selected Publications

A.1 Multi-Cyber Framework for Availability Enhancement of Cyber Physical Systems

A.2 Conjoint Trust Assessment for Secure Communication in Cognitive Radio Networks

A.3 Cognitive Radio Network Security:A Survey

A.4 Trust-Based Spectrum Sharing for Cognitive Radio Networks