José Manuel Meireles Marinho

MEDIUM ACCESS CONTROL-LEVEL SOLUTIONS FOR OPTIMIZED SPECTRUM DECISION IN DISTRIBUTED COGNITIVE RADIO SCENARIOS

Tese do Programa de Doutoramento em Ciências e Tecnologias da Informação, orientada pelo Professor Doutor Edmundo Heitor da Silva Monteiro
e apresentada ao Departamento de Engenharia Informática da Faculdade de Ciências e Tecnologia da Universidade de Coimbra

Julho de 2015

· U C ·

UNIVERSIDADE DE COIMBRA

Medium Access Control-Level Solutions for Optimized Spectrum Decision in Distributed Cognitive Radio Scenarios

Department of Informatics Engineering
Faculty of Sciences and Technology
University of Coimbra

José Manuel Meireles Marinho

Thesis submitted as partial fulfilment of the requirements of the Doctoral Program on Information Science and Technology in the University of Coimbra, for the award of Doctor in the domain of Telematics Networking and Communications under care of advisor Professor Doutor Edmundo Heitor da Silva Monteiro.

2015

Advisor

Professor Doutor Edmundo Heitor Silva Monteiro

Full Professor
Department of Informatics Engineering
Faculty of Sciences and Technology of the University of Coimbra

“To have a great idea, have a lot of them.”

Thomas A. Edison

Acknowledgments

I would like to express my gratitude to Professor Edmundo Monteiro, my thesis advisor, for his encouragement, guidance, and support during the course of this research.

The main ideas within this thesis have been improved thanks to the comments of various anonymous reviewers and to interesting discussions when presenting versions of the developed work at the meetings organized by the Laboratory of Communications and Telematics of CISUC (Centre for Informatics and Systems of the University of Coimbra).

I am very grateful to the Polytechnic Institute of Coimbra - Coimbra Engineering Institute, CISUC, and PROTEC, a Portuguese PhD supporting program. Their support created favourable conditions that helped this work reach a successful conclusion.

I also extend my gratitude to my colleagues and friends at the Polytechnic of Coimbra and CISUC for having aided me in many different ways. In particular, I would like to thank Cristina Chuva, Pedro Martins, and Luís Santos who gave me countless valuable advices.

Finally, I wish to express a heartfelt thanks to my parents and daughter for being a source of motivation and encouragement.

Abstract

The radio spectrum has been statically regulated, i.e., essentially partitioned into licensed frequency bands, which are accessed exclusively by authorized users, and unlicensed frequency bands that can be freely accessed. Due to this inflexible policy, large portions of the entire radio spectrum remain unused independently of time and location in the world, while some frequency bands suffer from increasing levels of saturation, particularly the unlicensed ones in densely populated areas. Cognitive Radio (CR) is a recent paradigm that aims at improving efficiency regarding spectrum utilization. Its principles consist in allowing unlicensed wireless devices (i.e., secondary users) to access licensed frequency bands provided that the respective incumbent users (i.e., primary users) do not suffer any harmful interference. The most preponderant CR approach consists in having a secondary user (SU) dynamically locating and accessing spectrum opportunities, i.e., frequency bands that are not being accessed by any primary user (PU) at a given time and location. Consequently, sensing the spectrum and learning through local observation and past experience, which enables proactive spectrum decision, are key CR issues. Despite CR has implications in all the layers of the communication protocol stack, its fundamentals are mainly related to the physical (PHY) and medium access control (MAC) levels. In fact, CR MAC protocols are at the heart of spectrum access control and cooperation between SUs. PUs are expected to be unware of CR operations and, consequently, should not suffer any modification under CR scenarios.

This thesis provides five contributions, essentially related to the MAC level, with the aim of improving the protection of PUs and the communication performance of SUs in cooperative distributed CR networks, particularly when there is no access to any a priori known information, such as the locations of primary transmitters. In this type of scenario, there are no central entities that collect and fuse data, or take spectrum decisions. That is, the proposed solutions fit into totally autonomous and cooperating SUs, i.e., SUs that take their own decisions based on local observation, on learning outcomes if any is available, and on data they exchange with each other.

The first contribution of this thesis consists in a description of the CR area through an in-depth state of the art.

The second contribution lies in the definition of a CR MAC protocol that follows a novel approach, named Cooperative Sense-Before-Transmit (COSBET), which provides a higher protection of PUs in distributed CR scenarios that suffer from the hidden PU problem. This issue occurs when a SU cannot sense the activities of a given PU despite it can cause harmful interference to its coverage area.

As already mentioned, CR considers that the SUs might have learning capabilities based on local observation and past experience. However, in distributed scenarios, the hidden PU problem affects the accuracy of learning and, therefore, the effectiveness of PU protection. For that reason, in this thesis we also discuss this issue and propose a novel solution that addresses it. This solution is based on a key concept named FIBASC (Filtering Based on Suspicious Channels).

Utilizing a common control channel (CCC), i.e., a channel that is available to all the SUs in a CR network, for signalling purposes is a frequent practice concerning existing distributed CR MAC solutions. It is also the solution adopted by COSBET-MAC. However, a CCC is susceptible to saturation and can, therefore, become a performance bottleneck that inhibits the SUs from taking full advantage of CR potentialities. Consequently, the fourth contribution of this thesis consists in analysing this issue and addressing it through a novel solution, which we named CORHYS (Cognitive Radio Hybrid Signalling). CORHYS is based on a hybrid signalling approach that performs signalling over the CCC and over the allocated data channels simultaneously.

The fifth and last contribution of this thesis consists in a MAC-level strategy that aims at further improving the performance of SUs in distributed CR scenarios that are based on a CCC. The key guidelines for this strategy are optimizing the spatial reuse of the radio spectrum and reducing control traffic.

The CR solutions that resulted from this thesis were evaluated through simulation, which is a common practice, particularly due to time and other resource restrictions. For this purpose, we used OMNET++ (Objective Modular Network Testbed in C++), an open source discrete event simulator.

The contributions of this thesis can be applied jointly and were successfully integrated with each other, which resulted in an optimized CR MAC solution that addresses the two main concerns in distributed CR scenarios: protecting the PUs from harmful interference; and improving the communication performance of the SUs. To the best of our knowledge, the proposed solutions and the level of completeness that they jointly achieve are not found in any other existing distributed CR MAC proposal. We also note that they define directions that can be followed by other CR MAC protocols, particularly those that target distributed CR networks.

Resumo

O espectro rádio tem vindo a ser regulado de um modo estático. Ou seja, este encontra-se essencialmente dividido em bandas de frequência licenciadas, com utilização restringida a um número limitado de utilizadores autorizados, e em algumas bandas de frequência não licenciadas para utilização livre. Devido à falta de flexibilidade resultante desta abordagem, partes significativas do espectro rádio encontram-se subutilizadas. Em simultâneo, outras bandas de frequência estão a ficar cada vez mais saturadas, nomeadamente as não licenciadas em áreas densamente povoadas.

O Rádio Cognitivo é um paradigma recente cujo objetivo é melhorar o nível de eficiência na utilização do espectro rádio. Os seus princípios gerais consistem em permitir que dispositivos sem fios não licenciados (os denominados Utilizadores Secundários) possam aceder às bandas de frequência licenciadas desde que estes não interferiram de forma prejudicial com os utilizadores licenciados (os denominados Utilizadores Primários). A abordagem preponderante na área de Rádio Cognitivo consiste em ter utilizadores secundários com capacidade para, de um modo dinâmico, detetar e aceder a oportunidades espectrais, ou seja, bandas de frequência que não estão a ser acedidas pelos respetivos utilizadores primários num determinado momento numa determinada localização. Neste contexto, os utilizadores secundários devem ser capazes de analisar o espectro rádio com precisão e, de preferência, possuírem mecanismos de aprendizagem baseados em observação local e experiência passada. Apesar da área de Rádio Cognitivo ter implicações na totalidade das camadas das pilhas protocolares de comunicação, os seus problemas fundamentais localizam-se nos níveis físico (PHY) e de controlo de acesso ao meio (MAC). Em particular, os protocolos de controlo de acesso ao meio desempenham um papel fundamental no âmbito de operações de controlo de acesso ao espectro rádio e de suporte à cooperação entre utilizadores secundários. Os utilizadores primários, quanto a eles, devem manter-se abstraídos das operações de Rádio Cognitivo e, em consequência, não estarem sujeitos a qualquer tipo de alteração em cenários de Rádio Cognitivo.

Esta tese apresenta cinco contribuições, essencialmente relacionadas com o nível do controlo de acesso ao meio, com o objetivo de incrementar os níveis de proteção dos utilizadores primários e de desempenho dos utilizadores secundários em redes de Rádio Cognitivo distribuídas, especialmente quando os utilizadores secundários não têm antecipadamente acesso a qualquer tipo de informação, tal como a localização de utilizadores primários. Neste tipo de cenário, não existe qualquer entidade central responsável por recolher e processar dados de origem diversa ou tomar decisões de acesso ao espectro rádio. Ou seja, as soluções propostas

adequam-se a utilizadores secundários que operam de um modo autónomo e cooperativo. Estes tomam as suas decisões baseando-se, essencialmente, em observações locais, em eventuais resultados de aprendizagem e em dados trocados entre si.

A primeira contribuição desta tese consiste numa descrição da área de Rádio Cognitivo através de um estado da arte detalhado.

A segunda contribuição resulta na definição de um protocolo de controlo de acesso ao meio apoiado num mecanismo inovador, designado COSBET (*Cooperative Sense-Before-Transmit*), que oferece um nível superior de proteção dos utilizadores primários em cenários de Rádio Cognitivo distribuídos sujeitos ao problema do utilizador primário oculto. Este tipo de anomalia ocorre quando um utilizador secundário é incapaz de detetar as atividades de um determinado utilizador primário apesar de poder provocar interferências na respetiva área de abrangência.

Tal como já foi referido, na área de Rádio Cognitivo, é considerado desejável os utilizadores secundários terem capacidades de aprendizagem baseadas em observação local e experiência passada. No entanto, em cenários distribuídos, o problema do utilizador primário oculto afeta negativamente a qualidade dos resultados de aprendizagem obtidos e, em consequência, o nível efetivamente alcançado em termos de proteção dos utilizadores primários. Sendo assim, esta tese também analisa esta questão e propõe uma solução destinada a tratá-la, estando esta terceira contribuição baseada num conceito chave designado FIBASC (*Filtering Based on Suspicious Channels*).

A troca de informação de controlo em redes de Rádio Cognitivo distribuídas é frequentemente suportada por um canal partilhado e acessível à globalidade dos utilizadores secundários. Este é o designado canal de controlo comum (CCC), sendo igualmente esta a abordagem seguida pelo protocolo COSBET-MAC proposto. No entanto, os CCC estão sujeitos a problemas de saturação. A ocorrência deste tipo de problema impede os utilizadores secundários de tirarem pleno proveito das potencialidades oferecidas pelo Rádio Cognitivo, acabando por limitar os níveis de desempenho de comunicação alcançáveis. Sendo assim, nesta tese também analisamos esta questão e propomos uma solução destinada a abordá-la, correspondendo esta à nossa quarta contribuição. A solução proposta, designada CORHYS (*Cognitive Radio Hybrid Signalling*), baseia-se num esquema de sinalização híbrido que recorre simultaneamente a um CCC e aos canais de dados que vão sendo alocados de forma dinâmica.

A quinta e última contribuição desta tese consiste na definição de uma estratégia adicional, igualmente localizada no nível do controlo de acesso ao meio, destinada a melhorar o desempenho dos utilizadores secundários em cenários de Rádio Cognitivo distribuídos em que se recorre a um

CCC. Fazem parte das suas linhas orientadoras a otimização da reutilização espacial do espectro rádio e a redução do tráfego de controlo gerado entre utilizadores secundários.

As soluções de Rádio Cognitivo propostas no âmbito desta tese foram avaliadas em ambiente de simulação, sendo esta uma prática comum, nomeadamente devido a limitações de tempo e de outros tipos de recursos. Para o efeito, recorreu-se ao OMNET++ (*Objective Modular Network Testbed in* C++), um simulador baseado em eventos discretos e de código aberto.

A totalidade das contribuições da presente tese podem ser aplicadas em conjunto. A integração destas deu origem a uma solução única e otimizada de controlo de acesso ao meio destinada a cenários de Rádio Cognitivo distribuídos. Esta aborda as duas principais preocupações existentes em cenários de Rádio Cognitivo: proteger os utilizadores primários de qualquer tipo de interferência prejudicial; e melhorar o desempenho de comunicação dos utilizadores secundários. Tanto quanto sabemos, as várias soluções propostas e o nível de completude que a utilização conjunta destas permite não são oferecidos por qualquer outra proposta de controlo de acesso ao meio existente para cenários de Rádio Cognitivo distribuídos. As contribuições desta tese também apontam direções que podem ser seguidas no âmbito de outros protocolos de controlo de acesso ao meio, especialmente aqueles que se destinam a redes de Rádio Cognitivo distribuídas.

Foreword

The work described in this thesis was conducted at the Laboratory of Communication and Telematics (LCT) of the Centre for Informatics and Systems of the University of Coimbra (CISUC) under the following projects:

- COST Action IC0906: WiNeMO - Wireless Networking for Moving Objects.
- Project iCIS - Intelligent Computing in the Internet of Services, reference CENTRO-07-0224-FEDER-002003.

The performed work resulted in the following publications:

- Marinho, J. and Monteiro, E. (2011, November). Cognitive Radio Simulation based on OMNeT++/MiXiM. *Proc. of the 11ª Conferência sobre Redes de Computadores. CRC 2011.*
- Marinho, J. and Monteiro, E. (2012). Cognitive Radio: Survey on Communication Protocols, Spectrum Decision Issues, and Future Research Directions. *Wireless Networks*, 18(2), 147-164. doi: 10.1007/s11276-011-0392-1 (2013 Impact Factor: 1.055; number of citations on July 2015: 57).
- Marinho, J. and Monteiro, E. (2012). Cooperative Sensing-Before-Transmit in Ad-hoc Multi-hop Cognitive Radio Scenarios. *10th International Conference on Wired/Wireless Internet Communications. WWIC 2012*. (pp. 186-197). Springer Berlin Heidelberg. doi: 10.1007/978-3-642-30630-3_16 (acceptance rate: 46%; ERA ranking: B).
- Marinho, J. and Monteiro, E. (2012). Enhanced Protection of Hidden Primary Users through Filtering based on Suspect Channels Classification. *2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* (pp. 419-426). IEEE. doi: 10.1109/WiMOB.2012.6379107 (acceptance rate: 24.5%; ERA ranking: C).
- Marinho, J. and Monteiro, E. (2015). CORHYS: Hybrid Signaling for Opportunistic Distributed Cognitive Radio. *Computer Networks*, 81, 19-42. doi: 10.1016/j.comnet.2015.01.019 (2013 Impact Factor: 1.252).

- Marinho, J., Granjal, J., and Monteiro, E. (2015). A Survey on Security Attacks and Countermeasures with Primary User Detection in Cognitive Radio Networks. *EURASIP Journal on Information Security*, 2015(4), 1-14. doi: 10.1186/s13635-015-0021-0.

Table of contents

CHAPTER 1 INTRODUCTION 1

1.1 MOTIVATION 1
1.2 OBJECTIVES AND CONTRIBUTIONS 5
1.3 OUTLINE 6

CHAPTER 2 COGNITIVE RADIO 9

2.1 INTRODUCTION 10
2.2 RELATED TECHNOLOGIES AND STANDARDS 13
2.3 STANDARDIZATION ACTIVITIES 15
2.4 CR ARCHITECTURAL APPROACHES 16
2.5 MAIN CR ISSUES 18
  2.5.1 Self-coexistence 18
  2.5.2 Spectrum Sensing 19
  2.5.3 Signalling 24
  2.5.4 Spectrum decision 27
  2.5.5 Seamless spectrum handover 28
  2.5.6 Security 28
  2.5.7 Energy Efficiency 32
  2.5.8 Validation of CR proposals 32
2.6 COMMUNICATION PROTOCOLS FOR COGNITIVE RADIO SCENARIOS 34
  2.6.1 Medium Access Control protocols 35
  2.6.2 Network Layer protocols 40
  2.6.3 Transport Layer protocols 42
  2.6.4 Application Layer protocols 43
2.7 INTELLIGENT SPECTRUM DECISION IN CR 43
  2.7.1 Learning based on observation and past experience, and prediction in CR scenarios 44
  2.7.2 Primary user traffic modelling 45
  2.7.3 Cognitive Radio proposals with prediction-based capabilities 48
2.8 SUMMARY 51

CHAPTER 3 COOPERATIVE SENSE-BEFORE-TRANSMIT 53

3.1 INTRODUCTION 54
3.2 RELATED WORK AND CONTRIBUTIONS 54
3.3 COOPERATIVE SENSE-BEFORE-TRANSMIT APPROACH 56
  3.3.1 Channel selection phase 58
  3.3.2 Cooperative sensing phase 59
  3.3.3 Further cooperation 61
  3.3.4 Decision phase 63
3.4 PERFORMANCE EVALUATION 64
  3.4.1 Evaluation methodology 64
  3.4.2 Simulation settings 66
  3.4.3 Communication performance 68
  3.4.4 Protection of primary users 73
  3.4.5 Impact of sensing imperfections 75
  3.4.6 Simultaneous channel access by two-hop neighbours 77
3.5 SUMMARY 79

CHAPTER 4 FILTERING BASED ON SUSPICIOUS CHANNELS CLASSIFICATION 81

4.1 Introduction ... 82
4.2 Related work and contributions ... 86
4.3 Effective utilization of prediction capabilities ... 87
  4.3.1 Classification of channels as suspicious ... 88
  4.3.2 Filtering based on suspicious channels ... 90
  4.3.3 Integrating FIBASC with COSBET-MAC ... 94
4.4 Performance evaluation ... 98
  4.4.1 Methodology and simulation settings ... 98
  4.4.2 Protection of PUs ... 98
  4.4.3 Utilization of channels ... 103
  4.4.4 Impact on communication Performance ... 104
4.5 Summary ... 107

CHAPTER 5 HYBRID SIGNALLING FOR DISTRIBUTED COGNITIVE RADIO ... 109

5.1 Introduction ... 110
5.2 Related work and contributions ... 112
5.3 Cognitive Radio hybrid signalling ... 116
  5.3.1 Out-of-band handshake ... 117
  5.3.2 In-band signalling with multi-frame channel access ... 118
  5.3.3 Multi-frame channel reservation ... 122
5.4 Performance evaluation ... 127
  5.4.1 Simulation setup ... 127
  5.4.2 Throughput and channel utilization efficiency ... 129
  5.4.3 Throughput and latency with channel access time limitation ... 135
  5.4.4 Impact of sensing time ... 142
  5.4.5 Impact of the number of secondary users ... 144
  5.4.6 Impact of joint traffic pattern ... 147
  5.4.7 Impact of primary user activity ... 149
5.5 Summary ... 152

CHAPTER 6 ENHANCING THE SPATIAL REUSE OF THE SPECTRUM AND LOWERING CONTROL TRAFFIC ... 155

6.1 Introduction ... 156
6.2 Related work and contributions ... 157
6.3 PEL strategy ... 161
  6.3.1 Improved spatial utilization of the spectrum ... 162
  6.3.2 Reduction in the number of transmitted control frames ... 169
6.4 Performance evaluation ... 174
  6.4.1 Simulation setup ... 174
  6.4.2 Effectiveness of the PEL strategy ... 176
  6.4.3 Comparison with single-channel access approach ... 178
  6.4.4 Protection of primary users ... 179
  6.4.5 Joint utilization of the PEL strategy with CORHYS ... 183
6.5 Summary ... 187

CHAPTER 7 CONCLUSIONS AND FUTURE WORK ... 189

7.1 Conclusions ... 189
7.2 Future work ... 191

REFERENCES ... 193

List of Figures

Figure 2.1. Opportunistic/dynamic spectrum access ... 11

Figure 2.2. Generic Cognitive Radio Architecture ... 13

Figure 2.3. Basic Cognitive Radio cycle ... 14

Figure 2.4. Main CR architectural approaches ... 17

Figure 2.5. Sense-before-transmit approach ... 20

Figure 2.6. The hidden primary user problem ... 21

Figure 2.7. Cooperative sensing approaches in distributed and centralized CR scenarios ... 22

Figure 2.8. Signalling based on a common control channel ... 25

Figure 2.9. Communication protocol issues in Cognitive Radio scenarios ... 35

Figure 2.10. Primary user traffic ... 46

Figure 2.11. Semi-Markov process ... 50

Figure 3.1. Interaction between secondary users ... 57

Figure 3.2. A scenario with hidden primary users and hidden secondary users ... 62

Figure 3.3. A secondary user architecture based on a multi-radio model ... 65

Figure 3.4. Aggregate throughput (scenario with 2 transmitter-receiver pairs) ... 70

Figure 3.5. Aggregate throughput (scenario with 4 transmitter-receiver pairs) ... 70

Figure 3.6. Aggregate throughput (scenario with 6 transmitter-receiver pairs) ... 70

Figure 3.7. Aggregate throughput with variable sensing time and variable data frame payload size (2 Mbit/s load per transmitter and 4 transmitter-receiver pairs) ... 72

Figure 3.8. Aggregate throughput vs. primary user traffic characteristics (2 Mbit/s load per transmitter and 0.5 milliseconds sensing time) ... 74

Figure 3.9. Variation in the rate of missed PU detections and aggregate throughput due to the cooperation of idle neighbours in sensing (scenario in Figure 3.2) ... 75

Figure 3.10. Variation in the rate of missed PU detections and aggregate throughput due to the cooperation of idle neighbours in sensing (scenario in Figure 3.2 with 50 additional idle neighbours) ... 75

Figure 3.11. Probability of false alarm with COSBET-MAC ... 77

Figure 3.12. Probability of missed PU detection with COSBET-MAC ... 77

Figure 3.13. Aggregate throughput with different missed detection and false alarm probabilities ... 78

Figure 3.14. Aggregate throughput with 2 Mbit/s load per transmitter and 32 secondary users randomly placed with a uniform distribution ... 79

Figure 4.1. A scenario with hidden primary users and hidden secondary users ... 84

Figure 4.2. Impact of fully accurate prediction capabilities on missed PU detections and interferences to PUs ... 85

Figure 4.3. Channel selection pattern of pair 1-2 in Figure 4.1 when using COSBET-MAC ... 86

Figure 4.4. Channels to be avoided in Figure 4.1 due to the hidden PU problem ... 91

Figure 4.5. Channels the transmitter-receiver pairs avoid in Figure 4.1 when using two-hop FIBASC ... 91

Figure 4.6. Channel selection with two-hop FIBASC 93

Figure 4.7. Variation in the rate of missed PU detections when compared to COSBET-MAC with no prediction capabilities 99

Figure 4.8. Variation in the rate of interferences to PUs when compared to COSBET-MAC with no prediction capabilities 99

Figure 4.9. Variation in the number of missed PU detections when comparing a generic sense-before-transmit approach to COSBET-MAC with no prediction capabilities..... 101

Figure 4.10. Variation in the number of interferences to PUs when comparing a generic sense-before-transmit approach to COSBET-MAC with no prediction capabilities 101

Figure 4.11. Variation in the number of missed PU detections when compared to COSBET-MAC with no prediction capabilities (scenario with 20 additional SUs)..... 102

Figure 4.12. Variation in the number of interferences to PUs when compared to COSBET-MAC with no prediction capabilities (scenario with 20 additional SUs)..... 102

Figure 4.13. Channel selection pattern when using COSBET-MAC with two-hop FIBASC and assuming fully accurate prediction capabilities..... 103

Figure 4.14. Global channel selection pattern when using COSBET-MAC with two-hop FIBASC and assuming fully accurate prediction capabilities..... 104

Figure 4.15. Global channel selection pattern when using COSBET-MAC with two-hop FIBASC and assuming fully accurate prediction capabilities (scenario with 20 additional SUs) 104

Figure 4.16. Variation in aggregate throughput when compared to COSBET-MAC with no prediction capabilities 105

Figure 4.17. Variation in aggregate throughput of a generic sense-before-transmit approach when compared to COSBET-MAC with no prediction capabilities 106

Figure 4.18. Aggregate throughput when there are no hidden PUs and the SUs have fully accurate prediction capabilities..... 106

Figure 5.1. Common control channel saturation problem..... 112

Figure 5.2. Out-of-band handshake..... 117

Figure 5.3. Transmission of multiple data frames with in-band signalling 119

Figure 5.4. Transmission of multiple data frames without in-line cooperative sensing 121

Figure 5.5. Aggregate throughput 129

Figure 5.6. Comparison with the proposal of Jia and Zhang [2009] concerning aggregate throughput..... 133

Figure 5.7. Impact of CSI control frames on aggregate throughput 134

Figure 5.8 Impact of parameter λ (upper limit for channel reservation time) on aggregate throughput (2 Mbit/s load per transmitter, 4 channels with 8 Mbit/s aggregate bit rate, and MAC output queues with 50 frames maximum size)..... 136

Figure 5.9 Impact of parameter λ (upper limit for channel reservation time) on average latency (2 Mbit/s load per transmitter, 4 channels, and MAC output queues with 50 frames maximum size)..... 137

FIGURE 5.10 IMPACT OF PARAMETER λ (UPPER LIMIT FOR CHANNEL RESERVATION TIME) ON AGGREGATE THROUGHPUT (2 MBIT/S LOAD PER TRANSMITTER, 4 CHANNELS WITH 8 MBIT/S AGGREGATE BIT RATE, AND MAC OUTPUT QUEUES WITH 400 FRAMES MAXIMUM SIZE) 139

FIGURE 5.11 IMPACT OF PARAMETER λ (UPPER LIMIT FOR CHANNEL RESERVATION TIME) ON AVERAGE LATENCY (2 MBIT/S LOAD PER TRANSMITTER, 4 CHANNELS, AND MAC OUTPUT QUEUES WITH 400 FRAMES MAXIMUM SIZE) 140

FIGURE 5.12. EFFECT OF SENSING TIME ON AGGREGATE THROUGHPUT (2 MBIT/S LOAD PER TRANSMITTER)....................142

FIGURE 5.13 AGGREGATE THROUGHPUT WHEN CSI FRAMES ARE ALSO USED AS ACKNOWLEDGEMENT FRAMES (2 MBIT/S LOAD PER TRANSMITTER)....................143

FIGURE 5.14 AGGREGATE THROUGHPUT VS. NUMBER OF TRANSMITTER-RECEIVER PAIRS (2 MBIT/S LOAD PER TRANSMITTER, AND 4 CHANNELS WITH 8 MBIT/S AGGREGATE BIT RATE)....................144

FIGURE 5.15 AGGREGATE THROUGHPUT VS. NUMBER OF TRANSMITTER-RECEIVER PAIRS (2 MBIT/S LOAD PER TRANSMITTER, AND 8 CHANNELS WITH 16 MBIT/S AGGREGATE BIT RATE)....................145

FIGURE 5.16 AGGREGATE THROUGHPUT VS. NUMBER OF TRANSMITTER-RECEIVER PAIRS WHEN USING IEEE 802.11 (2 MBIT/S LOAD PER TRANSMITTER, 1 CHANNEL WITH 2 MBIT/S BIT RATE)....................146

FIGURE 5.17. AGGREGATE THROUGHPUT WHEN USING JOINT SU TRAFFIC....................147

FIGURE 5.18. AGGREGATE THROUGHPUT WHEN USING JOINT SU TRAFFIC AND PROCESSING THE FRAME AT THE FRONT OF THE MAC OUTPUT QUEUE....................149

FIGURE 5.19. AGGREGATE THROUGHPUT VS. PRIMARY USER BUSY TIME (2 MBIT/S LOAD PER TRANSMITTER, DISJOINT TRAFFIC, NO PREDICTION CAPABILITIES, AND 8 CHANNELS WITH 16 MBIT/S AGGREGATE BIT RATE) 151

FIGURE 5.20. AGGREGATE THROUGHPUT VS. PRIMARY USER BUSY TIME WHEN FULLY ACCURATE PREDICTION IS AVAILABLE (2 MBIT/S LOAD PER TRANSMITTER, DISJOINT TRAFFIC, AND 8 CHANNELS WITH 16 MBIT/S AGGREGATE BIT RATE)....................152

FIGURE 6.1. ISSUES TO BE ADDRESSED AND PROPOSED SOLUTIONS....................161

FIGURE 6.2. SPATIAL REUSE OF THE SPECTRUM 163

FIGURE 6.3. MINIMUM TRANSMISSION RANGE BASED ON DISTANCE TO RECEIVERS 167

FIGURE 6.4. A SCENARIO PRONE TO IGNORED INITIAL CONTROL FRAMES....................170

FIGURE 6.5. SIMULATION SCENARIO 175

FIGURE 6.6. GAINS PROVIDED BY THE PEL STRATEGY....................177

FIGURE 6.7. COMPARISON WITH IEEE 802.11 (AGGREGATE THROUGHPUT AND DATA FRAME LOSS)....................179

FIGURE 6.8. COMPARISON WITH IEEE 802.11 (LATENCY AND JITTER)....................180

FIGURE 6.9. PROTECTION OF PUS AND COMMUNICATION PERFORMANCE WITHOUT PREDICTION CAPABILITIES (2 MBIT/S LOAD PER TRANSMITTER)....................181

FIGURE 6.10. PROTECTION OF PUS AND COMMUNICATION PERFORMANCE WITH PREDICTION CAPABILITIES AND 2-HOP FIBASC (2 MBIT/S LOAD PER TRANSMITTER)....................182

FIGURE 6.11. INTEGRATION WITH CORHYS (2 MBIT/S LOAD PER TRANSMITTER) 184

FIGURE 6.12. INTEGRATION WITH CORHYS AND COOPERATION OF IDLE NEIGHBOURS IN SENSING (2 MBIT/S LOAD PER TRANSMITTER) 185

FIGURE 6.13. INTEGRATION WITH CORHYS, TWO-HOP FIBASC, AND 100% PREDICTION PRECISION (2 MBIT/S LOAD PER TRANSMITTER) 186

List of Tables

TABLE 2.1: CLASSIFICATION OF EXISTING CR MAC PROPOSALS 37

TABLE 2.2: SUPPORTED OPTIMIZATIONS 38

TABLE 2.3: TYPES OF TRAFFIC PATTERNS 47

TABLE 2.4: CR PROPOSALS WITH PREDICTION-BASED CAPABILITIES 49

TABLE 3.1: SIMULATION SETTINGS 67

TABLE 3.2: STANDARD DEVIATION OF AGGREGATE THROUGHPUT IN KBIT/S (DATA POINTS IN FIGURE 3.4) 71

TABLE 3.3: STANDARD DEVIATION OF AGGREGATE THROUGHPUT IN KBIT/S (DATA POINTS IN FIGURE 3.5) 71

TABLE 3.4: STANDARD DEVIATION OF AGGREGATE THROUGHPUT IN KBIT/S (DATA POINTS IN FIGURE 3.6) 71

TABLE 3.5: MAXIMUM NUMBER OF CHANNELS SIMULTANEOUSLY USED (4 CHANNELS, 4 TRANSMITTER-RECEIVER PAIRS, AND 2 MBIT/S LOAD PER TRANSMITTER) 73

TABLE 3.6: STANDARD DEVIATION OF AGGREGATE THROUGHPUT IN KBIT/S WITH DIFFERENT MISSED DETECTION AND FALSE ALARM PROBABILITIES 78

TABLE 4.1: SUSPICIOUS CHANNELS IN FIGURE 4.1 89

TABLE 4.2: FIELDS IN RTS, CTSS, AND FCTSS FRAMES OF COSBET-MAC RELATED TO CHANNEL SELECTION AND TRACKING OF SUSPICIOUS CHANNELS 95

TABLE 5.1: PARAMETERS COMPUTED BY THE TRANSMITTER BASED ON ALGORITHM 5.1 125

TABLE 5.2: SIMULATION SETTINGS 128

TABLE 5.3: STANDARD DEVIATION OF AGGREGATE THROUGHPUT IN KBIT/S (DATA POINTS IN FIGURE 5.5) 130

TABLE 5.4: MAXIMUM NUMBER OF CHANNELS SIMULTANEOUSLY ACCESSED (VARIABLE LOAD PER TRANSMITTER) 131

TABLE 5.5: MAXIMUM NUMBER OF CHANNELS SIMULTANEOUSLY ACCESSED (2 MBIT/S LOAD PER TRANSMITTER) 132

TABLE 5.6: STANDARD DEVIATION OF AGGREGATE THROUGHPUT IN KBIT/S (DATA POINTS IN FIGURE 5.6) 133

TABLE 5.7: STANDARD DEVIATION OF AGGREGATE THROUGHPUT IN KBIT/S (DATA POINTS IN FIGURE 5.7) 135

TABLE 5.8: DATA FRAME LATENCY AND THROUGHPUT FAIRNESS 141

TABLE 5.9: STANDARD DEVIATION OF AGGREGATE THROUGHPUT IN KBIT/S (DATA POINTS IN FIGURE 5.17) 148

TABLE 5.10: STANDARD DEVIATION OF AGGREGATE THROUGHPUT IN KBIT/S (DATA POINTS IN FIGURE 5.18) 150

TABLE 6.1: PEL STRATEGY 173

TABLE 6.2: SIMULATION SETTINGS 176

List of Algorithms

ALGORITHM 3.1. COOPERATIVE SENSE-BEFORE-TRANSMIT 57

ALGORITHM 3.2. COOPERATION OF A NEIGHBOUR DURING A SENSING PHASE 60

ALGORITHM 4.1. FILTERING BASED ON SUSPICIOUS CHANNELS CLASSIFICATION (TWO-HOP APPROACH) 92

ALGORITHM 4.2. TRACKING OF SUSPICIOUS CHANNELS BASED ON RECEIVED/OVERHEARD RTS OR CTSS FRAMES (TWO-HOP APPROACH) 95

ALGORITHM 4.3. TRACKING OF SUSPICIOUS CHANNELS BASED ON RECEIVED/OVERHEARD CTS OR FCTS FRAMES (TWO-HOP APPROACH) 97

ALGORITHM 5.1. SELECTION OF CANDIDATE CHANNELS AND NUMBER OF FRAMES TO BE TRANSMITTED DURING CHANNEL ALLOCATION TIME (EXECUTED BY THE TRANSMITTER) 123

ALGORITHM 5.2. CHANNEL SELECTION MADE BY A RECEIVER 124

ALGORITHM 6.1. VERIFICATION MADE BY A SU TO DETERMINE IF IT CAN UTILIZE A GIVEN DATA CHANNEL 165

ALGORITHM 6.2. VERIFICATION MADE BY A SU THAT IS ALREADY ACCESSING A DATA CHANNEL AND THAT OVERHEARS A CONTROL FRAME INDICATING THE SELECTION OF A CHANNEL 166

ALGORITHM 6.3. TRANSMISSION OF INITIAL CONTROL FRAMES BASED ON THE USE OF REGULAR AND EXTENDED TIMEOUTS 172

List of Acronyms

AMRCC	Adaptive Multiple Rendezvous Control Channel
AoA	Angle of Arrival
ARIMA	Auto-Regressive Integrated Moving Average
C-CSMA/CA	Cognitive radio CSMA/CA
C-MAC	Cognitive-MAC
CBS	Coordinated Bandwidth Sharing
CBS-MAC	Coordinated Bandwidth Sharing-MAC
CCC	Common Control Channel
CFB	Contention-Free Burst
CLBO-MAC	Cross-Layer Based Opportunistic –MAC
CogMAC	Cognitive MAC
CORE+	Cognitive Radio Trial Environment+
CORHYS	Cognitive Radio Hybrid Signalling
CORNET	Cognitive Radio Network
CorteXlab	Cognitive Radio Testbed Experimentation Lab
COSBET	Cooperative Sense-Before-Transmit
CR	Cognitive Radio
CRAHN	Cognitive Radio Ad-Hoc Network
CREW	Cognitive Radio Experimentation World
CROWN	Collective Routing, Scheduling and Frequency Assignment for Wireless Ad-Hoc Networks with Spectrum-Agile Nodes
CSI	Channel Sensed Idle
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
CTSS	Clear to Sense
DCA-MAC	Distributed channel assignment-MAC
DCF	Distributed Coordination Function
DCS	Dynamic Channel Selection
DCS 1800	Digital Cellular Service 1800
DCSS-MAC	Distributed Coordinated Spectrum Sharing-MAC
DDH-MAC	Dynamic De-Centralized Hybrid-MAC
DFA-MAC	Distributed Frequency Agile-MAC
DFS	Dynamic Frequency Selection

DoS	Denial of Service
DOSP	Dynamically Optimized Spatiotemporal Prioritization
DOSS MAC	Dynamic Open Spectrum Sharing MAC
DSA	Dynamic Spectrum Access
DSA-MAC	Dynamic Spectrum Allocation-MAC
DSC	Dynamic Channel Selection
DySPAN	Dynamic Spectrum Access Networks
DySPAN-SC	Dynamic Spectrum Access Networks Committee
ECMA	European Computer Manufacturing Association
EDCF	Enhanced Distributed Coordination Function
ETSI	European Telecommunications Standards Institute
FCC	Federal Communication Community
fCTS	Forwarded Clear To Send
fCTSS	Forwarded Clear to Sense
FIBASC	Filtering Based on Suspicious Channels Classification
GPS	Global Position System
HC-MAC	Hardware Constrained-MAC
IC	Initial Control
IDE	Integrated Development Environment
IEEE	Institute of Electrical and Electronics Engineers
INSA	Institut National des Sciences Appliquées
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
ISP	Internet Service Provider
ITU	International Telecommunication Union
ITU-R	ITU Radio communication sector
MAC	Medium Access Control
MF	More Fragments
MiXiM	Mixed Simulator
MMAC-CR	Multichannel MAC protocol for CR networks
MTU	Maximum Transfer Unit
OMNET	Objective Modular Network Testbed
OOB	Out-of-Band
ORBIT	Open-Access Research Testbed for Next-Generation Wireless Networks
OS-MAC	Opportunistic Spectrum-MAC

OSA	Opportunistic Spectrum Allocation
OSA-MAC	Opportunistic Spectrum Access-MAC
OSI	Open Systems Interconnection
P-MAC	Predictive-MAC
PEL	Power control, avoidance of the Exposed node problem, and Late replies
PHY	Physical
POMDP	Partially Observable Markov Decision Process
PU	Primary User
QoE	Quality of Experience
QoS	Quality of Service
RRS	Reconfigurable Radio System
RSSI	Received Signal Strength Indicator
RTS	Request To Send
SCA	Software Communications Architecture
SCA-MAC	Statistical Channel Allocation-MAC
SCC41	Standards Coordinating Committee 41
SDR	Software Defined Radio
SEARCH	Spectrum Aware Routing Protocol for Cognitive Ad-Hoc Networks
SH-MAC	Slow Hopping-MAC
SIFS	Short Inter-frame Space
SRAC MAC	Single Radio Adaptive Channel MAC
SSC	Shared Spectrum Company
SU	Secondary User
SYN-MAC	Synchronized-MAC
TC	Technical Committee
TCP/IP	Transmission Control Protocol/Internet Protocol
TCP	Transmission Control Protocol
TPC	Transmit Power Control
UHF	Ultra High Frequency
U-NII	Unlicensed National Information Infrastructure
USB	Universal Serial Bus
USRP	Universal Software Radio Peripheral
UWB	Ultra Wide Band
VHF	Very High Frequency
WiNC2R	Winlab Network Centric CR

WP	Working Party
WRAN	Wireless Regional Area Networks

Chapter 1

Introduction

This thesis is focused on Cognitive Radio (CR), a recent paradigm that makes a shift to a more flexible and, therefore, efficient utilization of the radio spectrum, which is a resource with an ever growing scarcity, for wireless data communications. The fundamentals of CR consist in allowing unlicensed wireless devices to access licensed frequency bands provided that the respective incumbent users do not suffer harmful interferences. The contributions of this thesis consist in medium control access-level solutions that aim at increasing the performance of ad-hoc CR networks. These contributions relate to cooperative sensing, effective utilization of prediction capabilities based on learning through past experience and local observation, and communication performance improvement. Performance optimization is twofold under CR: increasing the protection of licensed users; and improving the communication performance of CR devices (i.e., unlicensed users). Therefore, this thesis makes contributions to solve both problems. The current chapter discusses the motivation for the work this document describes as well as its objectives and contributions, and presents the outline of the thesis.

1.1 Motivation

The radio spectrum has been regulated by inflexible policies that allocate most of it to the so-called licensed or incumbent users, which have exclusive access to their respective frequency bands, and dedicates a limited portion of it to unlicensed accesses. That is, the spectrum is statically divided into licensed and unlicensed frequencies. Therefore, the few existing unlicensed frequency bands must be shared by numerous technologies such as wireless local area networks and cordless phones. These regulatory policies result in an increasing scarcity of the radio spectrum and overcrowding of the unlicensed frequency bands, especially in urban areas. However, a report from the Federal Communication Community (FCC) concluded that licensed frequency bands are often underutilized [FCC Spectrum Policy Task Force, 2002]. That is, due to the current regulatory policies, the radio spectrum is being inefficiently used, and the aforementioned scarcity can be considered artificial. These conclusions also suggest that the temporally available spectrum opportunities, which directly result from the underutilization of large portions of the entire spectrum, can be used to address the inefficient utilization of the radio spectrum. Basically, unlicensed wireless devices (i.e., secondary users) should be allowed to freely and opportunistically access the entire radio spectrum or at least a wide range of frequencies, as long as they do not harmfully interfere with licensed systems (i.e., primary users). Enabling more flexible regulation policies and developing related technologies are the aim of CR, being its two main goals: increasing the communication performance of secondary users (SUs); and avoiding harmful interferences to primary users (PUs).

A SU is expected to have the capability to observe and learn from its environment, and to dynamically and autonomously adjust its transmission parameters, such as the operating frequency and transmission power, in order to increase its performance on a non-interference basis. A key enabler of CR is the availability of Software Defined Radios (SDR), i.e., radio systems with components implemented in software rather than in hardware, which enables them to dynamically reconfigure their operating parameters (e.g., frequency range, transmission power, and modulation type). In opportunistic CR scenarios, the type of CR approach this thesis focuses, the SUs are allowed to opportunistically access temporally vacant spectrum bands (i.e., the so-called white spaces, spectrum holes, or spectrum opportunities). This approach results in dynamic multichannel spectrum access and enables distinct SUs to communicate simultaneously over a wide range of frequency bands (i.e., channels). Therefore, the SUs must be able to precisely locate spectrum opportunities, which is thus the most fundamental and challenging issue in opportunistic CR environments. Among other capabilities, this objective requires accurate spectrum sensing techniques, signalling schemes that enable gathering relevant information from the SUs or exchanging pertinent data among them, and learning through past experience and observation, which allows optimized spectrum decisions. Moreover, CR expects the PUs to suffer no modifications (i.e., CR operations must be transparent for the PUs).

A CR network might adopt a centralized (i.e., infrastructure-based) or a distributed (i.e., ad-hoc) architecture. With a centralized approach, spectrum decisions are performed and coordinated by a central entity (e.g., a base station) based on the fusion of data collected from the SUs. The central entity can additionally rely on geo-location databases that provide the coordinates of known primary transmitters (e.g., television transmitter towers) and their respective regions of potential interference. In distributed CR networks, each SU supports its own spectrum decisions based on local observation and learning. Beyond centralized and distributed architectures, CR mesh networks might also be considered and consist in spectrum decision being performed by several mesh gateways or by the SUs themselves, with optional utilization of geo-location databases accessible through the gateways. With cooperative distributed schemes, each SU also uses signalling information provided by its neighbours (e.g., sensing reports), acting, therefore, as a data fusion centre. Cooperative schemes have more communication overhead than non-cooperative solutions, but might result in higher spectrum usage efficiency and sensing accuracy. For example, local sensing is known to be incapable of delivering totally satisfactory results, namely due to sensor imperfections, adverse signal propagation effects, and the hidden PU problem (i.e., a SU does not succeed sensing the activities of PUs it can interfere with). Therefore, cooperative sensing approaches, which consist in combining the sensing outputs of different SUs or dedicated sensors, and, therefore, taking advantage of spatial diversity, are more accurate.

Even when local or cooperative sensing is perfect, it remains possible that PU activities appear on a channel sensed idle before being accessed by a SU. A possible approach for addressing this issue consists in using learning through past experience and observation, which is a core issue in CR [Akyildiz et al., 2009; Höyhtyä et al., 2008; Clancy et al., 2007; Xiukui and Zekavat, 2008]. Basically, it enables prediction, i.e., probabilistically determining busy and idle periods on the targeted channels, and, therefore, selecting a channel that will probably be sensed idle and won't experience any PU activity during data transmission. Learning enables proactive spectrum decisions. Several research works have indicated that channel occupancy and traffic patterns can be statistically modelled, which makes prediction based on learning feasible [Wang et al., 2010b].

However, learning through local observation does not cope with the hidden PU problem and, therefore, does not provide the expected gains when this issue affects the CR network. That is, if a SU is not capable of listening to the activities of a given PU, it models the respective channel as being always vacant, even if it actually interferes with it. This anomaly might degrade the gains obtained from prediction capabilities, invalidate it, or even result in an increased number of PU interferences [Marinho and Monteiro, 2012c]. In order to support the exchange of signalling information amongst the SUs, using a common control channel (CCC) associated with a dedicated radio on each SU is a common practice since it enables simpler protocol architectures. However, this approach, which requires the SUs to have at least two radios, can saturate and, therefore, become a performance bottleneck.

This thesis specifically targets cooperative distributed CR networks with no access to any a priori information, such as the locations of known primary transmitters and their respective regions of potential interference. Therefore, the medium access control-level solutions it defines are for SUs that only rely on their own observations and learning capabilities, and on any signalling information provided by neighbours, i.e., totally autonomous and cooperating SUs. CR has implications in all the layers of the communication protocol stack. Nevertheless, from the previous discussion, we can conclude that its fundamentals are mainly related to the Physical (PHY) and Medium Access Control (MAC) levels. The scope of this thesis is centred in the MAC sublayer, which is at the heart of spectrum access, signalling, and cooperation between the SUs. It specifically targets the definition of MAC-level solutions that jointly result in higher protection of PUs and better communication performance for the SUs in distributed CR networks. These solutions are based on: the effective utilization of learning through observation and past experience in scenarios with hidden PUs; cooperation among the SUs in terms of sensing, learning, and access to the data channels; power control; distance estimation; and mitigation of the CCC saturation problem.

Although learning, cooperation among the SUs, power control, distance estimation, alternatives to the dedicated CCC, and distributed CR MAC protocols have already been studied in the literature, they are usually designed separately and result in incomplete solutions [Ren et al., 2012]. According to Ren et al. [2012], most protocols for distributed CR networks perform spectrum allocation without cooperation among the SUs and most existing researches do not take into account the hidden PU problem. The same authors consider also that most existing CR protocols do not take full advantage of intelligence and learning abilities to perform spectrum prediction and improve performance, despite these characteristics are important features of CR networks.

Salameh et al. [2010] argue that most exiting CR MAC proposals were developed without exploiting transmission distance, are limited to the analytical aspects of MAC design, and lack complete operational details. Hassan et al. [2011] review existing research works that consider transmission power control. Xiang et al. [2010] also consider that the majority of existing studies about power control are theoretical proposals and that detailed MAC protocols designed with such features are lacking. For instance, the solutions of Qu et al. [2010], Pirmoradian et al. [2012], and Hassan et al. [2011] include power control features. However, they are not jointly specified with any MAC solution and make a few ideal assumptions (e.g., a priori knowing the information on the side of each PU). The work of Wang et al. [2010c] uses power control in order to increase spatial reuse efficiency and support concurrent transmissions. However, it follows a time-slotted access approach, which is distinct from the CR approach this thesis targets.

In their works, Jia and Zhang [2009] do not address sensing and Choi et al. [2006] do not cope with the possibility of hidden PUs. The work of Yuan et al. [2007] is not appropriate for dynamic CR scenarios in terms of PU activity, and Timmers et al. [2010] assume that sensing and communication can be performed simultaneously, which is not compatible with energy detection, the currently most practical approach for sensing the spectrum [Marinho and Monteiro, 2012b]. Su and Zhang [2008] assume that all the SUs have the same channel availability, which is not suitable for large scenarios with spatial heterogeneity. In their work, Zhang and Su [2011] assume that each SU is equipped with n sensors and that it is capable of sensing n channels simultaneously. This is a costly assumption in practical terms.

1.2 Objectives and contributions

From the previous section, we can globally conclude that existing CR MAC proposals are focused on optimizing and addressing a limited number of topics. Actually, several CR challenging issues have already been satisfactory addressed and many still need further investigation, making CR an open research area. On the contrary of existing CR MAC protocols, the contributions in this thesis enable achieving a complete distributed CR MAC solution that follows a cooperative approach and that simultaneously targets the following objectives: efficient spectrum sensing; effective utilization of learning capabilities based on observation and past experience; efficient spatial utilization and reuse of the spectrum; effective protection of PUs in scenarios with spectrum diversity (i.e., when the PU activity sensed by SUs is not consistent over the entire network, even between neighbouring SUs); reduction of the CCC saturation problem; and improvement of the performance that is delivered to the SUs. Considerations on practicality have guided all the design process. We note that the definition of specific mechanisms for learning, traffic modelling, prediction, automated distance estimation, and transmit power control are out of the scope of this thesis. The proposed MAC-level contributions are based on the assumption that these capabilities are available and aim at effectively utilizing them in distributed CR scenarios.

As already mentioned, this thesis proposes contributions that apply to distributed CR networks and globally address the two main concerns of CR: protecting PUs from harmful interferences; and improving the communication performance of SUs. The outcomes of these contributions consist in:

- A CR MAC protocol that copes with hidden PUs and hidden SUs, avoids complex and heavy synchronization schemes, and includes a cooperative sensing solution that is based on a non-mandatory cooperation of idle SUs and improves the protection of hidden PUs.
- A cooperative scheme that, based on learning and sensing outcomes, allows the SUs to identify channels that possibly suffer from the hidden PU problem.

- A channel filtering solution that aims at reducing the level of interference to PUs and enables making an effective utilization of underlying prediction capabilities based on past experience and observation.
- An alternative to exclusively utilizing a dedicated CCC for improving the communication performance of SUs.
- The incorporation of power control and distance estimation in order to improve the spatial reuse of the spectrum and, therefore, the communication performance of SUs.
- A novel solution that enables reducing control traffic among SUs.

All the solutions proposed in this thesis can be used jointly and have been successfully integrated with each other, which resulted in a complete CR MAC protocol that is aware of the two main concerns of CR: protecting PUs from harmful interferences; and improving the communication performance of SUs. We also note that these contributions define directions that can be considered under other CR MAC protocols, particularly those that target distributed CR networks and use a dedicated CCC for control traffic. To the best of our knowledge, the proposed solutions and the level of completeness they jointly achieve are not found in any other existing CR MAC proposal.

1.3 Outline

The remainder of this thesis is organized as follows:

Chapter 2: Cognitive Radio. This chapters provides a comprehensive and self-contained description of the CR area through an in-depth state of the art. It establishes the background that the remaining chapters require.

Chapter 3: Cooperative sense-before-transmit. This chapter describes and analyses the performance of a CR MAC protocol that follows a novel approach, named Cooperative Sense-Before-Transmit approach, which provides a higher protection of PUs in distributed CR scenarios and allows the SUs to make an effective utilization of spectrum opportunities for communication performance improvement.

Chapter 4: Filtering based on suspicious channels classification. This chapter starts demonstrating that, in fully distributed scenarios with hidden PUs, it is not trivial to effectively use prediction capabilities based on learning through observation and past experience. Then, it proposes and evaluates a MAC-level cooperative solution that successfully addresses the identified problem, and integrates it with the CR MAC protocol defined in Chapter 3.

Chapter 5: Hybrid signalling for distributed Cognitive Radio. Utilizing a dedicated CCC for signalling purposes is a frequent practice concerning existing distributed CR MAC solutions. It is also the solution adopted by the CR MAC protocol defined in Chapter 3. However, a CCC can also be a performance bottleneck that inhibits the SUs from taking full advantage of CR potentialities. This chapter characterizes this issue and defines a solution that successfully addresses it.

Chapter 6: Enhancing the spatial reuse of the spectrum and lowering control traffic. This chapter proposes a MAC-level strategy with great potential for improving the performance of SUs in distributed CR networks that are based on the utilization of a CCC. This strategy aims at increasing the spatial reuse of the spectrum and minimizing control traffic. This chapter also provides a summary of all the contributions provided in this thesis since it takes into account the solutions proposed in previous chapters when evaluating the proposed strategy. That is, it evaluates a distributed CR MAC protocol that integrates all the solutions this thesis proposes.

Chapter 7: Conclusions and future work. This chapter draws the final conclusions about the contributions this thesis makes to the CR area. It also discusses possible directions for future work.

Chapter 2

Cognitive Radio

The radio spectrum has been statically allocated and divided between licensed and unlicensed frequencies. Due to this inflexible policy, some frequency bands are growing in scarcity, while large portions of the entire radio spectrum remain unused independently of time and location. Cognitive Radio (CR) is a recent network paradigm that aims a more flexible and efficient use of the radio spectrum [Mitola and Maguire, 1999]. Basically, it allows wireless devices to opportunistically access portions of the entire radio spectrum without causing harmful interferences to licensed users. The objective of CR is avoiding the existence of crowded frequency bands while large portions of the spectrum remain vacant at the same time and location.

This chapter aims at providing a comprehensive and self-contained review of developments in the CR research area, and resulted in the following publications:

- Marinho, J. and Monteiro, E. (2012). Cognitive Radio: Survey on Communication Protocols, Spectrum Decision Issues, and Future Research Directions. *Wireless Networks*, 18(2), 147-164. doi: 10.1007/s11276-011-0392-1.
- Marinho, J., Granjal, J., and Monteiro, E. (2015). A Survey on Security Attacks and Countermeasures with Primary User Detection in Cognitive Radio Networks. *EURASIP Journal on Information Security*, 2015(4), 1-14. doi: 10.1186/s13635-015-0021-0.

It is organized as follows. Section 2.1 introduces the genesis and objectives of CR. Section 2.2 discusses related technologies and standards. Section 2.3 introduces CR-specific standardization activities. Section 2.4 discusses the architectural approaches that are applicable to CR networks. Relevant CR issues are introduced in Section 2.5. Section 2.6 is dedicated to communication protocols that target CR scenarios. Since one of the foundations of CR consists in having wireless nodes being capable of learning through observation and past experience, Section 2.7 discusses the applicability of such kind of capabilities in spectrum decision. Finally, conclusions are drawn in Section 2.8.

2.1 Introduction

Currently, the radio spectrum is divided into licensed and unlicensed frequencies. The licensed spectrum is for the exclusive use of designated users. For instance, it includes the UHF/VHF television frequency bands. The unlicensed spectrum can be freely accessed by any user, following certain rules (e.g., not exceeding a defined limit for transmission power). It includes, for example, the ISM (Industrial, Scientific and Medical) and U-NII (Unlicensed National Information Infrastructure) frequency bands. ISM is shared by technologies such as high speed wireless local area networks and cordless phones. It is used by well-known technologies such as IEEE (Institute of Electrical and Electronics Engineers) 802.11b and IEEE 802.11g. U-NII includes frequency bands that are used by the IEEE 802.11a technology and by internet service providers (ISPs). Therefore, many wireless technologies operate and must coexist in the same frequency bands, and devices must compete with neighbours for the same spectrum resources. Appropriate dynamic frequency selection mechanisms have already been proposed to enable license-free wireless devices to make an efficient use of the unlicensed spectrum. However, the number of non-overlapping frequency bands in the unlicensed spectrum is limited and, therefore, performance degradation cannot be avoided as the spectrum becomes more crowded, especially in densely populated areas.

Nevertheless, while the unlicensed spectrum is becoming more crowded, especially ISM, and the spectrum available to be licensed is growing in scarcity, a report from the Federal Communication Community (FCC) concluded that licensed frequency bands are often underutilized, creating temporally available spectrum opportunities that are variable in time and space [FCC Spectrum Policy Task Force, 2002]. In this report, measurements taken in various major cities of the United States of America show that many portions of the spectrum below 1 GHz are not in use for significant periods of time. Other measurements, taken between January 2004 and August 2005 by the company Shared Spectrum Company (SSC), indicate that, on the average, only 5.2% of the spectrum between 30 MHz and 3 GHz is in use at six different locations in the United States of America. These measurements clearly show that large portions of the licensed spectrum remain unused by the respective primary users (PUs) independently of time and location.

Initially, most of the studies concerning how different frequency bands are used have been done in the United States of America. However, some measurements have also been taken in other regions of the world, such as in New Zealand and in some European countries (e.g., see the work of Lopez-Benitez et al. [2009]). Unused portions of the licensed spectrum can naturally be viewed as spectrum opportunities for unlicensed users, also designated as secondary users (SUs).

Malicious users, which try to cause as much damage as they can, are a third type of users that can also be considered, beyond primary and secondary users. According to Tsagkaris et al. [2008], the underutilization of the radio spectrum is explained by the aforementioned static assignment policies and also by what they designate as governments' overregulation.

CR has therefore emerged as one of the keys that can help addressing the inefficient utilization of the radio spectrum without requiring the allocation of new frequency bands. It exploits unused licensed radio frequencies, often called spectrum holes, white spaces, or spectrum opportunities, opening it to SUs. A SU can opportunistically use these opportunities to increase its performance, provided it does not cause harmful interferences to the respective PUs (see Figure 2.1). The operating spectrum band, other transmission parameters, and the access technology are dynamically and intelligently chosen by a SU based on spectrum availability. Spectrum mobility, spectrum sensing, learning based on past experience and observation, and intelligent decision making are main CR issues [Akyildiz et al., 2008; Ghaboosi et al., 2008; Niyato and Hossain, 2009; Vuran and Akyildiz, 2007].

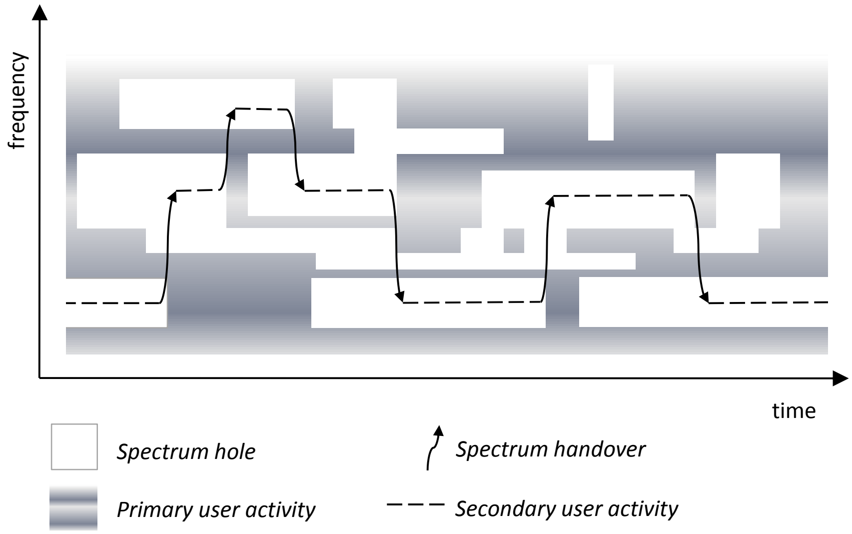


Figure 2.1. Opportunistic/dynamic spectrum access

Akyildiz et al. [2009] state that there are two general models for assigning spectrum usage rights in CR networks: (1) the exclusive use model, which is the classical view of opportunistic spectrum access with no harmful interference to any PU; and (2) the commons model, which does not provide interference protection to any particular user, requiring users to adhere to etiquettes. Beltrán et al. [2010] argue that CR will also contribute to a shift to a more competitive telecommunication landscape, where new operators will collectively and seamlessly provide customers with more flexible and dynamic spectrum arrangements. It can also be noted that the CR paradigm is clearly included by Chen et al. [2008b] in the critical path to future wireless networks.

CR depends on the availability of software defined radio (SDR) solutions, which define a kind of radio that can be reconfigured by software and, therefore, enable dynamically modifying the operating parameters of the SUs. Depending on the level of sophistication of a SDR device, several parameters are reconfigurable (e.g., the operating frequency centre, the bandwidth, the modulation scheme, and the transmission power). SDRs allow a kind of operation that is often designated as Dynamic Spectrum Access (DSA), Opportunistic Spectrum Allocation (OSA), Spectrum Allocation Access, or Spectrum Agile Radio. Basically, a CR is a SDR that is able to intelligently adapt the way it uses the spectrum based on the dynamic behaviour of the radio environment and according to some predefined objectives (e.g., performance, availability, and reliability). Hence, efficient algorithms for learning based on past experience and observation, and for intelligent decision making are highly desirable and expected. Mueck et al. [2010] provide a joint discussion of SDR and CR standards.

CR is highly interdisciplinary, being concerned with distinct engineering and computer science disciplines, such as signal processing, communication protocols, and machine learning [Chowdhury and Melodia, 2010]. Therefore, CR issues can span all the layers of the communication protocol stack (see Figure 2.2) and often require spectrum decisions to be taken according to a cross-layer and transversal approach, which Figure 2.2 depicts as the CR engine module. Nevertheless, its basics are mostly limited to the physical (PHY) and medium access control (MAC) layers. Since this thesis is focused on CR MAC-level solutions, details related to the physical layer, which includes spectrum sensing techniques, and related SDR area remain out of the scope of the discussion. Refer to the work of Yucek and Arslan [2009] for an introduction and comparison of various spectrum sensing methods for CR at the PHY layer.

The main functionalities required for channel management in CR scenarios are spectrum sensing, spectrum decision, spectrum sharing, and spectrum mobility (see Figure 2.3). This results from the fact that SUs must be able to: locate the spectrum holes (spectrum sensing), possibly through coordination with neighbouring SUs; select the best spectrum opportunities in order to meet the user communication requirements (spectrum decision and quality of service provisioning); coordinate access to the selected channels with CR neighbours (spectrum sharing); switch to the selected opportunities (spectrum handover/mobility); maintain seamless communication during CR operations; and avoid harmfully interfering with PUs.

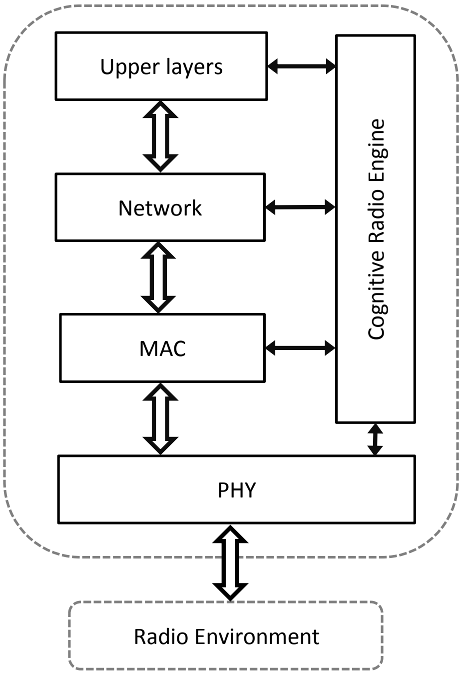


Figure 2.2. Generic Cognitive Radio Architecture

Chen et al. [2008b] define the following requirements for the evolution of wireless networks: (1) wireless devices should configure themselves according to the surrounding; (2) wireless devices will integrate multiple radios to adapt to a wide range of radio scenarios and network architectures; (3) vertical handovers [IEEE 802.21, 2012; Piri and Pentikousis, 2009], i.e., handovers between heterogeneous network technologies, will be frequent due to the mobile and dynamic behaviour of the environment; and (4) components for continuously monitoring the radio and network environment, and for reconfiguration will be needed. From requirements (1) and (4), we conclude that CR, which remains an open research area, is clearly included by Chen et al. [2008b] in the critical path to future wireless networks.

2.2 Related technologies and standards

This section briefly presents non-CR technologies and standards that are related with CR and that can provide a sense of its evolution.

As already mentioned, CR relies on the availability of SDRs, which makes possible dynamically modifying the operating parameters of SUs, and MAC protocols play a central role in CR networks (see Section 2.1). However, CR MAC protocols are not based on totally new methods. Several multichannel MAC protocols have already been proposed as extensions to wireless standards, namely IEEE 802.11-based networks [O'hara and Petrick, 2005], in order to reduce the level of interference between users and increase throughput [Yau et al., 2008]. Multichannel and CR MAC protocols have in common the fact that they operate various channels. CR protocols essentially differ from multichannel protocols as they must be aware of non-deterministic activities from higher priority users (i.e., PUs) and, consequently, must cope with a variable set of available channels. Hence, MAC protocols for multichannel networks cannot be directly applied to CR networks and need additional functionalities in order to be fully qualified as CR [Yau et al., 2008].

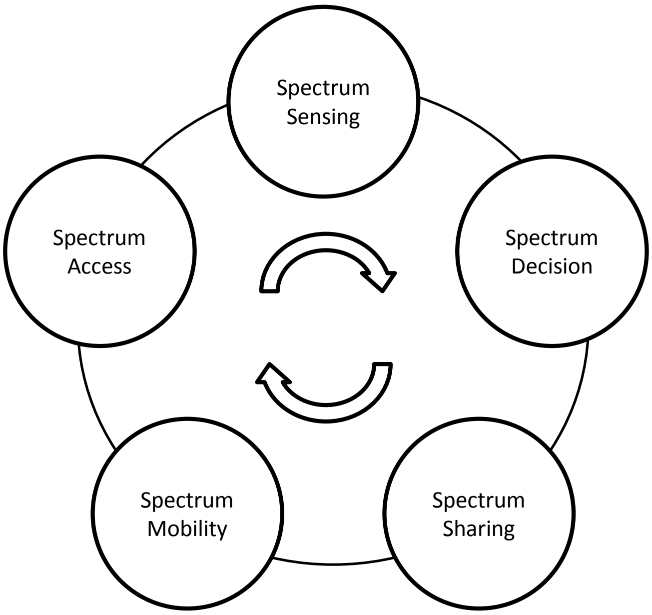


Figure 2.3. Basic Cognitive Radio cycle

Akyildiz and Wang [2005] divide multichannel MAC protocols into three distinct groups based on the hardware platform: (1) Multichannel Single-Transceiver; (2) Multichannel Multi-Transceiver; and (3) Multi-radio. Multichannel MAC protocols can also be classified in terms of the number of channels that can be used at any time to exchange control information: (1) Single Rendezvous, i.e., only one control channel; and (2) Multiple Rendezvous, i.e., multiple control channels [Timmers et al., 2010]. Within the Single Rendezvous approach, several categories can be further distinguished [Yau et al., 2008].

Mody et al. [2008] state that there are non-CR standards that have been addressing issues implicitly related to CR, such as the coexistence of radios that use different protocols in the same spectrum bands. Non-CR networks, such as IEEE 802.11 (Wireless Local Area Networks), IEEE 802.15.4 (Low-Rate Wireless Personal Area Networks) and IEEE 802.16 (Wireless Metropolitan

Networks), already include some degree of CR features, but without being fully cognitive [Sherman et al., 2008]. In fact, coexistence has been considered for many years within IEEE standards, initially through tedious manual coordination and frequency planning, and CR techniques are a means to facilitate coexistence [Sherman et al., 2008]. Coexistence techniques, such as Dynamic Frequency Selection (DFS), Dynamic Channel Selection (DCS), which is similar to DFS, and Transmit Power Control (TPC), have been standardized and essentially completed before 2005. IEEE 802.11h-2003, IEEE 802.16.2 2004, IEEE 802.15.4-2006 and IEEE 802.15.2-2003 are examples of such standardization efforts (see Sherman et al. [2008] for further details). Although IEEE 802.22 [IEEE 802.22 Working Group on Wireless Regional Area Networks, 2013] is the first cognitive standard effort, many of its physical, MAC, security, and QoS (Quality of Service) features were adopted or inspired by IEEE 802.16 standards [Sherman et al., 2008].

2.3 Standardization activities

CR has resulted in a significant amount of standardization and regulation activities at distinct organizations worldwide, being the FCC the first regulatory body that envisioned using it for efficient spectrum management. The outcomes of these activities are fundamental for the success of CR. For example, the Institute of Electrical and Electronics Engineers (IEEE) developed the CR standards known as IEEE 802.22 and IEEE DySPAN-SC (Dynamic Spectrum Access Networks Committee). The latter was formerly known as IEEE SCC41 and as P1900 [Mody et al., 2008; Masonta et al., 2013].

IEEE 802.22 [IEEE 802.22 Working Group on Wireless Regional Area Networks, 2013] defines CR techniques that specifically aim at enabling unlicensed devices to exploit television white spaces in the VHF and UHF bands (54-862 MHz) on a non-interfering basis for the deployment of Wireless Regional Area Networks (WRAN). Its functionalities are related to both the MAC and PHY layers, and space is left for the development of new algorithms for channel sensing and classification [Ko et al., 2010]. For the protection of PUs, which is one of the main goals of channel management in CR environments, IEEE 802.22 uses techniques based on both spectrum sensing and geo-location databases. It adopted a centralized single-hop model (i.e., each mobile device is associated with a base station), being wide coverage provided by several base stations. IEEE 802.22 also enables operations across three channels simultaneously (i.e., channel bonding) for higher throughput. Refer to Ko et al. [2010] for a description of the main characteristics of channel management in IEEE 802.22.

IEEE DySPAN-SC addresses the area of dynamic spectrum access networks and aims at developing standards for next generation radio and advanced spectrum management. It includes several working groups that address specific issues such as interference and coexistence (P1900.2), and spectrum sensing (P1900.6). IEEE 1900.4 (Architectural Building Blocks Enabling Network-Device Distributed Decision Making for Optimized Radio Resource Usage in Heterogeneous Wireless Access Networks), the first IEEE SCC41/DySPAN-SC standard, was published in 2009. It provides architectural concepts and specifications for network management between incompatible wireless networks [Mody et al., 2008].

There are other relevant standards and ongoing standardization activities related to the utilization of television white spaces, such as ECMA (European Computer Manufacturing Association)-392, IEEE 802.11af, and IEEE 802.19. ECMA-392 specifies a MAC sublayer and a PHY layer, and was published in 2009. IEEE 802.11af aims at introducing modifications to both the MAC and PHY layers of IEEE 802.11. The IEEE 802.19 wireless coexistence working group aims at defining coexistence methods for IEEE wireless standards [Mueck et al., 2010]. Finally, we mention the International Telecommunication Union (ITU) and the European Telecommunications Standards Institute (ETSI) since they are also active in the standardization of CR systems, namely under ITU-R (ITU Radio communication sector) Working Party (WP) 1B and WP 5A, and ETSI Reconfigurable Radio Systems (RRS) Technical Committee (TC) [Nguyen et al., 2012; Filin et al., 2011; Masonta et al., 2013]. ITU-R WP 1B identifies different types of CR deployment scenarios, including cooperative and opportunistic spectrum access, and WP 5A concentrates on technical characteristics of CR systems. Among other aspects, ETSI RRS-TC focuses on defining functionalities for managing and controlling reconfigurable radio systems.

2.4 CR architectural approaches

The architecture of CR networks can either be centralized or distributed (see Figure 2.4). Spectrum allocation and access are controlled by a central entity with the centralized approach (e.g., a base station in an infrastructure-based network) and by the SUs themselves with the distributed approach. Centralized CR networks can also be designated as infrastructure-based CR networks and distributed CR networks as CR ad-hoc networks. According to Renk et al. [2008], when the number of CR devices increases, it becomes computationally complex for a central entity to make spectrum allocation decisions. Therefore, the distributed approach, where decision-making is processed by each SU, has the ability to reduce complexity and increase network scalability.

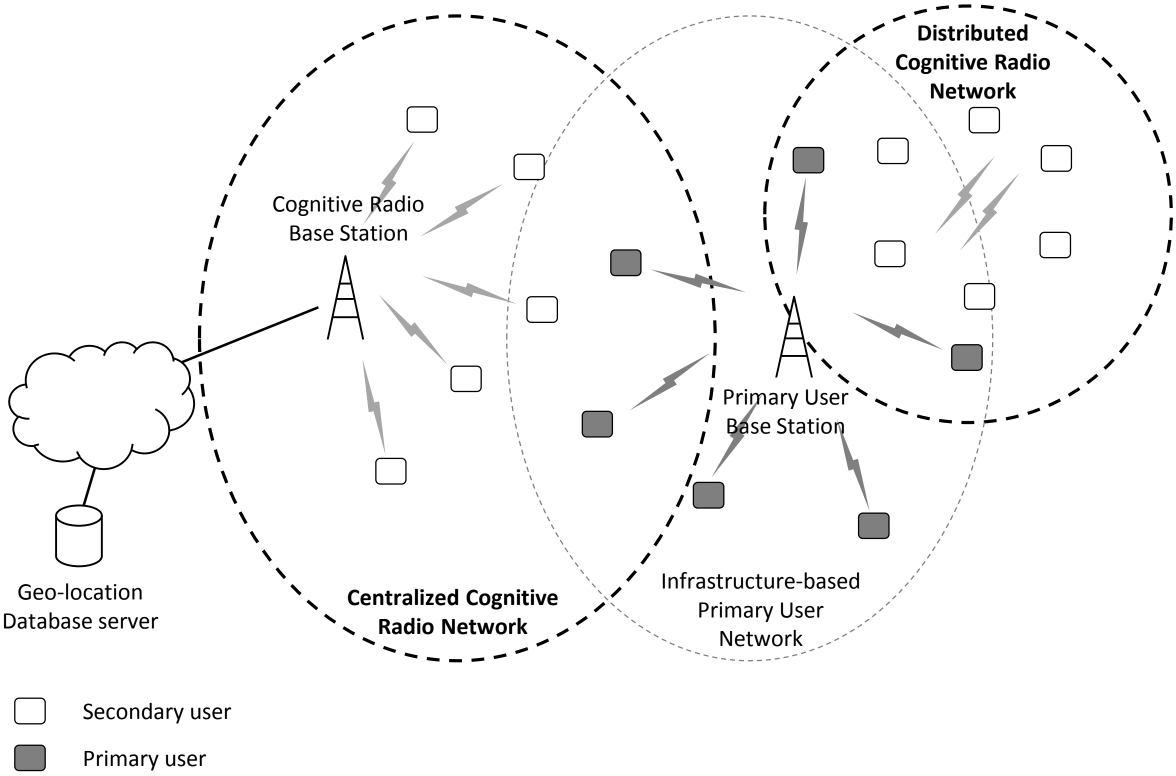


Figure 2.4. Main CR architectural approaches

In distributed CR networks, the SUs, which can be fixed or mobile, need to incorporate all the CR-related capabilities and spectrum allocation can either be achieved cooperatively or non-cooperatively. With the non-cooperative approach (i.e., device-centric), selfish users only use local policies and local knowledge for accessing the spectrum, do not share any information with each other, and try to maximize their own interests. This greedy attitude not only results in less communication overhead but also in higher sensing inaccuracy and spectrum sharing inefficiency. In cooperative distributed CR networks, the SUs share information with each other (e.g., signalling data, sensing results, and learning outcomes) for optimized spectrum decision and, therefore, serve a common goal.

Although the distributed CR network illustrated in Figure 2.4 follows a one-hop approach since every SU is in the transmission range of each other, multi-hop approaches are also possible. As Celbi and Arslan [2007] state, centralized and distributed approaches may be considered the two extreme architectural limits between which various CR approaches can be developed. For instance, a CR mesh network might be considered where spectrum decision is performed by different mesh gateways and/or by the SUs themselves (as with a pure distributed approach), with optional utilization of geo-location databases (see Figure 2.4) accessible through the gateways.

Retrieving the locations of existing PUs from geo-location databases is a means to enhance spectrum decision in CR environments, yet it is not always feasible or trivial, especially with mobile PUs. Television towers or cellular base stations are examples of PUs with a priori known and fixed locations.

2.5 Main CR issues

The previous sections have discussed the main objectives of CR, related technologies, standards, and possible network architectures. The current section describes the main issues that must be addressed in order to meet the objectives of CR.

2.5.1 Self-coexistence

One of the most important and specific issue of CR is avoiding the SUs to cause harmful interferences to PUs. Coexistence can be defined as the ability of a radio to coexist with other radios in the same spectrum bands using different protocols. Therefore, CR can be thought as an evolution of self-coexistence, i.e., automated coexistence based on non-manual coordination techniques. However, self-coexistence is difficult to achieve in CR scenarios since well-defined cellular architectures and frequency allocations are not provided, PUs have non-deterministic activity patterns, and neighbouring SUs compete for the same spectrum holes. According to Mody et al. [2008], coexistence does not require the use of cognitive techniques, but the latter can be used to facilitate the former.

Overlay and underlay are two possible spectrum access techniques. With the underlay approach, the SUs are constrained to keep transmission power below the noise floor of PUs, i.e., the interference temperature as defined by the FCC [Akyildiz et al., 2008]. This can be achieved through spreading the transmitted signal over a wide frequency band (e.g., higher than 500 MHz), which enables a short range high data rate to be achieved with very low transmission power [Zhao and Swami, 2007]. UWB (Ultra Wide Band) is an example of such radio technology. The underlay approach is also known as the interference-tolerant approach. It does not suffer from service interruption losses, does not include spectrum handover operations, was developed for cellular networks, and requires sophisticated spread spectrum techniques [Liu et al., 2007; Issariyakul et al., 2009].

With the overlay approach, which requires dynamic spectrum access (DSA) and has received much more attention from the research community, a SU accesses the network using a portion of the spectrum that is not being used by the respective PUs (see Figure 2.1). Therefore, restrictions are imposed on when and where the SUs can transmit, not on transmission power. In this case, service interruption losses can be caused by the appearance of PUs, which is a CR specific issue, and can affect the performance of any layer in the communication protocol stack. For instance, Issariyakul et al. [2009] study performance issues at the transport layer in overlay CR networks. Service interruption losses are different from losses due to network congestion or channel errors. They do not depend on network conditions, channel characteristics, or MAC mechanisms, but instead on PU activities, which in turn depend on extraneous factors such as geographic location and time of the day. For instance, Wang and Salous [2008] analyse a specific frequency band that experiences a 24 hours seasonality, with an every day's peak occupancy between 10:00 and 18:00, and minimum occupancy between 2:00 and 6:00.

Overlay CR requires appropriate and accurate sensing and signalling features to cope with PU activity in CR scenarios. Sensing and signalling are described in the next two sections. In this thesis, the underlay approach is not addressed and, therefore, CR implicitly denotes the overlay approach.

2.5.2 Spectrum Sensing

Spectrum sensing, which is a sampling process related to the PHY and MAC protocol entities, aims at accurately and timely locating spectrum holes. Therefore, it is the most fundamental and challenging issue in CR environments.

Concerning the PHY layer, Akyildiz et al. [2009] briefly describe three groups of PU detection techniques: (1) transmitter detection; (2) primary receiver detection, which is only feasible for the detection of TV receivers; and (3) interference temperature management, which is difficult to achieve. They mention that most of the current research effort focuses on the transmitter detection technique and also describe three schemes that can be applied to this end in terms of their strengths and shortcomings. These schemes are: (1) matched filter detection; (2) energy detection; and (3) feature detection. Energy detection is the easiest scheme to implement since a channel is considered busy when the strength of the detected signal level is above a certain threshold. However, it requires coordinated quiet periods to avoid false alarms since it cannot distinguish PU activity from SU activity. Quiet periods can introduce additional delays in the decision making process. A simple theoretical model of an energy detector is provided by Yu et al. [2009]. Refer to Wellness and Mähönen [2010] for some examples of theoretical formulations as well as practical approaches for spectrum sensing at the PHY layer. The remainder of this section proceeds with MAC-related issues concerning PU detection.

Usually, the access to the spectrum is achieved through a sense-before-transmit approach (see Figure 2.5), i.e., a channel is sensed before data transmission and another one is searched if it is busy. Therefore, the basic operation of a SU before any new data transmission is as follows: (1) select a channel to sense; (2) sense the selected channel; (3) if the channel is busy, go back to step (1); (4) if the channel is idle, use the channel for data transmission; and (5) if any PU activity is detected during transmission, stop transmission immediately and go back to step (1). In order to minimize the level of interference to PUs, SUs can be limited to transmit just a single data frame in one sense-before-transmit round. Cormio and Chowdhury [2009] discuss the trade-off between sensing and transmission times, considering that the total time is either limited or fixed (e.g., due to periodic sensing). Therefore, according to these authors, higher sensing times result not only in higher precision but also in throughput decrease since less time remains for transmission.

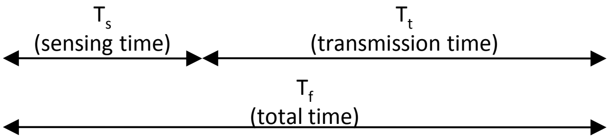


Figure 2.5. Sense-before-transmit approach

Cormio and Chowdhury [2009] mention three different types of approaches concerning the optimization of spectrum sensing and transmission times: (1) independent sensing duration optimization, in which the objective is to minimize missed detection and false alarm probabilities; (2) independent transmission duration optimization, in which the optimal transmission duration is determined, while keeping the sensing duration constant, in order to maximize the throughput and keep interference to PUs under a certain threshold; and (3) joint sensing and transmission duration optimization. Moreover, Zhao and Sadler [2007] state that complicated trade-offs between trusting the detector and overlooking spectrum opportunities must exist when the access strategy considers the imperfect nature of spectrum detectors, i.e., missed detection and false alarm probabilities.

Approaches for the localization of vacant spectrum bands based exclusively on local sensing do not offer satisfactory results [Lu et al., 2012]. Thus, cooperative MAC protocols, which enable the SUs to share sensing information with each other, are also required for an efficient and accurate characterization of channel activity. Cooperative sensing helps solving the hidden PU problem, i.e., when a SU cannot sense the activity of a PU it can interfere with (see Figure 2.6). It is also a means to address the inherently imperfect nature of sensing hardware, which results in missed PU detections and false alarms. Globally, cooperative sensing addresses issues that result from problems such as the adverse effect of noise uncertainty, multi-path fading, and shadowing [Yucek and Arslan, 2009; Akyildiz et al., 2011], which are main factors that degrade the efficiency of PU detection in CR networks.

For instance, in the proposal of Timmers et al. [2010], the SUs cannot use a channel if it is sensed busy by any of the SUs in the network. With this so-called OR-rule, SU_1 and SU_3 in Figure 2.6 are not allowed to use the channel assigned to base station BS when SU_2 reports it as being occupied. Malady and Silva [2008] state that the OR-rule can result in an inefficiency designated as “false spectrum access denial", i.e., a SU is denied access to a given channel despite being out of the region of potential interference to the respective primary system. These authors also present various clustering methods that aim at addressing this issue. We note that the accuracy of cooperative sensing is highly dependent on the density of SUs in the network [Wang et al., 2010b].

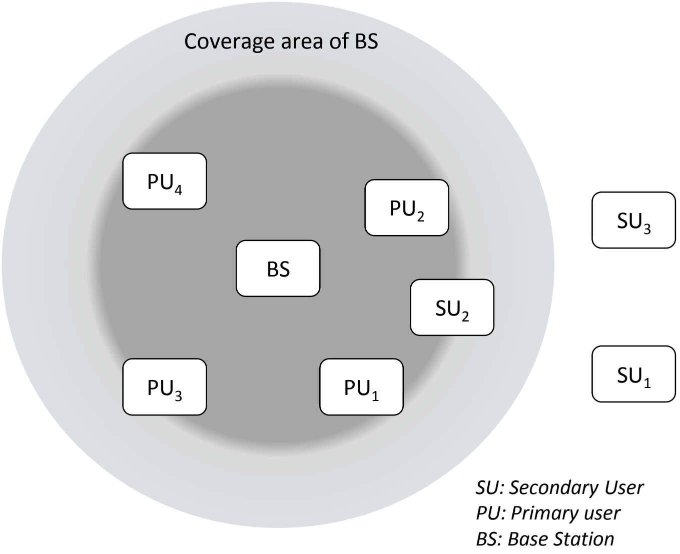
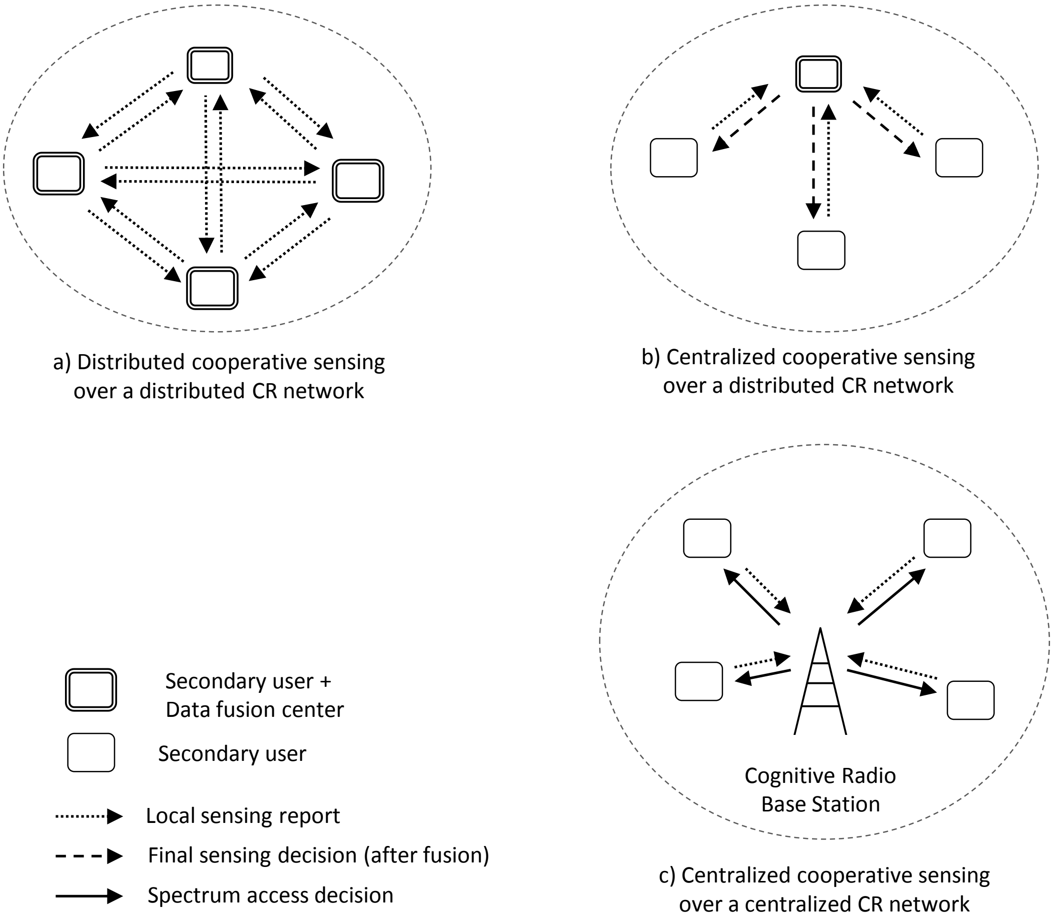


Figure 2.6. The hidden primary user problem

With cooperative sensing solutions, the final decision regarding spectrum access is based on the fusion of sensing outcomes from multiple SUs. Centralized, distributed, and external sensing are possible approaches for cooperative sensing. With centralized sensing (see Figure 2.7), which is more appropriate but not limited to centralized architectural approaches, a central unit (e.g., a base station or an access point) or a designated SU, which acts as a common data fusion centre, collects sensing information from the SUs, processes this input for decision making through some data fusion process, and broadcasts the obtained result to the SUs and/or other central units in the network [Wang et al., 2010b; He et al., 2014]. On the other hand, with distributed sensing (see

Figure 2.7), which is appropriate for cooperative distributed architectural approaches, the SUs act as both sensing terminals and fusion centres, collecting reports from their neighbours and performing data fusion and spectrum decision individually. With external sensing, an external agent performs sensing and broadcasts the obtained channel occupancy information to the SUs.



a) Distributed cooperative sensing over a distributed CR network

b) Centralized cooperative sensing over a distributed CR network

c) Centralized cooperative sensing over a centralized CR network

Figure 2.7. Cooperative sensing approaches in distributed and centralized CR scenarios

The IEEE 802.22 standard (see Section 2.3) and DSAP (Dynamic Spectrum Access Protocol) [Brik et al., 2005] are examples of CR solutions that incorporate a distributed cooperative sensing feature. DSAP, a protocol for coordinated spectrum access, uses a central entity, the so-called DSAP server, for managing and controlling the access to the spectrum. The states and channel conditions of the network nodes are collected by the server and kept in a database named *RadioMap*. Based on this information and on administrator-defined policies, an optimal channel allocation is determined by the central entity. With DSAP, the channels are leased by the server to the network nodes. Relay entities are also provided to enable multi-hop architectures with nodes that are located out of the coverage area of the DSAP server.

Distributed approaches are usually preferable for cooperative sensing since a centralized fusion centre represents a single point of failure against the operability of the entire CR network. Nevertheless, signalling overhead increases with the number of SUs when both distributed and centralized cooperative sensing schemes are utilized. Collaborative cluster-based solutions are often considered as a means to address this issue and any other communication overhead (e.g., routing protocol overhead [Huang et al., 2014]) in wireless networks. For instance, the work of Baddour et al. [2011] forms clusters of SUs based on the number of available channels the SUs have in common. In the work of Renk et al. [2008], which uses swarm intelligence to detect spectrum holes, the SUs form a swarm that is further divided into several cooperating clusters. Lo and Akyildiz [2013] identify and address other possible overhead causes and effects that limit the gains of cooperative sensing. Finally, we can mention the work of Chen et al. [2013] on compressive spectrum sensing in which the SUs only transmit part of their sensing information as a strategy to reduce overhead.

With cooperative sensing, each SU can either follow a hard-decision or a soft-decision approach to report its sensing results. With hard-decision, each SU reports its outcomes in a binary form (i.e., a channel is busy or idle), while with soft decision it reports the energy levels it senses. In terms of sensing performance, Wang et al. [2010a] conclude that hard-decision performs almost the same as soft-decision when cooperative users face independent fading (e.g., when the SUs are not nearby each other). Additionally, hard-decision reduces the overhead in reporting sensing results [Zeng et al., 2010]. Concerning soft-decision, Clouquer et al. [2001] conclude that it is superior to hard-decision when fault-tolerance is not required, or when sensors are highly reliable and fault-free.

Various approaches have been proposed regarding the fusion of sensing outcomes in CR environments. Three commonly used fusion approaches are the previously mentioned OR-rule, the AND-rule, and the voting-rule. The OR-rule considers that PU activity is present if detected by at least one sensor, while the AND-rule requires that all the participating sensors detect any PU activity. With the voting-rule, a PU is declared to be present if more than a given fraction of the sensors detects any activity [Mody et al., 2009]. The OR-rule is the most commonly used approach, especially when a hard-decision approach is followed [Clouqueur et al., 2001]. However, when it is applied, the risk of false spectrum access denials (i.e., access is denied despite transmission does not interfere with any PU) increases with the number of SUs [Malady and da Silva, 2008]. Nasipuri and Li [2005] propose a hard-decision process in which the decisions are performed comparing the number of positive local decisions (i.e., activity detected) against a threshold. This approach results in the OR-rule when the threshold is set to one.

Other approaches are also possible for fusing sensing results. For example, the average fusion rule computes the average of the sensing outputs and compares it against a given threshold [Clouqueur et al., 2001]. Malady and Silva [2008] propose a centralized soft-decision approach that computes a weighted sum of the signal strengths the SUs report, being a channel considered busy if the computed value is greater than a particular threshold. Fatemieh et al. [2010] state that the utilization of statistical median provides results that are more robust to excessively high or excessively low reports than using statistical mean. In their solution, they jointly employ both estimators in order to achieve a mix of accuracy (i.e., with the mean) and robustness (i.e., with the median) in the decision process.

2.5.3 Signalling

SUs need a means to exchange and overhear control information among them in order to identify common spectrum opportunities, coordinate access to the spectrum, and initialize communication between each other [Shah et al., 2011; Masri et al., 2010]. Depending on the adopted approach, CR MAC protocols can be classified according to three generic categories: (1) split phase; (2) dedicated common control channel (CCC); and (3) frequency hopping [Mo et al., 2008; Zhang and Lazos, 2013]. Split phase and dedicated CCC approaches use a predefined CCC (see Figure 2.8) that is distinct from the data channels and, therefore, perform a kind of signalling designated as out-of-band signalling. Lo [2011] defines a CCC as being a channel that is temporarily or permanently allocated in the licensed or unlicensed spectrum, and that is available to two or more SUs. A CCC enables efficient broadcasting and must allow the SUs to operate it without any disruption. According to Hamdaoui and Shin [2008], and to Wang et al. [2007], dedicating a piece of the spectrum as a common good (i.e., the CCC) is an absolute necessity to achieve efficient spectrum access.

Lo [2011] classifies existing CCC design schemes into four major types: sequence-based CCC; group-based CCC; dedicated CCC; and UWB (Ultra-Wideband) CCC. With the sequence-based approach, a CCC is allocated according to a random or predefined channel hopping sequence. The group-based approach results in a CCC being allocated to a channel available to a group of neighbouring SUs. A dedicated CCC, which is often allocated in frequency bands not affected by PU activity [Lo, 2011], is predetermined and globally available to all the SUs in the network. With the UWB approach, a CCC is allocated in licensed frequency bands and control traffic is transmitted in low power such that it does not result in harmful interference to PU activities.

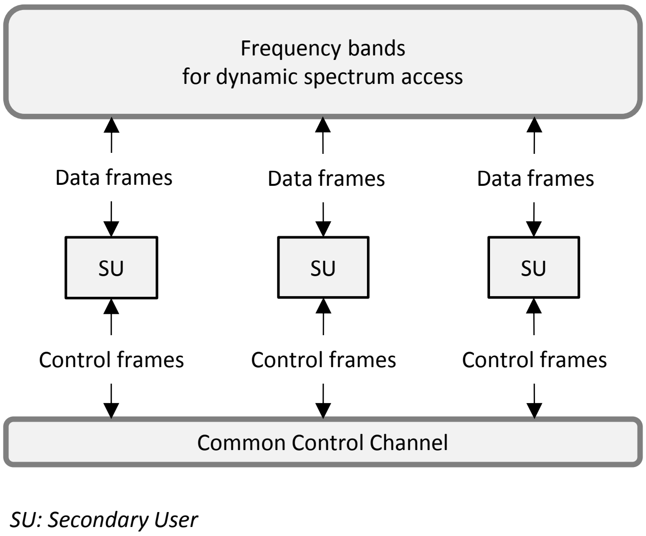


Figure 2.8. Signalling based on a common control channel

CR MAC protocols that belong to the split phase category divide time into alternating signalling and data transmission phases. During the first phase, the SUs tune to a CCC and exchange signalling information in order to share sensing results and negotiate channel access. In CR networks, split phase approaches might result in inefficient spectrum utilization since most channels remain idle during the signalling phase [Lo, 2011]. With the dedicated CCC-based CR MAC category, the SUs are often equipped with at least two transceivers, being one of them dedicated to operate the control channel and the other(s) to support data transmission. Consequently, the SUs are able to constantly transmit, receive, and overhear control information, being capable of achieving what Salameh et al. [2010] designate as passive learning.

Out-of-band signalling through a dedicated CCC is easy to implement, simplifies the design of CR MAC solutions, and, therefore, results in one of the most popular approaches for distributed CR MAC design [Cormio and Chowdhury, 2009; Lo, 2011]. Nevertheless, a dedicated CCC is prone to saturation and can therefore become a potential bottleneck for performance and scalability since data channels remain underutilized while the SUs contend for it [Luo et al., 2009; Nezhadal et al., 2012; Ren et al., 2012; Lo, 2011]. Scalability means that performance parameters, such as throughput and latency, do not degrade when the number of nodes, traffic load, and mobility increase. There are already some proposals that aim at addressing the CCC saturation problem [Cormio and Chowdhury, 2010]. For instance, DOSS MAC (Dynamic Open Spectrum Sharing MAC) [Ma et al., 2005] alleviates the CCC saturation problem through the joint utilization of three mechanisms: (1) keeping control traffic under a certain threshold (traffic limiting); (2) adjusting the bandwidth ratio between the CCC and the data channel to avoid the CCC to become a bottleneck; and (3) allowing the CCC to migrate towards a better channel. Cormio and Chowdhury [2010] propose AMRCC (Adaptive Multiple Rendezvous Control Channel), a CCC design for ad-hoc CR networks that is based on frequency hopping and aims at overcoming CCC limitations. They also discuss some related works that aim to set up and maintain reliable CCCs while addressing inherent challenges.

CCCs are also prone to jamming attacks by malicious users, which is one of the main classes of Denial of Service (DoS) attack threats in CR networks [Brown and Sethi, 2008]. Brown and Sethi [2008] describe the vulnerabilities that are specifically enabled by CR operations and propose a qualitative analysis approach for the assessment of these risks. One of their goals is providing CR design recommendations in terms of protection against DoS attacks. According to Brown and Sethi [2008], security measures must be incorporated in the early stages of CR development. Timmers et al. [2010] state that selecting different common control channels in the licensed spectrum for different successive time periods, through a hopping sequence, can help circumvallating CCC jamming attacks.

The frequency hopping-based CR MAC category results in every SU hopping between the available licensed channels according to given sequences. Each SU has its own hopping sequence and any two sequences have a minimum degree of overlapping in time designated as rendezvous. For instance, in the proposal of Bahl et al. [2004], each node hops among every channel according to a pseudorandom sequence such that neighbouring nodes have channels overlapping in time periodically. When two SUs meet on a given data channel that is free of PU activity, they can exchange data or agree on future synchronized actions for data transmission. Frequency hopping implements signalling over the available data channels (i.e., in-band signalling) and results in a sequence-based CCC design scheme [Lo, 2011].

With frequency hopping, split phase, or any other solution based on the utilization of a single radio per SU, the SUs are unable to transmit or receive signalling information during data transmission. Therefore, they have stringent synchronization requirements in order to be able to exchange control and data packets between them in specific periods. However, time synchronization over an entire network is not always feasible, increases overhead and complexity, and also compromises network scalability [Lo, 2011; Luo et al., 2009]. Additionally, single transceiver schemes are prone to the hidden multichannel problem [De Domenico et al., 2012]. That is, a node accessing a data channel misses any signalling information sent over another channel. On the contrary, dedicated CCC-based approaches avoid the cost of synchronization and make coordination, broadcasting and overhearing control information (i.e., passive learning) easier, even during data exchange periods. Consequently, monitoring the busy status of other SUs and data channels in the neighbourhood results in a simple task [Mo et al., 2008].

2.5.4 Spectrum decision

In CR scenarios, the SUs are expected to dynamically choose the best available channels and transmission parameters [Sharma and Belding, 2008]. However, spectrum decision is still underexplored despite being a core issue in CR [Akyildiz et al., 2008]. In fact, CR should not be thought as being similar to generic MAC problems in existing wireless networks and limited to wireless resource allocation issues [Ji and Liu, 2007]. For instance, CR MAC protocols should be able to determine the order spectrum bands must be searched (i.e., sensed) for minimizing time and energy spent to find a spectrum opportunity [Cormio and Chowdhury, 2009]. Ji and Liu [2007] define Dynamic Spectrum Access (DSA) as a multi-objective optimization problem that is difficult to analyse and solve. They propose to model DSA networks as cooperative and non-cooperative dynamic spectrum sharing games. Amanna and Reed [2010] state that some of the open research issues in CR are: (1) developing more proactive approaches that seek to make changes before they are needed; (2) adapting prediction algorithms from other research areas to the CR area; and (3) investigating the application of lesser known Artificial Intelligence algorithms.

A simple yet sufficiently accurate statistical model of spectrum utilization by PUs is crucial to obtain efficient solutions for tracking, selecting, and accessing spectrum opportunities [Zhao and Swami, 2007]. It essentially enables decision making even when accurate real-time information is not available (e.g., due to hardware limitations and energy constraints). Hence, collecting data about the history of spectrum utilization can help the SUs to predict its future use and take rewarding spectrum decisions (e.g., selecting a vacant channel). Collected data must be statistically analysed and used to model PU activity in a given channel, such as in the work of Issariyakul et al. [2009]. This is a so-called learning based on past experience approach, which is further discussed in Section 2.7. Niyato and Hossain [2009] enumerate several methods that can be applied for observation, learning, or decision making in CR. They are estimation technique, game theory, evolutionary computation, fuzzy logic, Markov decision process, pricing theory, theory of social science, and reinforcement learning.

Concerning spectrum decision, it can also be mentioned that different frequency bands have different characteristics (e.g., path loss, link error) that should be considered by MAC protocols for accurate spectrum decision and for avoiding spectrum outages. For instance, the coverage area of a transmitter decreases as the operating frequency increases. Therefore, spectrum handovers to a higher frequency can result in a loss of connectivity. According to Brown and Sethi [2008], available spectrum opportunities at higher frequencies can be useless due to excessively high propagation losses. The work of Jo et al. [2009] is an example of a CR solution that considers the propagation characteristics of the frequency in use.

2.5.5 Seamless spectrum handover

Seamless transition with minimum quality degradation is a fundamental goal for spectrum handover solutions in CR networks, particularly for some classes of data traffic that require Quality of Service (QoS) or Quality of Experience (QoE) assurance (e.g., multimedia streams and real-time traffic). In such situations, spectrum handovers can result in unacceptable service interruptions or degradation of performance. The associated latency should not be noticed by users, which may require upper layers of the protocol stack to be involved in the handover process.

Globally, when QoS is a concern, observation, learning, and decision making must be performed at the PHY, MAC, network (routing), transport (congestion control), and application layers [Niyato and Hossain, 2009]. For instance, if estimation for spectrum handover latency is known in advance, an application that plays video streams from the network can buffer enough data before handover starts and, then, deliver it while that process takes place [Akyildiz et al., 2008]. This approach brings new challenges in turn, such as estimating spectrum handover duration, defining how to anticipate data gathering, and deciding at which protocol layer should buffering be performed. Spectrum handovers also affect link state parameters and, therefore, can be wrongly perceived as network instability (e.g., congestion or link errors) by protocols in upper layers (e.g., transport and routing protocols). Sherman et al. [2008] state that the type of information to be accessed, QoS, and security requirements for data streams should be considered. According to Akyildiz et al. [2008], there are still many open research topics to be investigated concerning spectrum handover.

2.5.6 Security

Given their wireless nature, CR environments are vulnerable to attacks that are inherent to any kind of wireless communication technology, particularly at the PHY and MAC layers, such as radio frequency jamming and MAC address spoofing [Marinho et al., 2015]. Therefore, well-known security solutions may help addressing many of such attacks in CR networks (e.g., encryption and authentication mechanisms). Additionally, there are security threats that are due to the specificities of CR operations and that aim at compromising the protection of PUs and the fairness of spectrum sharing between SUs.

In CR environments, a SU can be fooled by attackers since it relies on local observation and, possibly, on cooperation for spectrum decision and learning. As already mentioned in Section 2.1, malicious users are a third type of users that can also be considered in CR scenarios, beyond PUs and SUs. Among other types of threats, two assume particular importance on CR environments: PU emulation and data falsification attacks. A PU emulation attack allows an attacker to mimic a PU in order to force other SUs to vacate a specific frequency band and, consequently, cause the disruption of the operation of the network and unfairness on spectrum sharing. On the other hand, the falsification of reports in cooperative schemes consists in providing false information to neighbours or to a data fusion centre, and affects the effectiveness of spectrum decision.

Attackers can have malicious or greedy intents, i.e., target the disruption of the operation of the network or maximize their own performance, respectively. Generally, both types of attackers have the common objective of causing DoS effects to legitimate SUs [Xin and Song, 2014]. It is important to note that many existing CR proposals employ statistics collected about the observed PU activity in order to learn and make prediction based on beliefs that result from current and past observations (see Section 2.7). Consequently, manipulated and faulty data may lead to what Clancy and Goergen [2008] designate as belief-manipulation attacks. That is, any manipulation may potentially affect future spectrum decisions. In non-cooperative networks, an attack against a SU does not affect other SUs. On the contrary, when a cooperative or centralized scheme is employed, an attack to a single device may affect the outcomes of the entire CR network.

Reliable inputs or inputs from reliable SUs must be appropriately filtered and accepted before executing fusion and decision processes. One of the possible strategies consists in using a combination of solutions for authentication, data integrity, and data encryption in order to restrict data inputs only to those from trustworthy users and, consequently, prevent illegitimate manipulation of data [Clancy and Goergen, 2008]. The work of Rifà-Pous and Garrigues [2012], and the IEEE 802.22 standard include such type of features. For the detection of spurious sensing data, another commonly used approach consists in outlier detection [Khaleghi et al., 2013], also named anomaly or deviation detection. That is, in a given set of values, an outlier corresponds to data that appears to be inconsistent with the remaining values. One of the main difficulties in outlier detection consists in preventing valid data from being erroneously classified as an outlier. Zhang et al. [2010] state that it may be difficult to pre-classify normal and abnormal sensing data in terms of PU activity.

Some authors also consider that the number of malicious and faulty nodes cannot be greater than the number of properly behaving and honest nodes. For instance, Min et al. [2009] assume in their work that at least two thirds of the nodes are well behaving. On the contrary, Wang and Chen [2014] propose a data fusion scheme for centralized CR networks that tolerates a high percentage of malicious SUs. This strength results from allowing the data fusion centre to also sense the spectrum and use its own outcomes to assess the honesty of the SUs. Zhang et al. [2010] state that existing outlier detection techniques do not take node mobility or dynamically changing topologies into account. They also mention that decentralized approaches (i.e., with operations performed locally, such as in distributed cooperative sensing) should be used in order to keep communication overhead, memory, and computational costs as low as possible. There are simple and straightforward outlier detection techniques that may be employed during the fusion process (e.g., ignoring extremely low or extremely high sensing reports, or the m largest and m smallest reported values). The work of Chen et al. [2014] is an example of a solution that uses more complex statistics for detecting spurious sensing data in cooperative sensing. However, in this work, the authors assume that the locations of PUs are known to each SU and that each SU is also location-aware. These aspects might limit the practicality of the proposal.

The detection of outliers can also be a means to dynamically draw conclusions about the quality of the information the SUs report. This approach enables the utilization of trust-based security schemes that may, for instance, attribute more relevance to the reports of more trustworthy SUs in a fusion scheme (e.g., adaptively assigning different weights to the SUs according to their reputation levels) [Fragkiadakis et al., 2013; Chen et al., 2012a; Min et al., 2009; Atakli et al., 2008]. It also enables ignoring the sensing reports from SUs with reputation values under a defined threshold [Zeng et al., 2010; Suen and Yasinsac, 2005; Wang and Chen, 2014]. Globally, when a SU reports sensing data not tagged as an outlier or consistent with the final decision, its reputation is increased. Otherwise, its reputation value decreases [Atakli et al., 2008]. Examples of solutions that follow this approach are found in the collaborative sensing solutions proposed by Zeng et al. [2010], Wang et al. [2010a], and Wang and Chen [2014].

Spectrum status is often assumed to be correlated for SUs in close proximity. A SU is thus very likely to have an erroneous sensing decision if most nearby SUs have the opposite decision (i.e., it is an outlier) [Zhang et al., 2010]. In this case, spatially non-correlated data is assumed to be spurious data. This results in the so-called nearest neighbour-based approaches or distance-based clustering approaches (i.e., sensors in close proximity are grouped into clusters). The works of Min et al. [2009], Chen et al. [2012b], and Nasipuri and Li [2005] include features based on this principle. However, defining which SUs are in close proximity remains a challenging issue and requires appropriate geo-location techniques [Yang et al., 2010].

Regarding PU emulation attacks in CR environments, they aim at forcing the SUs to avoid using specific frequency bands and, therefore, may cause the same adverse effect as always reporting a channel to be busy under cooperative sensing. Thus, a PU emulation attacker does not aim at causing interference to PUs. This threat is materialized through the transmission of fake PU signals and does not necessarily require the attackers to participate in any underlying cooperative scheme. For instance, energy detection, which does not investigate any particular characteristic of the signals (see Section 2.5.2), is the detection scheme that is most susceptible to PU emulation attacks, given the simplicity of generating a signal with a particular energy level in the same frequency as a PU [Jin et al., 2009]. According to Araujo et al. [2012], PU emulation is the most studied attack against CR.

The detection of PU emulation attacks is addressed mostly estimating the locations of the transmitters and comparing it with the a priori known locations of the legitimate PUs, such as IEEE 802.22 does [Fragkiadakis et al., 2013; Jin et al., 2009; Chen and Park, 2006]. If the estimated location of a transmitter deviates from the known locations of the PUs, then the likelihood of this transmitter being a PU emulation attacker increases. With this type of approach, it is usual to assume that each SU is equipped with a positioning device enabling self-positioning capabilities [Jin et al., 2009; Tingting and Feng, 2013; Chen and Park, 2006], in particular GPS (Global Position System) [Celebi and Arslan, 2007; Niculescu, 2004]. However, GPS presents various limitations such as not being appropriate for indoor utilization and being inefficient in terms of power consumption [Kim et al., 2012; Xiao et al., 2007].

Having the locations of the legitimate PUs known to all the SUs is straightforward when the PUs have no mobility (e.g., television towers and cellular base stations) and geo-location databases are available. However, such requirements may not be met in many CR scenarios. Moreover, countermeasures based on geo-location are not appropriate for scenarios with mobile PUs and mobile SUs [Blesa et al., 2013]. Idoudi et al. [2014] state that existing solutions against PU emulation attacks do not handle PU and SU mobility appropriately. For example, the proposals of Yuan et al. [2012] and León et al. [2012] only consider the possibility of PUs with fixed and known PU locations, and, thus, cannot cope with the emulation of PUs that have unknown locations (e.g., wireless microphones). On the contrary, Kai et al. [2014] propose what they argue to be the first PU emulation detection solution that contemplates mobile attackers.

There are several existing proposals that address the detection of PU emulation attacks estimating the distances to the transmitters based on the received signal strength indicator (RSSI) of received signals (see Chapter 6 for additional details). An alternative approach with higher precision consists in deploying an additional network of sensors to cooperatively determine the locations of the transmitters and, therefore, of the potential PU emulation attackers [Chen et al., 2008a; Jin et al., 2009]. Other alternatives exist in the literature, such as the proposal of Yuan et al. [2012], which is named belief propagation, avoids deploying an additional network of sensors, and does not require estimating the exact location of PU emulation suspects.

2.5.7 Energy Efficiency

CR related issues should be addressed by mechanisms that are energy efficient, i.e., that have limited communication and resource requirements, since SUs are likely to be battery powered. Hence, lightweight protocols are expected for estimation, learning and decision making operations. The number of sensed channels must also be minimized through appropriate prioritisation mechanisms since sensing is one of the main sources of energy and time consumption in CR scenarios. We can mention that cooperative sensing can indirectly address the energy efficiency problem since it enables the utilization of simpler CR devices with no or limited sensing capabilities (e.g., IEEE 802.22). However, cooperation induces signalling overhead, which can have a significant impact on network performance.

According to Grace et al. [2009], the excess bandwidth that is made available by CR can be fully exploited for power efficient strategies, i.e., for strategies that give priority to minimizing power consumption instead of maximizing spectrum use efficiency (i.e., the higher the bandwidth that is used for transmission the smaller the modulation rate and transmission power that are required). Grace et al. [2009] describe a variable power/bandwidth efficient modulation strategy that takes into account the channel occupancy probability. These authors also suggest the exploitation of antenna directionality as a means for improving energy efficiency in CR scenarios.

Timmers et al. [2010], Eljack et al. [2009], and Grace et al. [2009] are examples of works that address energy efficiency in CR scenarios. The CR MAC solution that Timmers et al. [2010] propose successfully applies a sleep-based mode to prolong the battery life of mobile SUs. With the proposal of Eljack et al. [2009], which assumes that the SUs are equipped with a GPS receiver, another approach is followed to achieve energy efficiency. That is, the SUs in a CR network exchange their coordinates, compute the distances to each other, evaluate the path losses, and accordingly adjust transmission power to the minimum required values.

2.5.8 Validation of CR proposals

Most existing CR proposals (see Sections 2.6 and 2.7) were validated through simulation or analytically, which is not totally convincing in many situations. Chowdhury and Melodia [2010] argue that current simulators make simplifying assumptions concerning the characteristics of real systems, resulting in questionable results. For example, Saleem and Rehmani [2014] state that real traces should be considered to improve the accuracy of PU activity models used in CR research. Furthermore, they mention that although such type of measurements have already been conducted (see discussion in Section 2.1) they are proprietary and, therefore, not publicly available.

Newman et al. [2010] also state that CR research has been mostly limited to theoretical frameworks and simulations, or to prototypes for small-scale experiments in few cases. Theoretical models and simulations enable to achieve a view of what the limits could be, i.e., performance goals, and provide steady conditions suitable for reproducibility. However, experimental tesbeds enable an evaluation and refinement of the models. They provide additional results, especially concerning practicality, limitations, and the proof that harmful interference to PUs is avoided [Newman et al., 2010]. Hence, the existence of experimental platforms and testbeds is highly desirable, and a few proposals already exist.

Jia and Zhang [2009] present a testbed development framework for CR networks that enables evaluation at the PHY, MAC, and network layers, through a cross-layer management approach. For the PHY layer, it uses a platform based on the Universal Software Radio Peripheral (USRP) open source hardware platform and on the GNU Radio, an open source project that provides a free software toolkit for developing software defined radios running on general purpose computers. USRP connects to a general purpose computer using the Universal Serial Bus (USB). GNU/USRP is suitable for small-scale proof-of-concept.

In their work, Chowdhury and Melodia [2010] analyse the main characteristics of several hybrid platforms (i.e., with software and hardware components) for experimental evaluation of distributed CR networks, such as WiNC2R (Winlab Network Centric CR). They state that most of them rely on GNU/USPR-based platforms. Chowdhury and Melodia [2010] also mention software platforms, such as SCA (Software Communications Architecture). Finally, Sutton et al. [2010] describe Iris, another software architecture for building reconfigurable radio networks and that is designed to run on a wide variety of general-purpose platforms.

For large-scale validation, a few solutions already exist, such as ORBIT (Open-Access Research Testbed for Next-Generation Wireless Networks) [Orbit, 2011] and CORNET (Cognitive Radio Network) [Newman et al., 2010]. ORBIT is a radio grid testbed, at Rutgers University, which consists of an indoor radio grid emulator for controlled experimentation and an outdoor field trial network for end-user evaluation under real-world settings. It is made of 400 Personal Computer-based nodes, arranged in a 20 by 20 grid. According to Newman et al. [2010], ORBIT has a limited PHY layer. CORNET is a testbed from Virginia Tech, which is spread over a four floors building and includes 48 wireless nodes. Chowdhury and Melodia [2010] also describe some experimental deployments of CR testbeds, which include the aforementioned CORNET and ORBIT solutions, and establish some challenges and architectural considerations about experimental CR platforms and testbeds.

Other solutions exist for CR testing and development, such as the European projects known as CorteXlab (Cognitive Radio Testbed Experimentation Lab) [FIT/CorteXlab - Cognitive Radio Testbed, 2015], CREW (Cognitive Radio Experimentation World) [CREW Project, 2015], and CORE+ (Cognitive Radio Trial Environment+) [The CORE+ project, 2015]. CorteXlab is a large scale radio testbed that integrates SDR nodes. It is located at INSA (Institut National des Sciences Appliquées) Lyon, France. CREW provides an open federated test platform for research on spectrum sensing, CR, and cognitive networking strategies. It integrates five heterogeneous testbeds at five different locations (Berlin, Dresden, Dublin, Ghent, and Ljubljana). CORE+ aims at developing experimental environments for CR in Finland.

2.6 Communication protocols for Cognitive Radio scenarios

This section discusses and overviews relevant proposals for communication protocols in CR scenarios. As already mentioned, the main operations in CR scenarios are mostly related to the PHY and MAC layers. Therefore, the design of appropriate MAC protocols, which are by definition responsible for controlling the access to the communication medium, is a CR core issue and, consequently, has received much more attention from the research community. However, CR capabilities are also expected to have significant impact on the performance of upper layers and, therefore, bring communication issues that can span different protocol layers, as illustrated in Figure 2.9 [Guan et al., 2010; Akyildiz et al., 2009].

For instance, when QoS is a concern, observation, learning, and decision making must also be performed at the network, transport, and application layers [Niyato and Hossain, 2009]. Issariyakul et al. [2009] investigate performance issues at the transport layer in overlay CR networks. Akyildiz et al. [2009] discuss key challenges concerning performance and open research issues faced at the network and transport layers in CR Ad-Hoc Networks (CRAHNs). Therefore, the discussion in this section is organized based on the MAC, network, transport, and application layers. In this discussion as well as in Figure 2.9, we assume the TCP/IP (Transmission Control Protocol/Internet Protocol) notion of application layer, which combines the application, presentation, and session layers of the OSI (Open Systems Interconnection) model.

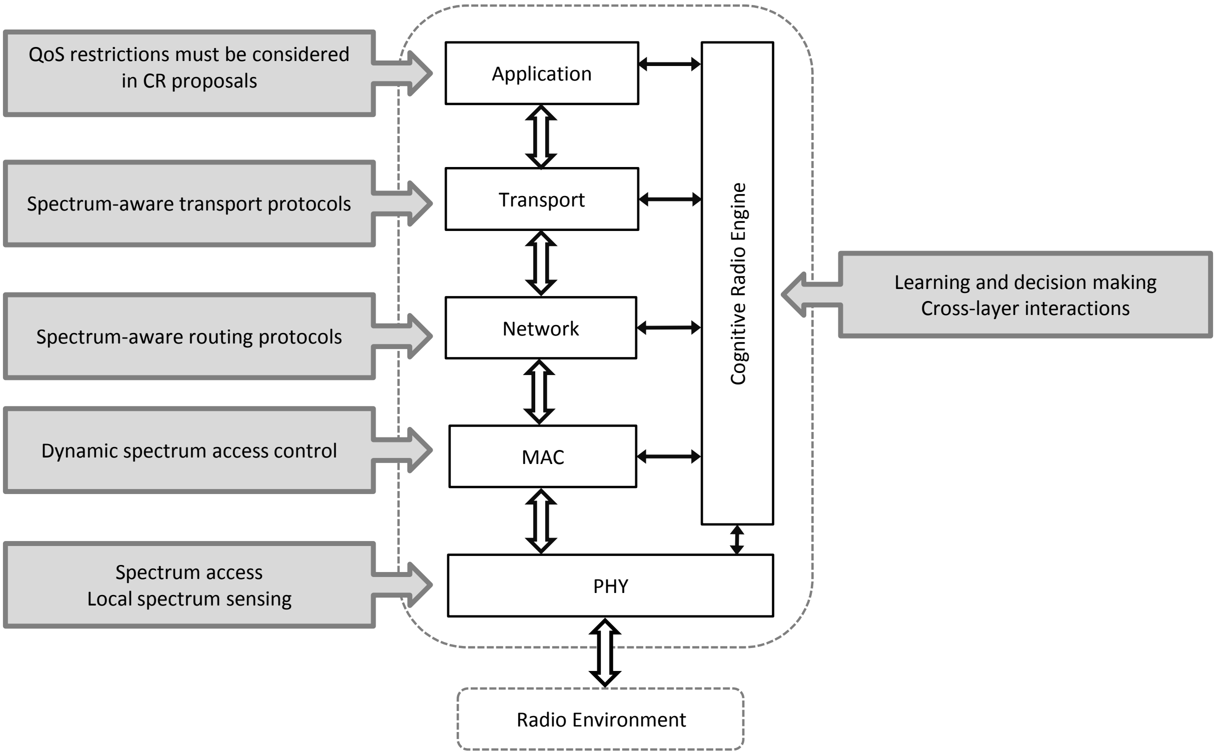


Figure 2.9. Communication protocol issues in Cognitive Radio scenarios

2.6.1 Medium Access Control protocols

Cormio and Chowdhury [2009] state that the most important functions of CR MAC protocols are deciding on the optimal sensing and transmission times, and on spectrum access coordination. The aim is protecting PUs from harmful interferences and achieving an efficient and fair utilization of the spectrum, which are the two main concerns of CR. Therefore, CR MAC protocols have received more attention from the research community than CR issues related to upper layers. This section uses twenty eight proposals (see Table 2.1 and Table 2.2) to draw global conclusions about the main characteristics of existing CR MAC protocols. Section 2.6.1.1 classifies these proposals according to four fundamental parameters: targeted network types; adopted approaches for spectrum access; number of required radios/transceivers per SU; and if a common control channel is used (see Table 2.1). Section 2.6.1.2 complements this analysis by identifying relevant optimizations (see Table 2.2).

2.6.1.1 Classification of existing proposals

Cormio and Chowdhury [2009] investigate the characteristic features, advantages, and limiting factors of some existing CR MAC protocols concerning sensing, synchronization, spectrum access, and the required number of transceivers. Their work considers both infrastructure and ad-hoc networks. Wang, Qin, and Zhu [2008] also provide a brief survey on a few existing MAC protocols for opportunistic spectrum access in CR. It can be noted that Cormio and Chowdhury [2009] define three main approaches for spectrum access, i.e., for enabling multiple SUs to determine who will access a particular data channel: (1) CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) like access for data and control traffic (i.e., random access protocols); (2) synchronized time slots for control and data traffic (i.e., time-slotted protocols); and (3) partially time-slotted and partially random access (i.e., hybrid protocols). This taxonomy is used in Table 2.1 from which it can be concluded that most current CR MAC proposals: (1) target ad-hoc network structures; (2) are random-based in terms of spectrum access; (3) require at least two radios/transceivers per SU; and (4) use a common control channel (CCC) for signalling purposes (see Figure 2.8). In most cases, when more than one transceiver/radio is required, one of them is dedicated to operate the CCC, i.e., signalling is performed over a dedicated CCC (see Section 2.5.3).

Some of the analysed CR MAC protocols are inspired by or are based on legacy systems, especially IEEE 802.11 DCF[1], which is one of the today's main protocols for wireless local area networks. For instance, DCA-MAC [Pawelczak et al., 2005] and DSA-MAC [Joe and Son, 2008] are based on IEEE 802.11 DCF. The proposal of Choi et al. [2006] can use a MAC scheme similar to IEEE 802.11 DCF for data transmission, and DCSS-MAC [Nan et al., 2007] exchanges RTS (Request To Send) and CTS (Clear To Send) packets from IEEE 802.11 DCF over a control channel. Concerning DFA-MAC [Ghaboosi et al., 2008], it is an enhancement to the IEEE 802.11s standard, which is an IEEE 802.11 amendment for mesh networking. However, only a small number of CR MAC proposals, such as DFA-MAC [Ghaboosi et al., 2008] and C-CSMA/CA [Zhang et al., 2008], maintain backward compatibility with the legacy systems (see Table 2.2). Concerning CBS-MAC [Hsieh et al., 2008], it allows for coordinated bandwidth sharing (CBS) between SUs and legacy IEEE 802.11 nodes in the unlicensed bands.

The analysed proposals include some examples of time-slotted and hybrid approaches for spectrum access, which are more complex than random-based solutions. For instance, DCSS-MAC [Nan et al., 2007] includes a time-slotted listening mechanism in which a specific time slot corresponds to a particular data channel. SYN-MAC [Kondareddy and Agrawal, 2008] divides total time into fixed time slots, one for each channel. With CLBO-MAC [Su and Zhang, 2008], a time-slotted approach is used to access the control channel, where each time slot includes a reporting phase and a negotiating phase for the transmitter and the receiver to agree on the

---

[1] DCF (Distributed Coordination Function), which is based on the CSMA/CA algorithm, is one of the basic access protocols supported by the IEEE 802.11 standard.

channel to be used. With OSA-MAC [Le and Hossain, 2008], time-slots are named beacon intervals (i.e., synchronization is achieved through the periodic transmission of beacons) and each slot is divided into three phases: channel selection; sensing; and data transmission. Similarly, with the solution proposed by Chang et al. [2014], each channel is also divided into beacon intervals. These periods are of equal length and consist of a negotiation window and data window, which is further divided into multiple data slots. A transmitter and a receiver exchange data over a previously reserved data slot.

Table 2.1: Classification of existing CR MAC proposals

Proposal	Network Architecture	Spectrum Access	Number of Radios/ Transceivers	Common Control Channel
Single Radio Adaptive Channel MAC (SRAC MAC)[1]	Ad-hoc	Random	1	-
Hardware Constrained-MAC (HC-MAC)[1]	Ad-hoc	Random	1	Yes
Cognitive-MAC (C-MAC)[1]	Ad-hoc	Time-slotted	Multiple	-
Partially Observable Markov Decision Process (POMDP) based MAC[1,2]	Ad-hoc	Hybrid	1	-
Opportunistic MAC[1]	Ad-hoc	Hybrid	2	Yes
Distributed channel assignment-MAC (DCA-MAC)[1,3]	Ad-hoc	Random	1 or 2	Yes
Distributed Frequency Agile-MAC (DFA-MAC)[4]	Mesh	Random	2	Yes
Coordinated Bandwidth Sharing-MAC (CBS-MAC)[5]	Infrastructure	Time-slotted	2	Yes
Dynamic Spectrum Allocation-MAC (DSA-MAC)[6]	Ad-hoc	Random	Multiple	Yes
Distributed Coordinated Spectrum Sharing-MAC (DCSS-MAC)[7]	Ad-hoc	Hybrid	2	Yes
Synchronized-MAC (SYN-MAC)[1,8]	Ad-hoc	Hybrid	2	-
Opportunistic Spectrum-MAC (OS-MAC)[1,9]	Ad-hoc	Hybrid	1	Yes
Cognitive radio CSMA/CA (C-CSMA/CA)[10]	Infrastructure	Random	1[a] or Multiple[b]	-
Cross-Layer Based Opportunistic -MAC (CLBO-MAC)[11]	Ad-hoc	Time-slotted	2	Yes
Opportunistic Spectrum Access-MAC (OSA-MAC)[12]	Ad-hoc	Time-slotted	1	Yes
Statistical Channel Allocation-MAC (SCA-MAC)[13]	Ad-hoc	Random	2	Yes
Dynamic Open Spectrum Sharing MAC (DOSS MAC)[1,14]	Ad-hoc	Random	3	Yes
Multichannel MAC protocol for CR networks (MMAC-CR)[15]	Ad-hoc	Random	2	Yes
Dynamic De-Centralized Hybrid-MAC (DDH-MAC)[16]	Ad-hoc	Random	2	Yes
Slow Hopping-MAC (SH-MAC)[17]	Ad-hoc	Random	1	No
Predictive-MAC (P-MAC)[18]	Ad-hoc/Infra.	Random	1	Yes
Cognitive MAC (CogMAC)[19]	Ad-hoc	Random	1	No
[Choi et al., 2006]	Ad-hoc	Random	2	Yes
[Ghaboosi et al., 2009]	Ad-hoc	Random	2	Yes
[Niyato and Hossain, 2009]	Mesh	Random	1	-
[Jia and Zhang, 2009]	Ad-hoc	Random	2	Yes
[Pandit and Singh, 2013]	Ad-hoc	Hybrid	1	Yes
[Chang et al., 2014]	Ad-hoc	Time-slotted	1	No

[1] [Cormio and Chowdhury, 2009]
[2] [Zhao et al., 2007]
[3] [Pawelczak et al., 2005]
[4] [Ghaboosi et al., 2008]
[5] [Hsieh et al., 2008]
[6] [Joe and Son, 2008]
[7] [Nan et al., 2007]
[8] [Kondareddy and Agrawal, 2008]
[9] [Hamdaoui and Shin, 2008]
[10] [Zhang et al., 2008]
[11] [Su and Zhang, 2008]
[12] [Le and Hossain, 2008]
[13] [Hsu et al., 2007]
[14] [Ma et al., 2005]
[15] [Timmers et al., 2010]
[16] [Shah et al., 2011]
[17] [Lee and Kim, 2012]
[18] [Hussein et al., 2013]
[19] [Ansari et al., 2013]

[a] Secondary users.
[b] Access points.

2.6.1.2 Supported Optimizations

The previous subsection has classified several CR MAC proposals according to four fundamental parameters. This subsection aims to complement this discussion by highlighting relevant optimizations that have been identified in the analysed protocols (see Table 2.2).

Table 2.2: Supported Optimizations

Proposal	Channel Aggregation	QoS Provisioning	Backup Channel	Backward Compatibility	Energy Efficiency	Balanced Usage of Opportunities	Awareness of Imperfection in Sensing [b]
SRAC MAC[1]	Yes	Yes	-	-	-	-	-
HC-MAC[1]	Yes	-	-	-	-	-	Yes
C-MAC[1]	Yes	-	Yes	-	-	Yes	-
POMDP[2]	-	-	-	-	-	-	-
Opportunistic MAC[1]	-	-	-	-	-	-	-
DCA-MAC[1,3]	-	-	Yes	Yes	Yes	-	-
DFA-MAC[4]	-	-		Yes	-	-	-
CBS-MAC[5]	-	Yes	Yes	-(a)	-	-	-
DSA-MAC[6]	Yes	Yes	-	-	-	-	-
DCSS-MAC[7]	-	-	-	-	-	-	-
SYN-MAC[1,8]	-	-	-	-	-	-	-
OS-MAC[1,9]	-	-	-	-	-	Yes	-
C-CSMA/CA[10]	-	-	Yes	Yes	-	-	-
CLBO-MAC[11]	-	-	-	-	-	Yes	-
OSA-MAC[12]	-	-	-	-	-	Yes	-
SCA-MAC[13]	Yes	Yes	-	-	-	-	-
DOSS MAC[14]	-	-	-	-	-	-	-
MMAC-CR[15]	-	-	-	-	Yes	-	Yes
DDH-MAC[16]	-	-	-	-	-	-	-
SH-MAC[17]	-	-	-	-	-	-	-
P-MAC[18]	-	-	-	-	-	-	-
CogMAC[19]	-	-	-	-	-	Yes	-
[Choi et al., 2006]	-	-	-	-	-	-	-
[Ghaboosi et al., 2009]	-	-	-	-	-	Yes	-
[Niyato and Hossain, 2009]	-	-	-	Yes	-	-	-
[Jia and Zhang, 2009]	-	-	-	-	-	Yes	-
[Pandit and Singh, 2013]	-	-	-	-	-	-	-
[Chang et al., 2014]	-	-	-	-	-	Yes	-

[1] [Cormio and Chowdhury, 2009]
[2] [Zhao et al., 2007]
[3] [Pawelczak et al., 2005]
[4] [Ghaboosi et al., 2008]
[5] [Hsieh et al., 2008]
[6] [Joe and Son, 2008]
[7] [Nan et al., 2007]
[8] [Kondareddy and Agrawal, 2008]
[9] [Hamdaoui and Shin, 2008]
[10] [Zhang et al., 2008]
[11] [Su and Zhang, 2008]
[12] [Le and Hossain, 2008]
[13] [Hsu et al., 2007]
[14] [Ma et al., 2005]
[15] [Timmers et al., 2010]
[16] [Shah et al., 2011]
[17] [Lee and Kim, 2012]
[18] [Hussein et al., 2013]
[19] [Ansari et al., 2013]

[a] IEEE 802.11-aware.
[b] False alarms and missed detections.

Channel aggregation, which consists in combining different channels in order to create another one of greater capacity, can be a means to achieve tolerance to PU appearance and also to enable QoS provisioning by means of throughput enhancement. For instance, with DSA-MAC [Joe and Son, 2008], multiple data channels can be allocated for communication between nodes.

Concerning SCA-MAC [Hsu et al., 2007], it uses statistics that are recorded for each channel in order to define the maximum channel aggregation level. The existence of backup channels is also an effective means to avoid or minimize the number of service interruption losses due to the appearance of PU activities. For instance, DCA-MAC [Pawelczak et al., 2005] assumes that an emergency channel and the unlicensed bands (i.e., ISM) are always available backup alternatives for data traffic, and CBS-MAC [Hsieh et al., 2008] allows the use of the unlicensed spectrum when no licensed spectrum opportunities are available. As already mentioned, some of the analysed CR MAC protocols are inspired by or based on legacy systems, especially IEEE 802.11 DCF, and some of them maintain backward compatibility.

Energy efficiency is a main concern in any wireless scenario due to the existence of battery supplied devices (see Section 2.5.7). However, only two of the analysed CR MAC proposals include energy efficiency concerns in their design. DCA-MAC [Pawelczak et al., 2005] follows a hierarchical architecture in which mobile devices are clustered into different groups. In each cluster, it is the most capable device (in terms of processing capacity, storage, and power supply) that is selected as the group gateway. This feature addresses in some way the energy efficiency issue. Concerning MMAC-CR [Timmers et al., 2010], energy efficiency is achieved through a mechanism that allows the SUs to go dozing when no communication is taking place and to go through a dual-phase sensing scheme (similar to IEEE 802.22) in which an accurate scan (i.e., fine sensing) is performed only after a change is detected during a periodically scheduled low-power scan (i.e., fast sensing).

All the analysed CR MAC proposals assume that the SUs know the states of the channels and select the best opportunities, and some of them specify specific methods for spectrum selection. With DSA-MAC [Joe and Son, 2008], statistics about spectral utilization are exploited for channel access decision. CLBO-MAC [Su and Zhang, 2008] supports random-based and negotiation-based sensing approaches. With the latter approach, a SU knows which channels have already been sensed by its neighbours and avoids selecting them. OSA-MAC [Le and Hossain, 2008] includes two random channel selection schemes: uniform channel selection and spectrum opportunity-based channel selection. With the first approach, the channels are selected with the same probability. With the opportunity-based selection mechanism, the higher the probability of a channel to be available the higher the probability to be chosen. SCA-MAC [Hsu et al., 2007] uses statistics that are recorded for each channel to define the optimum spectrum range to sense and the spectrum opportunity that requires the shortest waiting time.

Ghaboosi et al. [2009] use a probabilistic channel selection approach that targets spectrum load balancing and takes into account PU activity in distributed CR scenarios. In this proposal, the

SUs tag every channel with the probability of PU appearance during the time required to transmit an average size data frame and its acknowledgement frame when applying the lowest possible rate. With MMAC-CR [Timmers et al., 2010], a SU selects the vacant channel that has the lowest expected load. The proposal of Niyato and Hossain [2009] uses fuzzy-logic and an intelligent learning algorithm for selecting the best channel. POMDP based MAC [Zhao et al., 2007] accumulates channel history and learns which channel is best suited for long term access. Similarly, Ansari et al. [2013] also gather channel history regarding the outcomes of past sensing operations. Finally, concerning spectrum selection, we note that most existing solutions do not target a balanced utilization of spectrum opportunities among the SUs (see Table 2.2).

The majority of existing CR MAC proposals require the transmitter and the receiver to agree on the channel to use prior transmission. However, with DFA-MAC [Ghaboosi et al., 2008] and the proposal of Choi et al. [2006], the transmitter temporarily switches to the channel that is tuned by the receiver during data transmission. For instance, in the proposal of Choi et al. [2006], a node has its receiving transceiver permanently tuned to an available channel. It also informs its neighbours about its selection broadcasting this information on a CCC right after choosing a new channel and after random periods.

Cormio and Chowdhury [2009] state that additional work is needed in order for CR MAC protocols to account for false alarm and missed detection probabilities. In Table 2.2, only HC-MAC [Cormio and Chowdhury, 2009] and MMAC-CR [Timmers et al., 2010] address this issue. The same authors also present various drawbacks concerning the proposals they have analysed, such as low scalability, significant signalling overhead, time synchronization overhead, and waste of spectrum. It can also be noted that the QoS requirements of some data traffic types (e.g., multimedia streams) are not a concern for the majority of existing CR MAC protocols.

2.6.2 Network Layer protocols

In CR networks, routing protocols must also take into account the activity of PUs and the resulting implications (e.g., service interruption losses) to determine the best routes. This is the main difference with traditional routing protocols. Akyildiz et al. [2009] classify existing works about CR routing according to three distinct approaches: (1) routing with spectrum decision (i.e., joint selection of both the channel to access and the next hop); (2) routing with joint spectrum decision and PU awareness (i.e., establishing routes that avoid locations with PU activity); and (3) routing with joint spectrum decision and re-configurability (i.e., establishing routes that recover from PU appearance). In their work, Wang and Garcia-Luna-Aceves [2011] also consider that there is a correlation between dynamic frequency assignment, routing, and scheduling of accesses in wireless networks. Therefore, they state that these components should be treated jointly.

SEARCH (Spectrum Aware Routing Protocol for Cognitive Ad-Hoc Networks) [Chowdhury and Felice, 2009] is a routing protocol for mobile CR ad-hoc networks that follows a geographical forwarding approach and is spectrum aware (i.e., aware of PU activity). In geographic routing, a node knows the locations of the destination and of the candidate forwarding nodes within its range, and, therefore, can choose the next hop that is closer towards the destination. SEARCH is completely decentralized, requires the SUs to be equipped with a single radio, and assumes location determination through GPS or triangulation techniques. Chowdhury and Felice [2009] also describe some related works about centralized and distributed routing protocols for CR networks, as well as existing geographic routing protocols. They conclude that existing geographic routing protocols are only appropriate for single-channel networks and have no support for CR specific issues. They also argue that centralized approaches are not feasible for mobile CR ad-hoc networks (e.g., some of the referred protocols require collecting the entire network topology). Concerning existing distributed routing protocols for CR, Chowdhury and Felice [2009] state that they scale well but have a relevant problem in their viewpoint: they first start identifying the best paths and only then choose the preferred channels along them. These authors argue that path and channel decision should be made jointly.

Since switching from one channel to another can take a substantial amount of time, the number of spectrum handovers along a path must be minimized to avoid degrading final end-to-end performance. However, the aforementioned work of Chowdhury and Felice [2009] brings significant improvements when compared to a single-channel approach despite it allows different channels to be accessed along an end-to-end path. Also, when a PU is detected at either end of a link, the routing protocol must take the decision of either switching to another channel in the affected link or determining an alternate path. This decision must take into account the end-to-end delay or any other end-to-end performance metric. That is, if the cost of the detour is lower than the delay that results from switching to a new channel [Akyildiz et al., 2009; Chowdhury and Felice, 2009]. In CR networks, when disconnection is not caused by PU appearance (e.g., it is due to node mobility), the only alternative is determining another path.

Wang and Garcia-Luna-Aceves [2011], who consider that dynamic frequency assignment, routing, and scheduling of accesses should be treated jointly, present CROWN (Collective Routing, Scheduling, and Frequency Assignment for Wireless Ad-Hoc Networks with Spectrum-Agile Nodes). This solution is a distributed scheme that incorporates dynamic frequency assignment and scheduling information in the routing metric. CROWN aims at efficiently exploiting frequency diversity and spatial reuse at the MAC and network layers in order to reduce spectrum wastage and co-channel interference. However, it is based on the assumption that the nodes can only operate on unlicensed bands and, therefore, does not address the PU problem. Wang and Garcia-Luna-Aceves [2011] also describe some previous works on joint scheduling and routing in wireless networks and CR networks. On the contrary, the routing scheme for multi-hop CR networks proposed by Shu et al. [2014] includes PU activity in the criteria it uses for choosing the best route.

2.6.3 Transport Layer protocols

CR must improve end-to-end performance when compared to traditional wireless technologies in order to be viable. However, its dynamic spectrum access nature can affect end-to-end connections, mainly due to negative side effects, which result from delays inherent to CR operations, on the performance of the transport layer. For example, since the TCP entity on a SU cannot transmit acknowledgement packets during ongoing quiet periods dedicated to sensing, PU activities, and spectrum handover operations, there is a risk of excessive number of retransmissions and packet losses on paths that include any node in such states [Kumar and Shin, 2012a]. This issue results from delays being wrongly perceived as congestion situations. Therefore, it is necessary to avoid invoking congestion control mechanisms unnecessarily, making the transport layer aware of CR operations (i.e., interaction between MAC and transport entities is necessary). Wang et al. [2014] state that the performance of the transport layer impacts QoE more directly than the performance of lower layers does.

Stopping transmission at the transport layer or reducing its rate towards an optimal value, which avoids buffer overflow at intermediate nodes while maintaining transmission, are two possible approaches. Globally, transport protocols need to be spectrum aware in CR scenarios and, therefore, require new algorithms (e.g., for congestion window scaling in TCP) [Akyildiz et al., 2009]. Akyildiz et al. [2009] describe a TCP-based protocol for distributed CR networks and state that it is the first work aiming at addressing the transport layer challenges in such type of environment. There are a few other proposals that aim to address the impact of CR on the performance of the transport layer. For example, Kumar and Shin [2012a] propose a solution that addresses the adverse effects of DSA-related operations on TCP and UDP traffic. It is based on buffering and traffic shaping, and maintains compatibility by avoiding any changes to existing implementations of TCP and UDP protocols. This work only considers infrastructure-based wireless networks and the proposed solution runs on base stations. Wang et al. [2014] investigate the impact of PU activity and imperfect sensing on the performance of TCP, particularly on its back-off process, and the interaction between TCP and lower layers.

2.6.4 Application Layer protocols

Yu et al. [2011] state that any QoS degradation perceived by the SUs at the application layer can limit the success of CR technologies. These authors mention that most of the previous work about CR considers maximizing the throughput of SUs and mostly ignores other QoS measures. They argue that recent work in cross-layer design shows that maximizing throughput does not necessarily benefit QoS at the application layer for some applications, particularly those that require minimum guarantees (e.g., video transmission). Kumar and Shin [2012b] also state, concerning DSA, that gains at the channel level do not necessary result in gains regarding application performance and that QoS considered in existing DSA proposals is mostly related to channel-level metrics. The reasons are the same as stated in previous section, i.e., negative side effects that result from additional delays due to DSA operations. Therefore, application QoS must be carefully considered in CR solutions and channel allocation schemes should be application-aware [Yu et al., 2011; Kumar and Shin, 2012b; Shu et al., 2014].

Yu et al. [2011] describe a solution for multimedia transmission in CR networks, which was designed as an extension to POMDP based MAC [Zhao et al., 2007] (see sections 2.6.1 and 2.7.3). This solution jointly optimizes QoS at the application layer, spectrum access, and spectrum sensing. Kumar and Shin [2012b] propose a cross-layer application-aware framework that enables DSA protocols to improve application performance. This solution uses application QoS hints (i.e., minimum bandwidth, maximum delay, and maximum jitter on an end-to-end basis) and follows a reinforcement learning-based adaptive approach. Finally, the work of Shu et al. [2014] includes a channel selection scheme for multi-hop CR networks that takes into account application types with distinct QoS requirements, i.e., real-time and non-real-time applications.

2.7 Intelligent spectrum decision in CR

CR expects the availability of mechanisms for intelligent decision making in order to maximize the performance of SUs and avoid harmful interferences to PUs. Therefore, the applicability and feasibility of learning based on past experience and observation are often considered a core issue in CR. In distributed CR networks, a SU can be defined as a software defined radio (see Section 2.1) equipped with an independent CR engine (see Figure 2.2 and Figure 2.9). The CR engine is essentially responsible for learning based on past experience and observation, and for spectrum decisions. According to Clancy et al. [2007], it is conceptually composed of a knowledge base, a learning engine, and a reasoning engine. At any time, conclusions are generated based on the information that is defined in the knowledge base. The learning engine is responsible for manipulating the knowledge, based on experience, and its outcomes are intended to be accessed in the future by the reasoning engine for decision making.

In CR environments, instead of using a predefined list of countless actions in order to account for all possible radio states, it is more reasonable to have a learning engine that auto-generates the actions based on experience. Therefore, the learning engine is responsible for enriching the list of actions, which allows the SUs to adapt to their changing environment [Clancy et al., 2007]. At given times, the reasoning engine looks at the current state and determines which actions are executable under that state. The action which maximizes an objective function is executed and the output it produces is used to update the knowledge base. In centralized CR networks, this discussion about the CR engine mainly applies to the central entities. That is, with such type of CR architecture, central entities collect data from the SUs, process it, and take spectrum decisions on behalf of the SUs (see Section 2.4).

Given this brief conceptual description of the CR engine, the next section highlights the expected gains of learning based on past experience and prediction in CR scenarios concerning spectrum decision. Then, modelling of PU traffic is discussed. Finally, we present the main characteristics of some CR proposals with prediction-based capabilities.

2.7.1 Learning based on observation and past experience, and prediction in CR scenarios

In CR scenarios, the SUs should be able to dynamically, intelligently, and on the fly decide on their operating frequency bands and on other transmission parameters based on: (1) the observed spectrum availability/radio environment; (2) policies; (3) capabilities; (4) predefined goals (e.g., performance and QoS requirements); and (5) learning based on observation and past experience. The relevance of learning based on observation and past experience can be easily justified if we consider its potential benefits under a sense-before-transmit process (see Section 2.5.2). Basically, it enables to model and, consequently, predict (i.e., probabilistically determine) busy and idle times on channels.

Some of the consequences of predictive spectrum decision are: (1) a decrease of time and energy spent to find an idle channel before any transmission period, since channels can be prioritized according to their probabilities of availability; (2) a decrease in the number of spectrum handovers and service interruption losses since the channels can be prioritized according to their expected durations of availability; and (3) a decrease in terms of interference to PUs since PU appearance can be anticipated before and during transmission. However, other less obvious benefits can also result from traffic prediction in CR scenarios. For instance, according to Guanat al. [2010], routing should be forward-looking (i.e., proactive). Chowdhury and Felice [2009], which present a novel routing protocol for mobile CR ad-hoc networks (see Section 2.6.2), also consider that their work can be further enhanced by incorporating a learning-based feature that defines the characteristics of PU activity in every link's region. Network monitoring and the protection against jamming attacks, which is a main concern in CR scenarios, can also be enhanced by traffic modelling [Salah-Eldeen et al., 2007].

Adaptive traffic prediction enables minimizing delays, maximizing throughput, and reducing interference to primary systems in CR scenarios. These mechanisms are mostly based on autonomous learning and enable the SUs to track the variations in the radio environment [Akyildiz et al., 2009]. According to Clancy et al. [2007], the application of machine learning to CR Networks can be defined as follows: "CR users should be able to remember lessons learned from the past and act quickly in the future". They also state that, usually, the most intelligence is put behind the learning and decision making process, the slower they are and the higher the consumption of resources is. Therefore, it is important to select the techniques to use taking into account the constraints that are inherent to CR scenarios (e.g., real-time operations and limited capacity in terms of processing, memory, and energy).

In the literature, different Machine Learning algorithms are assumed to be adequate for spectrum prediction in CR scenarios, such as: Semi-Markov Processes; Hidden Markov Models; Bayesian Networks; Neural Networks; Genetic Algorithms; and Data Mining. For instance, Genetic Algorithms can make the radio go through additional states until a globally optimal state is found. With this kind of approach, each new state is evaluated with the aim of maximizing an objective function. Concerning hidden Markov models and Bayesian networks, they enable determining the most likely traffic pattern which could have generated an observed sequence of busy and idle periods.

The next section discusses PU traffic modelling, which is an issue of major importance concerning learning based on observation and past experience, and prediction in CR scenarios.

2.7.2 Primary user traffic modelling

Integrating models about PU activity in the characterization of data channels enables prediction, probabilistic reasoning, and intelligent spectrum decision. Several research works have indicated that channel occupancy exhibits behavioural patterns and can be statistically modelled, and several solutions have been proposed in the literature to model PU activity [Wang et al., 2010b; Saleem and Rehmani, 2014]. However, different traffic models apply to different applications (e.g., voice communication, video data, and general packet data) and there is not a single PU activity model applicable to all the CR networks and spectrum bands [Li and Zekavat, 2009; Saleem and Rehmani, 2014].

In CR scenarios, PU traffic is often modelled as a binary sequence of alternating busy (ON) and idle (OFF) states with variable durations (see Figure 2.10). Therefore, the main concern is predicting the durations of ON and OFF periods. For example, when a PU appears or is expected to appear, predicting the duration of the incoming ON period enables deciding if a SU should stay in its current channel and wait until it becomes idle again, or switch to an available channel instead. The latter option is the preferred one when occupancy time is expected to be shorter than time necessary to perform a spectrum handover operation.

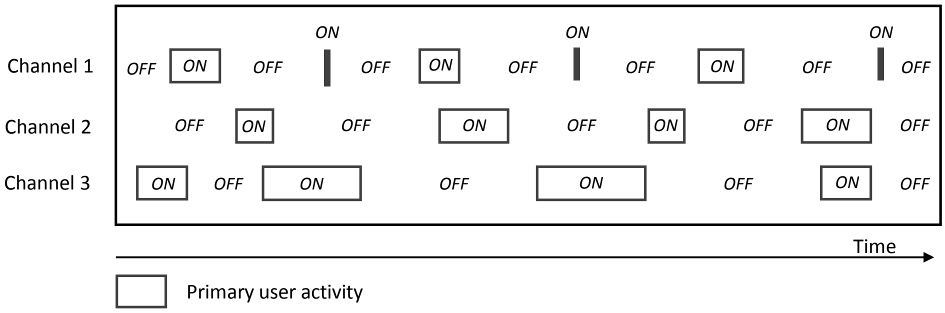


Figure 2.10. Primary user traffic

There are two elementary traffic classes in wireless scenarios: (1) deterministic patterns; and (2) stochastic (i.e., random or non-deterministic) patterns. Stochastic traffic can only be described in statistical terms (e.g., exponentially distributed) and usually varies slowly over time in data networks [Xiukui and Zekavat, 2008]. Deterministic traffic includes fixed or periodic OFF and ON times. For instance, Lopez-Benitez et al. [2009] state that some portions of the DCS (Digital Cellular Service) 1800 downlink frequency band show a well-defined periodic utilization pattern that could be exploited by SUs. As described in Table 2.3, the ON and OFF times that build up a traffic sequence must be classified separately when they are independent [Höyhtyä et al., 2008]. Different types of traffic patterns require different prediction methods/algorithms and, consequently, adaptive schemes must be considered [Höyhtyä et al., 2008; Saleem and Rehmani, 2014]. For instance, the type of traffic pattern can be determined during an initial learning phase (i.e., a discovery phase) through the gathering of enough data. In this case, it can be assumed that ON and OFF times are random before the learning is concluded [Höyhtyä et al., 2008].

Table 2.3: Types of traffic patterns

ON times	OFF times
Random	Random
Deterministic	Random
Random	Deterministic
Deterministic	Deterministic

Most of the research in CR assumes that transitions between ON and OFF states follow a Poisson arrival process, which implies exponentially distributed lengths [Issariyakul et al., 2009; Wang et al., 2010b; Saleem and Rehmani, 2014; Bicen et al., 2012; Bao and Fujii, 2011]. However, Wang et al. [2010b] also mention that this assumption may not be valid in real world situations. Therefore, they also evaluate their proposal, the DOSP (Dynamically Optimized Spatiotemporal Prioritization) algorithm, under different assumptions (e.g., constant rate traffic).

Akyildiz et al. [2009] briefly describe the main characteristics of some proposals about PU activity modelling. They also conclude that some of them are not practical and that more practical models must be developed. Amanna and Reed [2010] overview several cognitive frameworks and conclude that some existing models are so complex that they could never be practical. Saleem and Rehmani [2014] provide a detailed survey about PU activity modelling. They classify existing solutions based on different types such as: Markov processes; queuing theory; time series; ON/OFF periods; and real spectrum occupancy measurement. Concerning the latter type, Saleem and Rehmani [2014] mention that it is not trivial to adopt it due to time and cost restrictions, government rules, and telecommunication policies. They also state that there is a need for correlation between real measurements and mathematical models, as well as for developing mathematical models based on measurements.

Fixed models based on offline measurements are not totally appropriate for CR scenarios and, therefore, real-time based PU traffic models are needed for achieving optimizations based on spectrum prediction. Nevertheless, Wellness and Mähönen [2010] introduce a statistical model they argue enabling a more realistic modelling of spectrum utilization, i.e., closer to real traces obtained during a measurement campaign. In their work, the comparison is made with other models, such as constant duty cycle and uniformly distributed duty cycle. Finally, regarding traffic modelling in CR scenarios, we can also mention the applicability of time series-based approaches. For instance, according to Wang and Salous [2008], a sequence of spectrum measurements, typically performed at regular intervals, can be analysed by time series-based approaches in order to enable prediction. In their work, these authors collected the occupancy data set (i.e., measured series) of a specific frequency band, at Durham Campus in the United Kingdom, each hour during seven days. Then, they successfully applied a time series-based analysis to it. The model they used, i.e., ARIMA (Auto-Regressive Integrated Moving Average) [Wang and Salous, 2008; Li and Zekavat, 2009; Saleem and Rehmani, 2014], resulted in fitted series with good agreement with the measured data.

2.7.3 Cognitive Radio proposals with prediction-based capabilities

Despite the aforementioned relevance of prediction for spectrum decision, existing CR proposals mostly perform channel selection based on random and simple statistics-based approaches (see Section 2.5.7). Höyhtyä et al. [2008] state that prediction based on traffic pattern characterization has not been explored much in the literature. However, there are already some machine learning-based proposals in the CR area that aim at exploiting the characteristics of PU traffic and estimating the duration of occupancy times [Xiukui and Zekavat, 2008]. This objective is accomplished through a statistical analysis of gathered data that enables evaluating the probability of availability of a frequency band within a specific period. Consequently, time to find an available channel, interference to PUs, and the rate of spectrum handovers decrease since the selected channel will probably be available during the entire sensing and transmission periods. Nevertheless, with probabilistic-based approaches, blocking (i.e., transmitting in a channel that becomes busy in terms of PU traffic) remains possible. Table 2.4 summarizes the main characteristics of eight CR proposals with prediction-based features in terms of their main objectives, global approaches, and estimation methods.

In the work of Höyhtyä et al. [2008], since the traffic characteristics of a channel can change over time, estimations only consider data that has been gathered within a limited (sliding) time-window. This mechanism aims to limit the history of events (i.e., past experience) remembered at any given time in order to adapt to changes in spectrum occupancy. Höyhtyä et al. [2008] show, through simulation, that random selection, which is the most commonly used approach in CR and only uses instantaneous information about the environment, is outperformed by their solution, in terms of both the number of spectrum handovers and interferences to PUs. As a direct consequence, delays in transmission are also reduced and throughput increased. Tsagkaris et al. [2008] follow a similar approach. The CR learning engine they propose is based on an artificial neural network and uses a time-window of *N* slots that represent past experience. Each slot has a weight associated to it and the more recent is the slot the greater is its weight, which gives more importance to recent observations.

Table 2.4: CR proposals with prediction-based capabilities

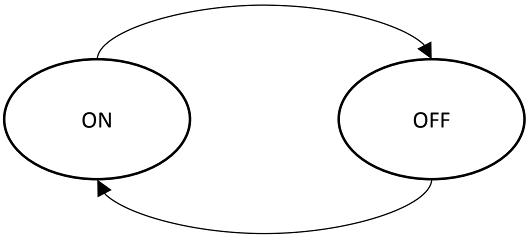
Proposal	Main Objective	Global Approach	Estimation Method
[Höyhtyä et al., 2008]	Minimizing the interference to primary users.	Predicting future idle times and switching to better channels before the appearance of PUs on the current channel.	Pattern type detection and availability time prediction.
[Tsagkaris et al., 2008]	Increasing the achievable data rate.	Learning schemes that behave as predictors for the data rate that can be achieved when specific configurations are applied to the radio.	Artificial neural networks.
[Jiang et al., 2008a]	Reducing the number of spectrum sensing operations.	Every user assigns to every channel a weight, which is updated every time the channel is accessed, through the assignment of a reward (increase) or a punishment (decrease) depending on the success of the action.	Reinforcement learning.
[Kim and Shin, 2008]	Efficient discovery of spectrum opportunities.	Characterization of PU activity on each data channel.	Semi-Markov process with two states.
POMDP based MAC[1]	Optimized selection of the next channels to be sensed/accessed.	Past history is accumulated and used in order to learn which channel is best suited for long term use.	Partially observable Markov decision process.
Dynamically Optimized Spatiotemporal Prioritization (DOSP)[2]	Improving the overall likelihood of channel access.	Long-term statistical information is exchanged between cooperative secondary users.	Statistics-based.
CogMAC[3]	Selection of the channels with higher availability.	Each channel has an associated weight that is dynamically updated based on sensing outcomes.	Reinforcement learning.
P-MAC[4]	Efficient utilization of spectrum opportunities.	Characterization of PU activity on each data channel.	Exponential Smoothing Model.

[1] [Zhao et al., 2007]
[2] [Wang et al., 2010b]
[3] [Ansari et al., 2013]
[4] [Hussein et al., 2013]

Jiang et al. [2008a; 2008b] assign each channel a specific weight. The values of the weights are dynamically adjusted based on the outcomes of the accesses through a rewarding-punishment scheme. That is, a higher value for a weight means a more successful access to the corresponding channel in the past. Jiang et al. [2008a] also state that their proposal is low in complexity because it never requires trying every possible channel. Globally, the SUs keep using the channels they have successfully used in the past.

Kim and Shin [2008] use an estimation method that supports two novel schemes: (1) optimization of the sensing period; and (2) an algorithm for optimal channel sequencing (prioritizing) that minimizes delays in searching for an opportunity. They define an estimation method that is used to capture time periods in which the SUs can transmit without causing harmful interferences to PUs (i.e., during OFF times). The durations of busy times T_{ON}^{i} and idle times T_{OFF}^{i} of a given channel i are modelled through probability density functions (see Figure

2.11). These functions, which can be any distribution function, can be assumed in advance or determined online based on gathered data. In their work, Kim and Shin [2008] assume that ON and OFF periods are independent and are equally distributed. Their approach is solely based on statistics and assumes that the channel parameters for the distribution of ON and OFF periods vary slowly over time. This assumption enables the SUs to track, through sampling and estimation making, the time-varying parameters of the probability density functions as well as their confidence intervals. In order to avoid high processing costs, Kim and Shin [2008] do not make estimations every time a sample is collected, i.e., every time sensing is performed.



$$T^i_{ON} \sim f_{T^i_{ON}}(y), y > 0 \qquad T^i_{OFF} \sim f_{T^i_{OFF}}(y), y > 0$$

Figure 2.11. Semi-Markov process

Observable Markov decision process (POMDP) based MAC protocol [Zhao et al., 2007; Cormio and Chowdhury, 2009] assumes that the network state cannot be fully observed due to partial spectrum sensing or sensing error. It divides time into slots and follows a sense-before-transmit approach (see Figure 2.5) in each slot. At the start of a slot, past history is used to select the channels to be sensed in priority. POMDP based MAC performs spectrum selection probabilistically and requires no prior knowledge about primary traffic statistics. This solution assumes that the environment is similarly seen over either ends of a communication pair, which allows the transmitter and the receiver to synchronously select the same frequency band without requiring any type of coordination. According to Cormio and Chowdhury [2009], one of the limitations of POMDP based MAC is that it does not cope with frequent and random primary traffic pattern changes, and it does not perform well in the initial learning stage, a situation that may last for large periods.

With DOSP (Dynamically Optimized Spatiotemporal Prioritization) [Wang et al., 2010b], a statistics-driven algorithm, the statistical information that is exchanged between the SUs can be fused with local statistics about channel availability through what the authors designate as a dynamic statistical learning process. The resulting information is then used to prioritize access to the channels. DOSP uses four types of channel occupancy statistics, as well as knowledge about the success of past decisions: (1) instantaneous statistics; (2) short-term statistics, which include observations taken over a previous short period (e.g., 10 milliseconds); (3) local long-term statistics, which take into account local observations taken for a long period (e.g., 24 hours); and (4) cooperative long-term statistics, which result from the fusion of local long-term statistics exchanged among the SUs. With DOSP, a SU that enters the network can acquire and start using long-term statistics from its neighbours.

With CogMAC [Ansari et al., 2013], a SU associates a specific weight with each channel that belongs to its channel pool and senses all these channels before trying to transmit a data frame. During these sensing periods, the weights of the channels are updated based on obtained sensing outcomes. That is, the weight of a channel increases if that channel is sensed vacant and decreases otherwise. The resulting weights are used to maintain a smaller number of channels with higher weights in the channel pool (i.e., with higher quality) and, therefore, to limit its size, which enables reducing the duration of sensing periods and improving performance. CogMAC additionally maintains the history of channel weights in order to avoid including in the pool poor quality channels recently eliminated.

Finally, P-MAC [Hussein et al., 2013] aims at predicting PU activity on the channels in order to utilize OFF periods more effectively while reducing sensing time, control traffic, and interference to PUs. It assumes that PU traffic is a sequence of alternating ON and OFF states, supports various distribution types (e.g., Normal and Exponential distributions), and is based on the assumption that the SUs are able to observe and accurately characterize the spectrum continuously. P-MAC includes a prediction model, named Exponential Smoothing Model, which determines the current channel access time as a weighted average of the previous channel access time and previous observed channel OFF time.

2.8 Summary

CR aims at enabling an efficient utilization of the radio spectrum and is still in its infancy, particularly since it is a highly multidisciplinary and, consequently, complex area that attracts numerous research efforts. This chapter provided a global vision of CR under different perspectives, addressing related technologies, standardization activities, architectural approaches, relevant issues, communication protocols, and learning through observation and past experience. We can conclude from the discussion in this chapter that several challenging CR issues have already been satisfactory addressed and that many still need further investigation, which makes

CR an open and interdisciplinary research area. CR is without any doubt in the critical path to the future wireless networks. However, a significant amount of work remains to be done.

According to our vision of CR, which was detailed in this chapter, some of the main open challenges for the deployment of efficient CR scenarios are: (1) effective protection of PUs through appropriate sensing and prediction solutions; (2) seamless spectrum mobility; (3) efficient and balanced utilization of spectrum opportunities; (4) energy efficiency; (5) practical solutions against data falsification and PU emulation attacks; (6) robust and scalable alternatives to the utilization of common control channels; and (7) QoS provisioning. All the mentioned issues require appropriate mechanisms that are intimately linked but not limited to MAC protocols. For instance, integrating practical learning capabilities with CR proposals is a core challenge in CR since it enables making decisions when accurate real-time information is not available, i.e., through prediction. Beyond the issues that have been discussed with some detail throughout this chapter, other domains must also be considered, such as business models and regulation.

This thesis defines solutions that target both the protection of hidden PUs and the performance of SUs in distributed CR networks. They specifically aim at: (1) increasing sensing accuracy through a cooperative approach (see Chapter 3); (2) making an effective utilization of learning based on local observation and past experience features (see Chapter 4); (3) addressing the dedicated common control channel saturation problem (see Chapter 5); (4) optimizing the spatial reuse of the spectrum (see Chapter 6); and (5) reducing the amount of control traffic between SUs (see Chapter 6).

Chapter 3

Cooperative sense-before-transmit

This chapter defines and evaluates COSBET (Cooperative Sense-Before-Transmit) MAC, an opportunistic CR MAC protocol that follows a novel approach for higher PU protection. This solution targets distributed multi-hop CR scenarios with high variability in terms of the availability of spectrum opportunities in time and space. COSBET-MAC assumes fully autonomous SUs (i.e., SUs that make spectrum decisions exclusively based on local observation and cooperation with each other) and PUs that are totally unaware of CR operations. Its main objective is providing higher protection of PUs against interferences from SUs while allowing the SUs to effectively utilize spectrum opportunities.

The work presented in this chapter resulted in the following publications:

- Marinho, J. and Monteiro, E. (2011, November). Cognitive Radio Simulation based on OMNeT++/MiXiM. *Proc. of the 11ª Conferência sobre Redes de Computadores. CRC 2011.*
- Marinho, J. and Monteiro, E. (2012). Cooperative Sensing-Before-Transmit in Ad-hoc Multi-hop Cognitive Radio Scenarios. *10th International Conference on Wired/Wireless Internet Communications. WWIC 2012*. (pp. 186-197). Springer Berlin Heidelberg. doi: 10.1007/978-3-642-30630-3_16.

The remainder of this chapter is organized as follows. Section 3.1 emphasis CR issues that are relevant concerning COSBET-MAC design. Section 3.2 identifies the limitations of related work it intends to overcome. Section 3.3 describes COSBET-MAC in detail. Section 3.4 evaluates it, through simulation, in terms of both the performance it delivers to SUs and the protection of PUs it achieves. Finally, Section 3.5 summarizes the contributions of COSBET-MAC.

3.1 Introduction

According to the overlay approach of CR, the SUs can opportunistically access vacant frequency bands in order to increase their own performance provided that they do not cause harmful interferences to the respective PUs (see Chapter 2). Thus, they are intended to dynamically and intelligently choose their operating frequency bands and other transmission parameters (e.g., transmission power) based on spectrum availability. The existence of appropriate MAC solutions is therefore of major importance and many have already been proposed (see Section 2.6.1), being the effective protection of PUs and communication performance improvement of SUs the main objectives. However, based on the outcomes of the literature review provided in Chapter 2, we can state that existing CR MAC solutions omit relevant issues, are too complex, or are based on simplistic or unpractical assumptions. Therefore, more research is needed on this topic.

Many existing CR solutions access the spectrum through a sense-before-transmit approach, i.e., the selected channel is sensed before data transmission and another one is searched if it is busy (see Section 2.5.2). This approach reduces the probability of harmfully interfering with PUs since sensing is performed before every access. In distributed CR networks, the type of scenario we target in this thesis, it is up to the SUs to perform sensing locally and accordingly take their own decisions. However, due to spatial diversity in terms of spectrum state, it is possible that a channel is idle at one side of a communication link and busy at the other side. Therefore, channel selection must be cooperatively decided by the transmitter and receiver. Furthermore, in wireless networks, there is a so-called hidden node problem when two wireless nodes cannot sense each other but have interference ranges that overlap each other. This issue implies that, in some circumstances, a SU can interfere with the coverage area of a PU even when it cannot sense its activity. Therefore, cooperative sensing schemes, in which the SUs share and combine sensing outcomes, are a means to increase sensing accuracy and efficiency (see Section 2.5.2). To support cooperation between SUs, many CR MAC protocols use a dedicated CCC (Common Control Channel) that must be continuously available (i.e., deployed over frequency bands with no PU activity). In this situation, a SU is typically equipped with an extra radio/transceiver that is dedicated to operate the CCC (see Section 2.5.3).

3.2 Related work and contributions

With some existing distributed CR MAC proposals that include cooperative sensing features, such as with the work of Timmers et al. [2010], a SU cannot use a specific channel if it is sensed busy by at least one of the SUs in the network. This is the so-called OR-rule and it aims at coping with the hidden PU problem (see Section 2.5.2). However, this approach can result in an inefficiency named “false spectrum access denial”, i.e., a SU is denied access to a given channel despite it is out of its region of potential interference [Malady and da Silva, 2008]. Also, several authors make ideal assumptions concerning the detection of PUs, which limits the practicality of their solutions. For example, Hassan et al. [2011] and Chen et al. [2014] assume that all the SUs are location-aware and know the locations of all the PUs, and Zhao et al. [2007] assume that the SUs can obtain information from the PUs, which does not comply with the rule that CR does not imply modifications to the PUs. COSBET-MAC avoids such types of assumptions.

Concerning how spectrum access is performed, most current CR MAC proposals are based on random access, i.e., they are similar to CSMA/CA (see Section 2.6.1), for data and control traffic [Cormio and Chowdhury, 2009]. COSBET-MAC, which aims at being simple and practical, follows this approach too. Time-slotted and hybrid alternatives are more complex since they require stringent time synchronization schemes. Furthermore, time synchronization over an entire network is not always feasible, increases overhead, and also compromises network scalability [Lo, 2011; Luo et al., 2009]. Several CR MAC proposals based on random access have already been proposed for distributed CR networks (see Section 2.6.1). However, on the contrary of COSBET-MAC, none of them addresses the following issues jointly: cooperative sensing; coordinated access to existing opportunities; support of high variability in terms of spectrum opportunities; and protection of hidden PUs. For instance, amongst the random access-based CR MAC solutions analysed in Section 2.6.1, only the works of Ghaboosi et al. [2009] and Jia and Zhang [2009] have the SUs coordinating spectrum access with each other. The proposal of Jia and Zhang [2009], which is based on the overhearing of control frames issued by neighbours, assumes that each SU has an up to date list of locally available channels. Therefore, on the contrary of COSBET-MAC, these authors omit and let sensing issues open, despite being a major concern in CR environments.

In the work of Choi et al. [2006], the channel to be accessed is unilaterally selected by the receiver and, therefore, it does not account for the hidden PU problem and spatial diversity in terms of spectrum state. Similarly, the work of Yuan et al. [2007], which targets the utilization of spectrum opportunities in television frequency bands, does not propose any solution aiming at protecting hidden PUs (e.g., through a cooperative sensing approach). Finally, the work of Timmers et al. [2010], which is very complete in terms of the issues it addresses, applies the OR-rule globally in the network. Therefore, it is more prone to the mentioned “false spectrum access denial” problem (see Section 2.5.2) than COSBET-MAC is. The work of Timmers et al. [2010] also assumes that sensing and communication can be performed simultaneously. Therefore and on the contrary of COSBET-MAC, it is not compatible with energy detection, which is the preferred sensing scheme in practical terms and cannot make the distinction between PU and SU activities (see Section 2.5.2). Besides, most CR solutions assume the utilization of half-duplex transceivers, which are either in transmit or receive mode at any instant.

Being identified the limitations of previous distributed CR MAC solutions that follow a random access strategy, the next section proceeds with the description of COSBET-MAC, a CR MAC solution that targets distributed CR scenarios with totally autonomous SUs and with PUs that are unaware of CR operations. Key aspects of COSBET-MAC consist in coping with hidden PUs and hidden SUs, avoiding complex and stringent synchronization schemes, having spectrum access coordinated between the SUs, avoiding unrealistic assumptions, and allowing idle SUs to cooperate in sensing on a non-mandatory basis.

3.3 Cooperative sense-before-transmit approach

COSBET-MAC strictly follows a sense-before-transmit approach (see Section 2.5.2) and includes a novel cooperative sensing scheme that aims at increasing the protection of PUs through the participation of idle neighbours [Marinho and Monteiro, 2012a]. Spectrum access is random-based and the utilization of spectrum opportunities is intended to be coordinated between the SUs. We also assume that the SUs perform sensing through energy detection. In this proposal, every SU is equipped with two half-duplex radios. One of them is devoted to operate a dedicated CCC and the other, which is dynamically reconfigurable, to access data channels. Finally, as we target multi-hop distributed CR networks, COSBET-MAC accounts for the possibility of hidden PUs and hidden SUs.

Figure 3.1 illustrates the basics of COSBET-MAC and the four phases each cooperative sense-before-transmit cycle includes: selection; cooperative sensing; decision; and access. The first and third phases are both based on a three-way handshake scheme, and negotiation between a transmitter and a receiver spans the first three phases. The approach COSBET-MAC follows, which we designate as cooperative sense-before-transmit, results in a fully decentralized version of Algorithm 3.1. With COSBET-MAC, a SU transmits control frames over the dedicated CCC and data frames through its reconfigurable radio. An RTS (Request To Send) frame, which is the first control frame to be issued in a negotiation process (see Figure 3.1), is transmitted through a contention-based scheme similar to IEEE 802.11 DCF and, more generally, to CSMA/CA principles (see Section 2.6.1). Since neighbours set the CCC as being reserved after overhearing an RTS frame, no contention or back-off schemes are considered for issuing the remaining control frames, i.e., until decision phase ends. On data channels, as reservation is previously accomplished through negotiation on the CCC, transmission is directly achieved without any additional contention or coordination procedure.

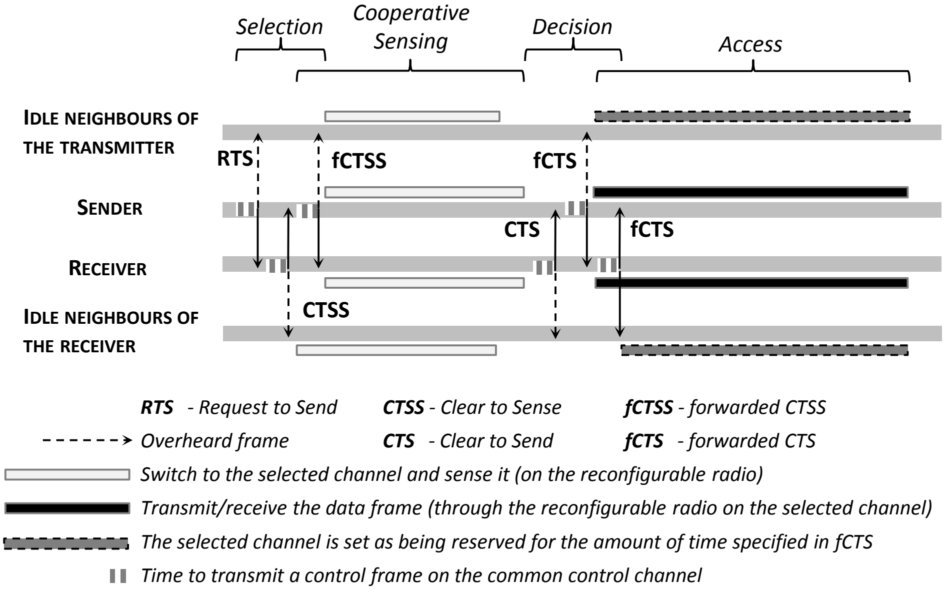


Figure 3.1. Interaction between secondary users

```
Inputs: $N$, neighbours of the transmitter-receiver pair;
        $N_{idle}$, idle neighbours of the transmitter-receiver pair;
        $C_s$, the set of non-reserved channels at the transmitter;
        $C_r$, the set of non-reserved channels at the receiver;
        $C_n$, the set of non-reserved channels at neighbour $n$.
Output: A channel $c$ that is free of any activity; or a selection failure.
if $(C_s \cap C_r) = \varnothing$ then return selection failure
$c \leftarrow f(C_s \cap C_r)$  [$f(x)$ implements the channel selection scheme (e.g., uniform random)]
if $\{n \in N / c \notin C_n\} \neq \varnothing$ then return selection failure
for the transmitter, the receiver and {neighbours $\in N_{idle}$ / $c$ not already set as reserved} do
    sense $c$
end for
$R \leftarrow$ set of obtained sensing results from transmitter, receiver, and {neighbours $\in N_{idle}$ / $c$
    not already set as reserved}
if $\{r \in R / r = (c \text{ is busy})\} \neq \varnothing$ then return selection failure
return $c$
```

Algorithm 3.1. Cooperative sense-before-transmit

In order to work properly, COSBET-MAC requires the transmission ranges to be the same on both radios, i.e., on the CCC and on data channels, for all the SUs. The main reason is that neighbourhood must be similar on the CCC and on data channels. For instance, if a SU is able to decode the control frames that are sent by another SU, it assumes that both are also in the transmission ranges of each other on data channels. On the contrary, if a SU is out of the transmission range of another SU on the CCC, then, we assume in the design of COSBET-MAC that both SUs are also out of the transmission ranges of each other on data channels.

Since path loss increases with increasing operating frequency, COSBET-MAC must adjust the transmission power of a reconfigurable radio when switching it to a new channel in order to keep its transmission range stable. Consequently, COSBET-MAC requires appropriate propagation models that enable modelling the signal attenuation between wireless transceivers. Such models exist and have been developed for distinct scenarios (e.g., indoor, outdoor, cities) [Phillips et al., 2013]. Their results are predictive in nature and, consequently, not fully accurate. However, our objective consists in keeping the CCC and the data channels with a similar transmission range, whatever this value is. That is, we do not aim at setting the transmission ranges to precise values. Therefore, we can state that our assumption about COSBET-MAC requiring the availability of suitable propagation models does not limit practicality. Details about radio propagation modelling remain out of the scope of this thesis.

Given this overview of COSBET-MAC, a detailed description of its operation is provided in the next subsections.

3.3.1 Channel selection phase

In the initial phase (i.e., selection phase), the transmitter starts delivering an RTS frame to the intended receiver. This frame includes, among other usual fields (e.g., source and destination MAC addresses), a list of channels that are not already reserved by any of its neighbours, such as in the work of Jia and Zhang [2009], as well as the payload size of the data frame waiting to be transmitted. Since transmitter-receiver pairs must handshake through the CCC prior data transmission in order to select the targeted channel, a SU can keep record of which channels are being reserved in its neighbourhood by simply overhearing control traffic. That is, knowledge can be acquired through passive learning provided that the control frames include appropriate information (see Section 2.5.3).

The neighbours of the transmitter that overhear the RTS frame set the CCC as being reserved for a defined amount of time, which corresponds to the time that is expected to elapse before issuing the corresponding fCTSS (forwarded Clear to Sense) frame plus a safety margin.

This kind of reservation scheme, which is based on overheard control frames, is a common practice in the field of wireless communications. IEEE 8021.11 standard [O'hara and Petrick, 2005] and the work of Jia and Zhang [2009] are two such examples. We do not consider the time that is necessary to conclude handshake entirely in order to account for the possibility of an RTS frame not being correctly received by the receiver and, consequently, to avoid neighbouring SUs from being denied access to the CCC for an excessively large and unnecessary period.

If the intended destination of an RTS frame receives it while being in idle state (i.e., while not using its reconfigurable radio), it selects a channel that is not reserved at both ends, based on some predefined selection strategy (see step 2 in Algorithm 3.1), and replies with a CTSS (Clear to Sense) frame. This frame includes the selected channel and a reservation time for the CCC, which accounts for the time necessary to conclude handshake plus a safety margin. In order to avoid the hidden SU problem in multi-hop networks, the transmitter forwards the information provided by the CTSS frame through a corresponding fCTSS (forwarded CTSS) frame.

The SUs in the neighbourhood of the transmitter-receiver pair overhear the CTSS and/or fCTSS frames, and set the CCC as being busy for the specified amount of time. If, upon the reception of an RTS frame, the receiver and the transmitter have no common data channels set as unreserved, the receiver replies with a CTSS packet with no channel selected. In this case, CCC reservation time is set to the time that is expected to elapse before the related fCTSS frame is issued, i.e., before handshake concludes prematurely. Then, the transmitter forwards the CTSS frame through as an fCTSS frame, with CCC reservation time set to zero, and enters a random back-off period before initiating another attempt. When the number of handshake attempts exceeds a defined threshold, the data frame in the front of the output MAC queue is eliminated.

3.3.2 Cooperative sensing phase

After an fCTSS frame is issued with a valid channel selection, the transmitter and the receiver switch their reconfigurable radios to the selected channel and start sensing it. Since the longer is sensing time the higher is accuracy and also the resulting overhead, a trade-off must usually be made [Cormio and Chowdhury, 2009]. Moreover, idle neighbours of the transmitter-receiver pair that do not consider the selected channel as being already reserved get also involved in sensing (see Algorithm 3.2). That is, they also switch their reconfigurable radios to the selected channel and sense it, such as the transmitter and the receiver do. This cooperative sensing approach aims at increasing efficiency in terms of the detection of any activity on the selected channel, namely by addressing the hidden PU and hidden SU problems. COSBET-MAC assumes the use of energy detection at the PHY layer, which makes distinction between PU and SU activities unfeasible (see Section 2.5.2). Therefore, vacancy decision is made in terms of both primary and secondary traffic.

```
Inputs: $c$, a channel selected in an overheard CTSS or fCTSS frame;
        $s$, the source of the overheard control frame.

if status = idle and not using $c$ and $c$ not already reserved by neighbours then
    switch reconfigurable radio to $c$
    sense $c$
    if activity sensed on $c$ then
        notify $s$ through a CTS frame
    end if
else if using $c$ or $c$ already reserved by neighbours then
        notify $s$ through a CTS frame
end if
```

Algorithm 3.2. Cooperation of a neighbour during a sensing phase

The neighbours that cooperate in sensing must stop sensing the selected channel before the transmitter and the receiver do (see Figure 3.1). The reason is as follows. If after performing sensing, a neighbour concludes that the targeted channel is not vacant, it must inform the transmitter or the receiver before they enter the decision phase. This operation is accomplished through the transmission of a CTS (Clear To Send) frame with the selected channel set as unavailable. A transmitter or a receiver that does not receive any control frame or does not detect any activity on the CCC while sensing the selected channel concludes that there are no neighbours considering the targeted channel as being busy or already reserved by another transmitter-receiver pair. That is, COSBET-MAC follows a so-called negative feedback strategy concerning the cooperation of neighbours.

A neighbour that wants to prevent access to the channel under investigation issues a CTS frame directly, i.e., without any contention scheme, in order to speedup notification and make the required time deterministic. Furthermore, a neighbour that detects any activity on the CCC, while sensing the data channel, desists from issuing a CTS frame since it assumes that another SU has already taken a similar initiative. This approach might result in collisions if two or more cooperating neighbours perform negative feedback simultaneously. That is why any activity detected during the sensing phase on the CCC is also considered by the SUs as a negative feedback concerning the availability of the selected channel.

3.3.3 Further cooperation

Any neighbour, either it is idle or busy, which considers the selected channel as being already reserved by neighbours or by itself does not participate in sensing. However, it still issues a CTS frame with the selected channel set as unavailable during the cooperative sensing phase (see step 3 in Algorithm 3.1 and step 7 in Algorithm 3.2). That is, the cooperative sensing phase also includes a type of negative feedback that relates to the reservation status of the selected channel. Since a SU can operate simultaneously the CCC and a data channel, it keeps processing incoming control frames while sensing or accessing a data channel.

If a transmitter-receiver pair has a channel set as unreserved on both ends despite a neighbour is already accessing it, the most probable cause lies in any adverse propagation effect that prevented the control frames with the intended information to be properly overheard (see the control frames used in decision phase in Figure 3.1). It is also possible that a neighbour not accessing the channel announced in a CTSS or fCTSS frame has it set as being already reserved. Beyond the already mentioned adverse propagation effects, another reason for this occurrence is that, on the contrary of that neighbour, the transmitter-receiver pair is out of the transmission ranges of the SUs that have already gained access to the channel. That is, they are not one-hop neighbours and, thus, passive learning had no effect since the transmitter and the receiver were not able to decode the control frames announcing the reservation decision.

Nevertheless, interference on the commonly selected channel is still possible if two transmitter-receiver pairs, which are not in the transmission ranges of each other, are in the interference ranges of each other. The interference range of a SU is the range within which the frames it transmits interfere with signals from legitimate sources so that they cannot be correctly received. On the contrary, transmission and sensing ranges are the ranges within which the transmitted frames can, respectively, be received correctly and sensed with high probability. Passive learning is limited to the transmission range. It is usually assumed that transmission range is lower than or equal to interference range, which in in turn is lower than or equal to sensing range [Anastasi et al., 2003]. For instance, Anastasi et al. [2003] give an example of a simulation tool that models the characteristics of the PHY layer with 250 meters transmission range and 550 meters interference and sensing ranges.

Most existing MAC protocols do not cope with the difference between transmission and interference ranges, which results in hidden node problems (i.e., nodes that are close enough to raise interference issues but too far to allow passive learning). Even mechanisms that aim at handling the hidden node problem, such as “Request To Send/Clear To Send” handshake in IEEE

802.11 [O'hara and Petrick, 2005], cannot totally prevent this issue [Jia and Zhang, 2009]. With COSBET-MAC, negative feedback from neighbours due to already reserved channels enables addressing the issue that results from the difference between transmission and interference ranges. That is, it allows two distinct transmitter-receiver pairs to access the same channel simultaneously only is they are at least three hops apart. For example, in Figure 3.2, there is no two transmitter-receiver pairs allowed to access to same channel simultaneously with COSBET-MAC. However, if we modify this scenario such that SU_4-SU_{10} and SU_3-SU_9 form two pairs, then, COSBET-MAC allows SU_4-SU_{10} and SU_1-SU_2 to utilize the same channel simultaneously.

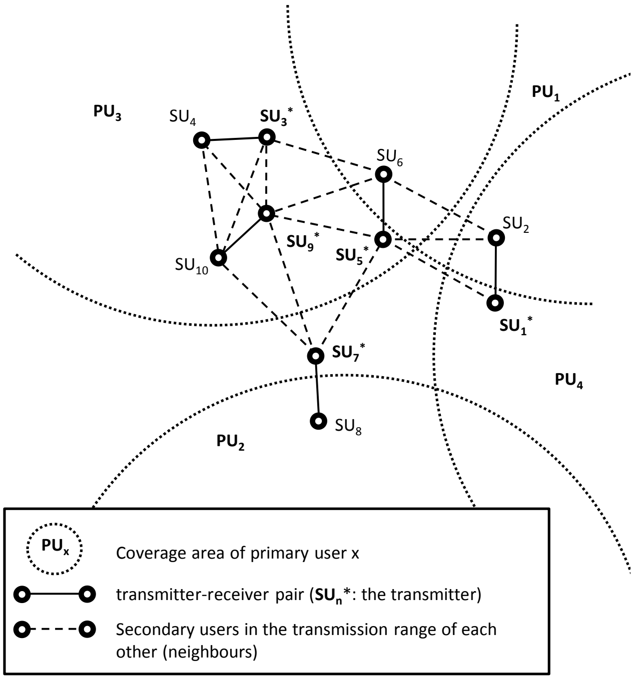


Figure 3.2. A scenario with hidden primary users and hidden secondary users

Since sensing range is assumed to be equal to or greater than interference range [Anastasi et al., 2003], and COSBET-MAC handshake includes a sensing phase, any activity from a non-neighbouring SU that is already using the selected channel and that raises the issue related to the difference between transmission and interference ranges is likely to be detected. In this case, the channel ends up not being accessed. Therefore, with COSBET-MAC, the interference issue under discussion only occurs when all the competing transmitter-receiver pairs perform sensing simultaneously, i.e., when there is no pair transmitting while the others perform sensing, which is expected to occur with low probability with random-based access MAC solutions.

It results from the above discussion that the probability of two transmitters harmfully interfering with each other (i.e., with data frames being lost) is likely to be very low or negligible. If we assume this probability as being acceptable, then, step 3 of Algorithm 3.1 and expression "*c* already reserved by neighbours" in step 7 of Algorithm 3.2 can be ignored. This variation of COSBET-MAC increases the spatial reuse of the spectrum at the expense of a possibly higher level of interference between two-hop neighbours. That is, two-hop neighbours are allowed to use the same channel simultaneously, which can positively impact performance in multi-hop scenarios with less available channels than transmitters. Network density (e.g., high SU density vs. low SU density) and data traffic pattern (e.g., larger data frames vs. smaller data frames) strongly influence the relative benefits and disadvantages that result from the suggested alternative. This issue is evaluated in Section 3.4.

3.3.4 Decision phase

The third phase in Figure 3.1 starts with the receiver sending to the transmitter a CTS frame with its decision about the status of the selected channel, which takes into account its own sensing outcome and any negative feedback from neighbours. COSBET-MAC adheres to the OR-rule (see Section 2.5.2) concerning the fusion of the multiple sources of information it uses during cooperative sensing phases (i.e., local sensing outcomes and beliefs about channel reservations in progress at the transmitter, receiver, and one-hop neighbours). Such as with any other control frame, a CTS frame is overheard by neighbours and processed accordingly. It also includes an updated CCC reservation time. Then, upon the reception of a CTS frame, the transmitter determines the final decision about the availability of the selected channel. For this purpose, it uses the conclusion reported by the receiver and its own decision, which in turn is provided by local sensing and any negative feedback from neighbours.

Finally, the transmitter replies with an fCTS frame that carries the final decision and also includes a field for data channel reservation time. If the selected channel is considered available, the transmitter simultaneously starts sending the data frame (see Figure 3.1). The channel reservation time field is set to a value that accounts for the time necessary to switch the reconfigurable radio from receive to transmit mode, and to complete the transmission of the data frame. Due to the possibility of the hidden SU problem, the receiver broadcasts this fCTS frame in turn, adjusting the data channel reservation time in order to account for the time that has already elapsed since data transmission started (see Figure 3.1). The reception or overhearing of an fCTS frame also dictates the conclusion of negotiation and, consequently, releases the CCC (i.e., fCTS frames include a zero seconds CCC reservation time).

The cooperative sensing approach of COSBET-MAC results in an implicit clustering scheme. In this case, clusters are defined by the transmission ranges of the transmitter-receiver pairs. Therefore, a cluster only includes the respective pair and its one-hop neighbours, which helps reducing the occurrence of false alarms when compared to approaches that apply data fusion based on the OR-rule to the entire network (see Section 2.5.2). Finally, COSBET-MAC is also compatible with sensing based on energy detection. That is, in terms of SU activity on a given channel, it tends to create silent periods in the neighbourhood of the transmitter-receiver pair during sensing periods.

3.4 Performance evaluation

This section is dedicated to the evaluation of COSBET-MAC. It starts specifying the global methodology we use to this end. A similar methodology is followed to evaluate the other solutions this thesis proposes in remaining chapters. Then, we specify the simulation settings. Finally, we present and discuss results that relate to distinct metrics, namely, achievable throughput and occurrence of missed PU detections. The work of Jia and Zhang [2009], IEEE 802.11, and a generic CR sense-before-transmit approach (i.e., without cooperation of neighbours) are used as comparison basis. These solutions are representative of distributed CR solutions that do not follow the sense-before-transmit approach, license-free single-channel access solutions, and distributed CR solutions that are based on the sense-before-transmit approach, respectively. We also evaluate the impact of the imperfect nature of sensing devices (see Section 2.5.2), which are characterized by false alarm and missed PU detection probabilities, and of the modification suggested in Section 3.3.3, which allows two-hop neighbouring COSBET-MAC pairs to access the same channels simultaneously.

3.4.1 Evaluation methodology

Most existing CR MAC proposals have been validated and evaluated through simulation. This common practice is especially due to time and other resource restrictions. For the same reasons, we also followed this approach, having chosen OMNET++/MiXiM [OMNeT++ Network Simulation Framework, 2010; MiXiM, 2010] as our simulation platform. OMNET++, which stands for Objective Modular Network Testbed in C++, is an open-source object-oriented modular discrete simulator. MiXiM, which stands for Mixed Simulator, is a simulation framework for wireless and mobile networks that was developed on top of OMNeT++. Among the reasons that motivated our selection, we highlight the well-organized and modular architecture of the framework, existing documentation, and the provided integrated development environment (IDE). Also, to the best of our knowledge, there was no support for CR in any existing open-source simulation framework at the starting point of the work described in this thesis.

We first developed a generic CR simulation framework for OMNET++/MiXiM. Most existing distributed CR MAC solutions, including COSBET-MAC, assume that the SUs are equipped with two or more radios (see Section 2.6.1). Usually, one of them is dedicated to operate a dedicated CCC that is used to exchange control frames. The other radios, which are dynamically reconfigurable (i.e., they are software defined radios), are used for data transmission. Therefore, our generic simulation framework assumes that the architecture of a SU follows the multi-radio model that is illustrated in Figure 3.3. With this model, the MAC entity of each radio implements a spectrum access protocol that defines how to achieve frame transmission and reception. Consequently, distinct radios can follow different access strategies.

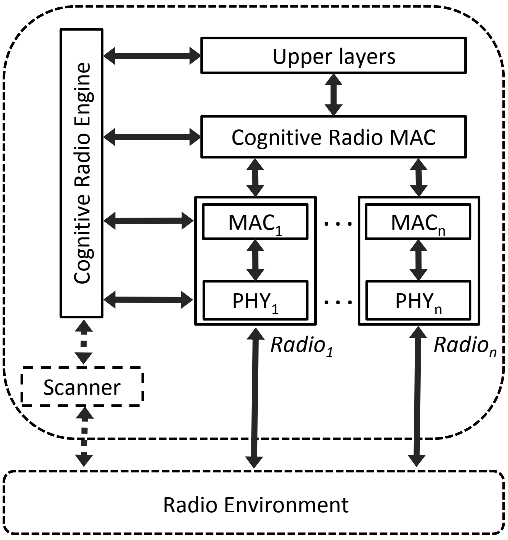


Figure 3.3. A secondary user architecture based on a multi-radio model

Concerning the CR MAC entity in Figure 3.3, it runs on top of the radios and supports the CR access strategy, being concerned with issues such as coordination and cooperation between SUs. The scanner component, which acts as a dedicated detector, is optional since sensing can also be performed by the reconfigurable radios. This is the case for most existing CR MAC proposals, including COSBET-MAC. For example, the scanner component can be used in CR solutions that require up-to-date information about spectrum availability, such as with the work of Jia and Zhang [2009]. Here, the scanner can be utilized to sense the channels continuously or periodically. The CR engine component is dedicated to learning and decision making (see Chapter 2).

Since schemes that consist in using multiple data channels simultaneously, such as channel bonding, are out of the scope of this thesis, our implementation of COSBET-MAC only uses two radios. One of them is dedicated to access the data channels (i.e., it is the reconfigurable radio) and the other to operate the CCC. Our COSBET-MAC implementation allows dynamically adjusting the transmission power and the operating frequency of the PHY components of the radios. Furthermore, COSBET-MAC assumes that the CCC is deployed over a fixed frequency band that is free of any PU activity. The CR engine component is dedicated to learning and decision making functions (e.g., it keeps record of channels being reserved in its one-hop neighbourhood based on the control frames it overhears on the CCC). The optional scanner component in Figure 3.3, which is dedicated to sensing, is not utilized since sensing is performed by the radio dedicated do data transmission on each SU. Therefore, our implementation of COSBET-MAC consists in all the modules in Figure 3.3, except the so-called scanner.

3.4.2 Simulation settings

Table 3.1 lists the global settings that are used to evaluate COSBET-MAC. Other parameters and variations, specifically related to some of the experiments that follow, are specified any time they apply. The presented results are averaged over 15 runs of 300 seconds simulated time and with different seeds. As already mentioned, in the developed simulation model, transmission power and, consequently, the resulting transmission range of data radios can be dynamically adjusted. In our experiments, we use the default simple path loss model of MiXiM [MiXiM, 2010] and transmission power is set such that transmission range results in 100 meters for all the radios, independently of the operating frequencies in use. This transmission range value is frequently assumed for wireless nodes in the literature (e.g., see the works of Jing et al. [2012], Ahmed et al. [2013], Tung et al. [2013], and Sam and Raj [2014]).

On the receiver's side, we implement a uniform random channel selection scheme for choosing the next channel to be sensed (see function *f(x)* in step 2 of Algorithm 3.1). We use the work of Jia and Zhang [2009], a generic sense-before-transmit approach, and IEEE 802.11 as comparison basis for determining the gains COSBET-MAC provides in terms of communication performance, when compared to other CR and single-channel access schemes. Therefore, maximum limit for the number of RTS tries is set to seven on COSBET-MAC, which corresponds to the value we use for IEEE 802.11 short retry count, in order to make fair comparisons. For the same reason, IEEE 802.11 long try count is set to one (the default value is four) since our implementation of COSBET-MAC does not contemplate the retransmission of data frames. The same remarks apply to the implementation of the work of Jia and Zhang [2009], and to the implementation of the generic sense-before-transmit approach we also use as comparison basis.

The SUs are allowed to dynamically contend for and access four distinct channels on a non-interference basis. Every channel is licensed to a single PU with activities characterized by alternating idle and busy periods that are exponentially distributed with parameters λ_i and λ_b, respectively. According to Akyildiz et al. [2009], this is a common practice. We use idle and busy periods with means $1/\lambda_i = 0.1$ seconds and $1/\lambda_b = 0.01$ seconds, respectively, such as in the work of Issariyakul et al. [2009].

Table 3.1: Simulation settings

Parameter	Value	Remark
Simulation scenarios	50m x 50m area Scenario in Figure 3.2 200m x 200m area	All the SUs are in the transmission range of each other with the 50m x 50m scenario
Number of SUs (50 m x 50 m area)	12	
Number of SUs (200 m x 200 m area)	32	
Positioning of the SUs (50 m x 50 m area)	Uniform random	
Positioning of the SUs (200 m x 200 m area)	Uniform random	
Transmission range	100 m	
Simulation time	300 s	
Runs	15	
Number of channels	4	
Bit rate on data channels and CCC	2 Mbit/s	
Maximum transfer unit	18432 bits	Similar to IEEE 802.11.
Channel selection (*f*(x) in Algorithm 3.1)	Uniform random	
Mean data frame payload size	16 Kbit	
RTS retry limit per data frame	7	Same value as default IEEE 802.11 short retry count.
Channel switching time	10^{-4} s	Such as in the work of Jia and Zhang [2009].
Sensing time (10^{-3} s)	0.5 or 1.0	Fast sensing recommended to be under one millisecond [IEEE 802.22 Working Group on Wireless Regional Area Networks, 2013].
Transmit to receive time and receive to transmit time radio switch	10^{-6} s	Short Inter-frame Space (SIFS) value for the main IEEE 802.11 versions currently in use.
IEEE 802.11 long try count	1	Default value is 4.
IEEE 802.11 RTS-threshold	400 bits	
MAC queue size	50 frames	

We use three different simulation scenarios (see Table 3.1). The first one, which consists in a square area with side length 50 meters, is used to evaluate communication performance in

Section 3.4.3 and Section 3.4.5, and includes up to 12 SUs randomly placed with a uniform distribution. In this case, all the SUs are in the transmission range of each other, which is the most adverse scenario in terms of contention for the network resources (i.e., CCC and data channels). With the purpose of evaluating the protection of PUs (see Section 3.4.4), we use the scenario illustrated in Figure 3.2 since it includes hidden PUs, which enables evaluating the gains delivered by the cooperative sense-before-transmit feature that COSBET-MAC includes. Section 3.4.6, which evaluates the COSBET-MAC variation discussed in Section 3.3.3 and that aims at increasing spatial spectrum reuse, utilizes a square simulation scenario with side length 200 meters and 32 SUs randomly positioned with a uniform distribution. In this scenario, each of the 16 transmitter-receiver pairs is formed such that the distance between both ends never exceeds 100 meters (i.e., the defined transmission range).

Concerning data traffic generated by the SUs, mean load per transmitter varies up to 3 Mbit/s per transmitter, data frame payload size is 16 Kbit, and time between arrivals is exponentially distributed with the parameter adjusted according to the targeted mean load. Since sensing time dictates the accuracy of local sensing (see Section 2.5.2), some experiments are repeated with 0.5 and 1.0 milliseconds sensing times in order to highlight its impact on performance. These values were chosen based on the fact that the 802.22 Working Group [IEEE 802.22 Working Group on Wireless Regional Area Networks, 2013] specifies that fast sensing should be under 1 millisecond per channel. Finally, we assume perfect sensing, except in Section 3.4.5 that is dedicated to analyse the impact of missed detections and false alarms that are inherent to the imperfect nature of sensing devices.

3.4.3 Communication performance

The performance of COSBET-MAC is first evaluated in terms of the throughput it achieves. IEEE 802.11, a distributed CR sense-before-transmit approach, i.e., without cooperation of neighbours, and the solution of Jia and Zhang [2009] are used as comparison basis. The former is the most commonly used random-based single-channel access MAC protocol. The latter is representative of random-based distributed CR MAC solutions that do not include sensing in negotiation. That is, it simplistically assumes the availability of an underlying mechanism (e.g., periodic sensing) that enables a SU to know which channels are free of any activity at negotiation time. Consequently, COSBET-MAC is expected to have lower performance than the solution of Jia and Zhang [2009].

On the other hand, COSBET-MAC does not make the type of simplistic assumption mentioned above. It follows a practical cooperative sense-before-transmit approach that aims at determining if a selected channel is vacant immediately before accessing it. That is, performance penalty when compared to the solution of Jia and Zhang [2009] is a direct consequence of higher PU protection, which is a mandatory concern in CR. In fact, there is usually a trade-off between SU performance and PU protection in CR. Therefore, comparison with the solution of Jia and Zhang [2009] aims at evaluating the overhead that results from including cooperative sensing as we propose in the negotiation phase of COSBET-MAC for higher PU protection. The implementations of the solution of Jia and Zhang [2009] and of the (non-cooperative) sense-before-transmit approach also use the settings specified in Table 3.1.

Figure 3.4, Figure 3.5, and Figure 3.6 illustrate the obtained results in terms of aggregate throughput, regarding the scenario that consists in a square area with side length 50 meters, with 2, 4, and 6 transmitter-receiver pairs, respectively, and using the settings previously specified. In the last case (see Figure 3.6), there are more transmitter-receiver pairs than exiting channels, which results in additional contention between the SUs. A comparison is also established with IEEE 802.11, the solution of Jia and Zhang [2009], and the generic sense-before-transmit approach. Since there are occasionally less channels effectively vacant than transmitters willing to transmit, even when the number of transmitters in the scenario is not higher than the number of existing channels, due to PU activity, blocking probability always exists. In order to ease readability, the standard deviation of aggregate throughput between the runs is not provided as error bars on data points, but instead as values in Table 3.2, Table 3.3, and Table 3.4 for scenarios with 2, 4, and 6 transmitter-receiver pairs, respectively.

From the obtained results, we conclude that COSBET-MAC brings relevant performance benefits in terms of throughput when compared to IEEE 802.11, despite higher control overhead. In comparison with the results obtained with the solution of Jia and Zhang [2009], COSBET-MAC has lower communication performance. Nevertheless and as already discussed, this expected poorest performance results from the fact that COSBET-MAC effectively determines the status of channels. That is, it does not let this issue open, on the contrary of the work of Jia and Zhang [2009] that simplistically assumes that the required information is already known at selection time. Concerning comparison with the sense-before-transmit approach, no significant performance degradation is observed. This mainly results from the fact that only idle neighbours participate in sensing, only a single pair can negotiate over the CCC at any time, and the scenario in use does not suffer from the hidden PU and hidden SU problems (Section 3.4.4 takes into consideration a scenario with hidden PUs and hidden SUs).

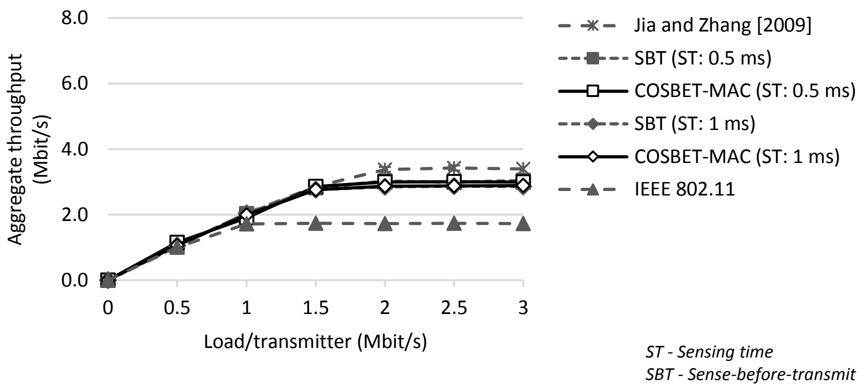


Figure 3.4. Aggregate throughput (scenario with 2 transmitter-receiver pairs)

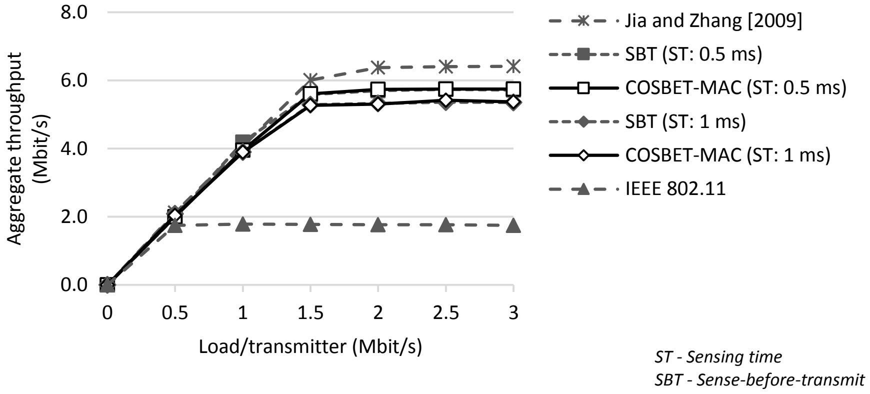


Figure 3.5. Aggregate throughput (scenario with 4 transmitter-receiver pairs)

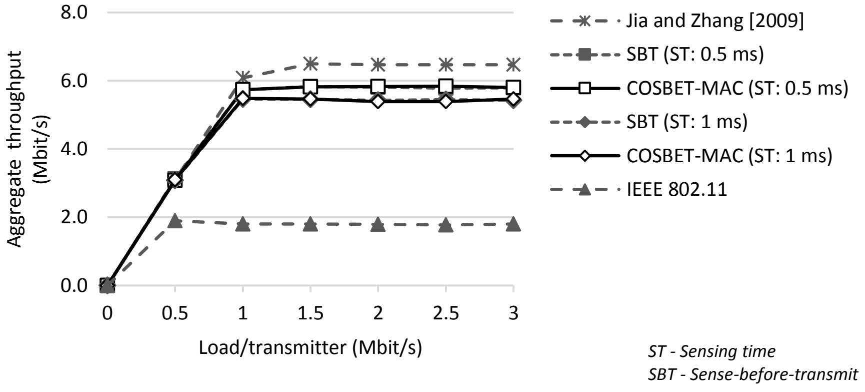


Figure 3.6. Aggregate throughput (scenario with 6 transmitter-receiver pairs)

In order to further characterize the impact of sensing time, data frame payload size, and PU traffic characteristics on COSBET-MAC performance, we focus on 2 Mbit/s load per transmitter, i.e., beyond saturation point, and make those parameters vary individually. We also use 0.5

milliseconds sensing time, except when specifically evaluating the impact of this parameter. Results are presented in Figure 3.7, Table 3.5, and Figure 3.8. The error bars show the standard deviation of aggregate throughput between the different runs.

Table 3.2: Standard deviation of aggregate throughput in kbit/s (data points in Figure 3.4)

Solution	Load/Transmitter (Mbit/s)					
	0.5	1	1.5	2	2.5	3
COSBET-MAC (ST[1]: 0.5 ms)	85.5	125.7	102.6	27.6	9.8	56.7
COSBET-MAC (ST: 1 ms)	79.6	103.5	32.7	37.3	7.7	17.7
SBT[2] (ST: 0.5 ms)	66.4	87.9	87.8	33.4	44.4	34.6
SBT (ST: 1 ms)	68.3	72.3	29.4	23.2	30.3	16.1
Jia and Zhang [2009]	115.2	131.7	168.5	77.7	74.4	77.2
IEEE 802.11	91.5	33.7	18.3	13.9	12.9	22.3

[1] Sensing time.
[2] Sense-before-transmit.

Table 3.3: Standard deviation of aggregate throughput in kbit/s (data points in Figure 3.5)

Solution	Load/Transmitter (Mbit/s)					
	0.5	1	1.5	2	2.5	3
COSBET-MAC (ST[1]: 0.5 ms)	169.6	248.6	64.5	59.5	15.4	35.3
COSBET-MAC (ST: 1 ms)	89.8	102.6	75.3	63.1	84.7	82.8
SBT[2] (ST: 0.5 ms)	96.4	80.5	108.5	52.1	7.8	16.5
SBT (ST: 1 ms)	68.1	143.9	47.5	32.2	23.9	36.7
Jia and Zhang [2009]	116.5	123.9	224.1	34.4	7.9	7.1
IEEE 802.11	67.5	13.7	19.8	29.8	12.7	26.8

[1] Sensing time.

[2] Sense-before-transmit.

Table 3.4: Standard deviation of aggregate throughput in kbit/s (data points in Figure 3.6)

Solution	Load/Transmitter (Mbit/s)					
	0.5	1	1.5	2	2.5	3
COSBET-MAC (ST[1]: 0.5 ms)	174.2	83.3	9.6	10.9	60.2	49.8
COSBET-MAC (ST: 1 ms)	255.8	38.2	72.8	47.1	26.3	74.5
SBT[2] (ST: 0.5 ms)	157.4	127.5	35.8	48.5	27.6	42.8
SBT (ST: 1 ms)	114.2	61.1	95.8	54.8	42.2	56.2
Jia and Zhang [2009]	209.3	150.7	84.8	15.5	26.8	18.1
IEEE 802.11	82.2	39.2	31.1	25.6	20.1	23.4

[1] Sensing time.
[2] Sense-before-transmit.

Time spent in sensing operations is one of the components of each COSBET-MAC access cycle (see Figure 3.1) and, therefore, it has a strong impact on the performance of COSBET-MAC. Figure 3.7 illustrates it presenting results obtained with sensing time varying from 0.5 to 2.5 milliseconds, with data frame payload size set to 1, 4, and 16 Kbit, and with 4 transmitter-receiver pairs. Since the sensing component of a handshake cycle is fixed, the throughput of SUs is expected to decrease linearly with increasing sensing time, which is essentially observed in Figure 3.7. Therefore, the availability of solutions that enable, at the PHY layer, fast and highly accurate sensing operations is a key issue for the performance of COSBET-MAC and of any other opportunistic CR MAC solution.

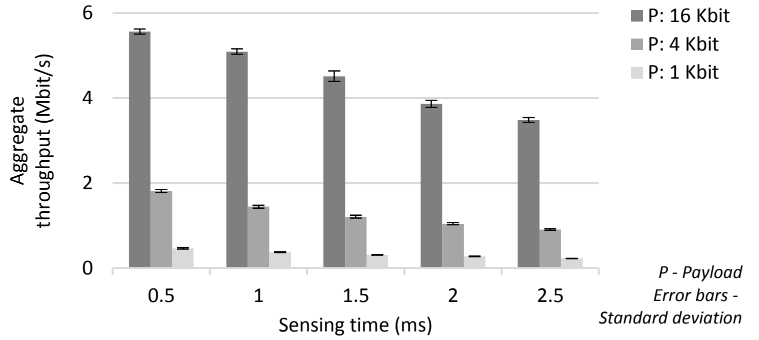


Figure 3.7. Aggregate throughput with variable sensing time and variable data frame payload size (2 Mbit/s load per transmitter and 4 transmitter-receiver pairs)

The experiments we described so far use a 16 Kbit data frame payload size (see Table 3.1). However, since COSBET-MAC performs negotiation on a data frame basis, control overhead proportion varies inversely with data frame payload size and, consequently, with channel access time. Similarly, contention on the dedicated CCC increases as payload size decreases since, for a given load per transmitter, the SUs try to gain access to the CCC more frequently. That is, for a particular scenario, the smaller are the data frames the sooner throughput saturation occurs and the smaller is the maximum performance that can be achieved. Results in Figure 3.7 also illustrate the effects of this issue, which are far from being negligible, independently of the sensing time in use.

Table 3.5 presents the maximum number of channels simultaneously accessed at any time in the simulation scenario when sensing time varies from 0.5 to 2.5 milliseconds and data frame payload size is 1, 4, and 16 Kbit. We observe that channel utilization efficiency increases with payload size, i.e., with increasing data channel access time. Sensing time, which directly influences COSBET-MAC handshake time, also has a great impact on how efficiently the existing channels are used. In fact, COSBET-MAC can degenerate to single-channel access under certain conditions. Chapter 5 is dedicated to further discuss the impact of data frame payload size and sensing time on the communication performance of SUs, which results directly from the fact that

COSBET-MAC performs handshake over a dedicated CCC on a data frame basis. It also proposes a novel solution that successfully addresses it.

Table 3.5: Maximum number of channels simultaneously used (4 channels, 4 transmitter-receiver pairs, and 2 Mbit/s load per transmitter)

Data frame payload size (Kbit)	Sensing time (ms)				
	0.5	1.0	1.5	2.0	2.5
1	1	1	1	1	1
4	2	1	1	1	1
16	4	4	3	3	3

To obtain the results presented in Figure 3.8, we still consider four channels with PU activities characterized by alternating idle and busy periods exponentially distributed. However, in this case, the sum of the respective means equals 0.1 seconds (i.e., $1/\lambda_i + 1/\lambda_b = 0.1$). Simulation runs are repeated with busy time varying from 0% (i.e., the channels are always vacant) to 80% and the number of transmitter-receiver pairs varying from two to six. As expected, performance decreases regularly with increasing PU busy time since the average number of channels that are effectively vacant at selection time also decreases linearly. We can define the effective average number of channels in a CR scenario as

$$nc = \sum_{i=1}^{n}(1 - b_i)\ , \tag{3.1}$$

being n the total number of channels and b_i the probability of channel i being busy in terms of PU activity. Excessive PU activity can, thus, make a CR scenario degenerate to a scenario with less than a single channel effectively available on the average, i.e., with lower performance than a license-free single-channel access approach (e.g., IEEE 802.11). This is what happens with 80% PU busy time in Figure 3.8 (compare with better results obtained with IEEE 802.11 in Figure 3.4, Figure 3.5, and Figure 3.6).

3.4.4 Protection of primary users

Figure 3.9 and Figure 3.10 illustrate the impact on PU protection and throughput that results directly from the cooperation of idle neighbours in sensing, as defined by COSBET-MAC, varying average load per transmitter from 250 kbit/s to 2 Mbit/s. The metric we use for evaluating PU protection consists in the rate of observed missed PU detections, i.e., PU activities that a transmitter-receiver pair cannot sense despite interfering with them (see Figure 3.2). Comparison is established with the obtained aggregate throughput and the rate of missed PU detections that occur when the cooperation of idle neighbours in sensing is inhibited. That is, when a transmitter-receiver pair only uses local sensing outputs such as with the commonly used sense-before-transmit approach (see Chapter 2). With COSBET-MAC, the probability of a SU being idle is lower for higher loads and, consequently, also is the probability that it cooperates in sensing on behalf of a neighbouring transmitter-receiver pair. The error bars in Figure 3.9 and Figure 3.10 show the standard deviation between the runs.

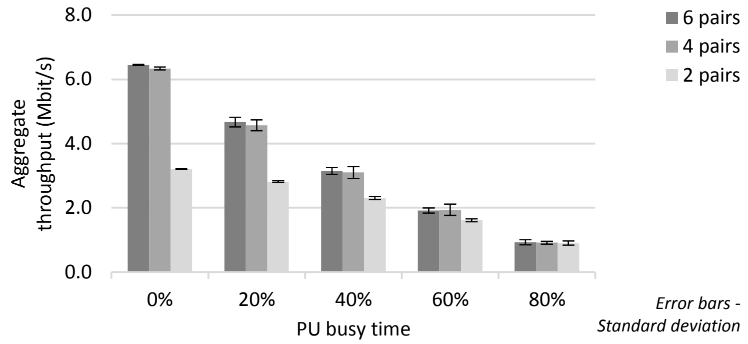


Figure 3.8. Aggregate throughput vs. primary user traffic characteristics (2 Mbit/s load per transmitter and 0.5 milliseconds sensing time)

Figure 3.9 and Figure 3.10 respectively relate to two distinct scenarios, i.e., the scenario that is illustrated in Figure 3.2 and a variation of the same scenario with 50 additional idle neighbours (i.e., that never have data to transmit or receive) randomly positioned with a uniform distribution. The scenario in Figure 3.2 aims at being representative of multi-hop distributed CR scenarios that experience the hidden PU problem. Each one of the four PUs accesses a predefined channel and the SUs only have access to this set of four channels. That is, there are four potential non-overlapped channels for five transmitter-receiver pairs. Sensing time is 0.5 milliseconds. PU traffic on the four channels is characterized by idle and busy periods with means equal to 0.05 seconds, and the other settings are the same as specified in Section 3.4.2.

From the obtained results, we can conclude that the proposed cooperative sensing solution effectively contributes to increase the protection of PUs in distributed CR scenarios. The performance penalty that is due to the involvement of idle neighbours in sensing (see negative throughput variation in Figure 3.9 and Figure 3.10) essentially results from the fact that there are less illegitimate (i.e., false) opportunities utilized by the SUs. Therefore, it is acceptable and unavoidable since the protection of PUs is a primary concern in CR environments. As depicted in Figure 3.9 and Figure 3.10, the gains that result from cooperation in terms of PU protection depend on the level of availability of the SUs for cooperating in sensing on behalf of neighbouring transmitter-receiver pairs (i.e., it decreases with increasing load per transmitter). Comparing results in Figure 3.10 with results in Figure 3.9 for similar loads, we also observe that the higher is the achieved protection of PUs the lower is the obtained throughput. The reason is that illegitimate accesses due to missed PU detection are more effectively avoided.

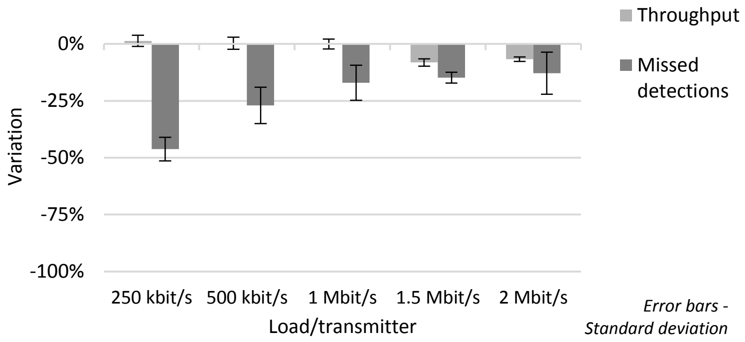


Figure 3.9. Variation in the rate of missed PU detections and aggregate throughput due to the cooperation of idle neighbours in sensing (scenario in Figure 3.2)

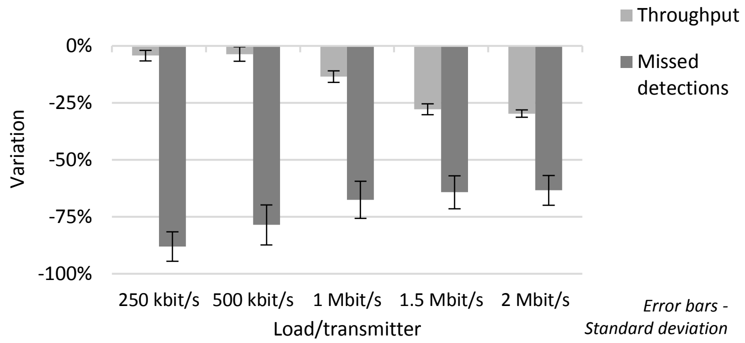


Figure 3.10. Variation in the rate of missed PU detections and aggregate throughput due to the cooperation of idle neighbours in sensing (scenario in Figure 3.2 with 50 additional idle neighbours)

3.4.5 Impact of sensing imperfections

Sensing is the primary functionality that is required in CR scenarios (see Section 2.5). The other main CR operations, such as detection of PUs, traffic modelling, traffic prediction, and spectrum decision rely on it. Sensing devices are not perfect, i.e., they inherently suffer from missed detections and false alarms. Missed detections result in more interferences to PUs. On the contrary, false alarms inadequately deny access to spectrum opportunities, which affects the performance of SUs. Thus, for the sake of realism, we evaluate the effect of sensing imperfection on COSBET-MAC in terms of both communication performance and protection of PUs. We also note that IEEE 802.22 [IEEE 802.22 Working Group on Wireless Regional Area Networks, 2013] requires, concerning the detection of television signals, missed detection and false alarm probabilities to be at most 10%.

COSBET-MAC follows the OR-rule for fusing sensing outputs (see Section 3.3). Therefore, if we assume that n neighbours cooperate in sensing on behalf of a transmitter-receiver pair and that false predictions and false alarms that affect distinct SUs are independent events, then, the probability of false alarm concerning final decision (see decision phase in Figure 3.1) can be defined as

$$p_f = 1 - \prod_{i=1}^{n+2}(1 - f_i) , \tag{3.2}$$

with f_i being the probability of false alarm of SU with index i. The value $n+2$ accounts for the participation of the transmitter-receiver pair in sensing. Similarly, the probability of missed detection can be defined as

$$p_m = \prod_{i=1}^{n+2} m_i , \tag{3.3}$$

being m_i the probability of false alarm of SU with index i.

Figure 3.11 and Figure 3.12 depict, based on Equation (3.2) and Equation (3.3), the expected false alarm and missed detection probabilities concerning final decision in COSBET-MAC against the number of idle neighbours that participate in sensing. These results are obtained assuming that all the SUs have similar missed detection and false alarm probabilities, and varying the respective probabilities from 5% to 15%. The occurrence of final decisions that result in missed detections is very low (i.e., imperceptible in Figure 3.12) when at least three idle neighbours cooperate in sensing. Concerning the quantity of final decisions that result in false alarms, it increases with the number of cooperating neighbours.

We repeat the experiments that resulted in Figure 3.5 (see Section 3.4.3) for COSBET-MAC and for the (non-cooperative) sense-before-transmit approach (i.e., with the cooperation of neighbours inhibited), assuming 0.5 milliseconds sensing time, 0%, 5%, and 10% missed detection probabilities, and 0%, 5%, and 10% false alarm probabilities for all the SUs. Since the simulation scenario we consider (i.e., the square area with side length 50 meters) does not include hidden PUs, the imperfection of sensing devices is the cause of all the resulting missed detections and false alarms. Figure 3.13 illustrates the obtained results regarding aggregate throughput. In order to ease readability, the respective standard deviation across the different runs is provided in Table 3.6.

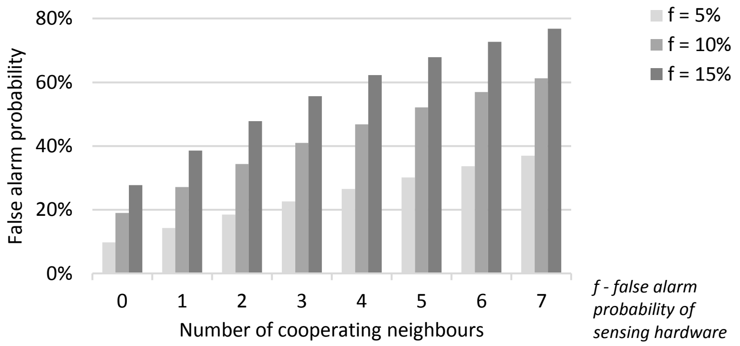


Figure 3.11. Probability of false alarm with COSBET-MAC

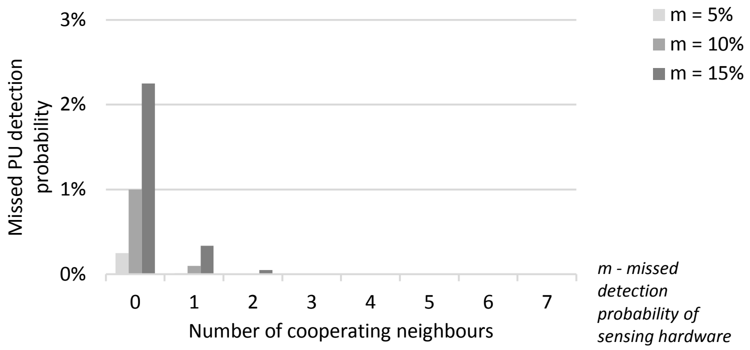


Figure 3.12. Probability of missed PU detection with COSBET-MAC

Due to the occurrence of false alarms on final access decisions, there is an expected decrease in performance since the SUs miss opportunities. With sensing hardware having any false alarm probability, degradation is higher for COSBET-MAC due to the cooperation of idle neighbours, which contributes to increase false alarms regarding final decisions. Nevertheless and as already mentioned, this apparent disadvantage of COSBET-MAC is tolerable since there is a simultaneous higher protection of PUs, which is a primary concern in CR (see Section 3.4.4). CR usually requires a trade-off between the performance of SUs and the protection of PUs.

3.4.6 Simultaneous channel access by two-hop neighbours

This section evaluates the effect that results on the communication performance of COSBET-MAC when step 3 of Algorithm 3.1 and expression "*c* already reserved by neighbours" in step 7 of Algorithm 3.2 are ignored (see related discussion in Section 3.3.3). That is, two-hop neighbours become allowed to use the same channel simultaneously, which potentially increases the spatial reuse of the spectrum. Therefore, this modified COSBET-MAC version can positively impact performance in multi-hop scenarios, especially when there are less spectrum opportunities than transmitters.

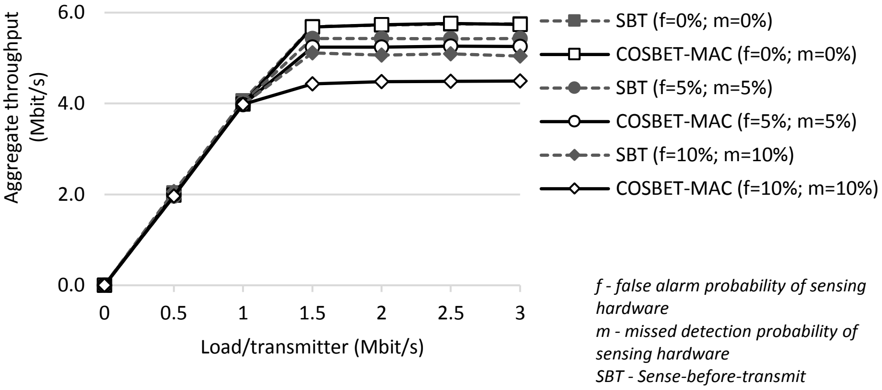


Figure 3.13. Aggregate throughput with different missed detection and false alarm probabilities

Table 3.6: Standard deviation of aggregate throughput in kbit/s with different missed detection and false alarm probabilities

Solution	Load/Transmitter (Mbit/s)					
	0.5	1	1.5	2	2.5	3
COSBET-MAC (f[1]=0%; m[2]=0%)	58.9	69.2	48.5	15.4	37.6	14.9
COSBET-MAC (f=5%; m=5%)	42.4	59.9	30.8	56.5	62.3	63.9
COSBET-MAC (f=10%; m=10%)	48.9	62.8	63.9	64.9	26.2	18.8
SBT[3] (f=0%; m=0%)	33.7	34.4	38.2	16.0	19.6	17.1
SBT (f=5%; m=5%)	40.9	63.1	37.9	30.4	21.9	15.9
SBT (f=10%; m=10%)	58.5	65.3	39.8	73.1	41.5	27.7

[1] False alarm probability of sensing hardware.
[2] Missed detection probability of sensing hardware.
[3] Sense-before-transmit

The simulation scenario consists in a square area with side length 200 meters, 32 SUs randomly placed with a uniform distribution, and 16 transmitter-receiver pairs formed such that the distance between both ends never exceeds 100 meters (see Table 3.1). It also considers a variable number of channels with the respective PUs having sensing ranges that cover all the SUs. The global settings are the same as defined in Section 3.4.2 and sensing time is 0.5 milliseconds. Figure 3.14 presents the results obtained with COSBET-MAC and its modified version regarding aggregate throughput. The error bars show the standard deviation between the different runs. We focus on 2 Mbit/s load per transmitter, i.e., beyond saturation point, and make the number of available channels vary from 2 to 6. Results show that the modified version of COSBET-MAC delivers higher throughput. That is, concurrent accesses to the spectrum result both from the combination of multiple accesses enabled by CR and enhanced spatial reuse of the spectrum due to the performed modification.

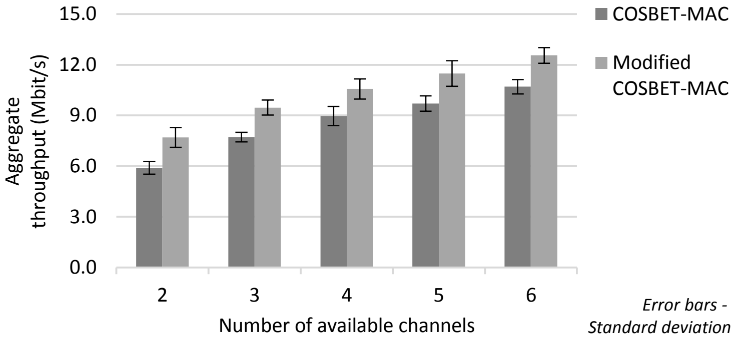


Figure 3.14. Aggregate throughput with 2 Mbit/s load per transmitter and 32 secondary users randomly placed with a uniform distribution

3.5 Summary

This chapter proposed and evaluated COSBET-MAC, a CR MAC protocol that specifically targets fully distributed CR networks that are exclusively based on autonomous SUs, local observation, and cooperation between one-hop neighbours, and which suffer from the hidden PU and hidden SU problems. The main concerns that drew its design were practicality, protection of PUs, effective increase of performance delivered to the SUs, and utilization of passive learning in order to keep control overhead as low as possible. COSBET-MAC includes a novel cooperative sense-before-transmit feature that increases the protection of PUs, based on a non-mandatory participation of idle neighbours.

The obtained evaluation results confirm that COSBET-MAC can result in relevant benefits, even when taking into account practical issues such as the imperfect nature of sensors. They also show that the communication performance COSBET-MAC delivers to the SUs is influenced by various operating parameters, such as sensing time, PU traffic characteristics, data frame payload size, and the imperfect nature of sensors that inherently have missed detection and false alarm probabilities. We also proposed an optional variation of COSBET-MAC that aims at increasing spectrum spatial reuse and, consequently, the performance of SUs.

COSBET-MAC can be further improved through additional features. For example, despite the scope of the contributions in this thesis is limited to layer-2 communication protocol issues, COSBET-MAC has great potential for supporting spectrum learning schemes, which is expected to occur in CR. That is, since control frames are overheard by one-hop neighbours, any SU can implicitly and dynamically collect statistics about the success of spectrum decisions made by its neighbours and about channel availability. Therefore, only a few additional fields must be added to existing control frames if needed and no further control frames are required. The next chapter proposes a solution that is based on such approach and that aims at enabling learning capabilities based on observation and past experience to be effectively utilized in multi-hop distributed CR scenarios with hidden PUs.

Results obtained in the current chapter show that data frame payload size has great impact on the communication performance of COSBET-MAC and, more generally, of any distributed CR solution that performs handshake over a dedicated CCC on a data frame basis. Therefore, Chapter 5 further analyses this issue and proposes a solution that successfully addresses it. Finally, Chapter 6 further improves the communication performance of COSBET-MAC through additional features that assist increasing the spatial reuse of the spectrum and minimizing control traffic.

Chapter 4

Filtering based on suspicious channels classification

In distributed CR scenarios, the SUs are expected to have learning capabilities based on observation and past experience. These features enable them to probabilistically (i.e., based on prediction) take proactive spectrum decisions, which might increase their communication performance and the protection of PUs (see Section 2.7). For instance, a channel is selected only if it is expected to be vacant until the end of the estimated access time. This chapter shows that, in fully distributed CR scenarios with hidden PUs, it is not trivial to make an effective utilization of prediction based on learning through observation and past experience. It also proposes a solution that addresses this issue.

The proposed solution is based on a key concept we named FIBASC (Filtering Based on Suspicious Channels) classification and was integrated with COSBET-MAC, the distributed CR MAC protocol described in Chapter 3. Nevertheless, the strategy the current chapter defines is not specifically designed for COSBET-MAC and can easily be integrated with any other distributed or centralized CR solution. Proposing any novel learning algorithm or evaluating any existing one remains out of the scope of this chapter. Simulation results show that FIBASC is effectively capable of delivering high levels of protection concerning the PUs, while retaining the communication performance of SUs at remarkable levels.

This chapter resulted in the following publication:

- Marinho, J. and Monteiro, E. (2012). Enhanced Protection of Hidden Primary Users through Filtering based on Suspect Channels Classification. 2012 IEEE *8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* (pp. 419-426). IEEE. doi: 10.1109/WiMOB.2012.6379107.

The remainder of this chapter is organized as follows. Section 4.1 presents and discusses the issue that motivated the solution presented in this chapter. Section 4.2 discusses related work and the contributions of this chapter. Section 4.3 describes FIBASC and its integration with COSBET-MAC. Section 4.4 evaluates FIBASC, through simulation, concerning the protection of PUs and its impact on the communication performance of SUs when combined with COSBET-MAC. Finally, Section 4.5 summarizes the discussion.

4.1 Introduction

In distributed CR scenarios, the SUs detect the spectrum holes through local sensing (see Chapter 2). Possible approaches include sensing a selected channel before accessing it (i.e., the so-called sense-before-transmit approach) or scanning the spectrum regularly in order to maintain an updated a list of spectrum opportunities. In order to increase sensing accuracy and, therefore, reduce the incidence of missed PU detections, which might occur due to the hidden PU problem, the imperfection of sensors, and other adverse propagation effects, cooperative sensing schemes are often considered. They basically consist in fusing the sensing outcomes of different SUs (see Section 2.5.2). COSBET-MAC, which is described and evaluated in Chapter 3, includes such feature. This CR MAC protocol effectively succeeds decreasing the rate of accesses that result in missed PU detections without excessively affecting communication performance (see performance evaluation in Section 3.4).

However, sensing is not sufficient to completely avoid harmful interferences to PUs since PU activities can appear on a channel sensed idle before access time. In this case, any ongoing secondary access results in PU interference, even if sensing is fully accurate. Therefore, the SUs are also expected to have learning capabilities that enable them to probabilistically determine busy and idle times on the targeted channels. In fully distributed CR scenarios, these traffic modelling capabilities are intended to result from learning based on past experience and observation, and are a core issue in CR [Akyildiz et al., 2009; Höyhtyä et al., 2008; Clancy et al., 2007; Xiukui and Zekavat, 2008]. Basically, existing proposals in this area try to efficiently exploit deterministic PU behaviours or to evaluate occupancy statistics over time for each channel [Wellens et al., 2010]. With such prediction capabilities, SUs are able to take optimized spectrum decisions (e.g., selecting a channel which won’t probably experience any PU activity until the estimated data transmission time ends). According to Wellens et al. [2010], the solutions that exploit PU activity statistics perform much better than those that are essentially random-based. Modelling traffic patterns is feasible since several research works have indicated that channel occupancy can be statistically modelled [Wang et al., 2010b; Saleem and Rehmani, 2014]. Section 2.7 discussed prediction and dynamic modelling of PU activity in CR scenarios and presented several existing proposals.

With a sense-before-transmit approach, such as COSBET-MAC does follow (see Chapter 3), priority must thus be given to a channel that is likely to be vacant during the entire sensing and transmission times. This approach is expected to result in a significant decrease regarding the number of harmful interferences to PUs. For instance, with COSBET-MAC, a transmitter-receiver pair randomly selects (with a uniform distribution) a channel for sensing among those that are available at both ends of the communication link (i.e., not already reserved for transmission in their neighbourhood). These channels are the designated candidate or feasible channels. Random selection is the approach followed by most existing distributed CR MAC proposals (see Section 2.6). However and as already mentioned, the applicability and feasibility of learning based on past experience and observation is often considered a core issue in CR since it has potential for incorporating prediction in spectrum decisions. That is, if a SU is based on a distributed CR MAC protocol that follows a sense-before-transmit approach, such as COSBET-MAC does, and has learning capabilities based on observation (i.e., local sensing), then, its set of candidate channels at the beginning of each cycle (see Figure 3.1) includes channels that are not already being accessed in its neighbourhood and, additionally, have no PU activity predicted until the end of the required access time. With this prediction-based restriction, the SUs are expected to perform better concerning the protection of PUs due to a decrease in the number of accesses to false opportunities.

In order to validate the above assumption about the positive effects of prediction based on past experience and observation, we modify our implementation of COSBET-MAC (see Section 3.4) such that the SUs have simulated prediction capabilities concerning the PU activities they can effectively sense (i.e., the SUs predict the activities of the PUs they are in the respective sensing ranges). Concerning stochastic (i.e., random or non-deterministic) PU traffic patterns, there are no learning or traffic modelling mechanisms based on observation and past experience that result in fully accurate prediction (see Section 2.7). However, since we aim at defining the upper limit that prediction based on learning through observation and past experience can achieve regarding PU protection, we consider that prediction is one hundred percent accurate and any initial learning/convergence period has already expired.

The modified version of COSBET-MAC is evaluated through simulation. We use the scenario in Figure 4.1 with 250 kbit/s and 1 Mbit/s constant bit rate loads per transmitter, and 2 Mbit/s physical bit rate. We consider four possible channels, being each one accessed by a specific PU (the rank of a PU in Figure 4.1 is used to designate the respective channel). The other simulation settings are similar to those specified in Table 3.1 in Chapter 3. In a scenario with no hidden PUs, the number of interferences would decrease one hundred percent with the modified version of COBET-MAC under the simulation settings in use since we assume perfect sensing, and fully accurate prediction capabilities.

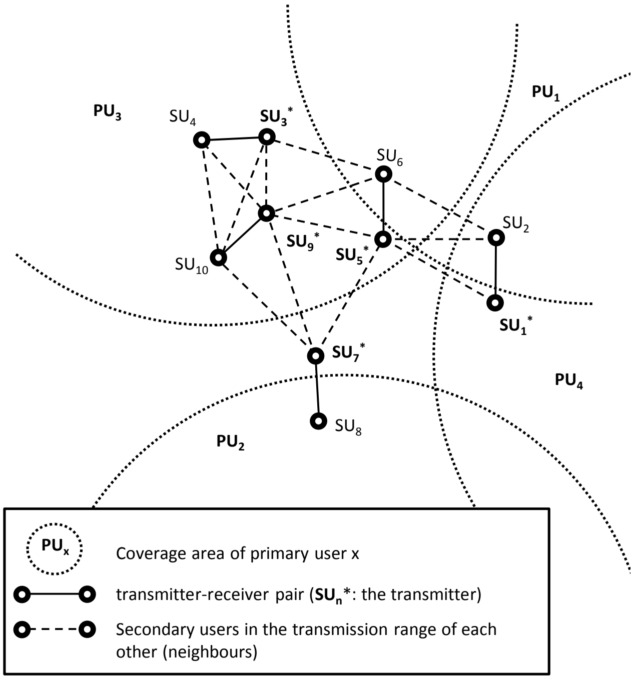
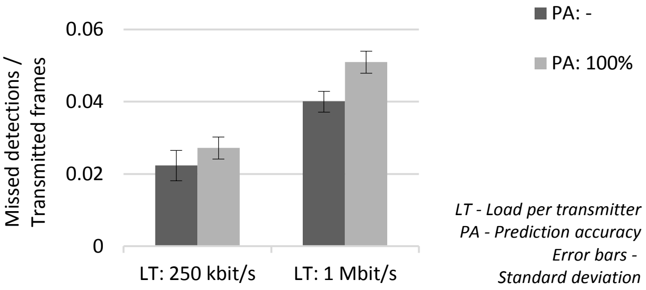
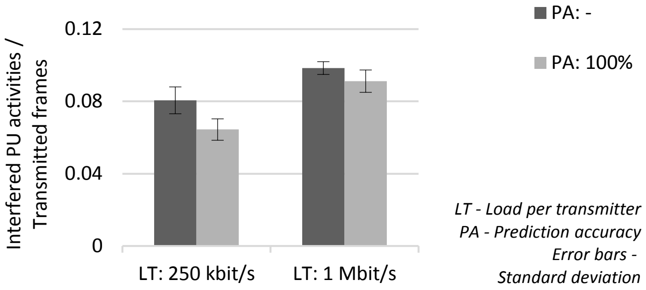


Figure 4.1. A scenario with hidden primary users and hidden secondary users

Figure 4.2 shows the ratios of missed PU detections and interfered PU activities to transmitted data frames, using COSBET-MAC and its modified version (i.e., with simulated fully accurate prediction capabilities based on local observation and past experience). The presented results are obtained averaging over 15 runs of 300 seconds simulated time and with different seeds, and the error bars show the standard deviation between the runs. We use the ratio to the number of transmitted data frames rather than absolute values in order to normalize the results and enable comparison across different simulation runs and configurations. Due to the hidden PU problem, the inclusion of prediction capabilities results in deceiving and even negative effects on the protection of PUs (see Figure 4.2). The reason is as follows. With learning based on observation, a SU assumes that a given channel is always idle if no activity has ever been observed in the past or in a given past time-window if it uses any forgetting scheme. Therefore, the channel that is accessed by a hidden PU is always a candidate channel, unless it is already reserved by any neighbouring SU. On the contrary, a SU that succeeds sensing PU activities on a given channel is able to appropriately model the respective traffic pattern through the underlying learning algorithm it uses. Therefore, it does not consider the channel as candidate whenever it predicts it to be busy.



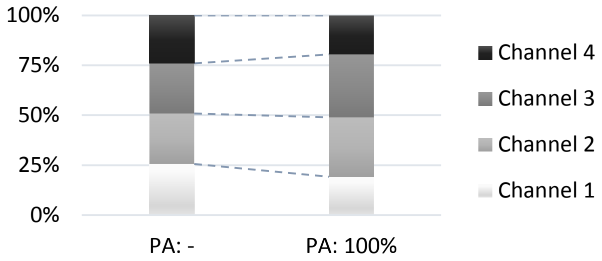
a) Missed detections



b) Interferences to PUs

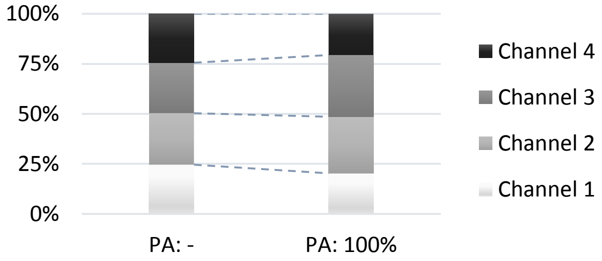
Figure 4.2. Impact of fully accurate prediction capabilities on missed PU detections and interferences to PUs

For instance, if the SUs in Figure 4.1 have fully accurate prediction capabilities based on observation and past experience, transmitter-receiver pair SU_1-SU_2 appropriately models the activities of channel 1 and channel 4, since it is located in the sensing ranges of the respective PUs. Consequently, it also successfully avoids interfering with them. On the contrary, pair SU_1-SU_2 predicts channel 2 and channel 3 as being always vacant in terms of PU traffic since it is positioned out of the sensing ranges of their PUs (i.e., the respective two PUs are hidden PUs in the perspective of pair SU_1-SU_2). Therefore, channel 2 and channel 3 are always candidate channels for pair SU_1-SU_2 when they are not already reserved by other pairs in its neighbourhood. This issue results in the unbalanced selection of channels that we observe in Figure 4.3 (i.e., channels 2 and 3 are more often selected by pair SU_1-SU_2 when prediction is enabled).



PA: Prediction accuracy

a) 250 kbit/s load per transmitter



PA: Prediction accuracy

b) 1 Mbit/s load per transmitter

Figure 4.3. Channel selection pattern of pair 1-2 in Figure 4.1 when using COSBET-MAC

4.2 Related work and contributions

CR proposals that aim at exploiting the characteristics of PU traffic in order to improve spectrum decision already exist in the literature (see Section 2.7). This objective is generally accomplished through a statistical analysis of gathered data that enables evaluating the probability of availability of a channel within a specific period. Nevertheless, none of the solutions analysed in Section 2.7 except DOSP [Wang et al., 2010b] are appropriate for CR scenarios that suffer from the hidden PU problem. Hence, they are prone to the problem discussed in the previous section, which might limit the effectiveness of prediction based on learning through observation and past experience, and, consequently, the protection of PUs. For example, POMDP based MAC protocol [Zhao et al., 2007] assumes that the environment is similarly seen over either ends of a communication pair, which does not account for spatial diversity. DOSP [Wang et al., 2010b] can be considered as an exception since the SUs exchange statistical information about channel availability between them and fuse it with local statistics, which results in a cooperative statistics-based scheme.

Fusing learning outcomes and statistics from different SUs, such as DOSP [Wang et al., 2010b] does, is a means to address the hidden PU problem in CR scenarios with learning through observation and past experience capabilities. However, since this approach results in the SUs employing similar PU traffic modelling and prediction outcomes, it can suffer from an inefficiency we designate as predictive false spectrum access denies. That is, with cooperative learning, the scope of the prediction outcomes of a given SU is not limited to its specific location but to a wider area that includes the locations of all the cooperating SUs. Consequently, the outcomes of cooperative learning are related over all the SUs in a CR network despite the environment might not be in similar states over their locations. A SU might thus be prevented from accessing a given channel despite it does not interfere with the respective PU and appropriately predicts that channel to be vacant based on learning through observation and past experience. With cooperative sensing, applying the OR-rule globally in a network has a comparable negative effect (see Section 2.5.2).

FIBASC, the solution this chapter proposes for CR networks with hidden PUs, aims at enabling an effective utilization of prediction capabilities based on learning through past experience and observation without following a cooperative learning approach. FIBASC consists in a novel strategy that enables the SUs to identify and avoid channels that suffer from the hidden PU problem, i.e., the channels we designate as suspicious. It does not focus on any particular learning scheme. To the best of our knowledge, no other existing CR solution addresses the negative impact that hidden PUs have on the effectiveness of learning through observation and past experience with a scheme similar to FIBASC. Additionally, no other CR MAC protocol described in the literature is analogous to the one that results from the integration of FIBASC with COSBET-MAC.

4.3 Effective utilization of prediction capabilities

This section describes FIBASC (Filtering Based on Suspicious Channels) classification, a solution that enables the effective utilization of any underlying prediction capability that is based on learning though past experience and observation. FIBASC addresses the problem discussed in Section 4.1 and that occurs in CR scenarios that suffer from the hidden PU problem. In this thesis, we specifically target cooperative distributed CR MAC protocols that utilize a dedicated CCC (Common Control Channel) and follow a sense-before-transmit approach, which is a common practice (see Section 2.6.1). Therefore, we also propose an implementation of a distributed version of FIBASC, i.e., with all the SUs running it and using passive learning, on top of COSBET-MAC. However, FIBASC can also be applied in other types of CR networks. For instance, with centralized CR networks, the central entity, which collects data from the SUs and takes spectrum decisions, can run a centralized version of FIBASC.

The remainder of the discussion is organized as follows. Section 4.3.1 defines the notion of suspicious channel. Then, Section 4.3.2 describes the proposed filtering based on suspicious channels algorithm (i.e., FIBASC). Finally, Section 4.3.3 describes the integration of FIBASC with COSBET-MAC based on a distributed approach.

4.3.1 Classification of channels as suspicious

In order to reduce the level of interference to hidden PUs, a SU should consider a channel to be suspicious if it believes this channel is free of any PU activity but a neighbour has an opposite opinion. That is, a SU classifies a channel as being suspicious if: (1) its underlying learning algorithm currently considers the probability of PU appearance to be zero for that channel and at least one of its neighbours does not; or (2) no PU activity was detected during previous sensing phases (see Figure 3.1) and at least one neighbour reported the contrary. When a given channel is effectively utilized by a PU, zero PU activity probability means that the SU was not able to observe any PU activity on that channel in the past or over a finite past time-window. The second condition for classifying a channel as suspicious is based on past sensing outcomes, which is a simple approach for deciding if a given channel has any chance of experiencing any PU activity. In order to account for scenarios with mobility or time-varying conditions, the SUs can remember sensed activities only for a given period, i.e., using a finite past time-window.

A SU stops classifying a channel as being suspicious when the underlying learning algorithm stops considering the probability of PU appearance to be zero for that channel or when it senses any activity on it. In addition, when scenarios with mobility and/or time-varying traffic patterns are considered, the classification of a channel as suspicious must be subject to a timeout process. That is, the SU reverts the status of the channel to non-suspicious if it does not have evidences of such status (i.e., learning and sensing outcomes from neighbours that are in opposition with its own conclusions) for a certain amount of time. The timeout value must be tuned according to the specificities of the scenario (i.e., smaller values are considered when changes in the scenario are frequent). Aging is a common practice concerning learning-based approaches for traffic modelling [Höyhtyä et al., 2008; Salah-Eldeen et al., 2007; Tsagkaris et al., 2008]. For example, Höyhtyä et al. [2008] only consider data that has been gathered within a limited time-window in order to limit the history of events (i.e., past experience) remembered at any given time, which enables adapting to changes in spectrum occupancy.

The channels the SUs in Figure 4.1 should classify as suspicious, i.e., the channels that are accessed by PUs they can interfere with but cannot sense or learn the respective traffic patterns (i.e., hidden PUs), are identified through shaded cells in Table 4.1. In the type of CR environment we target in our research work, the SUs are intended to track suspicious channels based exclusively on the contents of the control frames they receive and overhear on the dedicated CCC, i.e., through passive learning. If the related information in these frames only relate to the sensing and prediction outcomes of the respective transmitters, we get what we designate as one-hop approach (see Table 4.1-a). That is, the fusion of sensing and learning outcomes is limited to neighbouring SUs. The outcome of a SU regarding a given channel simply consists in if it considers that there is any chance of PU activity on that channel or not. Table 4.1 uses symbol √to identify the channels the SUs classify as suspicious, provided that enough information has already circulated on the CCC. We observe that 39% of the hidden PU situations in Figure 4.1 remain undetected with the one-hop approach (see Table 4.1-a).

Table 4.1: Suspicious channels in Figure 4.1

	SU$_1$	SU$_2$	SU$_3$	SU$_4$	SU$_5$	SU$_6$	SU$_7$	SU$_8$	SU$_9$	SU$_{10}$
	a) One-hop approach									
PU$_1$	▨ √		▨ √	▨	▨ √		▨		▨ √	▨
PU$_2$	▨				▨		▨ √			
PU$_3$	▨ √	▨ √					▨ √	▨		
PU$_4$					▨ √	▨ √	▨ √	▨		
	b) Two-hop approach									
PU$_1$	▨ √		▨ √	▨ √	▨ √		▨ √		▨ √	▨ √
PU$_2$	▨ √				▨ √		▨ √		√	
PU$_3$	▨ √	▨ √					▨ √	▨ √		
PU$_4$			√		▨ √	▨ √	▨ √	▨ √	√	
	c) Three-hop approach									
PU$_1$	▨ √		▨ √	▨ √	▨ √		▨ √	√	▨ √	▨ √
PU$_2$	▨ √	√	√	√	▨ √	√	▨ √		√	√
PU$_3$	▨ √	▨ √					▨ √	▨ √		
PU$_4$			√	√	▨ √	▨ √	▨ √	▨ √	√	√

▨ Channels that should be classified as suspicious.
√ Channels the SUs effectively classify as suspicious based on the proposed approach.

The protection of PUs can be further increased if the same scheme is used with a so-called two-hop approach (i.e., an approach that considers information from one-hop neighbours and their own one-hop neighbours) or higher distance approaches (see Table 4.1-b and Table 4.1-c). The set of “neighbours of neighbours” of a given SU might also include some of its own neighbours. Therefore, we do not name them two-hop neighbours. When the two-hop approach is applied to the scenario depicted in Figure 4.1, all the situations with potential risk of interference to hidden PUs are detected. With this approach, a SU also relays a summary of sensing and learning outcomes of its neighbours through the control frames it transmits over the CCC (see Section 4.3.3 for details). For any CR scenario, the minimum distance that is required for the proposed approach to be effective is determined by the number of hops between any SU and any other SU that is in the sensing range of any PU it can interfere with but cannot sense.

In Table 4.1, we observe the occurrence of what we designate as false suspicious, i.e., a SU considers a channel to be suspicious despite there is actually no hidden PU problem. False suspicious are cells in Table 4.1 that are not shaded despite being tagged as suspicious with symbol √. The impact of this issue increases as the approach follows a higher distance. Therefore, the number of hops to be used must be appropriately selected in order to maximize the detection of hidden PUs while minimizing the occurrence of false suspicious in the targeted scenario. Without loss of generality, we consider the scenario in Figure 4.1 and the two-hop approach from this point forward. It is possible to have a SU with all the channels tagged as suspicious (e.g., see SU_7 in Table 4.1-b and Table 4.1-c). Concerning how an affected SU deals with such situation, we identify three possible approaches: (1) the SU stops communicating until the situation reverts; (2) the SU starts using an unlicensed frequency band; or (3) the SU uses a lower distance approach or, if already using the one-hop approach, omits the classification of channels as suspicious in the spectrum decision process. All the approaches have pros and cons in the perspective of both the performance delivered to the SUs and the protection of PUs. From this point forward, we consider the last option, i.e., the channels tagged as suspicious are lower priority channels instead of forbidden channels.

4.3.2 Filtering based on suspicious channels

We address the lack of protection of hidden PUs by preventing the transmitter-receiver pairs to select channels with specific characteristics. Specifically, a transmitter-receiver pair filters, i.e., does not take into account, channels that: (1) suffer from the hidden PU problem on both sides; or (2) suffer from the hidden problem on one of the sides and the other side is out of its sensing area. That is, a channel is considered only if the hidden PU problem is not an issue on both sides or at least one of the sides is able to sense PU activities on that channel (i.e., it has sensed any PU activity in the past or any underlying learning algorithm currently models PU traffic as not being null). Figure 4.4 illustrates the outcome of this approach when applied to the scenario in Figure 4.1.

If we implement the proposed filtering scheme using the suspicious channel concept defined in the previous section, which aims at enabling the identification of hidden PUs, we get an algorithm that we designate as filtering based on suspicious channels classification (i.e., FIBASC) and apply it during channel selection phases (see Figure 3.1). For example, if we apply the two-hop approach of FIBASC (see Table 4.1-b), we obtain the result in Figure 4.5. The difference with

Figure 4.4 results from the occurrence of false suspicious. Concerning cooperative distributed CR MAC protocols that follow a sense-before-transmit approach, the type of solution we are interested in this thesis, FIBASC runs when a transmitter-receiver pair selects a channel before the sensing phase (see Figure 3.1). Regarding COSBET-MAC, a specific CR MAC solution, FIBASC modifies the way the set of candidate channels is determined. That is, it modifies expression $Cs \cap Cr$ in step 1 and step 2 of Algorithm 3.1.

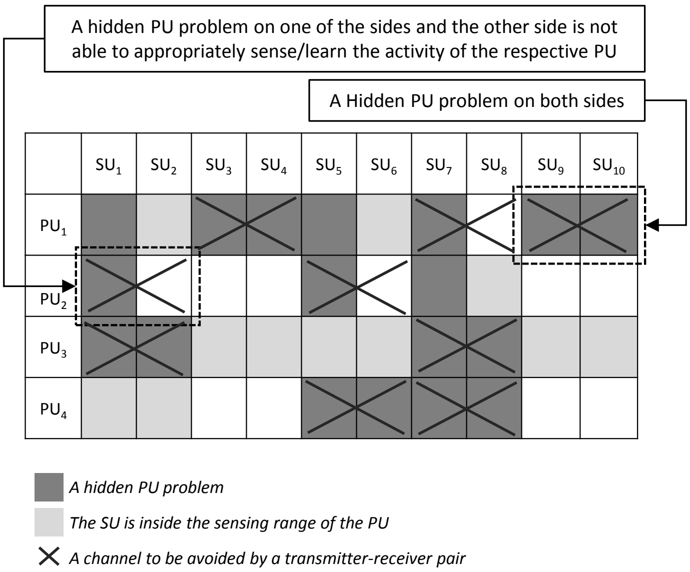


Figure 4.4. Channels to be avoided in Figure 4.1 due to the hidden PU problem

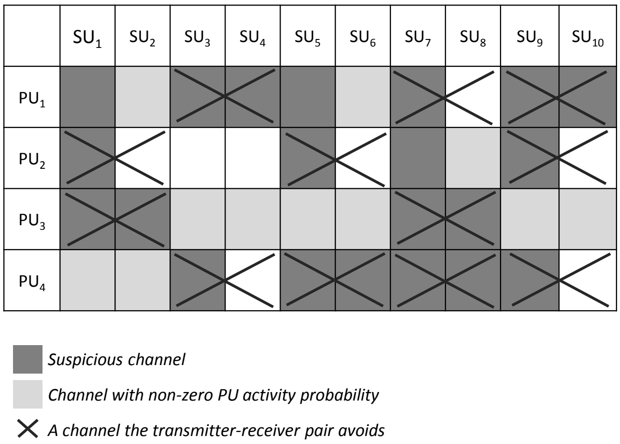


Figure 4.5. Channels the transmitter-receiver pairs avoid in Figure 4.1 when using two-hop FIBASC

Algorithm 4.1 describes FIBASC assuming the two-hop approach. For every SU, it requires making the distinction between channels that are not suspicious based on the outcomes of one-hop neighbours and those that are not suspicious based on the outcomes of “one-hop neighbours of one-hop neighbours”. This approach enables FIBASC to take into account two distinct criteria (i.e., Criterion 1 and Criterion 2 in Algorithm 4.1) as follows. If using the two criteria jointly (i.e., the two-hop approach) results in an empty set of channels, then, the operation is repeated omitting criterion N_{sr2}, i.e., following the one-hop approach (see step 6 in Algorithm 4.1). If the situation remains, no filtering based on suspicious channels is executed (see step 7 in Algorithm 4.1). This is one of the three possible approaches that were mentioned in Section 4.3.1. Figure 4.6 illustrates this channel selection process. As a final remark, Algorithm 4.1, i.e., FIBASC, can easily be adapted to higher distance approaches or to the one-hop approach, which requires altering the number of criteria that are considered and providing adequate inputs.

```
Inputs:  $C_t$, the channels that are not reserved and have no predicted PU activity at the
         transmitter;
         $C_r$, the channels that are not reserved and have no predicted PU activity at the
         receiver;
         $N_{t1}$, the channels which are not suspicious at the transmitter based on the
         outcomes of its one-hop neighbours;
         $N_{r1}$, the channels that are not suspicious at the receiver based on the outcomes of
         its one-hop neighbours;
         $N_{t2}$, the channels that are not suspicious at the transmitter based on the outcomes
         of the “one-hop neighbours of its one-hop neighbours”;
         $N_{r2}$, the channels that are not suspicious at the receiver based on the outcomes of
         the “one-hop neighbours of its one-hop neighbours”;
         $Q_t$, the channels the transmitter considers having non-zero PU activity probability;
         $Q_r$, the channels the receiver considers having non-zero PU activity probability.
Output:  $C_c$, a set of candidate channels for sensing/access.
1.  $C_{tr} \leftarrow C_t \cap C_r$.
2.  if $C_{tr} = \varnothing$ then return $\varnothing$
3.  $N_{tr1} \leftarrow (N_{t1} \cap N_{r1}) \cup (N_{t1} \cap Q_t) \cup (N_{r1} \cap Q_r)$ //Criterion 1
4.  $N_{tr2} \leftarrow (N_{t2} \cap N_{r2}) \cup (N_{t2} \cap Q_t) \cup (N_{r2} \cap Q_r)$ //Criterion 2
5.  if $(N_{tr1} \cap N_{tr2}) \neq \varnothing$ then $C_c \leftarrow C_{tr} \cap N_{tr1} \cap N_{tr2}$
6.  else if $N_{tr1} \neq \varnothing$ then $C_c \leftarrow C_{tr} \cap N_{tr1}$
7.  else $C_c \leftarrow C_{tr}$
8.  return $C_c$
```

Algorithm 4.1. Filtering based on suspicious channels classification (two-hop approach)

We can easily infer the meanings of the inputs in Algorithm 4.1 from previous discussion, except for what concerns Q_t and Q_r. Without the use of Q_t and Q_r, FIBASC would be as follows regarding step 3 and step 4: $N_{tr1} := N_{t1} \cap N_{r1}$; and $N_{tr2} := N_{t2} \cap N_{r2}$. This approach seems adequate since it only takes into account the channels that are not suspicious at both ends of the receiver-transmitter pair according to the two criteria in use. However, it raises an issue that affects performance. For instance, with such tactic, pair SU_1-SU_2 and pair SU_5-SU_6 in Figure 4.1 do not consider channel 1 despite SU_1 and SU_5 are able to sense it and, therefore, should always include it in their set of candidate channels (provided that it is not already reserved and no activity is predicted on it until the end of the estimated access time). Considering the union of the channel sets (i.e., $N_{tr} \leftarrow N_{t1} \cup N_{r1}$; and $N_{tr2} \leftarrow N_{t2} \cup N_{r2}$) is neither a feasible solution since it avoids the kind of problem we just mentioned but creates another one. For example, with this approach pair SU_3-SU_4 in Figure 4.1 wrongly considers channel 1 as being a candidate channel despite SU_3 classifies it as suspicious based on sensing and learning outcomes provided by neighbour SU_5, and SU_4 is out of its sensing range (i.e., there is a hidden PU problem concerning pair SU_3-SU_4 and PU_1).

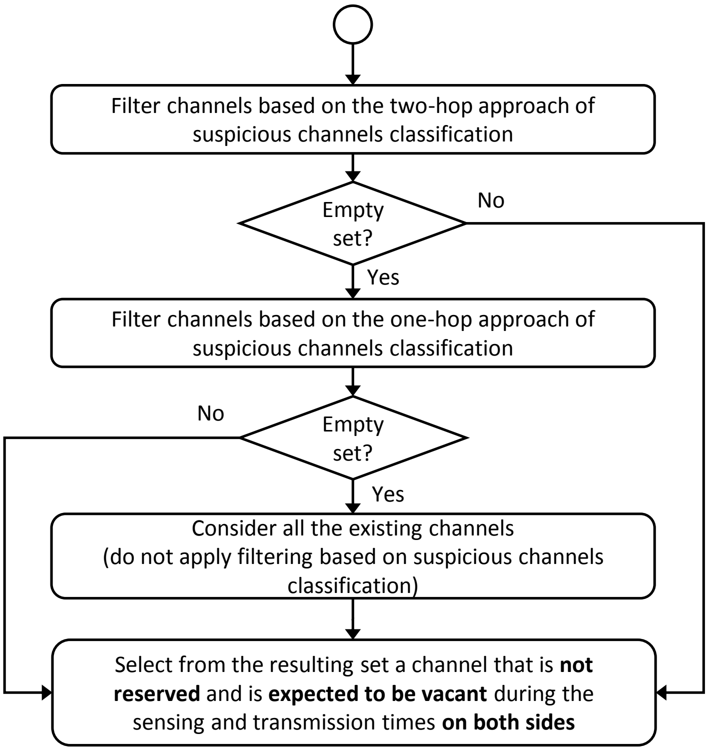


Figure 4.6. Channel selection with two-hop FIBASC

With Algorithm 4.1, if in a given transmitter-receiver pair only one of the SUs classifies a given channel as not being suspicious for a given criterion and that SU considers PU appearance probability to be non-zero on that channel, then, the transmitter-receiver pair includes that channel in the set of candidate channels, i.e., it does not filter it. The required information is provided by Q_t and Q_r in Algorithm 4.1. Globally, these two channel sets enable making distinction between two possible reasons that result in a given SU not classifying a channel as being suspicious: (1)

the SU is out of the sensing range of the respective PU and has not yet received or overheard any evidence from neighbours that makes it classify the channel as being suspicious; or (2) the SU is effectively inside the sensing range of the respective PU and can, therefore, effectively sense its activity. Channels that are set in Q_t and Q_r are channels that the SUs are probably inside the sensing ranges of the respective PUs, therefore, being able to properly sense and model their activity patterns. They summarize the sensing and learning outcomes that Section 4.3.1 mentions and, therefore, are also used by neighbours to track suspicious channels.

The next section describes how FIBASC is integrated with COSBET-MAC, i.e., how the processing, exchange, and utilization of relevant information (e.g., the channel sets used in Algorithm 4.1) is achieved for tracking suspicious channels. It also discusses how it can be applied in CR scenarios with mobility or any other time-varying characteristics, which essentially consists in a forgetting mechanism that enables, under some circumstances, invalidating the classification of a channel as suspicious or as having some probability of PU activity.

4.3.3 Integrating FIBASC with COSBET-MAC

With COSBET-MAC, FIBASC is executed by the receiver before it selects a given channel for sensing and informs the transmitter about this selection through a CTSS frame (see Figure 3.1). In this case, Algorithm 4.1 replaces expression $C_s \cap C_r$ in step 1 and step 2 of Algorithm 3.1. Hence, the receiver needs to know the channels the transmitter classifies as suspicious based on the two filtering criteria that the two-hop approach requires (see Criterion 1 and Criterion 2 in Algorithm 4.1). With COSBET-MAC, this information is provided through additional arrays of bits in RTS frames (see Table 4.2). Our implementation of COSBET-MAC identifies the channels through indexes and, therefore, the bit in the first position of an array relates to the status of the first channel and so on (see Chapter 3).

The two-hop approach in Algorithm 4.1 requires three additional arrays that are used to materialise N_{t1}, N_{t2}, and Q_t (i.e., a summary of the sensing and learning outcomes of the transmitter), respectively. Moreover, RTS frames also include a fourth array of bits that represents the designated Q_{tn} input that Algorithm 4.2 utilizes and that is required for tracking suspicious channels with the two-hop approach. That is, Q_n in Table 4.2 summarizes the learning and sensing outcomes of the neighbours of the transmitter of an RTS frame. If the bit that relates to a given channel is set in Q_n, it means that at least one of its neighbours considers the channel as having some PU activity based on its own observation.

Table 4.2: Fields in RTS, CTSS, and fCTSS frames of COSBET-MAC related to channel selection and tracking of suspicious channels

Field	Description	Goal	Size (bits)	RTS	CTSS
b	Number of bits to be sent in the next data frame	Channel selection	m [a]	yes	
C_t	The channels that are not reserved and have no predicted PU activity	Channel selection	n [b]	yes	
N_1	Non-suspicious channels based on the outcomes of one-hop-neighbours	Channel selection	n	yes	
N_2	Non-suspicious channels based on the outcomes of "one-hop-neighbours of one-hop neighbours"	Channel selection	n	yes	
Q	The channels that are considered to have some PU activity	Channel selection and tracking of suspicious channels	n	yes	yes
Q_n	The channels that at least one neighbour considers having some PU activity	Tracking of suspicious channels	n	yes	yes

[a] Large enough to represent the maximum transfer unit in use.
[b] The number of existing channels.

```
Inputs:  $Q_r$, $Q_t$, $N_{r1}$, and $N_{r2}$ (see Algorithm 4.1);
         $Q_{rn}$, the channels at least one neighbour of the receiver
         considers having non-zero PU activity probability;
         $Q_{tn}$, the channels at least one neighbour of the transmitter
         considers having non-zero PU activity probability.
Output:  Updated information about suspicious channels.
1.  for every channel $c \notin Q_r$
2.      if $c \in Q_t$ and $c \in N_{r1}$ then remove $c$ from $N_{r1}$
3.      if $c \in Q_{tn}$ and $c \in N_{r2}$ then remove $c$ from $N_{r2}$
4.  end for
5.  for every channel $c \in Q_t$
6.      add $c$ to $Q_{rn}$
7.  end for
```

Algorithm 4.2. Tracking of suspicious channels based on received/overheard RTS or CTSS frames (two-hop approach)

Algorithm 4.2 describes how COSBET-MAC uses the two arrays of bits that materialise Q and Q_n in RTS frames (i.e., Q_t and Q_{tn} in Algorithm 4.2, respectively) in order to track suspicious channels. Any time a SU is notified by a neighbour that a given channel has non-zero PU appearance probability (i.e., via Q in the received/overheard RTS frames), the SU includes that channel in its local channel set Q_n, which is designated as Q_{rn} in Algorithm 4.2 (see step 6 in Algorithm 4.2). It also compares that information with its own beliefs in order to track suspicious channels with the one-hop approach (see step 2 in Algorithm 4.2). The RTS frames a SU transmits include Q_n (see Table 4.2), which enables neighbours to track suspicious channels with the two-hop approach (see Q_{tn} and step 3 in Algorithm 4.2).

The four additional arrays required in COSBET-MAC RTS frames (i.e., N_1, N_2, Q, and Q_n in Table 4.2) are of equal size and only require as much bits as the number of existing channels (see Table 4.2), which results in low overhead (see simulation results in Section 4.4 for an evaluation of their impact on performance). For example, the scenario in Figure 4.1, which includes four possible channels, only requires sixteen additional bits in RTS frames. A SU that transmits a CTSS frame also includes in this frame the two arrays that relate to Q and Q_n (see Table 4.2) with the same purpose of enabling its neighbours to identify suspicious channels based on the one-hop and two-hop approaches, respectively (see Algorithm 4.2). This strategy enables a mutual exchange of information between the transmitter and the receiver, and provides additional information to overhearing neighbours (i.e., through passive learning).

In order to enable the SUs to track suspicious channels, four additional bits (i.e., s_t, s_{tn}, p_t, and p_{tn}) are also added to CTS and fCTS frames. These frames are sent after a sensing phase (see Figure 3.1) and specifically relate to the sensed channel. Algorithm 4.3 describes the meaning and utilization of these bits. As already mentioned in Section 4.3.1, any time a SU senses an activity on a given channel or its learning algorithm starts considering the channel as having non-zero PU appearance probability, the SU classifies that channel as not being suspicious for both the two-hop and one-hop criteria. That is, it considers itself as being in the sensing range of the respective PU. Consequently, the SU adds that channel to the respective three channel sets it uses to support FIBASC (i.e., N_1, N_2, and Q in Table 4.2).

If the targeted CR scenario includes mobility or any other time-varying characteristics, the SUs must use a forgetting mechanism (see Section 4.3.1). With this mechanism, a SU stops tagging a channel as being suspicious, for both the one-hop and two-hop approaches, when it stops having evidences of that status for a certain amount of time. In this case, a channel goes back to the sets of non-suspicious channels from where it was previously excluded (see N_{r1} and N_{r2} in Algorithm 4.2 and Algorithm 4.3). Evidences are based on the comparison of local sensing and learning outcomes (see Q_r in Algorithm 4.2 and Algorithm 4.3) with sensing and learning outcomes from one-hop neighbours and "on-hop neighbours of neighbours" (see Q_t and Q_{tn} in Algorithm 4.2, and s_t, s_{tn}, p_t, and p_{tn} in Algorithm 4.3). Similarly, if, for a certain amount of time, a SU does not receive or overhear any control frame that indicates that at least a one-hop neighbour of one of its one-hop neighbours considers a given channel as having non-zero PU activity, then, it excludes that channel from its respective set (i.e., Q_n in Table 4.2).

Inputs: Q_r, N_{r1}, and N_{r2} (see Algorithm 4.1);
t, the specified channel in the received/overheard frame;
s_t, a bit which indicates if the transmitter sensed any activity on t;
s_{tn}, a bit which indicates if any neighbour of the transmitter sensed any activity on t;
p_t, a bit which indicates if the transmitter considers t as having non-zero PU activity probability;
p_{tn}, a bit which indicates if any neighbour of the transmitter considers t as having non-zero PU activity probability.

Output: Updated information about suspicious channels.

```
if participated in sensing phase related to channel $t$ then
  if no activity was sensed on $t$ then
      if $s_t$ = true and $t \in N_{r1}$ then remove $t$ from $N_{r1}$
      if $s_{tn}$ = true and $t \in N_{r2}$ then remove $t$ from $N_{r2}$
  endif
endif
if $p_t$ = true and $t \notin Q_r$ and $t \in N_{r1}$ then remove $t$ from $N_{r1}$
if $p_{tn}$ = true and $t \notin Q_r$ and $t \in N_{r2}$ then remove $t$ from $N_{r2}$
```

Algorithm 4.3. Tracking of suspicious channels based on received/overheard CTS or fCTS frames (two-hop approach)

With the same concern, any PU activity that is sensed locally, which determines that a channel has non-zero PU appearance probability, is forgotten after a defined amount of time. The underlying learning algorithm should also give more importance to more recent observations and use a finite time-window over past-experience (see Section 2.7). The mentioned forgetting scheme is also a means to turn into temporary any wrong classification decision that, for instance, results from occasional false sensing alarms or inaccurate predictions. Defining the most appropriate forgetting time for a specific CR scenario is a critical issue, which is out of the scope of this thesis, since it might affect adaptability or stability if it is excessively high or excessively small, respectively.

The integration of FIBASC with COSBET-MAC takes full advantage of existing control frames and passive learning over the dedicated CCC. Consequently, this approach results in all the interactions FIBASC requires between the SUs to be provided at the expanse of just a few additional bits in existing control frames. In order to use an approach different from the two-hop approach, the number of additional bits in CTS and fCTS frames, and the number of additional arrays in RTS and CTSS frames must be adjusted. Modifying the algorithm accordingly is quite straightforward.

4.4 Performance evaluation

This section evaluates, through simulation, the effect of FIBASC on the protection of PUs and on the communication performance of SUs. For this purpose, we use the implementation that resulted from its integration with COSBET-MAC and that was described in Section 4.3.3.

4.4.1 Methodology and simulation settings

Since COSBET-MAC is already implemented on the OMNET++/MiXiM framework (see Section 3.4.1), we continue using this platform to implement and evaluate the simulation model of FIBASC. The PHY bit rate is 2 Mbit/s on the CCC and on the data channels, the MTU is 18432 bits, transmit to receive and receive to transmit switching times are 0.1 milliseconds on the reconfigurable radios, sensing time is 0.5 milliseconds, and PU activity on the data channels is characterized by alternating idle and busy periods exponentially distributed with means 0.1 and 0.01 seconds, respectively. We use the scenario in Figure 4.1 and set load per transmitter up to 2 Mbit/s. The presented results are obtained averaging over 15 runs of 300 seconds simulated time and with different seeds. The other simulation settings are the same that are described in Section 3.4.2 and summarized in Table 3.1. Variations to the mentioned simulation parameters and settings not already defined are specified at the time they are used.

4.4.2 Protection of PUs

Figure 4.7 and Figure 4.8 illustrate the variation that is observed in the rate of missed PU detections and interferences to PUs, respectively, when FIBASC is applied to COSBET-MAC and we assume the SUs have prediction capabilities based on learning through observation and past experience. The error bars show the standard deviation between the runs. We consider different configuration settings concerning: the utilization of FIBASC (i.e., not utilized, one-hop approach, and two-hop approach); prediction capabilities (i.e., not utilized, 100% accurate, 80% accurate, and 60% accurate); and load per transmitter (i.e., 250 kbit/s, 1 Mbit/s, and 2 Mbit/s).

A global missed PU detection occurs when a PU activity that a transmitter-receiver pair can interfere with is not detected during the sensing phase (see Figure 3.1). An interference occurs when the transmission of a data frame overlaps in time, frequency, and space a PU activity. We can observe in Figure 4.7 and Figure 4.8 that, when COSBET-MAC is utilized without FIBASC (see notation "T: -" in figures) and assuming fully accurate prediction (see notation "PA: 100%" in figures), the obtained results are deceiving and even poorest, especially regarding missed detections. The reason for this issue was already stated and discussed in Section 4.1, and consists in the problem this chapter addresses. The discussion in Section 4.3.1 explains the poor results that we also observe when FIBASC follows the one-hop approach. That is, there is a significant number of situations that raise the hidden PU problem and that are not appropriately detected (i.e., classified as suspicious) by the SUs (see Table 4.1-a).

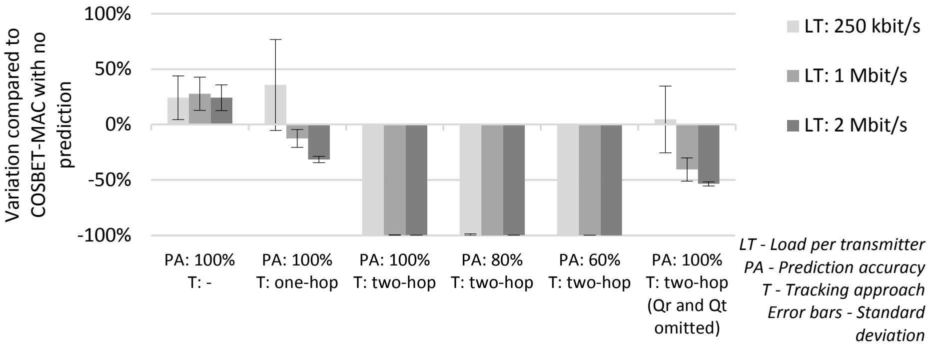


Figure 4.7. Variation in the rate of missed PU detections when compared to COSBET-MAC with no prediction capabilities

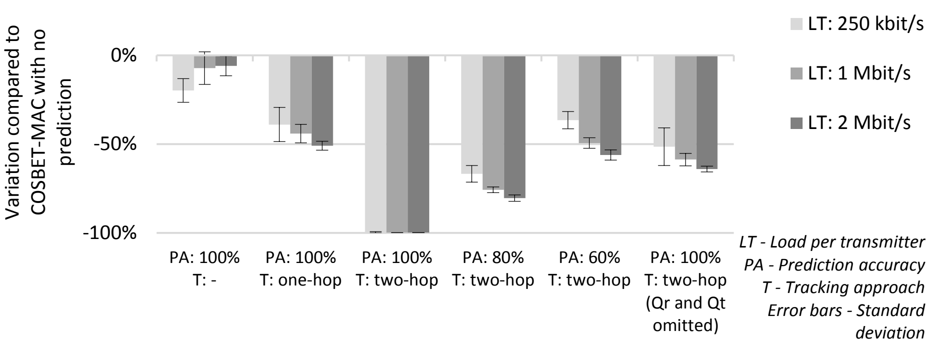


Figure 4.8. Variation in the rate of interferences to PUs when compared to COSBET-MAC with no prediction capabilities

In Figure 4.7 and Figure 4.8, we observe that not using FIBASC, utilizing it with the one-hop approach, or omitting parameters Q_t and Q_r (see Algorithm 4.1) results in substantial standard deviation between runs, i.e., the obtained results vary significantly with the random nature of PU and SU traffic in such circumstances. With 250 kbit/s load per transmitter, standard deviation is particularly high since inter-frame space is higher than with 1 Mbit/s and 2 Mbit/s loads per transmitter, which results in higher variability between the simulation runs in terms of the number of sensing and transmission periods that overlap PU activities (i.e., ON periods). On the contrary, two-hop FIBASC, the specific solution we propose, results in stable gains that are less prone to the randomness of PU and SU traffic, both concerning missed PU detections (see Figure 4.7) and interferences to PUs when prediction is fully accurate (see Figure 4.8).

With the two-hop approach and fully accurate prediction capabilities, missed PU detections and interferences to PUs are almost totally prevented in the simulation scenario in use. A limited number of missed detections and interferences occurs on start-up, i.e., when the number of handshakes between SUs is still not sufficient to have all the transmitter-receiver pairs with the proposed channel classification process concluded. Since the suspicious channels are appropriately identified and the filtering of channels never results in empty sets for any transmitter-receiver pair (see Table 4.1-b and Figure 4.5), the pairs only select the channels the transmitter and/or the receiver can effectively sense and, therefore, model the respective PU traffic, or that are not subject to the hidden PU problem on both sides (see Section 4.3.2). Consequently, the accessed channels are effectively vacant throughout the handshake and access phases. In our implementation, the SUs estimate transmission time based on the data bit rate and data frame size. Concerning handshake time (i.e., the delay between RTS transmission and fCTS reception in Figure 3.1), each SU uses an estimated value on start-up and continuously adjust it based on the values they observe subsequently.

If we consider prediction capabilities that are not one hundred percent accurate, which is a practical assumption, the protection of PUs naturally degrades. However, the gains provided by two-hop FIBASC remain relevant. Figure 4.7 and Figure 4.8 also illustrate the relevance of using parameters Q_t and Q_r in Algorithm 4.1, which was discussed in Section 4.3.2. When we modify FIBASC such that these parameters are not used in the filtering process (see Algorithm 4.1), results get considerably worse and less consistent over the simulation runs, which supports the related discussion in Section 4.3.2.

In order to generalize the conclusions about FIBASC, we repeat the same experiments inhibiting the cooperation of neighbours in the sensing phase, which is a specific feature of COSBET-MAC and is achieved through negative feedback. The objective is evaluating the effect of FIBASC on distributed CR MAC protocols that follow a generic (i.e., non-cooperative) sense-before-transmit approach. Figure 4.9 and Figure 4.10 present the observed variation concerning the rate of missed PU detections and interferences to PUs when compared to results obtained with native COSBET-MAC (i.e., without FIBASC and with no prediction). The error bars show the standard deviation between the runs. The presented results enable us to draw the same conclusions as previously concerning the gains provided by two-hop FIBASC in terms of PU protection. As already observed in Section 3.4.4, COSBET-MAC performs better than the sense-before-transmit approach in terms of PU protection when prediction is not enabled and FIBASC is not used (see notations “PA:-” and “T:-” in Figure 4.9 and Figure 4.10).

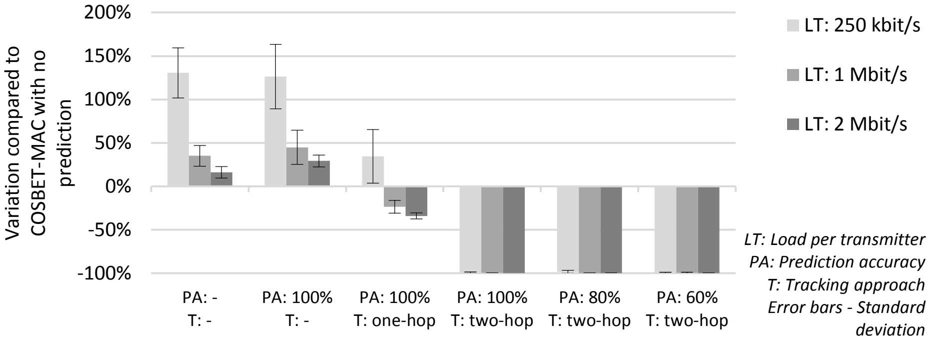


Figure 4.9. Variation in the number of missed PU detections when comparing a generic sense-before-transmit approach to COSBET-MAC with no prediction capabilities

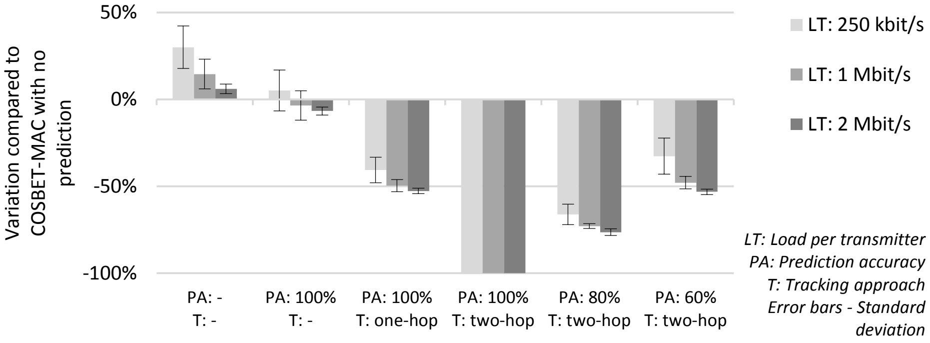


Figure 4.10. Variation in the number of interferences to PUs when comparing a generic sense-before-transmit approach to COSBET-MAC with no prediction capabilities

The density of SUs in the scenario illustrated in Figure 4.1 is relatively low. Therefore, in order to verify that FIBASC still performs well in terms of PU protection in scenarios with higher levels of contention, we populate the scenario in Figure 4.1 with twenty additional SUs, i.e., with ten additional transmitter-receiver pairs, randomly located with a uniform distribution. Figure 4.11 and Figure 4.12 present the obtained results when FIBASC is integrated with COSBET-MAC. The error bars show the standard deviation between the runs. The same conclusions apply concerning the benefits that result from using FIBASC. We observe, however, that with two-hop FIBASC the achieved reduction in the number of interferences and missed detections is lower than with scenario in Figure 4.1 for similar prediction accuracies (compare with results presented in Figure 4.7 and Figure 4.8). The cause is that there are more false suspicious channels and, therefore, more transmitter-receiver pairs that do not apply two-hop FIBASC since a higher number of false suspicious results in a higher number of empty channel sets (see Figure 4.6).

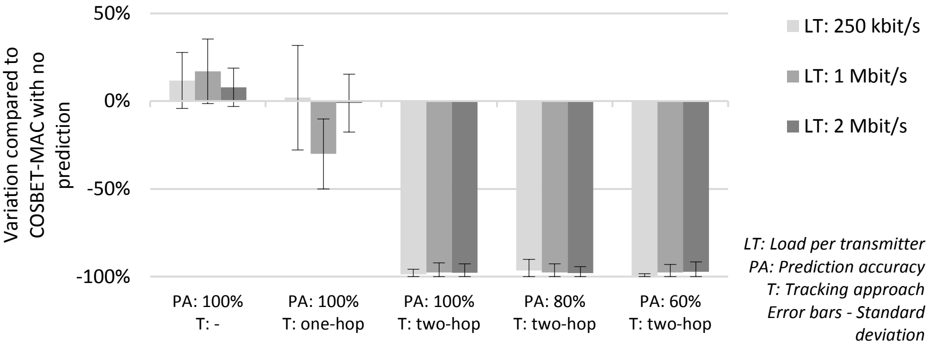


Figure 4.11. Variation in the number of missed PU detections when compared to COSBET-MAC with no prediction capabilities (scenario with 20 additional SUs)

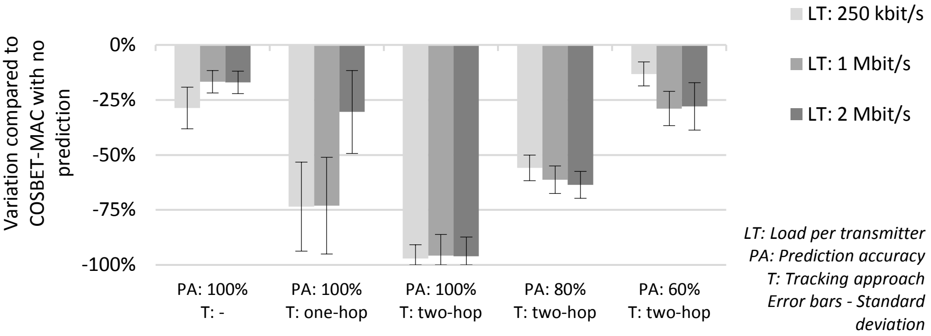
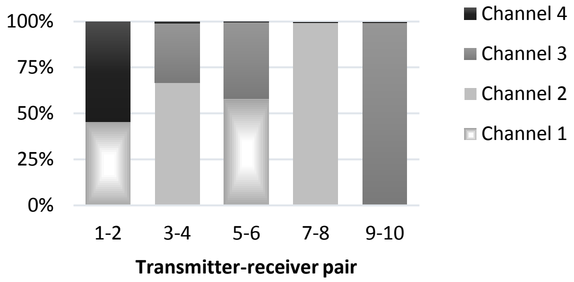


Figure 4.12. Variation in the number of interferences to PUs when compared to COSBET-MAC with no prediction capabilities (scenario with 20 additional SUs)

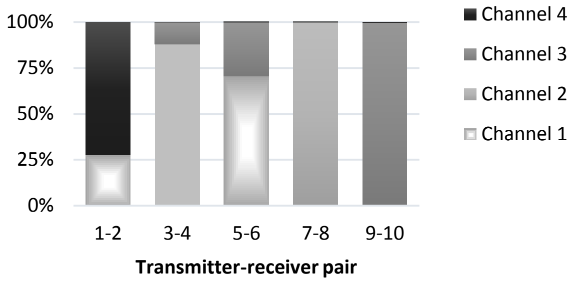
In Figure 4.11 and Figure 4.12, the observed standard deviation between runs increases when compared to previous results, particularly when not using FIBASC or using it with the one-hop approach, which is due to the random positioning of additional SUs in the scenario illustrated in Figure 4.1. That is, the relative position between SUs varies over the different simulation runs and, consequently, the interaction between them (e.g., the sources of the overheard sensing and learning outcomes) and the resulting channels each SU classifies as suspicious also. Nevertheless, we still conclude that, despite the random nature of the simulation scenario, two-hop FIBASC is effectively able to provide significant and consistent gains concerning the protection of PUs.

4.4.3 Utilization of channels

Figure 4.13 illustrates the selection pattern (i.e., how often a channel is selected) of the transmitter-receiver pairs in Figure 4.1 when two-hop FIBASC is integrated with COSBET-MAC and we assume that prediction is fully accurate. We observe that there is a match between the observed pattern and the pattern expected from Figure 4.5. Therefore, our implementation of FIBASC integrated with COSBET-MAC correctly implements the proposed solution for tracking and filtering suspicious channels. This naturally results in an unbalanced selection of channels, which is illustrated in Figure 4.14.



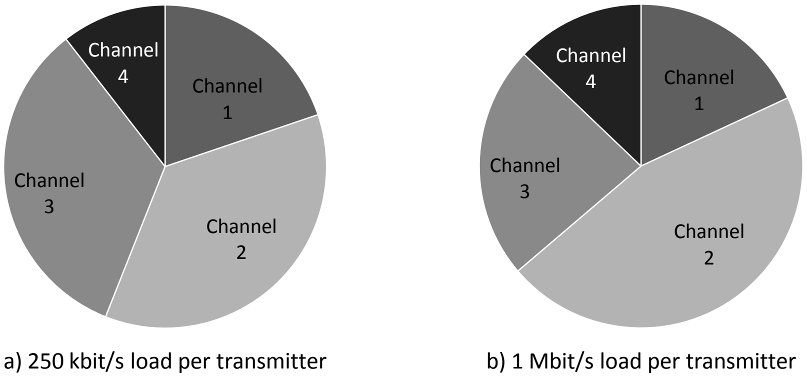
a) 250 kbit/s load per transmitter



b) 1 Mbit/s load per transmitter

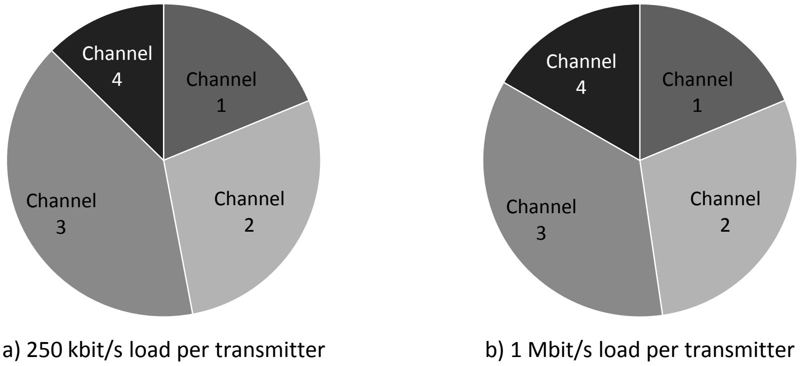
Figure 4.13. Channel selection pattern when using COSBET-MAC with two-hop FIBASC and assuming fully accurate prediction capabilities

In Figure 4.14, channel 2 is more often selected than the others since it is not classified as suspicious by pairs SU$_3$-SU$_4$ and SU$_7$-SU$_8$ (see Figure 4.5 and Figure 4.13), it is the only channel that pair SU$_7$-SU$_8$ selects, and pair SU$_3$-SU$_4$ considers it as having zero PU appearance probability. Channel 4 is the only channel that is considered non-suspicious by a single transmitter-receiver pair (i.e., pair SU$_1$-SU$_2$), which explains why it is less often selected than the other channels. Finally, channel 1 and channel 3 are considered as not being suspicious by two and three transmitter-receiver pairs, respectively. Figure 4.15 illustrates the channel selection pattern that is achieved when the simulation scenario in Figure 4.1 is populated with twenty additional SUs randomly placed with a uniform distribution. The observed unbalanced utilization of channels in Figure 4.14 and Figure 4.15 results from a higher protection of PUs, which is one of the goals with highest priority in CR environments.



a) 250 kbit/s load per transmitter b) 1 Mbit/s load per transmitter

Figure 4.14. Global channel selection pattern when using COSBET-MAC with two-hop FIBASC and assuming fully accurate prediction capabilities

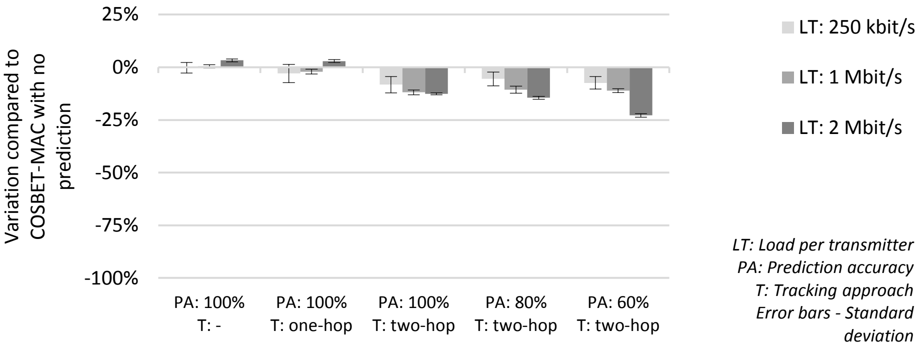


a) 250 kbit/s load per transmitter b) 1 Mbit/s load per transmitter

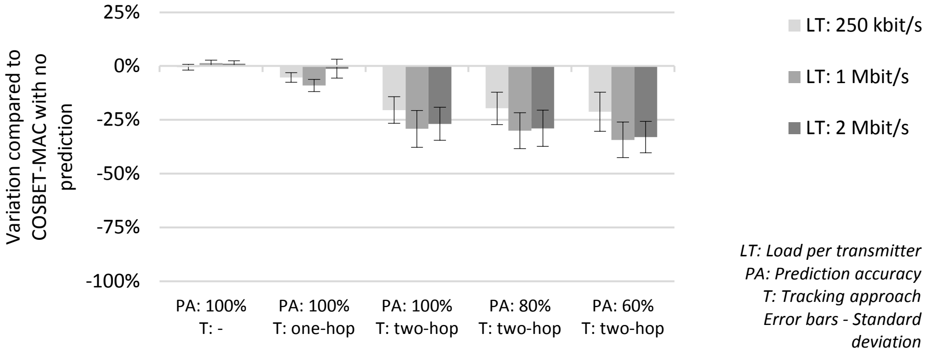
Figure 4.15. Global channel selection pattern when using COSBET-MAC with two-hop FIBASC and assuming fully accurate prediction capabilities (scenario with 20 additional SUs)

4.4.4 Impact on communication Performance

Figure 4.16 presents the average degradation of the communication performance of SUs that is observed when FIBASC is integrated with native COSBT-MAC. The error bars show the standard deviation between the runs. We consider the scenario in Figure 4.1 and a similar scenario with ten additional transmitter-receiver pairs randomly placed with a uniform distribution, and assume fully accurate prediction capabilities. The observed penalty is unavoidable since higher protection of PUs means less opportunities or, more precisely, less false opportunities being detected and accessed by the SUs. Also, it is definitively an acceptable cost when compared to the achieved benefits regarding PU protection, which is, as already mentioned, a main concern in CR environments. We recall that there is always a trade-off between the performance of SUs and the protection of PUs in CR. The same conclusions apply when repeating the same experiment with the (non-cooperative) sense-before-transmit approach and scenario in Figure 4.1 (see results in Figure 4.17). That is, observed better throughputs in Figure 4.17 result directly from a poorest protection of PUs, which is not a tolerable situation in CR environments. In Figure 4.16-b, we observe higher standard deviation values than in Figure 4.16-a. This situation is due to the random positioning of twenty additional SUs in the scenario in Figure 4.1, as already discussed when analysing the results depicted in Figure 4.11 and Figure 4.12.



a) Scenario in Figure 4.1



b) Scenario in Figure 4.1 with 20 additional secondary users randomly located

Figure 4.16. Variation in aggregate throughput when compared to COSBET-MAC with no prediction capabilities

Finally, Figure 4.18 depicts the results that are obtained when scenario in Figure 4.1 is modified such that the coverage areas of the PUs include all the SUs. In this case, there are no hidden PUs and, consequently, FIBASC has no effect on the achieved PU protection and, thus, becomes redundant. We observe that there is only a slight degradation in communication performance, essentially due to the inclusion of additional bits in already existing control frames (see Table 4.2), which indicates that FIBASC results in negligible overhead.

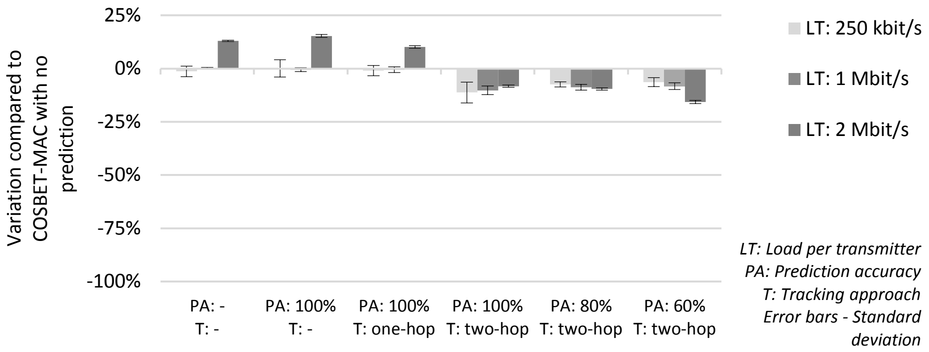


Figure 4.17. Variation in aggregate throughput of a generic sense-before-transmit approach when compared to COSBET-MAC with no prediction capabilities

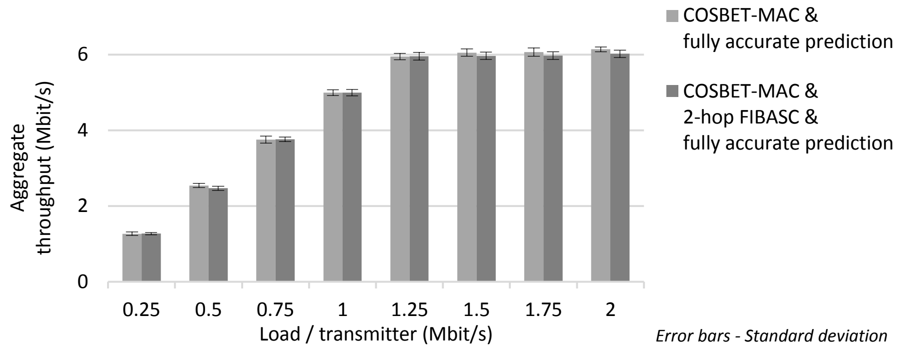


Figure 4.18. Aggregate throughput when there are no hidden PUs and the SUs have fully accurate prediction capabilities

Based on the results presented in the current section, we conclude that FIBASC, the filtering based on suspicious channels classification approach we propose, has potential to reduce the utilization of false spectrum opportunities and, therefore, to effectively contribute to increase the protection of PUs in CR scenarios with hidden PUs and SUs with learning capabilities based on observation and past experience.

4.5 Summary

This chapter started stating a problem that occurs in distributed CR networks that include hidden PUs and SUs with prediction capabilities based on learning through observation and past experience. It revealed that such prediction capabilities cannot be effectively utilized due to the hidden PU problem and, consequently, result in practical gains that are deceiving or even negative. The stated problem was successfully addressed through a novel scheme, named filtering based on suspicious channels (FIBASC) classification, which allows an effective utilization of learning outcomes that essentially result from local observation and past experience.

FIBASC includes two components. One of them enables tracking channels that probably suffer from the hidden problem in the perspective of each SU (i.e., the designated suspicious channels). For this purpose, a SU uses hints based on sensing and learning outcomes of other SUs in the network. Then, based on the outcomes of this classification as well as on past observation and learning of each SU, FIBASC tries to prevent a given transmitter-receiver pair from selecting channels with specific conditions that make the respective PUs more exposed to interferences from that pair. That is, channels that are suspicious at both ends of the communication link and channels that are suspicious on one side and the other side considers it as having no PU activity based on its own past observation and learning outcomes.

Additionally, FIBASC was successfully integrated with COSBT-MAC, the distributed CR protocol proposed in Chapter 3, and with a generic sense-before-transmit solution, which is representative of a common approach concerning existing distributed CR MAC protocols (see Chapter 2). The specific implementation of FIBASC we proposed in this chapter is a fully distributed MAC-level solution and assumes the utilization of a dedicated CCC for signalling and passive learning. Nevertheless, it can easily be envisaged for other types of CR scenarios, such as centralized CR networks.

The presented evaluation results show that FIBASC provides relevant gains concerning the protection of hidden PUs, enabling an effective utilization of prediction capabilities based on learning through observation and past experience. The performance that is delivered to the SUs slightly degrades, mainly as a direct and unavoidable consequence of higher PU protection (i.e., there are less accesses to false spectrum opportunities). Nevertheless, this cost remains within reasonable limits and is highly acceptable, particularly when taking into account the gains that are obtained in terms of PU protection, a main concern in CR scenarios. As a concluding remark, we can consider that COSBET-MAC equipped with FIBASC is an interesting MAC-level framework for supporting the evaluation and development of solutions related to learning based on past experience and observation for distributed CR scenarios. Most existing solutions in this area were not integrated with any CR MAC protocol and, therefore, were not properly evaluated concerning their practicality (see discussion in Section 2.7).

Chapter 5

Hybrid signalling for distributed Cognitive Radio

Opportunistic CR (Cognitive Radio) allows unlicensed wireless nodes to dynamically locate and access spectrum holes, i.e., licensed channels that are not being used by their incumbent users. Hence, sensing the spectrum is a key issue and performing it on a data frame basis maximizes the protection of PUs (Primary Users), as discussed in Chapter 2. Additionally, when the architecture of a CR network is distributed (i.e., ad-hoc), there are no central entities that are in charge of performing operations such as collecting and fusing data, and taking spectrum decisions. Therefore, the SUs (Secondary Users) must take their own decisions and cooperate with each other in order to exchange relevant information and coordinate access to the vacant channels. To achieve this goal, the utilization of a dedicated CCC (Common Control Channel) is a usual approach since it makes implementation and cooperation easier (see Section 2.5.3). However, a CCC can also saturate and become a bottleneck to communication performance, especially when handshake is performed on a packet basis.

This chapter defines a solution that performs signalling over the CCC and over the allocated data channels simultaneously, i.e., out-of-band (OOB) and in-band signalling, respectively. This MAC-level approach, named CORHYS (Cognitive Radio Hybrid Signalling), takes advantage of the strengths of OOB signalling, effectively limits the extent of the CCC saturation problem, and, therefore, has potential to improve the communication performance of SUs in distributed CR scenarios, particularly when they perform handshake and sensing on a data frame basis, and utilize a dedicated CCC. CORHYS also accounts for the possibility of the SUs having underlying prediction capabilities (see Section 2.7).

This chapter resulted in the following publication:

- Marinho, J. and Monteiro, E. (2015). CORHYS: Hybrid Signaling for Opportunistic Distributed Cognitive Radio. *Computer Networks*, 81, 19-42. doi: 10.1016/j.comnet.2015.01.019.

The remainder of this chapter is organized as follows. Section introduces the problem that CORHYS aims at addressing. Section 5.2 discusses related work and states the novel contributions of CORHYS. Section 5.3 describes CORHYS. Section 5.4 evaluates it through simulation. Finally, Section 5.5 draws final conclusions.

5.1 Introduction

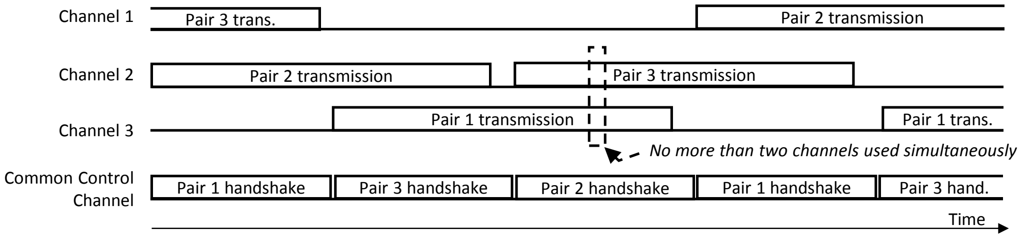
Opportunistic CR [Mitola and Maguire, 1999; Akyildiz et al., 2006] allows the SUs to opportunistically access licensed channels while they are not being accessed by the respective PUs, which results in multiple channels being accessed simultaneously by distinct users. The SUs require appropriate sensing schemes to precisely locate idle periods on the licensed channels (i.e., the so-called spectrum opportunities). They are also expected to have learning capabilities based on observation and past experience with the aim of optimizing spectrum decisions and maximizing the protection of PUs (see Section 2.7). In distributed CR networks [Akyildiz et al., 2009], the SUs also need to handshake with each other in order to meet on available data channels and exchange relevant information (e.g., sensing outputs). There is therefore a need for appropriate MAC level solutions that enable the SUs to exchange signalling information with each other.

As already described in Section 2.5.3, CR MAC protocols can be classified according to three generic categories: split phase; dedicated common control channel (CCC); and frequency hopping. Split phase and dedicated CCC approaches use a predefined CCC that is distinct from the data channels and, therefore, perform OOB signalling. With the split phase approach, time is divided into alternating signalling and data transmission phases. When using a dedicated CCC, the SUs must be equipped with at least two transceivers, being one of them dedicated to the control channel and the other(s) to data transmission. Consequently, the SUs are able to constantly transmit, receive, and overhear control information, achieving what Salameh et al. [2010] designate as passive learning. The third CR MAC category, i.e., frequency hopping, results in every SU hopping between the available channels according to given sequences. Each SU has its own hopping sequence and any two sequences have a minimum degree of overlapping in time designated as rendezvous. Frequency hopping implements signalling over the available data channels, i.e., in-band signalling.

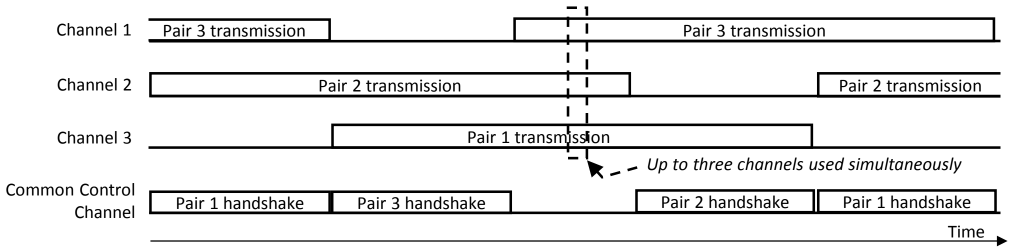
With split phase, frequency hopping, or any other solution based on a single radio per SU, the SUs are unable to transmit or receive signalling information during data transmission periods and, therefore, have stringent and challenging synchronization requirements for exchanging control and data packets in specific periods [Lo, 2011; Luo et al., 2009]. On the contrary, dedicated CCC-based approaches avoid the cost of synchronization and make broadcasting and overhearing control information (i.e., passive learning) easier, even during data exchange periods. Consequently, monitoring the busy status of other SUs and data channels in the neighbourhood is a simple task [Mo et al., 2008]. Globally, OOB signalling through a dedicated CCC is easy to implement, simplifies the design of CR MAC proposals, and, therefore, results in one of the most popular approaches for distributed CR MAC design (see Section 2.6.1). Nevertheless, a dedicated CCC can also saturate and become a performance bottleneck [Luo et al., 2009; Nezhadal et al., 2012; Ren et al., 2012].

This chapter proposes CORHYS, a solution to address the CCC saturation problem that affects distributed opportunistic CR MAC solutions that are based on a dedicated CCC, perform handshake on a packet basis, and sense the selected channels before any data transmission (i.e., that follow a sense-before-transmit approach), which is a common approach for existing CR MAC solutions (see Section 2.6.1). Globally, CORHYS is a hybrid solution that combines OOB and in-band signalling. The former simplifies implementation and naturally supports passive learning since it is based on a dedicated CCC. The latter enables increasing the utilization efficiency of available channels since it reduces the CCC saturation problem.

CORHYS aims at addressing the type of CCC saturation problem that is illustrated in Figure 5.1 and that limits the maximum number of data channels that can be utilized simultaneously in a CR network. This problem prevents taking full advantage of opportunistic CR. The upper limit for the number of channels that can be used simultaneously is defined by the ratio between average data channel access time and average handshake time. In Figure 5.1, we assume that there are three neighbouring transmitter-receiver pairs and three available data channels, channel negotiation is performed on a data frame basis, all the data frames have the same length, and transmitters have always data to transmit. When the mentioned ratio is higher than one and lower than or equal to two, no more than two channels are accessed simultaneously, which is inefficient since three channels are available and three SUs have data to transmit (see Figure 5.1-a). That is, increasing the number of channels beyond two does not result in any performance improvement since no more than one channel remains allocated upon the conclusion of a handshake process. When the mentioned ratio is higher than two and lower than or equal to three, the limit to the number of channels that are accessed at the same time rises to three (see Figure 5.1-b). Consequently, the overall performance of the SUs increases and the CCC does not result saturated. We recall that one of the effects of PU activity in CR scenarios consists in making the number of effectively available channels variable over time.



a) Transmission time to handshake time ratio ∈]1, 2]



b) Transmission time to handshake time ratio ∈]2, 3]

Figure 5.1. Common control channel saturation problem

To the best of our knowledge, CORHYS is the first MAC-level solution for distributed opportunistic CR networks that addresses the dedicated CCC saturation problem through a hybrid approach that combines OOB signalling, in-band signalling, multi-frame transmission, and sensing on a data frame basis, and that takes into account the possibility of the SUs having underlying prediction capabilities. For instance, none of the thirty CCC design schemes considered by Lo [Lo, 2011] follow a hybrid approach that combines in-band and out-of-band signalling, and all the dedicated CCC-based schemes it mentions are exclusively based on the out-of-band approach. With CORHYS, the SUs use OOB signalling for the exchange of relevant information, passive learning, and negotiation of multi-frame channel reservation. In-band signalling is considered during channel access periods for PU protection.

5.2 Related work and contributions

Many distributed CR MAC proposals based on a dedicated CCC make channel allocation on a data frame basis (see Chapter 2). Therefore, based on the previous discussion about the CCC saturation problem that Figure 5.1 illustrates, their efficiency in using the available channels depends on the sizes of the transmitted data frames. For example, Mo et al. [2008] conclude that using a dedicated CCC performs better than other approaches only when data frames are large. In fact, when the ratio between average data channel allocation time and average handshake time is not higher than one, multichannel access provided by CR degrades to single-channel access. Therefore, the CCC saturation problem that is illustrated in Figure 5.1 can be addressed allowing the transmitters to allocate channels for longer periods and, therefore, to access the CCC less frequently for OOB handshake. This approach increases transmission time to handshake time ratio and, consequently, the number of channels that can be allocated simultaneously by distinct transmitter-receiver pairs. In order to access a channel for a longer time, one can consider allocating it to transmit several frames for a given destination instead of making handshake on a single frames basis.

Lei et al. [2012] mention three strategies that enable improving performance in wireless networks, which is accomplished mainly via control overhead reduction, and that enable achieving this goal: concatenation, which concatenates multiple MAC frames into a super frame; packing, which combines multiple MAC frames into a single and longer MAC frame with a single header; and multi-frame transmission. The first two approaches result in more complex protocols, require higher processing times, have larger frame error rates, and make the loss of a longer frame result in the loss of multiple frames [Lei et al., 2012; Xiao Y. , 2004]. Additionally, they also increase the probability of harmful interference to PUs in CR networks since channel access time and, consequently, time between sensing operations increase with the lengths of the frames. The works of Bhushan and Murthy [2013], Liu et al. [U.S. Patent No. 8,204,005, 2012], Xiao [2004], and Ferré et al. [2008] are examples that include concatenation and packing features. The concept of aggregated frames is also a core element of IEEE 802.11n for higher throughput [Ferré et al., 2008].

Concerning multi-fame transmission, Lei et al. [2012] state that this approach is more practical than concatenation and packing. It is also more appropriate for CR networks since it enables implementing a sense-before-transmit approach (i.e., sensing the targeted licensed channel before the transmission of each data frame) such as many existing CR solutions do (see Section 2.6.1). That is, it enables preserving easily the level of protection of PUs that is achieved with common single-frame transmission strategies while improving communication performance. There are several non-CR MAC solutions that enable a wireless node to transmit multiple frames after it gains access to a channel, such as those that Zhao et al. [2005], Sadeghi et al. [2005], Biaz and Wu [2008], Choi and Nettles [2005], So and Vaidya [2004], and Lei et al. [2012] propose. The last two solutions consist in multichannel MAC protocols.

We can also mention the contention-based channel access mechanism of IEEE 802.11e, i.e., the so-called enhanced distributed coordination function (EDCF), since it includes a feature, named contention-free burst (CFB), which allows a node to transmit multiple MAC frames up to a defined duration limit [Choi et al., 2003; Suzuki et al., 2006; Al-Karaki and Chang, 2004]. EDCF is an enhancement to legacy IEEE 802.11 DCF (Distributed Coordination Function) and IEEE 802.11e is an amendment that defines a set of quality of service enhancements for IEEE 802.11. In their works, Choi et al. [2003] and Suzuki et al. [2006] evaluate the utility of the CFB feature. Concerning the few existing CR MAC solutions with multi-frame transmission features per channel access, we can cite the works of Jeon et al. [2012] and Ren et al. [2014]. Such as CORHYS, both target distributed CR networks.

A frequent approach in opportunistic CR consists in sensing the selected channel before transmitting each data frame in order to verify if it is free of any PU activity and if the operation is allowed to proceed. This is the so-called sense-before-transmit approach (see Section 2.5.2). When a channel is reserved for transmitting multiple data frames, the channel being accessed still requires to be sensed between successive data frame transmissions in order to ensure its availability. Additionally, signalling between the transmitter and the receiver must be performed in-line, i.e., on the allocated data channel, during access time in order to alleviate the utilization of the CCC. The main objective is allowing other neighbouring pairs to negotiate channel access meanwhile. It is worth mentioning that dedicating a radio/transceiver for operating the CCC makes the SUs keep their ability to receive, overhear, and learn out-of-band information from neighbours during data channel access times. That is, a SU is able to perform in-band and OOB signalling simultaneously during data channel access time. Several solutions have already been proposed to handle signalling and data transmission over the same channel (i.e., in-band signalling). For instance, IEEE 802.22 [IEEE 802.22 Working Group on Wireless Regional Area Networks, 2013] uses a logical in-band channel, Chowdhury and Akyildiz [2008] piggyback sensing information over data transmission, and the proposal of Zhang and Su [2011] dynamically allocates the CCC from available data channels.

Several authors consider that PUs can tolerate a limited amount of interference time. For example, in the work of Nezhadal et al. [2012], the channels are reserved for fixed periods, being the length of these periods such that if a PU appears it can tolerate the resulting interference. Zhang and Su [2011] assume that the SUs can continuously transmit on a data channel up to a given time threshold. In the work of Wang et al. [2011a], when the expected transmission time for a pair is longer than a specified limit, then, the data frame is fragmented in various shorter frames. Ansari et al. [2013] designate the time required for having the need to sense a channel in a multi-frame transmission as the channel probing time, relating it to the interference time that does not cause harmful interferences to PU transmission. More frequent sensing operations result in less PU outage but also consumes more energy [Jeon et al., 2012].

It is worth mentioning that some authors also propose alternatives to the aforementioned sense-before-transmit approach. For example, Jeon et al. [2012] apply the concept of opportunistic sensing, which consists in having the SUs performing sensing operations any time they have an opportunity (i.e., no data frames to transmit and no channels waiting for urgent sensing). With this approach, the SUs maintain a list of empty channels and, consequently, do not sense any channel before each data frame transmission. In this case, channel selection is directly performed on the list of empty channels and, therefore, experiences delays shorter than when performing sensing immediately before transmission. In the proposal of Jeon et al. [2012], since the SUs can only sense a single channel at a time, they also share sensing outputs with each other in order to obtain recent results for as many channels as possible.

Existing solutions that include multi-frame transmission, a key feature of the MAC-level CR solution the current chapter proposes (i.e., CORHYS), and that do not target CR networks are not concerned with PU activities, even when they have multichannel access features, which is the case of the solutions that So and Vaidya [2004], and Lei et al. [2012] define. Therefore and in contrast with CORHYS, they do not have to cope with a variable number of channels and with the detection of PU activities. Regarding the few existing CR MAC solutions that have multi-frame transmission features, they also have substantial differences and some limitations when compared to CORHYS. For instance, Ren et al. [2014] assume in their work that the status of a channel regarding PU activity remains unchanged during an entire channel access slot and, therefore, they do not cope with the possibility of PU appearance during multi-frame access, which is a limitation in practical terms. The same observation applies to the proposal of Jeon et al. [2012]. On the contrary, CORHYS performs sensing before the transmission of each data frame, even during multi-frame channel access, and includes an in-band signalling scheme that enables the transmitter and the receiver to cooperatively evaluate the availability of the channel they are accessing. We also note that, on the contrary of most existing CR proposals, CORHYS takes into account the possibility of the SUs having underlying prediction capabilities (see Section 2.7).

Split phase and any time-slotted-based solution require network-wide time synchronization, which is not always feasible in practical terms, and Cormio and Chowdhury [2009] state that solutions that do not need time synchronization are particularly suited for distributed CR networks. Regarding CORHYS, it is based on a permanently operated dedicated CCC, on random spectrum access, i.e., on the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) principle [Cormio and Chowdhury, 2009], and on a sense-before-transmit approach. Simultaneously, it addresses the CCC saturation problem through a solution that does not affect practicality, being in-band signalling and multi-frame transmission its key components. The majority of existing distributed CR MAC solutions based on a dedicated CCC do not cope with the inherent CCC saturation problem (see Section 2.6.1). The hybrid signalling approach that this chapter proposes can also be considered as a guideline to enhance the performance of distributed CR proposals that are based on a dedicated CCC while preserving their main characteristics.

Concerning the detection of PUs, which is a core CR issue, some distributed CR solutions do not perform sensing on a data frame basis, which reduces PU detection efficiency when compared to the sense-before-transmit approach that CORHYS follows, and make some assumptions that raise practical issues. For instance, Ren et al. [2014] assume that all the SUs simultaneously sense all the data channels during each sensing period, which might require a considerable amount of time. On the other hand, some authors, such as Jeon et al. [2012], state that a node is able to sense at most one channel at a time and Ansari et al. [2013] argue that scanning a larger number of channels adds latency to communication and reduces throughput. Since a half-duplex radio is either in reception or transmission mode, it is not able to detect any activity during transmission periods. Besides, some popular sensing methods, such as energy detection, do not allow to make distinction between PU and SU activities (see Section 2.5.2).

To the best of our knowledge, there are no other distributed MAC-level solutions based on a dedicated CCC that address the CCC saturation problem through a hybrid approach that combines OOB signalling, in-band signalling, multi-frame transmission, and sensing on a data frame basis, and that takes into account the possibility of the SUs having underlying prediction capabilities.

5.3 Cognitive Radio hybrid signalling

This section starts defining the out-of-band component of CORHYS. This component incorporates most of the characteristics that are commonly used by existing CR MAC proposals that target distributed opportunistic CR networks, achieve OOB signalling over a dedicated CCC, and perform sensing and signalling operations on a data frame basis. We globally designate this approach as OOB handshake (see Figure 5.2). Since OOB handshake is a generic solution that is illustrative of the type of distributed CR solutions that CORHYS aims at enhancing, it is used as a comparison basis for evaluating CORHYS in Section 5.4. Then, we present the details of the in-band component of CORHYS, which consists of in-band signalling and multi-frame transmission during channel access time (see Figure 5.2). Finally, we define how CORHYS selects, during OOB handshake, the data frames to be transmitted and the channel to be accessed.

5.3.1 Out-of-band handshake

OOB handshake uses a dedicated CCC implemented in a frequency band free of PU activities and operated by a dedicated transceiver such as this is the case for a large number of existing CR MAC proposals [Lo, 2011]. Access to the CCC is achieved through a contention-based scheme similar to IEEE 802.11 (e.g., it includes sensing and random back-off periods). The mechanisms it includes for effective PU protection and spectrum sharing among the SUs utilize the broadcast nature and permanent operation of the dedicated CCC. That is, the SUs passively learn the status and actions of neighbours and channels by overhearing control frames on the CCC. Supplementary information can be purposely included in the control frames to let the neighbours know any relevant information and use it if needed. Figure 5.2 illustrates the basic operation of OOB handshake and, therefore, of the out-of-band component of CORHYS. It follows a sense-before-transmit approach in order to increase PU protection and, therefore, includes sensing time. The CCC is dedicated to a single transmitter-receiver pair during an entire negotiation time.

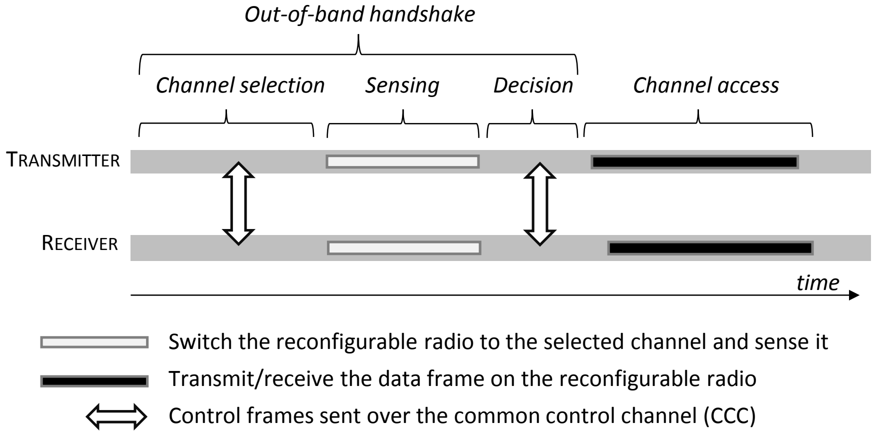


Figure 5.2. Out-of-band handshake

During the channel selection phase, the transmitter and the receiver exchange control frames over the CCC in order to select a channel with some favourable characteristics at both ends (e.g., not in use by neighbouring SUs). Overhearing on the CCC enables their neighbours to be aware of negotiation details. The basics of the selection phase are as follows. An idle SU that has data frames to transmit utilizes a random back-off timer that freezes any time the CCC is being accessed by neighbouring SUs, which it knows through the contents of the control frames it overhears on the CCC. When the back-off counter reaches zero, the transmitter sends the initial control frame of the channel selection phase to the receiver. Among other fields, this frame typically includes a list of candidate channels (e.g., channels not being used by neighbouring SUs) on the transmitter's side and a CCC reservation time, which is large enough for enabling the transmission of the remainder control frames without any contention. Then, if that initial control frame is correctly received, the receiver selects a channel that is feasible at both ends and provides this information back to the transmitter through another control frame.

When a three-way handshake process is used, such as with COSBET-MAC (see Chapter 3), the transmitter acknowledges the reply with a third control frame. Then, the transmitter and the receiver switch their reconfigurable radios, i.e., the radios that are dedicated to access the licensed channels, to the selected channel and start sensing it. Conclusions about its availability are drawn during the decision phase in Figure 5.2. This phase also includes the exchange of control frames and, consequently, the neighbours of the negotiating pair overhear the final decision and can record its details (i.e., allocated channel, allocation time, transmitter, and receiver). The selected data channel is accessed immediately without any contention if it is declared vacant by both the transmitter and the receiver. That is, contention only exists regarding the transmission of the initial control frame of OOB handshake on the CCC. Some existing CR MAC solutions assume that the SUs already know which channels are vacant when they start handshaking, such as with the solutions of Jeon et al. [2012] and Jia and Zhang [2009]. In this case, OOB handshake only incudes the channel selection phase. In the evaluation section (see Section 5.4), we also take this possibility into consideration and use it as a comparison basis for evaluating the gains provided by CORHYS.

As already mentioned in Section 5.1, the CCC saturation problem is an issue that seriously impacts the performance of OOB signalling-based CR MAC solutions. With the approach illustrated in Figure 5.2, the higher is sensing time the lower is channel access time to handshake time ratio and, therefore, the lower is channel utilization efficiency and communication performance. In scenarios with small average data frame lengths, a CR network might degrade to a single-channel access network despite the availability of various channels and, therefore, the possibility of concurrent accesses. The in-band component of CORHYS, which the next section describes, aims at addressing this issue while preserving the main characteristics and strengths of OOB signalling (e.g., ease of implementation and passive learning).

5.3.2 In-band signalling with multi-frame channel access

As described in the previous section, OOB handshake makes channel assignment on a frame basis and performs signalling over a dedicated CCC. Therefore, one-hop neighbouring transmitter-receiver pairs compete for the same CCC, which might result in CCC saturation, underuse of available data channels, and, consequently, performance penalty. We address this issue allowing the transmitter-receiver pairs to allocate channels for transmitting multiple frames, which results in larger access times, and to perform in-band signalling. The current section describes how CORHYS implements the channel access phase (see Figure 5.2) based on this strategy. Then, Section 5.3.3 provides details on how it selects the data frames to be transmitted and, consequently, allocation time.

When the decision phase of OOB handshake successfully concludes, the first data frame is immediately transmitted on the allocated channel as depicted in Figure 5.2. Then, sensing and in-band signalling are achieved before transmitting each one of the remaining data frames scheduled to be issued during channel access time (see Figure 5.3). This in-band approach, which we designate as in-band sense-before-transmit approach, enables alleviating the CCC. Since a transmitter might have imperfect sensing outcomes, the cooperation of the receiver in sensing increases the probability of PU detection and must be considered by CORHYS. CSI (Channel Sensed Idle) control frames are used to let the transmitter know if the receiver has sensed the channel as being vacant. Every data frame includes an additional bit, named MF (More frames), that let the receiver know if a frame is the last one to be received during current reservation time. If it is, the receiver does not enter a new sensing phase and does not reply with a CSI frame. Since CORHYS does not include any MAC-level retransmission scheme, CSI frames do not aim, therefore, at acknowledging the reception of data frames.

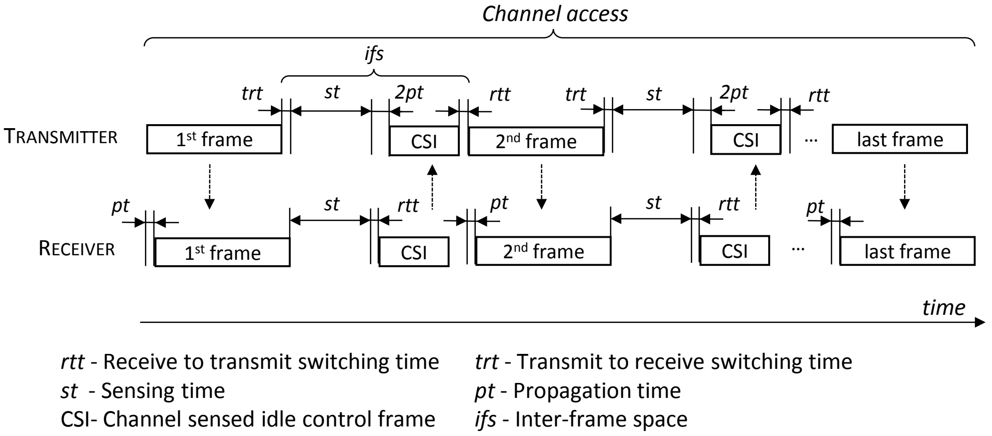


Figure 5.3. Transmission of multiple data frames with in-band signalling

In Figure 5.3, we observe that the transmitter senses the channel after issuing a data frame and the receiver does the same after receiving it. Then, the receiver transmits the respective CSI frame only if it concludes that the channel is vacant. For its part, the transmitter issues the next data frame only if it senses the channel idle and receives a CSI frame back. When a SU senses an activity or times-out while waiting for a CSI or a data frame, it gives up from further accessing the channel and concludes the current reservation time. In our in-band signalling scheme, if the transmitter fails detecting a PU activity and the receiver does not, no interference occurs since no CSI frame is sent back and the transmitter times-out. If the receiver fails detecting a PU activity, then, the CSI frame results in PU interference. Nevertheless, since CSI frames are very short (e.g., in the simulation section we use 200 bits), we can consider, as other authors do [Nezhadal et al., 2012; Zhang and Su, 2011; Wang et al., 2011a; Ansari et al., 2013; Wang et al., 2011b], that PUs can tolerate a limited amount of interference time and CSI transmission time does not exceed that threshold (see discussion in Section 5.2).

When a receiver-transmitter pair stops accessing the assigned channel prematurely (e.g., due to any sensed activity), the transmitter backs-off for a random period and starts OOB handshake again. Any sensed activity during channel access time is expected to be from PUs since neighbouring SUs refrain themselves from accessing channels already reserved by neighbours (see COSBET-MAC in Chapter 3 as an example). Additionally, a SU that overhears an ongoing OOB handshake process over the CCC invalidates any active channel reservation that it has recorded for the source or destination of the respective control frames. This approach enables the SUs to deal with the possibility of a channel access period ending earlier than it was announced during OOB negotiation, which can be the consequence of the detection of an activity during any in-band sensing time (see Figure 5.3) or a timeout while waiting for the reception of a data frame or CSI frame.

We recall that the approach that is illustrated in Figure 5.3 assumes that there is no MAC-level retransmission schemes and, therefore, CSI frames do not aim at acknowledging the reception of data frames. That is, retransmission is handled at higher protocol layers, which is a common approach in data communications. Nevertheless, if a MAC-level scheme is required, it is quite straightforward to adapt the proposed scheme in order to support it. In this case, the meaning of an issued CSI frame becomes that both no activity was sensed on the data channel and the received data frame was not corrupted. That is, CSI frames also act as acknowledgement frames. Additionally, on the receiver's side, the reception of the last data frame must be followed by a sensing phase (i.e., in order to verify that the data channel is still vacant) and by the transmission of a CSI frame such as what occurs with the data frames received previously (see Figure 5.3). With this variation, a data frame is removed from the MAC output queue of the transmitter only when the corresponding CSI frame is received back or a defined maximum number of retransmissions is reached.

In Figure 5.3, if a data frame is received corrupted and no activity was sensed on the data channel, it is also feasible to issue a CSI frame with a negative feedback in order to speed up the recovery process. In this case, if enough reservation time is left and if the transmitter has sensed the data channel idle, retransmission can proceed immediately instead of leaving the channel and entering out-of-band negotiation again. The first data frame to be transmitted is equally removed from the MAC output queue when the initial control frame of OOB handshake (see Figure 5.2) is transmitted without success (i.e., without any valid reply received back) for a defined maximum number of times.

If a transmitter has evidences that it is able to sense any PU activity on the accessed channel with high probability (e.g., the hidden PU problem is not an issue), which is not trivial to achieve in real deployments, then, the cooperation of the receiver in sensing can be omitted and CSI frames eliminated. In this case, we assume the availability of learning based on observation and past experience, access to geo-location databases, or other capabilities that are out of the scope of the work this thesis describes. In such situation, we can follow an alternative approach that is illustrated in Figure 5.4. That is, the transmitter decides to perform sensing alone and informs the receiver about this fact at the end of OOB handshake (i.e., through a specific field in the last control frame it transmits before multichannel access time). In this case, no MAC-level retransmission schemes can be supported since the receiver remains silent and, therefore, does not provide any feedback to the transmitter.

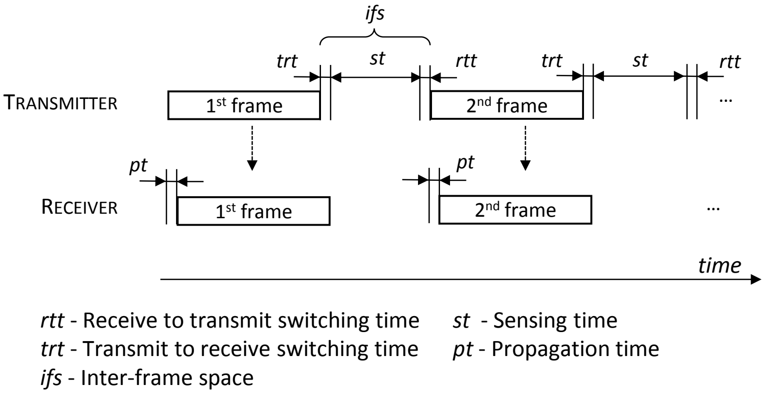


Figure 5.4. Transmission of multiple data frames without in-line cooperative sensing

The main advantage of the alternative depicted in Figure 5.4 consists in reducing inter-frame space and, consequently, enabling the transmission of more data frames during a given channel access period. Energy saving is another expected gain. The inter-frame space values in

Figure 5.3 and Figure 5.4 are defined by Equation 5.1 and Equation 5.2, respectively, being st the sensing time, pt the propagation time, cl the length of CSI frames in bits, br the bit rate, and rtt and trt the times required for the reconfigurable radio to switch from receive to transmit mode and vice-versa, respectively.

$$ifs = st + 2.pt + rtt + trt + cl / br \tag{5.1}$$

$$ifs = st + rtt + trt \tag{5.2}$$

Propagation time can be dynamically estimated if the SUs have appropriate capabilities (e.g., distance estimation based on received signal strength indication and on appropriate propagation models) or predefined (e.g., a fixed value based on the maximum transmission distance that is expected to occur). Inter-frame space is significantly smaller with the two in-band signalling solutions we propose (see Figure 5.3 and Figure 5.4) than with OOB handshake (see Figure 5.2) since a single CSI control frame is required at most and no contention or back-off periods exist.

Typical sensing time is in order of magnitude of several hundred or a few thousand microseconds (e.g., in Chapter 3, we used values of 0.5 and 1 milliseconds), and the overall contribution of the parameters of Equation 5.1 that are excluded from Equation 5.2 is in order of magnitude of a few tens of microseconds. Therefore, inter-frame space might reduce only slightly when the alternative in Figure 5.4 is applied. Additionally, the higher are the sizes of the data frames the lower is the perceptible effect of inter-frame space (see *ifs* in Figure 5.3 and in Figure 5.4). Therefore, the positive impact of the approach illustrated in Figure 5.4 on communication performance is expected to be small and, in some operating circumstances, negligible. Additionally, the number of data frames that might be transmitted in a given period is likely to neither suffer any increase. Illustrative results are presented and discussed in Section 5.4.

5.3.3 Multi-frame channel reservation

In distributed CR environments that are based on a dedicated CCC, if the data channels are allocated for more time than it is required to conclude *n* minus one OOB handshakes, then, *n* channels can be effectively accessed at the same time for data transmission by distinct neighbouring SUs, provided there are enough vacant channels (see Section 5.1). CORHYS increases channel reservation time through multi-frame access with in-band signalling, which was already described in Section 5.3.2. We now specify how the data frames to be included in a multi-frame channel access period (see Algorithm 5.1) and the channel to be accessed (see Algorithm 5.2) are selected during an OOB handshake process.

Inputs:

- Channels of type 1, channels the transmitter has no evidences that it is able to detect any PU activity on it;
- Channels of type 2, channels the transmitter has evidences that it is able to detect any PU activity on it;
- λ, upper limit for reservation time ($\lambda = \infty$ if not administratively defined);
- Ui, set of unreserved channels of type $i \in \{1, 2\}$;
- $\rho_i(x, d)$, computes the reservation time required to transmit the oldest x queued frames to destination d over channels of type $i \in \{1, 2\}$ (inter-frame space is defined by Equation 5.1 and Equation 5.2 for channels of type 1 and type 2, respectively);
- $\varphi(C, a)$, selects the channels in set C that are predicted to be free of any PU activity until the end of access time $a > 0$.

Output:

- d, destination of the oldest queued frame with a destination currently set as idle;
- Ai_t, set of channels of type $i \in \{1, 2\}$ that the transmitter considers as being candidate channels;
- k_i, number of frames to be transmitted over channels of type $i \in \{1, 2\}$;
- rt_i, reservation time over channels of type $i \in \{1, 2\}$.

```
if $d$ = no destination then return with no valid outputs
for i ← 1 to 2 do
    $n$ ← number of frames in queue with destination $d$
    while $n > 1$ and $\rho_i(n, d) > \lambda$ do $n \leftarrow n - 1$
[Version 1: underlying prediction capabilities are not supported/considered]
    $k_i \leftarrow n$
    $rt_i \leftarrow \rho_i(k_i, d)$
    $Ai_t \leftarrow Ui$
[end Version 1]
[Version 2: underlying prediction capabilities are supported/considered]
    $k_i \leftarrow n$
    while $k_i > 0$ and $\varphi(Ui, \rho_i(k_i, d)) = \varnothing$ do $k_i \leftarrow k_i - 1$
    $rt_i \leftarrow \rho_i(k_i, d)$
    if $k_i > 0$ then $Ai_t \leftarrow \varphi(Ui, rt_i)$ else $Ai_t \leftarrow \varnothing$
[end Version 2]
end for
return $d$, $A1_t$, $A2_t$, $k_1$, $k_2$, $rt_1$, and $rt_2$
```

Algorithm 5.1. Selection of candidate channels and number of frames to be transmitted during channel allocation time (executed by the transmitter)

Before transmitting the initial control frame of OOB negotiation (see Figure 5.2), the transmitter runs Algorithm 5.1 in order to determine the number of data frames to transmit during multi-frame channel access and, consequently, reservation time, as well as the set of channels it considers feasible for access (i.e., candidate channels) on its side of the communication link. Based on the control frames that are overheard on the dedicated CCC, a SU knows which neighbours are idle or engaged in any data channel access, either as transmitter or receiver, at any moment. Therefore, with CORHYS, a transmitter only starts handshaking with a given destination when it is set as idle. That is, it selects the first (i.e., oldest) data frame in the MAC output queue that has an idle destination. If all the frames in queue have destinations set as busy, then, it does not initiate handshake (see step 1 in Algorithm 5.1), backs-off, and makes a new attempt later.

Inputs:

- Ai_t, set of candidate channels of type $i \in \{1, 2\}$ that were selected by the transmitter (see Algorithm 5.1);
- Ai_r, set of channels of type $i \in \{1, 2\}$ that the receiver considers as being unreserved and, if prediction is enabled, with no predicted PU activity during reservation time rt_i, which was determined by the transmitter (see Algorithm 5.1);
- $S(X)$, selects a channel from channel set X using a given channel selection algorithm (e.g., uniform random selection).

Output: c, a channel selected for sensing/access.

```
1.  $C \leftarrow A2_t \cap A2_r$
2.  if $C = \varnothing$ then $C \leftarrow A1_t \cap A1_r$
3.  if $C = \varnothing$ then return selection failure
4.  $c \leftarrow S(C)$
5.  return $c$
```

Algorithm 5.2. Channel selection made by a receiver

The transmitter defines two distinct sets of candidate channels, named $A1_t$ and $A2_t$ in Algorithm 5.1 and Algorithm 5.2, in order to account for the possibility of applying the approach illustrated in Figure 5.4, and includes them in the initial control frame of OOB handshake (see the channel selection phase in Figure 5.2). We designate those types of channels as type 1 and type 2, respectively. Algorithm 5.1 also considers the possibility of SUs with prediction capabilities (i.e., Version 2 section in Algorithm 5.1), which details are out of the scope of this thesis. If we consider the possibility of not supporting the optimization illustrated in Figure 5.4, then, all the channels are of type 1 and the loop in Algorithm 5.1 (see step 2) does not go beyond the first iteration. Table 5.1 summarizes the parameters that are computed by the transmitter based on Algorithm 5.1. Some of them are also provided to the destination at the beginning of OOB handshake (e.g., through RTS frames if we use COSBET-MAC, the CR MAC protocol defined in Chapter 3).

Reservation times are defined as

$$rt = (b_{nf} + nf\,.\,cb)\,/\,br + (nf - 1)\,.\,ifs, \tag{5.3}$$

being nf the number of data frames to be transmitted during reservation time, b_{nf} the total number of data bits to be transmitted, cb the number of additional control bits required per data frame (i.e., headers and trailers), br the bit rate, and ifs the inter frame space, i.e., time in seconds elapsed between the end of transmission of a data frame and the start of transmission of the next data frame (see Figure 5.3, Figure 5.4, Equation 5.1, and Equation 5.2). Function $\rho_i(x, d)$ in Algorithm 5.1 is based on Equation 5.3.

Table 5.1: Parameters computed by the transmitter based on Algorithm 5.1

Alternative in Figure 5.4 supported	Alternative in Figure 5.4 not supported
k_1 and k_2	k_1
$A1_t$[a], $A2_t$[a], rt_1[a], and rt_2[a]	$A1_t$[a] and rt_1[a]

[a] Parameters that are also included as additional fields in the initial control frame of the channel selection phase (see Figure 5.2 and Algorithm 5.1).

Reservation times higher than n times OOB handshake time, being n the number of available channels, do not allow more data frames to be simultaneously transmitted. Until that threshold is reached, the communication performance of the SUs increases significantly with channel access time since there is a higher parallelism concerning spectrum utilization. That is, more SUs are able to transmit data frames simultaneously on distinct data channels, which increases the achieved throughput and reduces latency (i.e., the data frames leave the MAC output queues more quickly). Moreover, in-band signalling has less overhead than OOB handshake (see Figure 5.2) since it has less control frames, no contention, and no back-off periods (compare *ifs* in Figure 5.3 with *out-of-band handshake* in Figure 5.2). Therefore, these characteristics also contribute to improve communication performance, yet more modestly than increasing the number of channels that are accessed simultaneously in the CR network. Consequently, data channel access times that go beyond the mentioned threshold result in a slight increase in throughput, which is exclusively due to the fact that in-band signalling has less overhead than OOB handshake. They might also contribute to degrade latency and fairness between the SUs when they are excessively large since awaiting transmitters must wait more time for an unreserved channel to be available.

It follows from the final remark in the previous paragraph that Algorithm 5.1 also includes an upper limit that can be optionally defined in order to avoid the risk of excessive transmission delays and unfairness in given scenarios (see parameter λ and step 4 in Algorithm 5.1). This threshold cannot be exceeded if defined, unless it is not large enough to enable the transmission of a single data frame. If underlying prediction capabilities are considered (see Version 2 section in Algorithm 5.1), the number of frames to be transmitted might be further reduced in order to avoid null solutions (i.e., none of the predicted spectrum opportunities are large enough to support the defined reservation time). Since the maximum size of the MAC output queue and the maximum transfer unit (MTU) in use jointly define the upper limit for reservation time, it is not possible for a given SU to monopolize a specific channel indefinitely. Besides, PU activities cause channel access periods to end prematurely (i.e., when they are detected between the transmission of consecutive data frames) and, therefore, result in effective access times lower than computed access times. Therefore, defining a maximum channel access time limit might be a concern only when the maximum size of the MAC output queues and idle times on the data channels are both large. In Section 5.4.3, we further discuss this issue based on simulation results.

After receiving a control frame that includes the candidate channel sets and respective reservation times as defined by the transmitter based on Algorithm 5.1, a receiver runs Algorithm 5.2 in order to select which channel to access. If the alternative approach illustrated in Figure 5.4 does not apply, then, step 1 is skipped in Algorithm 5.2. In Algorithm 5.2, we observe that the channels that enable using shorter inter-frame spaces (i.e., channels of type 2), are selected in priority. The reservation time required for the selected channel is included in the control frames of the decision phase of OOB handshake (see Figure 5.2) and overheard by neighbours. Therefore, any SU is able to know which channels are being reserved in its neighbourhood at any time, the respective durations, and the identities of the SUs that have gained access to them.

If we consider that any kind of channel filtering scheme is utilized, such as FIBASC (see details in Chapter 4), expressions $A1_t \cap A1_r$ and $A2_t \cap A2_r$ in Algorithm 5.2 must be replaced by appropriate expressions. For instance, if the SUs apply FIBASC in order to account for the hidden PU problem when learning through observation and past experience is supported, the two mentioned expressions must be replaced by Algorithm 4.1 (i.e., parameter C in Algorithm 5.2 becomes C_c, the output of Algorithm 4.1). In this case, parameters C_t and C_r in Algorithm 4.1 become $A2_t$ and $A2_r$, respectively, when Algorithm 4.1 is used in step 1 of Algorithm 5.2. When applying it to step 2 of Algorithm 5.2, we use $A1_t$ and $A1_r$ instead.

5.4 Performance evaluation

This section aims at evaluating, through simulation, CORHYS in terms of its ability to make an effective utilization of the available channels and, consequently, increase the communication performance that is delivered to the SUs when compared to the commonly used OOB handshake-based approach. As a starting point and comparison basis, we use our implementation of COSBET-MAC (see Chapter 3), which is a representative instance of OOB handshake-based CR MAC protocols, i.e., CR MAC solutions that target fully distributed CR networks, follow a sense-before-transmit approach, and perform OOB signalling over a dedicated CCC on a single data frame basis. We implement our hybrid solution on top of it. With the concern of fair comparison when the SUs have variable destinations (see Section 5.4.6), COSBET-MAC was modified in order to select the oldest frame in the MAC output queue with a destination known to be idle, just as CORHYS does (see parameter d in Algorithm 5.1). This is a trivial modification since, with COSBET-MAC, the SUs are able to overhear control traffic on the dedicated CCC. Comparison is also made with the single-channel access (i.e., non-CR) approach, being IEEE 802.11 used to this end, and with the proposal of Jia and Zhang [2009], which is representative of CR MAC solutions that only include the channel selection phase in OOB handshake (see Figure 5.2).

5.4.1 Simulation setup

Simulation settings are similar to the ones Chapter 3 and Chapter 4 use. COSBET-MAC and, consequently, its CORHYS-based optimized version are implemented on the OMNeT++/MiXiM simulation platform [OMNeT++ Network Simulation Framework, 2010; MiXiM, 2010], being the most relevant settings for our discussion listed in Table 5.2. Some experiments employ variations of these settings. We specify them at the time they are used. The presented results are averaged over 15 runs of 300 seconds simulated time and with different seeds. In some of the experiments, we use the work of Jia and Zhang [2009] and IEEE 802.11 as comparison basis for determining the gains CORHYS provides in terms of communication performance. Therefore, the retry limit for transmitting the initial control frame of OOB handshake (see Figure 5.2) is set to seven for each channel access, which corresponds to the value we use for IEEE 802.11 short retry count, in order to make fair comparisons. For the same reason and as we do not consider MAC-level retransmissions of data frames, IEEE 802.11 long try count is set to one (the default value is four). We use the default simple path loss model of MiXiM and transmission power is set such that the transmission range is 100 meters on the CCC, on data channels, and for IEEE 802.11 nodes, independently of the operating frequencies in use.

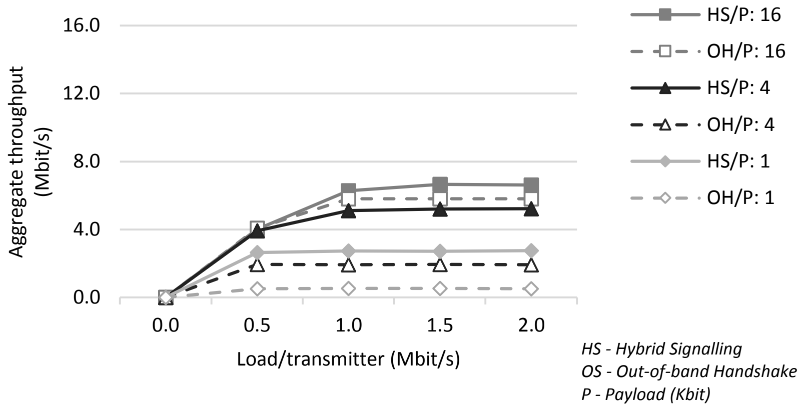
Each data channel is accessed by a dedicated PU with activities characterized by alternating idle and busy periods that are exponentially distributed with means 0.1 and 0.01 seconds, respectively, such as in the work of Issariyakul et al. [2009]. By default, we assume that the SUs have no prediction capabilities, which results in Version 1 section in Algorithm 5.1 being applied. For some experiments, we apply other PU activity characteristics and consider underlying prediction capabilities based on learning through observation and past experience (see Section 5.4.7). Since the simulation scenario consists in a square area with side length 50 meters, all the SUs are in range of each other, which is the most adverse scenario in terms of contention for network resources (i.e., CCC and data channels). The SUs are randomly placed with a uniform distribution. Mean load per transmitter varies up to 2 Mbit/s. Since data frame payload length has strong impact on performance due to the type of CCC saturation problem we address in this chapter, we consider 1 Kbit, 4 Kbit, and 16 Kbit data frame payload lengths. Time between arrivals of data to transmit is exponentially distributed with the parameter adjusted according to the targeted mean load.

Table 5.2: Simulation settings

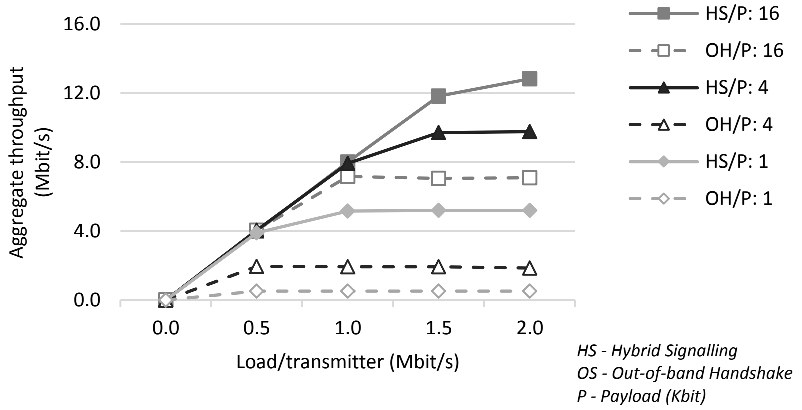
Parameter	Value	Remark
Size of the simulation area	50 m x 50 m	
Number of SU transmitters	8	
Number of SU receivers	8	
Positioning of the SUs	Uniform random	
Transmission range	100 m	
Simulation time	300 s	
Runs	15	
Number of channels	From 2 to 8	
Bit rate	2 Mbit/s	
Maximum transfer unit	18432 bits	Similar to IEEE 802.11.
Initial control frame retry limit per data channel access	7	IEEE 802.11 short retry count.
Channel switching time	10^{-4} s	Jia and Zhang [2009].
Transmit to receive time and receive to transmit time radio switch	10^{-5} s	Short Inter-frame Space (SIFS) value for the main IEEE 802.11 versions currently in use.
Sensing time	5×10^{-4} s	Fast sensing under one millisecond [IEEE 802.22 Working Group on Wireless Regional Area Networks, 2013].
Parameter λ in Algorithm 5.1	∞ (i.e., no access time limit defined)	
IEEE 802.11 long try count	1	Default value is 4.
IEEE 802.11 RTS-threshold	400 bits	
Channel Sensed Idle (CSI) frames length	200 bits	
Maximum MAC output queue size	50 frames	
Channel selection ($S(.)$ in Algorithm 5.2)	Uniform random	

5.4.2 Throughput and channel utilization efficiency

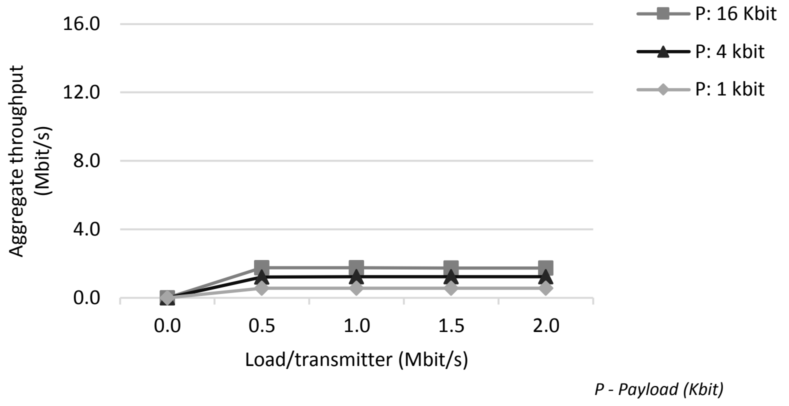
Figure 5.5 illustrates the aggregate throughput of all the SUs that is achieved when the sixteen SUs in the simulation scenario form eight fixed transmitter-receiver pairs, which results in disjoint traffic, load per transmitter varies up to 2 Mbit/s, and data frame payload size is 1 Kbit, 4 Kbit, and 16 Kbit.



a) 4 channels (8 Mbit/s aggregate bit rate)



b) 8 channels (16 Mbit/s aggregate bit rate)



c) Single channel access - IEEE 802.11 (2 Mbit/s bit rate)

Figure 5.5. Aggregate throughput

We provide, in Figure 5.5, results for CORHYS, i.e., the hybrid signalling solution this chapter proposes, for OOB handshake (i.e., COSBET-MAC), and for IEEE 802.11, which is representative of a single-channel access strategy. In order to ease readability, the standard deviation of aggregate throughput between the runs is not provided as error bars on data points, but instead as values in Table 5.3. We also consider two scenarios in terms of the number of available channels. With four channels, a total of 8 Mbit/s bit rate is available for eight transmitters, i.e., 1 Mbit/s per transmitter on the average. With eight channels, we get a total of 16 Mbit/s bit rate, i.e., 2 Mbit/s per transmitter on the average. Consequently, 8 Mbit/s and 16 Mbit/s define the upper limits for aggregate throughput with 4 and 8 channels, respectively. Since PU activity results in the number of effectively available channels varying over time, not all the channels might be available at any time.

Table 5.3: Standard deviation of aggregate throughput in kbit/s (data points in Figure 5.5)

Number of channels	Configuration	Load/Transmitter (Mbit/s)			
		0.5	1	1.5	2
4	HS[1]/P[2]: 1	32.3	47.3	61.6	54.3
	HS/P: 4	83.1	35.6	47.5	63.1
	HS/P: 16	63.6	57.9	52.6	46.4
	OH[3]/P: 1	31.8	16.3	8.5	22.9
	OH/P: 4	106.1	61.2	44.9	64.6
	OH/P: 16	77.3	14.4	33.1	46.3
8	HS/P: 1	32.0	25.6	46.6	44.9
	HS/P: 4	68.5	172.1	51.9	43.9
	HS/P: 16	39.2	92.4	110.5	130.5
	OH/P: 1	24.8	21.0	18.9	30.9
	OH/P: 4	87.6	79.6	80.2	101.0
	OH/P: 16	110.8	81.6	139.8	95.1
-	IEEE 802.11/P: 1	17.5	11.4	12.8	13.3
	IEEE 802.11/P: 4	18.7	21.1	21.3	20.8
	IEEE 802.11/P: 16	35.0	22.8	31.1	30.5

[1] Hybrid signalling (CORHYS).
[2] Data frame payload size (Kbit).
[3] Out-of-band handshake (COSBET-MAC).

Based on the results depicted in Figure 5.5, we conclude that OOB handshake and, consequently, the numerous existing CR MAC solutions that follow it (e.g., COSBET-MAC) require large frames for achieving a significant improvement of performance when compared to single-channel access solutions (see IEEE 802.11 data points in Figure 5.5-c). OOB handshake outperforms IEEE 802.11 significantly only when payload size is 16 Kbit. That is, it can deliver the gains expected from CR only in scenarios with large data frame payload sizes, which is rather limitative. With OOB handshake, we observe also that performance does not increase meaningfully when using eight channels instead of just four. That is, it results in a distributed CR solution that is not able to make an effective utilization of all the available channels. On the other hand, CORHYS increases performance significantly when compared to OOB handshake and to IEEE 802.11 under similar operating parameters (i.e., load per transmitter and data frame payload size). Moreover, communication performance delivered by CORHYS significantly increases when using eight channels instead of just four, independently of the lengths of the data frames, which demonstrates that it efficiently uses all the available channels. In Figure 5.5, we also observe that throughput increases with data frame payload size for the three solutions under analysis since less overhead (e.g., sensing time and control frames) exists for a given amount of transmitted data.

The gains that CORHYS (i.e., hybrid signalling) delivers are directly caused by its ability to take full advantage of all the available channels. Table 5.4 presents the maximum number of channels that were simultaneously accessed at any time during the simulation runs that produced the results depicted in Figure 5.5.

Table 5.4: Maximum number of channels simultaneously accessed (variable load per transmitter)

Number of available channels	Load per transmitter	CORHYS			Out-of-band handshake		
		P[a]: 1	P: 4	P: 16	P: 1	P: 4	P: 16
4	250 kbit/s	4	4	4	1	2	4
	500 kbit/s	4	4	4	1	2	4
	1 Mbit/s	4	4	4	1	2	4
	1.5 Mbit/s	4	4	4	1	2	4
	2 Mbit/s	4	4	4	1	2	4
8	250 kbit/s	8	5	5	1	2	5
	500 kbit/s	8	8	8	1	2	5
	1 Mbit/s	8	8	8	1	2	5
	1.5 Mbit/s	8	8	8	1	2	5
	2 Mbit/s	8	8	8	1	2	5

[a] P: Data frame payload size (Kbit).

In Table 5.4, we observe that the hybrid approach we propose is able to use all the available channels for multichannel access independently of data frame lengths. On the contrary, OOB handshake (i.e., COSBET-MAC) achieves poor efficiency in terms of channel utilization and gets results that strongly depend on the sizes of data frames. That is, it never achieves multichannel access with 1 Kbit data frame payload size, only uses up to two channels simultaneously with 4 Kbit payload size, and accesses a maximum number of five channels simultaneously with 16 Kbit payload size. For instance, if we focus on 2 Mbit/s load per transmitter, which is beyond saturation point for all the configurations under consideration and results in the MAC queues remaining filled, and make the number of channels vary from 2 to 8, we obtain the results presented in Table 5.5. This table provides results for CORHYS and for OOB handshake, and considers data frame payload sizes that are 1 Kbit, 4 Kbit, and 16 Kbit. Results in Table 5.5 reiterate the fact that CORHYS makes an effective use of the available channels and, therefore, increases performance as depicted in Figure 5.5.

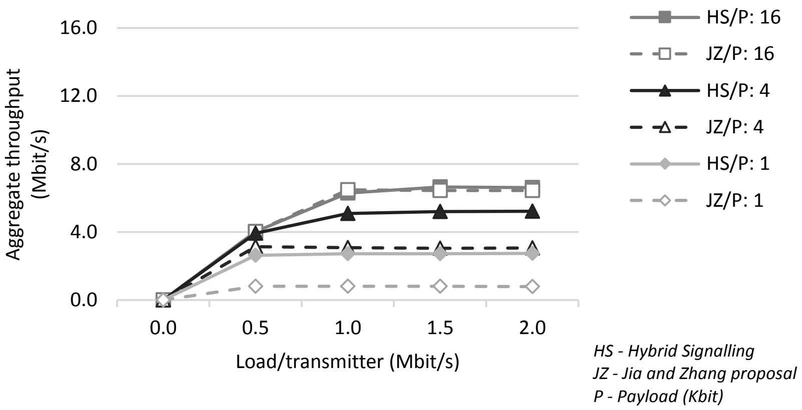
Table 5.5: Maximum number of channels simultaneously accessed (2 Mbit/s load per transmitter)

Number of available channels	CORHYS			Out-of-band handshake		
	P[a]: 1	P: 4	P: 16	P: 1	P: 4	P: 16
2	2	2	2	1	2	2
4	4	4	4	1	2	4
6	6	6	6	1	2	5
8	8	8	8	1	2	5

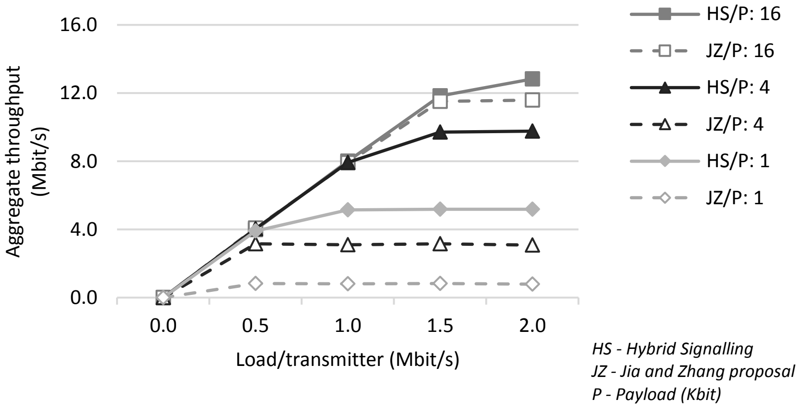
[a] P: Data frame payload size (Kbit).

We previously mentioned that there are some distributed CR MAC proposals that limit OOB handshake to the channel selection phase in Figure 5.2, namely because they assume that the SUs already know which channels are vacant at handshake time. Therefore, we also compare CORHYS with this type of approach. The proposal of Jia and Zhang [2009] is used to this end and Figure 5.6 presents the obtained results for aggregate throughput under the same simulation settings as defined previously. The standard deviation over the runs is provided in Table 5.6.

Having an updated list of vacant channels might be difficult to meet on real deployments. On the contrary, the sense-before-transmit approach, which our hybrid solution and OOB handshake follow, is more practical and effective for PU protection. Despite CORHYS performs sensing on a data frame basis, it globally remains the outperforming solution due to its ability to take full advantage of the available channels. Nevertheless, with 16 Kbit payload size the difference between our solution and the proposal of Jia and Zhang [2009] is largely smaller since the resulting transmission time enables the latter to effectively use all the available channels simultaneously (i.e., transmission time to handshake time ratio is higher than eight with the proposal of Jia and Zhang [2009]). Additionally, the proposal of Jia and Zhang [2009] has significantly lower handshake time than OOB handshake as it does not include PU detection time (i.e., sensing time).



a) 4 channels (8 Mbit/s aggregate bit rate)



b) 8 channels (16 Mbit/s aggregate bit rate)

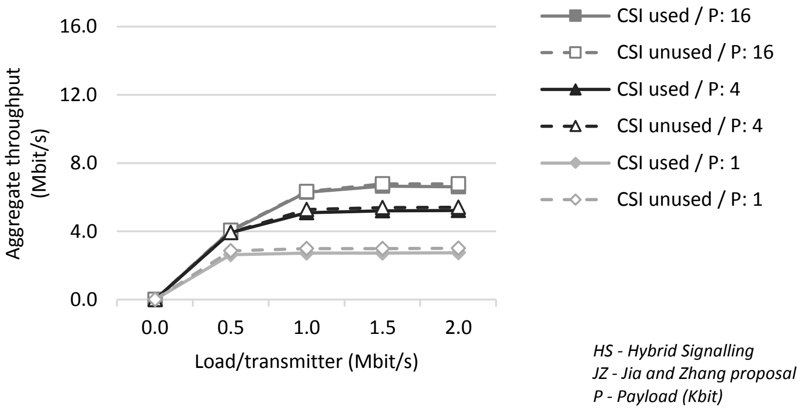
Figure 5.6. Comparison with the proposal of Jia and Zhang [2009] concerning aggregate throughput

Table 5.6: Standard deviation of aggregate throughput in kbit/s (data points in Figure 5.6)

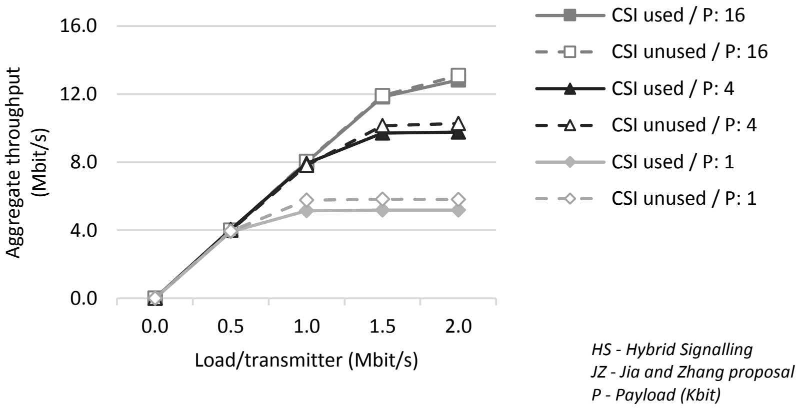
Number of channels	Configuration	Load/Transmitter (Mbit/s)			
		0.5	1	1.5	2
4	HS[1]/P[2]: 1	32.3	47.3	61.6	54.3
	HS/P: 4	83.1	35.6	47.5	63.1
	HS/P: 16	63.6	57.9	52.6	46.4
	JZ[3]/P: 1	28.4	40.3	35.2	32.8
	JZ/P: 4	85.2	79.2	71.1	97.0
	JZ/P: 16	100.3	41.4	10.1	6.1
8	HS/P: 1	32.0	25.6	46.6	44.9
	HS/P: 4	68.5	172.1	51.9	43.9
	HS/P: 16	39.2	92.4	110.5	130.5
	JZ/P: 1	24.7	41.6	43.4	36.2
	JZ/P: 4	114.8	107.6	152	101.3
	JZ/P: 16	68.5	172.1	51.9	43.9

[1] Hybrid Signalling (CORHYS).
[2] Data frame payload size (Kbit).
[3] Jia and Zhang [2009] CR MAC proposal.

Figure 5.7 illustrates, in terms of aggregate throughput, the effects of the optimization depicted in Figure 5.4 and that consists in omitting CSI frames when specific requisites are met (see Section 5.3.2). That is, when the transmitter has evidences that it is able to detect any PU activity on the accessed channel with high probability. In Figure 5.7, load per transmitter varies up to 2 Mbit/s and payload size is 1 Kbit, 4 Kbit, and 16 Kbit. Table 5.7 shows the standard deviation of aggregate throughput over the runs. As it was expected, the effects are not substantial since propagation time and CSI transmission time are low when compared to the other parameters that define inter-frame space during channel access time (see Equation 5.1). In fact, the positive effect of this optimization is more relevant for smaller frames, i.e., when more frames are sent for a given load. Nevertheless, this optimization has positive effects, as illustrated in Figure 5.4, and should be followed any time its utilization is feasible.



a) 4 channels (8 Mbit/s aggregate bit rate)



b) 8 channels (16 Mbit/s aggregate bit rate)

Figure 5.7. Impact of CSI control frames on aggregate throughput

Table 5.7: Standard deviation of aggregate throughput in kbit/s (data points in Figure 5.7)

Number of channels	Configuration	Load/Transmitter (Mbit/s)			
		0.5	1	1.5	2
4	CSI[1] used/P[2]: 1	32.3	47.3	61.6	54.3
	CSI used/P: 4	83.1	35.6	47.5	63.1
	CSI used/P: 16	63.6	57.9	52.6	46.4
	CSI unused/P: 1	32.0	25.7	28.1	37.9
	CSI unused/P: 4	80.0	26.4	55.5	42.3
	CSI unused/P: 16	102.9	58.0	60.9	65.9
8	CSI used/P: 1	32.0	25.6	46.6	44.9
	CSI used/P: 4	68.5	172.1	51.9	43.9
	CSI used/P: 16	39.2	92.4	110.5	130.5
	CSI unused/P: 1	80	45	58	62.6
	CSI unused/P: 4	66.9	173.4	53.8	64.2
	CSI unused/P: 16	144.7	107.1	130.7	58.9

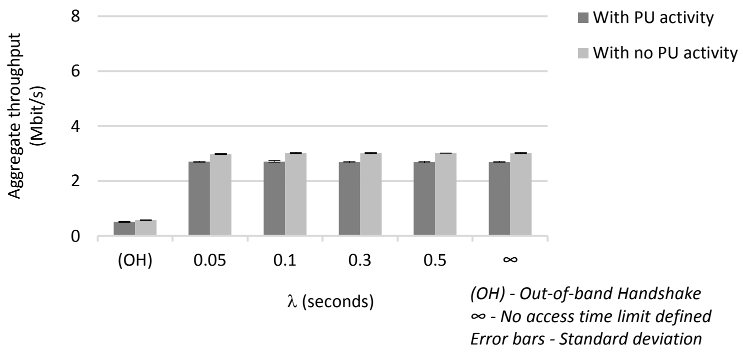
[1] Channel Sensed Idle control frames.
[2] Data frame payload size (Kbit).

5.4.3 Throughput and latency with channel access time limitation

Our default simulation settings do not specify any upper limit for channel reservation time (see parameter λ in Table 5.2 and in Algorithm 5.1). However, in Section 5.3.3 we stated that excessively large access times do not result in a major increase of throughput and might contribute to degrade latency and fairness between the SUs. Figure 5.8, Figure 5.9, Figure 5.10, Figure 5.11, and Table 5.8 present some results that enable evaluating this issue as well as the gains expected from CORHYS concerning latency and fairness, which was not done yet. For this purpose, we set load per transmitter to 2 Mbit/s, use four channels, i.e., less than the number of transmitters in order to always have SUs awaiting for unreserved channels, and make parameter λ vary from 0.05 seconds to 0.5 seconds.

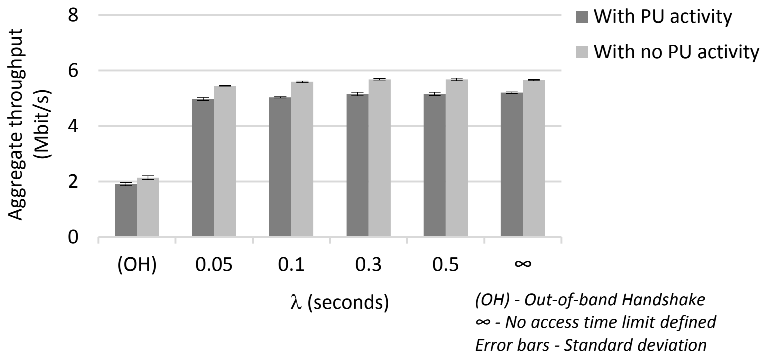
For a comparison basis, we also include results for OOB handshake and for CORHYS without any channel access limit defined (i.e., $\lambda = \infty$). Since access time is limited by the maximum size of MAC output queues (see discussion in Section 5.3.3), we consider queues with limits of 50 and 400 frames. That is, the default size in our simulation settings (see Table 5.2) and a larger size, respectively. Since PU activities reduce the effective average duration of access times (see related discussion in Section 5.3.3), we consider scenarios with and without PU activities too. As our implementation of CORHYS does not implement any scheme for managing the MAC output queues such that priority is given to new packets (e.g., discarding older packets when the buffer gets full or when they are considered outdated), a packet remains buffered until it is dispatched.

Figure 5.8 and Figure 5.9 present the obtained results concerning aggregate throughput and the latency of received frames, respectively, when maximum queue size is 50 frames, i.e., when multi-frame access is limited to 50 data frames. The error bars show the standard deviation between the 15 runs.



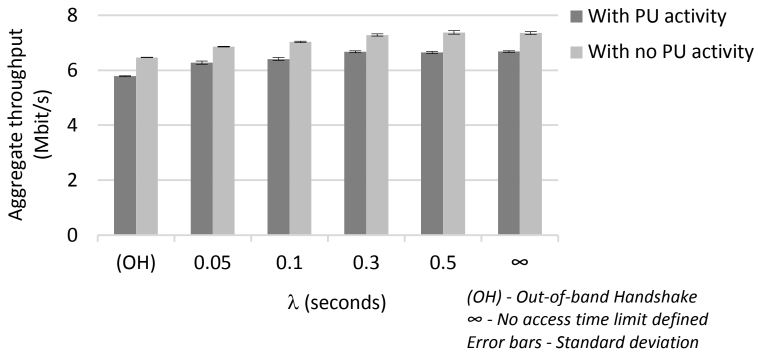
(OH) - Out-of-band Handshake
∞ - No access time limit defined
Error bars - Standard deviation

a) Payload size: 1 Kbit



(OH) - Out-of-band Handshake
∞ - No access time limit defined
Error bars - Standard deviation

b) Payload size: 4 Kbit

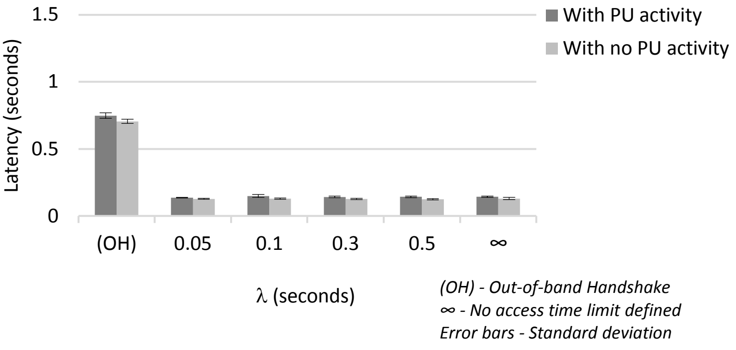


(OH) - Out-of-band Handshake
∞ - No access time limit defined
Error bars - Standard deviation

c) Payload size: 16 Kbit

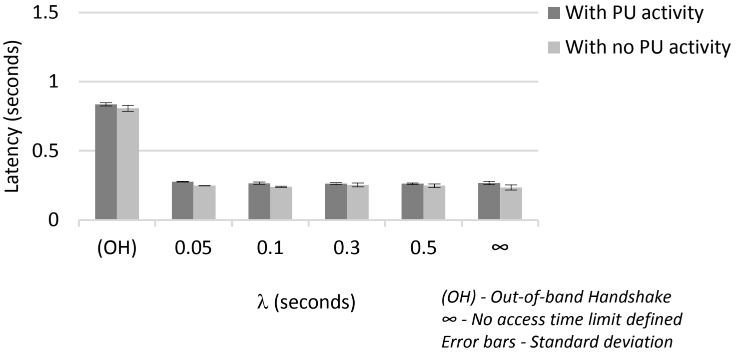
Figure 5.8 Impact of parameter λ (upper limit for channel reservation time) on aggregate throughput (2 Mbit/s load per transmitter, 4 channels with 8 Mbit/s aggregate bit rate, and MAC output queues with 50 frames maximum size)

We observe that throughput increases slightly in Figure 5.8 and latency decreases slightly in Figure 5.9 with the value of parameter λ increasing, which is essentially noticeable with 16 Kbit data frame payload size. Since with our simulation settings the four channels can be utilized simultaneously when channel access time is 0.05 seconds (i.e., 0.05 seconds is higher than four times out-of-band handshake duration), this gain is due to the already mentioned lower overhead of in-band signalling (see Section 5.3.3).



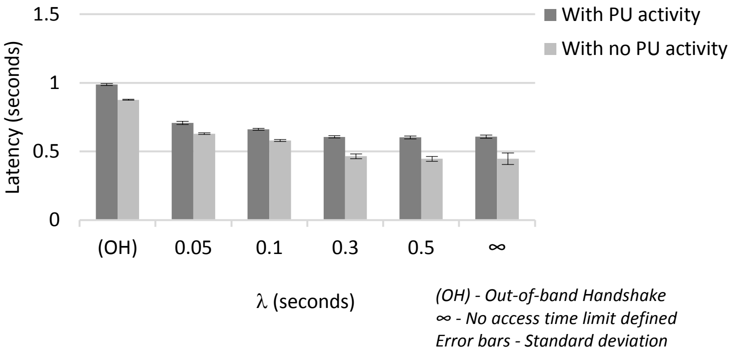
(OH) - Out-of-band Handshake
∞ - No access time limit defined
Error bars - Standard deviation

a) Payload size: 1 Kbit



(OH) - Out-of-band Handshake
∞ - No access time limit defined
Error bars - Standard deviation

b) Payload size: 4 Kbit



(OH) - Out-of-band Handshake
∞ - No access time limit defined
Error bars - Standard deviation

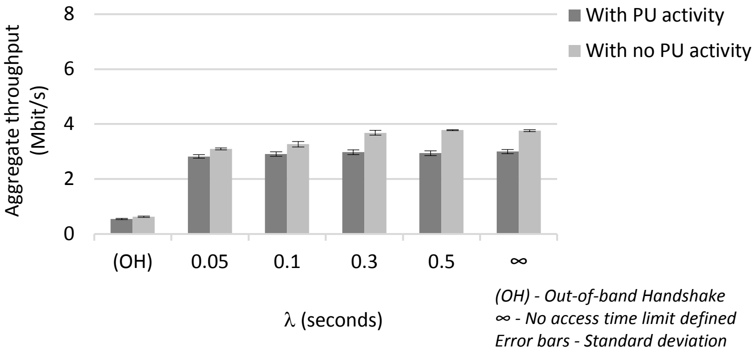
c) Payload size: 16 Kbit

Figure 5.9 Impact of parameter λ (upper limit for channel reservation time) on average latency (2 Mbit/s load per transmitter, 4 channels, and MAC output queues with 50 frames maximum size)

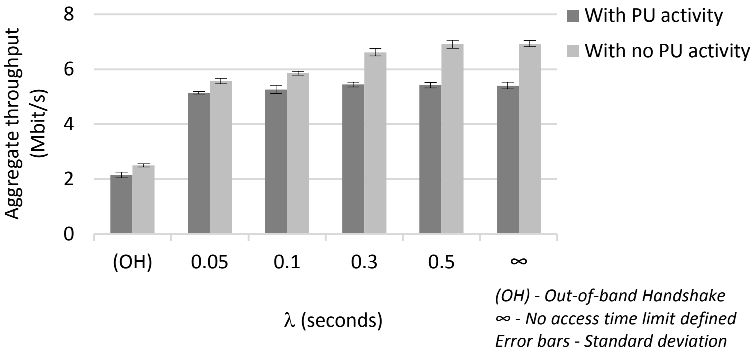
A multi-frame channel access can only include up to 50 data frames with maximum MAC output queue size set to 50 frames. Therefore, above the lowest values of parameter λ that are large enough to enable transmitting 50 frames per channel access, throughput and latency remain unchanged. With our simulation settings, when the value of parameter λ is set to 0.05 seconds, 0.1 seconds, or 0.3 seconds, and data frame payload size is 1 Kbit, 4 Kbit, or 16 Kbit, respectively, multi-frame channel accesses are still not large enough in time to include 50 frames. In Figure 5.8 and Figure 5.9, we observe that throughput and latency improve when there are no PU activities, which is expected since the data channels are always vacant. When compared to OOB handshake, CORHYS performs better in terms of both throughput and latency, independently of the value of parameter λ. Hence, we can conclude that with maximum queue size set to 50 frames, defining a limit to maximum channel access time does not result in any gain concerning throughput and latency.

With the maximum size of MAC output queues set to 400 frames (see results in Figure 5.10 and Figure 5.11), the number of data frames transmitted per multi-frame channel access can grow up to 400. This limit is reached if the MAC output queue is full and all the queued frames have the same destination when reservation time is computed (see parameters rt_i and n in Algorithm 5.1). Higher access times are required to allow multi-frame channel accesses to include up to 400 data frames instead of just 50. In Figure 5.10, we observe that aggregate throughput increases slightly with the value of parameter λ, which is especially perceptible with 16 Kbit data frame payload size or when there are no PU activities that prematurely interrupt multi-frame channel accesses.

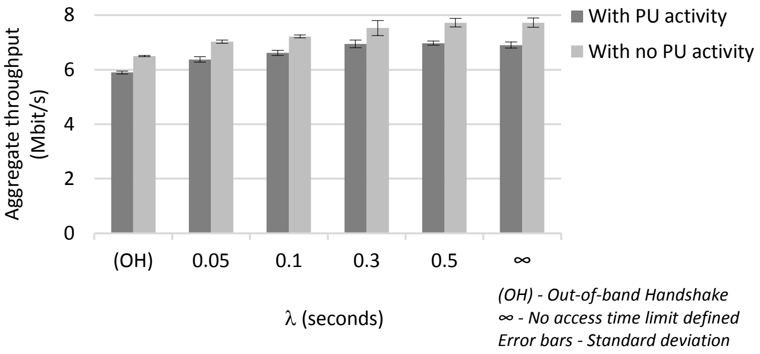
Concerning latency when maximum MAC output queue size is 400 frames (see Figure 5.11), we must make the distinction between the scenario with PU activities and the scenario with no PU activities on the data channels. When there are PU activities, which is expected to occur in CR environments, latency starts decreasing slightly and, then, remains stable as the value of λ increases. The main reason is that PU activities cause multi-frame channel accesses to end prematurely and, therefore, reduce their average duration, even when no maximum channel access time limit is defined (i.e., when $\lambda \neq \infty$). When there are no PU activities, channel accesses are not terminated prematurely and, therefore, their effective lengths are higher on the average. In this case, we observe that latency starts decreasing slightly as λ increases and, then, increases, which is particularly visible with 1 Kbit and 4 Kbit payload sizes. However, CORHYS still outperforms OOB handshake in terms of throughput and latency, even when no limit is defined for maximum channel access time and maximum MAC output queue size is large (i.e., when it equals 400 frames).



a) Payload size: 1 Kbit



b) Payload size: 4 Kbit



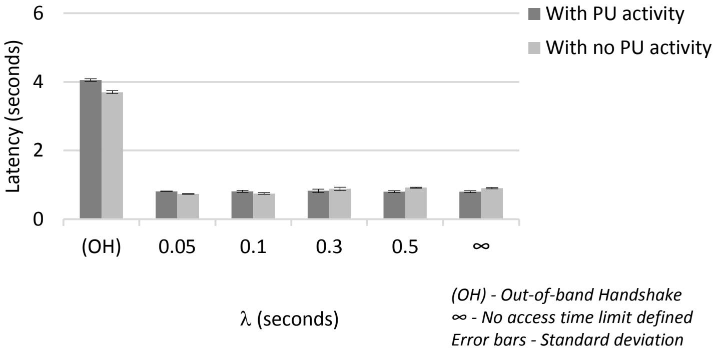
c) Payload size: 16 Kbit

Figure 5.10 Impact of parameter λ (upper limit for channel reservation time) on aggregate throughput (2 Mbit/s load per transmitter, 4 channels with 8 Mbit/s aggregate bit rate, and MAC output queues with 400 frames maximum size)

Higher channel access times might raise fairness issues between the transmitter-receiver pairs, even when no significant degradation is noticeable in terms of average throughput and average latency. Consequently, we determine how similar throughput and latency are among the pairs using Jain's fairness index [Jain et al., 1984], which is defined as

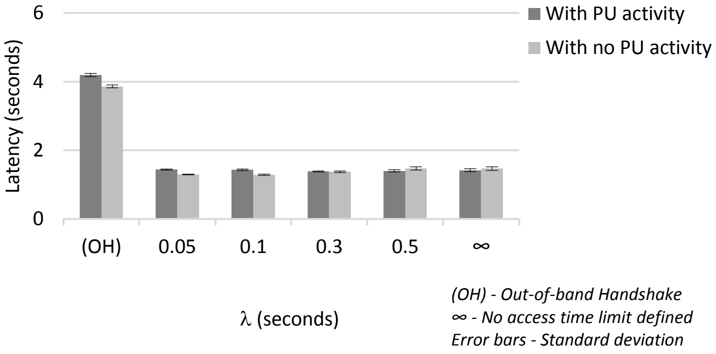
$$f(x_1, x_2, \dots, x_n) = \left(\sum_{i=1}^{n} x_i\right)^2 / \left(n \sum_{i=1}^{n} x_i^2\right), \qquad (5.4)$$

being n the number of competing pairs and x_i the performance metric under evaluation (i.e., throughput or data frame latency) of pair i. The value of this index is between $1/n$ and 1, which corresponds to absolute unfairness (i.e., all pairs except one have zero throughput or latency) and absolute fairness (i.e., all pairs have the same throughput or latency), respectively.



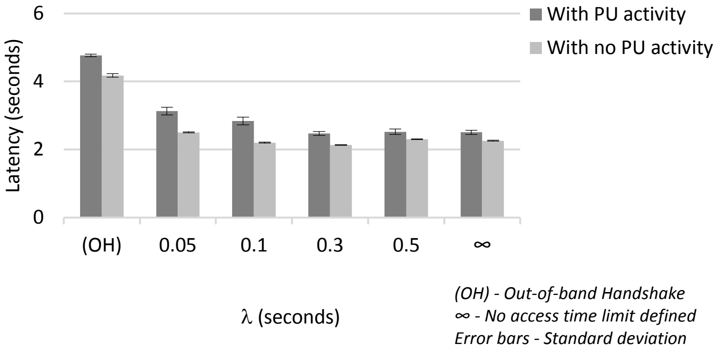
(OH) - Out-of-band Handshake
∞ - No access time limit defined
Error bars - Standard deviation

a) Payload size: 1 Kbit



(OH) - Out-of-band Handshake
∞ - No access time limit defined
Error bars - Standard deviation

b) Payload size: 4 Kbit



(OH) - Out-of-band Handshake
∞ - No access time limit defined
Error bars - Standard deviation

c) Payload size: 16 Kbit

Figure 5.11 Impact of parameter λ (upper limit for channel reservation time) on average latency (2 Mbit/s load per transmitter, 4 channels, and MAC output queues with 400 frames maximum size)

Table 5.8 presents the fairness indexes of the results that were obtained with CORHYS and are depicted in Figure 5.8, Figure 5.9, Figure 5.10, and Figure 5.11. In order to improve readability while providing enough details to draw appropriate conclusions, we use five distinct ranges instead of absolute values.

Table 5.8: Data frame latency and throughput fairness

MQL[a]	λ (sec.)	Latency						Throughput					
		P[b]: 1 Kbit		P: 4 Kbit		P: 16 Kbit		P: 1 Kbit		P: 4 Kbit		P: 16 Kbit	
		PA[c]	NPA[d]	PA	NPA	PA	NPA	PA	NPA	PA	NPA	PA	NPA
50	0.05	A	A	A	A	A	A	A	A	A	A	A	A
	0.1	A	A	A	A	A	A	A	A	A	A	A	A
	0.3	A	A	A	A	A	A	A	A	A	A	A	A
	0.5	A	A	A	A	A	A	A	A	A	A	A	A
	∞	A	A	A	A	A	A	A	A	A	A	A	A
400	0.05	A	A	A	A	A	A	A	A	A	A	A	A
	0.1	A	A	A	A	A	A	A	A	A	A	A	A
	0.3	A	D	A	B	A	C	A	C	A	C	A	B
	0.5	A	E	A	D	A	D	A	E	A	E	A	D
	∞	A	E	A	D	A	D	A	E	A	E	A	D

[a] MQL: maximum MAC output queue length (frames)
[b] P: data frame payload size
[c] PA: PU activity on the channels
[d] NPA: no PU activity on the channels

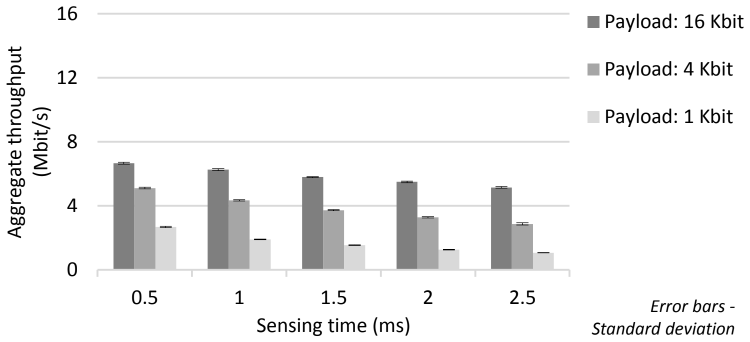
A: Jain's fairness index ∈]0.95, 1.0]
B: Jain's fairness index ∈]0.85, 0.95]
C: Jain's fairness index ∈]0.75, 0.85]
D: Jain's fairness index ∈]0.65, 0.75]
E: Jain's fairness index ∈]0.5, 0.65]

In Table 5.8, we observe that fairness indexes remain above 0.95, which corresponds to level A, except when maximum MAC output queue size is set to 400 frames and there is no PU activity on the data channels. The reasons are the same as previously stated when discussing the results in Figure 5.8, Figure 5.9, Figure 5.10, and Figure 5.11. In Table 5.8, we also observe that parameter λ should be set to a value below 0.3 seconds if we target fairness indexes above 0.85 (i.e., levels A and B) when maximum MAC output queue size equals 400 frames and there is no PU activity on the data channels. In such circumstances, not defining a channel access limit results in a degradation of fairness between the transmitter-receiver pairs, for both latency and throughput.

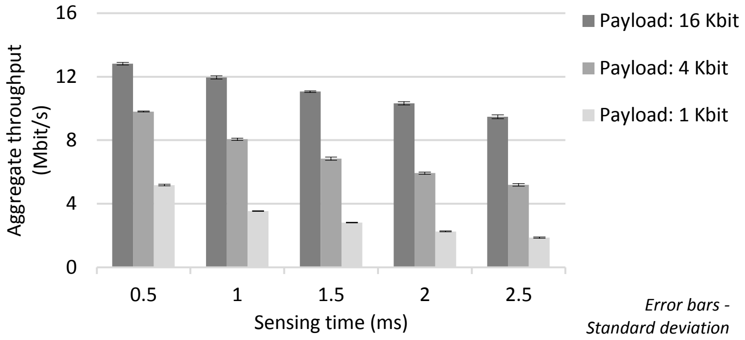
From results in Figure 5.8, Figure 5.9, Figure 5.10, Figure 5.11, and Table 5.8, we can conclude that defining a maximum channel access time limit with CORHYS (i.e., parameter λ in Algorithm 5.1) is relevant concerning fairness between the SUs, both for throughput and data frame latency, when MAC output queues have large maximum sizes and the channels are free of any PU activity for periods sufficiently large to enable the transmission of a great number of data frames. In any circumstance, this access time limit must be large enough to allow the effective utilization of all the available data channels simultaneously, i.e., at least n times out-of-band handshake duration, being *n* the number of available channels (see related discussion in Section 5.1 and Section 5.3.3).

5.4.4 Impact of sensing time

Since sensing time has a strong impact on the performance of CORHYS (and also on any OOB handshake-based solution), we run additional simulation experiments with different sensing time values, setting load per transmitter to 2 Mbit/s, i.e., beyond saturation point for all the configurations, and data frame payload size to 1 Kbit, 4 Kbit, and 16 Kbit. Figure 5.12 depicts the obtained aggregate throughput with the error bars showing the standard deviation between the runs. We observe that, even with significantly higher sensing times than used so far and, thus, higher sensing precision (see discussion in Section 2.5.2), our hybrid solution keeps performing better, except with 16 Kbit data frame payload size, than the optimistic approach of Jia and Zhang [2009] that does not include sensing in OOB handshake (compare with results in Figure 5.6 when load per transmitter is 2 Mbit/s). As already mentioned, CORHYS follows a more practical and effective approach for PU protection, i.e., a sense-before-transmit scheme, and it is not based on any ideal assumption such as a priori knowing the status of channels.



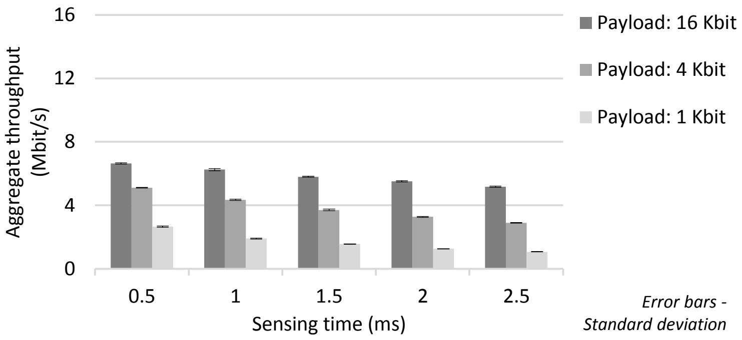
a) 4 channels (8 Mbit/s aggregate bit rate)



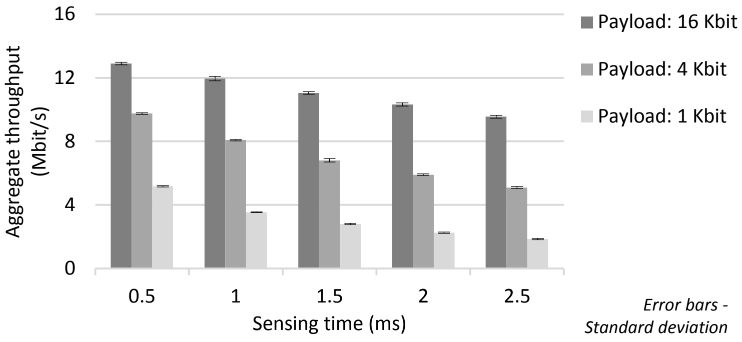
b) 8 channels (16 Mbit/s aggregate bit rate)

Figure 5.12. Effect of sensing time on aggregate throughput (2 Mbit/s load per transmitter)

In Section 5.3.2, we have discussed how CORHYS must be modified when a MAC-level retransmission scheme is required. The necessary modification is straightforward and consists in CSI control frames acting also as acknowledgement frames. In this case, the reception of the last data frame of a multi-frame channel access period must be followed by a sensing time and by the transmission of a CSI control frame similarly to what occurs upon the reception of previous data frames. Therefore, the additional overhead that results from the proposed modification of CORHYS is mostly influenced by sensing time. Figure 5.13 depicts the aggregate throughput that is achieved when this approach is followed, setting load per transmitter to 2 Mbit/s, using 1 Kbit, 4 Kbit, and 16 Kbit data frame payload sizes, and taking into account different sensing time values.



a) 4 channels (8 Mbit/s aggregate bit rate)



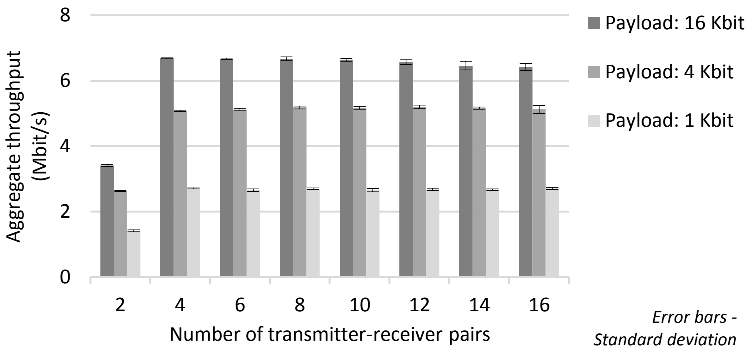
b) 8 channels (16 Mbit/s aggregate bit rate)

Figure 5.13 Aggregate throughput when CSI frames are also used as acknowledgement frames (2 Mbit/s load per transmitter)

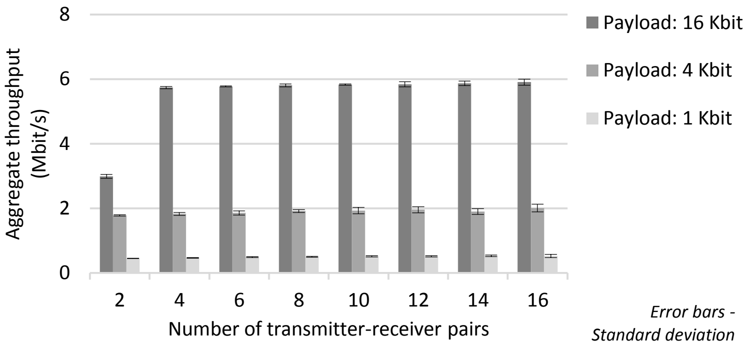
As expected, using the modified version of CORHYS that enables supporting a MAC-level retransmission scheme has negligible impact on throughput (compare results in Figure 5.13 with results in Figure 5.12). The cause is that the resulting overhead (i.e., an additional single inter-frame space in Figure 5.3) is small when compared to total multi-frame channel access time. Additionally, when a multi-frame channel access is aborted due to the appearance of a PU activity, which is a possibility in our simulation scenario, the additional overhead that results from the modified version of CORHYS does not even exist since the last scheduled data frame (see Figure 5.3) ends up not being transmitted.

5.4.5 Impact of the number of secondary users

The default simulation scenario that we use to evaluate CORHYS includes sixteen SUs that form eight distinct transmitter-receiver pairs (see Table 5.2). Nevertheless, it is also important to take into account scenarios with distinct numbers of SUs in order to generalize our conclusions about the performance gains that CORHYS is able to provide. For this purpose, Figure 5.14 and Figure 5.15 present the aggregate throughput that is achieved by CORHYS and OOB handshake (i.e., COSBET-MAC) when the number of transmitter-receiver pairs varies from two to sixteen.



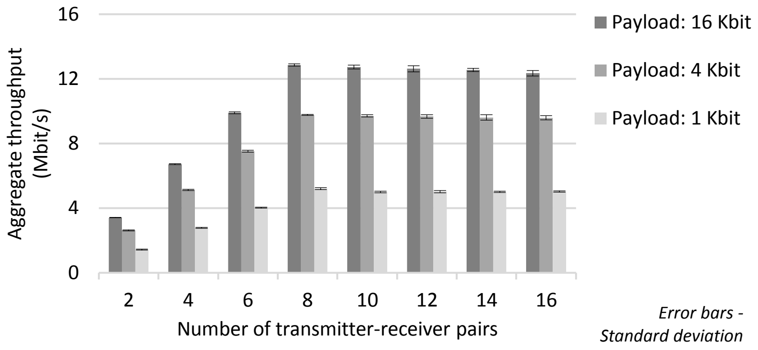
a) Hybrid signaling (CORHYS)



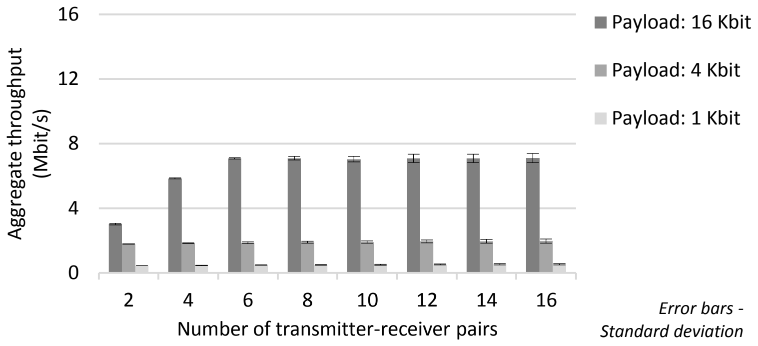
b) Out-of-band handshake (COSBET-MAC)

Figure 5.14 Aggregate throughput vs. number of transmitter-receiver pairs (2 Mbit/s load per transmitter, and 4 channels with 8 Mbit/s aggregate bit rate)

In Figure 5.14 and Figure 5.15, we consider four and eight channels, respectively, 2 Mbit/s load per transmitter, and 1 Kbit, 4 Kbit, and 16 Kbit data frame payload sizes. Figure 5.16 presents the results obtained with IEEE 802.11, i.e., a standard single-channel access solution, using similar settings for a comparison basis. Including up to sixteen transmitters-receiver pairs in the simulation scenario is sufficient to allow situations with significantly more transmitters than available channels, even when considering eight channels.



a) Hybrid signaling (CORHYS)



b) Out-of-band handshake (COSBET-MAC)

Figure 5.15 Aggregate throughput vs. number of transmitter-receiver pairs (2 Mbit/s load per transmitter, and 8 channels with 16 Mbit/s aggregate bit rate)

We can conclude from results in Figure 5.14 and Figure 5.15 that the hybrid solution we propose for distributed CR networks performs better than OOB handshake, which is a common practice regarding distributed CR solutions, independently of the density of SUs in the network. With four available channels (see Figure 5.14) and whatever is the data frame payload size in use, the aggregate throughput achieved by CORHYS increases until the network includes four transmitter-receiver pairs. Then, it remains quite stable. The reason is that CORHYS makes an effective utilization of the four channels even with 1 Kbit data frame payload size (see Table 5.5). With four channels available, the performance of OOB handshake is significantly lower than the performance of CORHYS, except with 16 Kbit payload size. The reason is that OOB handshake is able to effectively use the four channels only when payload size is 16 Kbit (see Table 5.5). With 16 Kbit payload size, the gain that is obtained with COHYS when compared to OOB handshake results from the fact that in-band signalling, which is achieved between successive data frames during multi-frame channel access, has less overhead than OOB handshake (i.e., less control frames, no contention, and no back-off periods).

With eight channels available (see Figure 5.15), the aggregate throughput achieved by CORHYS increases rather linearly with the number of transmitter-receiver pairs until the simulation scenario includes eight pairs. Then, it remains quite stable. The reason is the same as already stated for the four channels case and proves the ability of CORHYS to effectively use all the available channels and, therefore, to efficiently implement the CR paradigm. In Figure 5.15-b), we observe that OOB handshake achieves an increase in aggregate throughput only when payload size is 16 Kbit and until the network includes six transmitter-receiver pairs. The reason is that OOB handshake is able to effectively use a maximum of one, two, and five channels simultaneously when payload size is 1 Kbit, 4 Kbit, and 16 Kbit, respectively (see Table 5.5). With any payload size and any number of transmitter-receiver pairs, it performs worse than CORHYS.

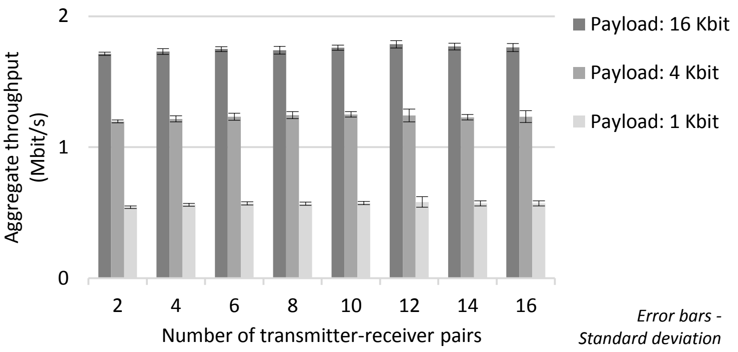
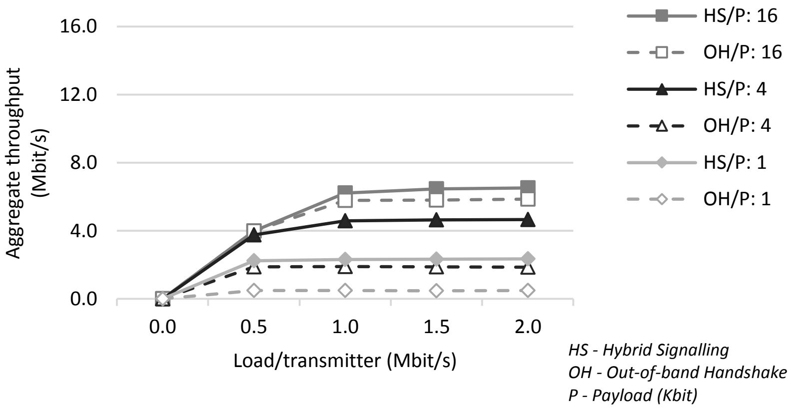


Figure 5.16 Aggregate throughput vs. number of transmitter-receiver pairs when using IEEE 802.11 (2 Mbit/s load per transmitter, 1 channel with 2 Mbit/s bit rate)

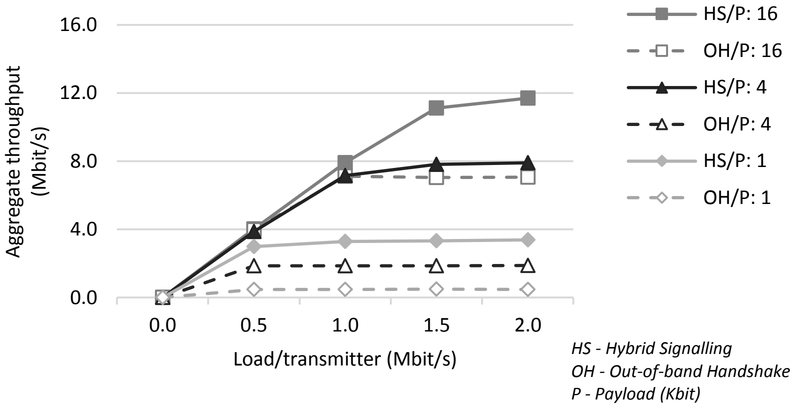
With 1 Kbit and 4 Kbit data frame payload sizes, the performance of OOB handshake does not improve when the number of available data channels is eight instead of four (see Figure 5.14 and Figure 5.15). The reason is that, with such payload sizes, only one and two channels are effectively accessed simultaneously in the simulation scenario, respectively (see Table 5.5). That is, increasing the number of channels beyond those limits has no practical effects on the throughput level that OOB handshake achieves. With 16 Kbit data frame payload size, there is an increase in performance when using eight channels since OOB handshake is able to effectively use five data channels in such conditions (see Table 5.5). From results in Figure 5.14, Figure 5.15, and Figure 5.16, we also conclude that CR performs better than the single-channel approach (see Figure 5.16), except when using OOB handshake jointly with 1 Kbit data frame payload size. In this specific condition, OOB handshake only uses a single channel at any time despite its CR nature.

5.4.6 Impact of joint traffic pattern

In order to generalize our conclusions about the gains provided by the hybrid solution we propose, Figure 5.17 depicts results on the aggregate throughput that is obtained with a type of SU traffic pattern that is less favourable and ideal than disjoint traffic, which we used so far. In this case, the destinations of the data frames in the MAC output queues are randomly selected (with a uniform distribution) among the eight possible receivers we consider in the simulation scenario. This approach results in a so-called joint traffic pattern and, therefore, in the possibility of contention for the same destination. Figure 5.17 depicts the obtained results for CORHYS and for OOB handshake, and considers data frame payload sizes that are 1 Kbit, 4 Kbit, and 16 Kbit. Table 5.9 shows the standard deviation of aggregate throughput over the runs.



a) 4 channels (8 Mbit/s aggregate bit rate)



b) 8 channels (16 Mbit/s aggregate bit rate)

Figure 5.17. Aggregate throughput when using joint SU traffic

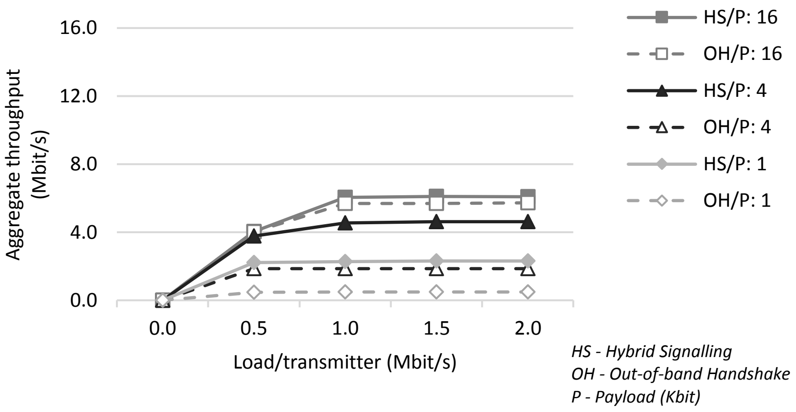
Table 5.9: Standard deviation of aggregate throughput in kbit/s (data points in Figure 5.17)

Number of channels	Configuration	Load/Transmitter (Mbit/s)			
		0.5	1	1.5	2
4	HS[1]/P[2]: 1	17.8	28.6	12.7	32.6
	HS/P: 4	48.6	31.1	32.4	34.0
	HS/P: 16	52.3	56.6	25.4	46.0
	OH[3]/P: 1	11.8	9.7	18.5	8.4
	OH/P: 4	58.8	29.0	44.5	42.3
	OH/P: 16	139.9	40.9	39.6	67.1
8	HS/P: 1	61.2	44.6	61.1	40.9
	HS/P: 4	78.9	115.4	56.2	59.2
	HS/P: 16	103.4	145.8	149.4	88.4
	OH/P: 1	14.3	19.9	15.8	11.6
	OH/P: 4	60.9	47.2	52.5	26.0
	OH/P: 16	91.5	35.9	62.8	68.6

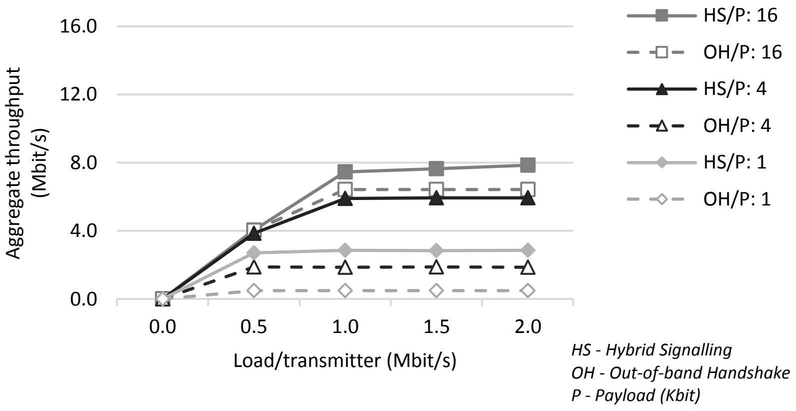
[1] Hybrid signalling (CORHYS).
[2] Data frame payload size (Kbit).
[3] Out-of-band handshake (COSBET-MAC).

With joint traffic and as expected, performance decreases when compared to results obtained with disjoint traffic and fixed transmitter-receiver pairs (compare with results depicted in Figure 5.5). Nevertheless, CORHYS still outperforms OOB handshake since it still achieves multi-frame access and in-band signalling, yet at a lower level. When compared to results obtained with disjoint traffic (see Figure 5.5), the observed decrease in performance remains relatively small since the SUs process the oldest queued frame with a destination known to be idle, which limits blocking when joint traffic is applied (see parameter d in Algorithm 5.1). We recall that, for a concern of fair comparison, COSBET-MAC, the OOB handshake-based solution we use, was modified in order to similarly follow this approach. When this approach is not followed, i.e., a SU only processes the frame located at the front of its MAC output queue and blocks if the respective destination is already engaged in communication, we obtain the results depicted in Figure 5.18. Table 5.10 shows the standard deviation of aggregate throughput over the runs.

In Figure 5.18, we observe a noticeable performance degradation, when compared to results in Figure 5.17, only when we assume the utilization of CORHYS with eight channels. The reason is as follows. When a given solution is able to effectively use up to n channels simultaneously, performance degradation occurs at a given instant only if there are less than n transmitters with distinct destinations in terms of the data frames at the front of their MAC output queues. The practical effect of this type of situation consists in less channels being accessed simultaneously than the achievable limit (e.g., based on results in Table 5.4 and Table 5.5, CORHYS is able to use up to 8 channels simultaneously while OOB handshake only uses up to 1, 2, and 5 channels with 1 Kbit, 4 Kbit, and 16 Kbit data frame payload sizes, respectively). Therefore, when compared to results in Figure 5.17, performance degradation is more noticeable with this situation occurring more frequently. That is, with eight transmitters in our simulation scenario and with destinations being randomly selected (with a uniform distribution) on a data frame basis, it is more probable to have less than eight transmitters with distinct destinations than having less than four transmitters with distinct destinations at a given moment.



a) 4 channels (8 Mbit/s aggregate bit rate)



b) 8 channels (16 Mbit/s aggregate bit rate)

Figure 5.18. Aggregate throughput when using joint SU traffic and processing the frame at the front of the MAC output queue

5.4.7 Impact of primary user activity

To conclude the evaluation of CORHYS, we analyse it under distinct PU activity characteristics. For this purpose, we consider that every data channel has PU activities characterized by alternating idle and busy periods exponentially distributed with parameters λ_i and

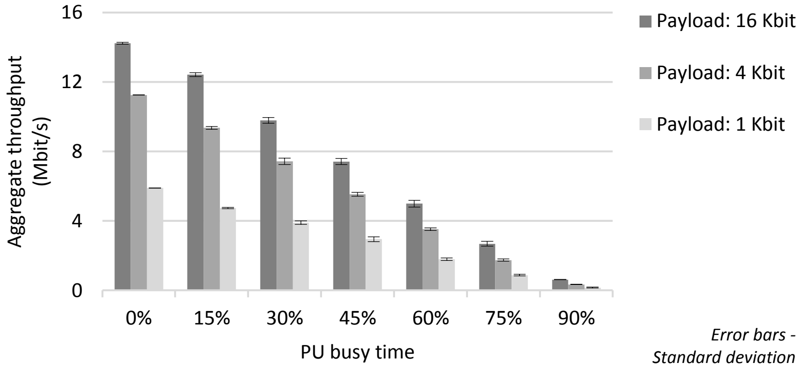
λ_b, respectively, being the sum of the respective means equal to 0.1 seconds (i.e., $1/\lambda_i + 1/\lambda_b = 0.1$). Figure 5.19 presents the obtained results when no prediction capabilities are available, as we have considered so far, load is set to 2 Mbit/s per transmitter, 8 channels are available, disjoint traffic is used, busy time varies from 0% (i.e., channels are always vacant) to 90%, and data frame payload size is 1 Kbit, 4 Kbit, and 16 Kbit. The error bars show the standard deviation of aggregate throughput between the runs. This figure provides results for CORHYS and OOB handshake. Performance decreases as busy time increases since the average number of vacant channels decreases and, consequently, the average number of concurrent accesses decreases too. The average duration of multi-frame channel access also decreases due to channel accesses being interrupted by the appearance of PU activities. Nevertheless, CORHYS still outperforms OOB handshake for all types of PU activities under consideration.

Table 5.10: Standard deviation of aggregate throughput in kbit/s (data points in Figure 5.18)

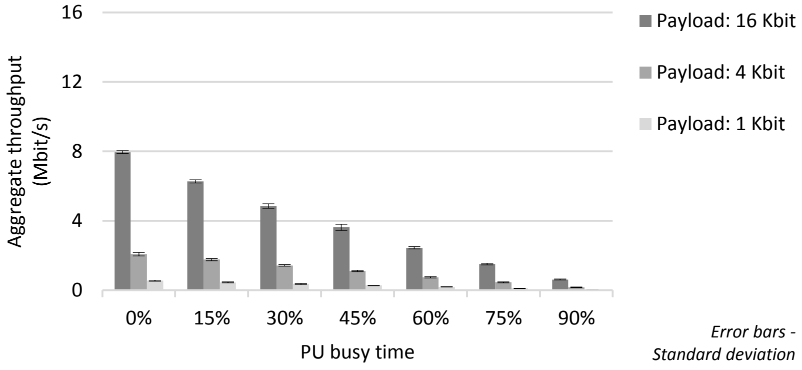
Number of channels	Configuration	Load/Transmitter (Mbit/s)			
		0.5	1	1.5	2
4	HS[1]/P[2]: 1	19.0	35.1	34.5	12.7
	HS/P: 4	113.2	44.7	26.0	60.1
	HS/P: 16	90.1	50.2	68.7	43
	OH[3]/P: 1	13.6	8.4	12.0	9.4
	OH/P: 4	25.7	33.6	41.6	38.3
	OH/P: 16	97.8	33.7	26.2	65.5
8	HS/P: 1	51.8	56.8	70.7	82.0
	HS/P: 4	77.6	105.4	150.1	236.1
	HS/P: 16	147.1	158.7	146.0	187.0
	OH/P: 1	15.5	13.5	12.8	13.2
	OH/P: 4	25.0	61.3	24.6	25.0
	OH/P: 16	85.8	76	77.1	85.8

[1] Hybrid signalling (CORHYS).
[2] Data frame payload size (Kbit).
[3] Out-of-band handshake (COSBET-MAC).

When the SUs have prediction capabilities, CORHYS runs Version 2 section in Algorithm 5.1 for selecting the set of candidate channels and the number of queued frames to be issued during channel access time. In order to evaluate CORHYS in such circumstances and assess the relevance of using Version 2 section instead of a variation of Version 1 section that also takes into account prediction outcomes, we repeat the experiments that resulted in Figure 5.19 with the SUs having fully accurate prediction capabilities. Step 7 in Algorithm 5.1 becomes $Ai_t \leftarrow \varphi(Ui, rt_i)$ in order to modify Version 1 section such that it omits unreserved channels (i.e., channels that belong to set Ui) with any PU activity predicted during reservation time rt_i. Figure 5.20 shows the obtained aggregate throughput and also includes, for a comparison basis, OOB handshake with the SUs having fully accurate prediction capabilities. The error bars show the standard deviation between the runs.



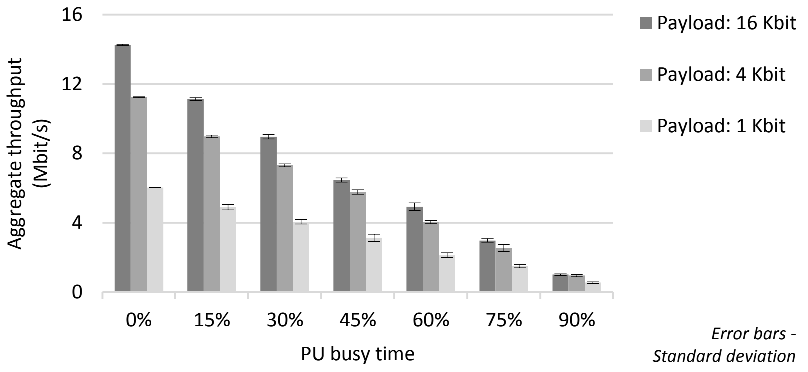
a) Hybrid signalling (CORHYS)



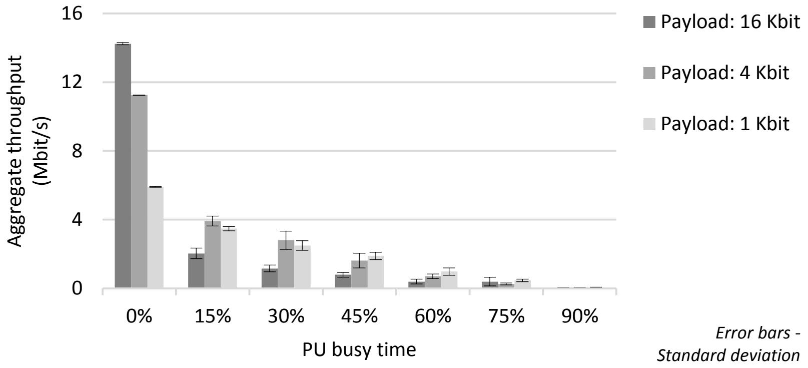
b) Out-of-band handshake (COSBET-MAC)

Figure 5.19. Aggregate throughput vs. primary user busy time (2 Mbit/s load per transmitter, disjoint traffic, no prediction capabilities, and 8 channels with 16 Mbit/s aggregate bit rate)

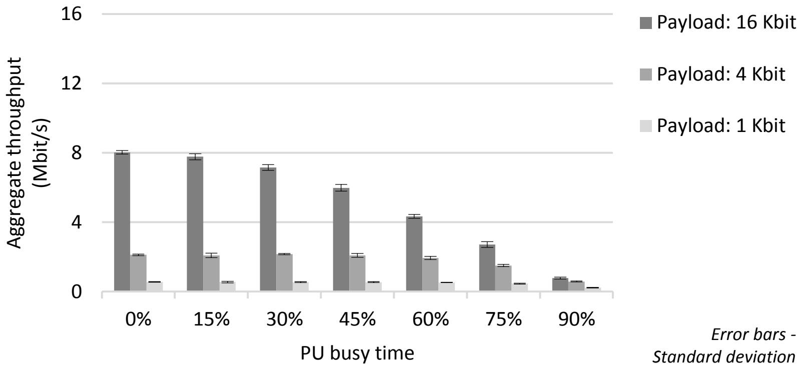
From results depicted in Figure 5.20, we can conclude that the utilization of Version 2 section is clearly mandatory in order to avoid a shortage of spectrum opportunities large enough in time to support the computed access times. Basically, it takes into account the predicted duration of the spectrum holes for defining the number of queued frames to transmit. Consequently, with prediction-aware Version 1 section in Algorithm 5.1 and 16 Kbit payload size, CORHYS performs worse than OOB handshake whenever there is any kind of PU activity. With 1 Kbit and 4 Kbit payload sizes, the same conclusion applies for PU busy times higher than 75% and 30%, respectively.



a) CORHYS with Version 2 section



b) CORHYS with prediction-aware Version 1 section



c) Out-of-band handshake

Figure 5.20. Aggregate throughput vs. primary user busy time when fully accurate prediction is available (2 Mbit/s load per transmitter, disjoint traffic, and 8 channels with 16 Mbit/s aggregate bit rate)

5.5 Summary

Distributed opportunistic CR MAC proposals that use a dedicated CCC for signalling, follow a sense-before-transmit approach, i.e., the candidate channel is sensed before each transmission, and perform handshake on a data frame basis are a common practice (see Chapter 2) that we designate as OOB handshake. Sensing the channel before any access reduces the risk of interfering with the PUs and is a practical approach. The utilization of a dedicated CCC simplifies the implementation of CR MAC solutions and enables passive learning. However, the efficiency of dedicated CCC-based solutions in utilizing all the available channels depends on the ratio between channel allocation time and handshake time. That is, when data frames are not large enough, potential spectrum utilization efficiency and performance improvement provided by opportunistic CR cannot be fully achieved.

This chapter successfully addressed the mentioned issue by proposing CORHYS (Cognitive Radio Hybrid Signalling), a hybrid signalling solution. This solution still follows OOB handshake in order to take full advantage of its strengths (e.g., ease of implementation, passive learning). Additionally, CORHYS expands OOB handshake with multi-frame channel access (i.e., a SU can allocate a channel for transmitting multiple data frames) and in-band signalling (i.e., control frames can be issued over allocated data channels and sensing is performed during channel access). It also accounts for the possibility of the SUs being equipped with prediction capabilities.

The obtained evaluation results show that the solution we propose effectively addresses the targeted issue since it allows more vacant channels to be simultaneously accessed on distributed opportunistic CR networks and, consequently, has potential to improve the communication performance of SUs.

Chapter 6

Enhancing the spatial reuse of the spectrum and lowering control traffic

CR (Cognitive Radio) aims at enabling SUs (Secondary Users) to opportunistically access frequency bands that are not being used by their respective incumbent users. In distributed CR networks, there are no central entities that collect and fuse data, and take spectrum decisions. In such environments, the SUs take their own decisions based on local observation and, optionally, on data they exchange with each other and on learning. Many existing cooperative distributed CR proposals use a dedicated CCC (Common Control Channel) for signalling purposes (see Chapter 2 and Chapter 5). In multi-hop CR scenarios, a CCC can suffer from the so-called hidden SU problem, which consists in the CCC being idle on the transmitter's side while it is busy on the receiver's side. This issue results in inappropriate and useless transmission of control frames, and, consequently, in performance degradation. Beyond accurately locating and accessing spectrum opportunities, appropriate spatial reuse of the spectrum is crucial in CR environments in order to enable the SUs to further increase spectrum utilization efficiency.

The current chapter proposes a strategy, which includes three components, with potential to improve the performance of distributed CR MAC protocols that are based on a dedicated CCC, perform handshake on a data frame basis, and are random-based in terms of spectrum access. It specifically enables increasing the spatial reuse of the spectrum and minimizing control traffic on the CCC. We designate the proposed solution as the PEL (Power control, avoidance of the Exposed node problem, and Late reply) strategy based on the names of its three components. Simulation results show that this strategy provides effective gains, even when accounting for limitations that might occur in real deployments. To the best of our knowledge, there are no existing distributed CR MAC proposals that follow the solution the current chapter proposes. Since the contributions of Chapter 3, Chapter 4, and Chapter 5 are also taken into account when evaluating the PEL strategy, the current chapter also contributes to summarize and aggregate the overall contributions of this thesis.

A paper is under preparation for presenting the outcomes of this chapter in the context of both CR and non-CR ad-hoc networks.

The remainder of this chapter is organized as follows. Section 6.1 states the main objectives of the current chapter. Section 6.2 discusses related work and states the contributions of this chapter. Section 6.3 describes the PEL strategy, i.e., the optimization solutions proposed in the current chapter and that lie at the MAC level. Section 6.4 evaluates it through simulation. Finally, Section 6.5 draws final conclusions.

6.1 Introduction

In opportunistic CR scenarios, the SUs can opportunistically access temporally vacant spectrum bands in order to improve their communication performance, provided that the PUs (Primary Users) do not suffer any harmful interference (see Chapter 2). This approach results in dynamic multichannel spectrum access and enables simultaneous transmissions over a wide range of spectrum bands. Therefore, one of the key issues of CR is enabling a SU to precisely locate and access spectrum opportunities without interfering with any PU. This objective requires accurate spectrum sensing techniques, cooperative schemes that enable the SUs to exchange relevant information between each other, and, if available, learning through observation and past experience capabilities. Achieving the goal of CR is a challenge as spectrum utilization is a temporal and spatial phenomenon, i.e., at a given moment it varies over distinct locations and at a given location it varies over time. Additionally, no modifications are expected to be done to the PUs (i.e., the PUs remain unaware of CR operations).

Beyond other architectural approaches and as detailed in Chapter 2, CR networks might be fully distributed [Akyildiz et al., 2009]. In this case, there are no central entities and, therefore, the SUs take their own spectrum decisions. Furthermore, if the SUs cooperate with each other and there is no access to any a priori information, such as the locations of known primary transmitters and their respective regions of potential interference, a SU only relies on its own observation and learning capabilities, and on any signalling information provided by neighbours, such as what occurs with cooperative sensing solutions [Akyildiz et al., 2011]. That is this kind of fully cooperative and decentralized CR scenarios the current chapter and, more generally, this thesis target (i.e., CR scenarios with totally autonomous and collaborating SUs).

The current chapter proposes MAC-level solutions for performance improvement in multi-hop distributed opportunistic CR networks that use a CCC for signalling, perform handshake on a data frame basis, and are random-based in terms of spectrum access. Optimizing the spatial reuse of the spectrum, reducing control traffic by accounting for the hidden SU problem on the CCC, and considering the possibility of transmission power control based on distance estimation are key guidelines. Detailed analysis or innovative proposals about automated distance estimation, one of the capabilities our proposal effectively utilizes and assumes to be available, remain out of the scope of this thesis.

6.2 Related work and contributions

Several opportunistic CR MAC solutions have already been proposed in the literature (see Chapter 2). The majority of them target distributed CR networks, are random-based in terms of spectrum access, use a dedicated CCC for signalization purposes, and require at least two radios, being one of them dedicated to operate the CCC (See Chapter 2). The contributions in the current chapter are devoted to this type of CR MAC protocols, which is one of the most common in the CR area [Salameh et al., 2010]. We have named this type of operating mode as OOB handshake in Section 5.3 and depicted it in Figure 5.2. Beyond the channel selection phase, OOB handshake-based distributed CR MAC protocols also include sensing and decision phases when the SUs follow a sense-before-transmit approach (see Figure 5.2). COSBET-MAC, the CR MAC protocol defined in Chapter 3, is such an example. In the current section, we discuss key capabilities, features, and assumptions that have been considered in the design of existing distributed CR MAC proposals and are relevant to the discussion in the current chapter. We also state the novel contributions of the PEL strategy.

Random-based access, i.e., CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) like access, is easy to implement, for both data and control traffic, since it does not require global network synchronization. Alternatives to this type of approach include time-slotted and hybrid (i.e., partially time-slotted and partially random access) solutions (see Chapter 2). For instance, Kondareddy and Agrawal [2008] propose a hybrid solution that uses different time slots to represent different channels and the work of Wang et al. [2010c] consists in a slotted protocol. However, these approaches need tight synchronization among the SUs, which is a challenging issue in real deployments [De Domenico et al., 2012]. Wang et al. [2010c] suggest using GPS (Global Positioning System) devices to enable synchronization between the SUs, claiming that the resulting extra cost is acceptable due to the expected improvement of network performance.

Using a dedicated CCC associated with a dedicated radio on each SU enables simpler protocol architectures. The main reason is that a SU obtains the information it needs from its neighbours overhearing control frames on the CCC continuously, even when it is accessing a data channel through another radio. In fact, CCC enables what Salameh et al. [2010] designate as passive learning, i.e., the SUs use the information inside the control frames they overhear. Using a radio dedicated to operate the CCC also avoids the so-called multichannel hidden terminal problem [Xiang et al., 2010]. This issue occurs in single radio-based protocols since a SU misses any control information, such as channel reservation indication by neighbours, sent over a channel it is not operating. The most relevant negative effect of this issue is an increase in the number of collisions among the SUs on the data channels. For instance, in the proposal of Jia, Zhang, and Shen [2008], which uses a single half-duplex radio and have no global synchronization, a SU is prone to the mentioned multichannel hidden terminal problem. Although using a dedicated CCC is widely accepted [Ren et al., 2012], it has known drawbacks such as being prone to saturation and security attacks. The works of Lo [2011] and Cormio and Chowdhury [2010] provide detailed information on CCC design, alternatives, and challenges in CR networks. Chapter 5 provided a solution, called CORHYS, which addresses the CCC saturation problem of OOB handshake-based distributed CR MAC solutions.

In opportunistic CR, accurate sensing is a key feature that is usually performed before each data channel access in order to locate spectrum opportunities and avoid interfering with PUs (see Section 2.5.2). This is the so-called sense-before-transmit approach. However, local sensing is known to be incapable of delivering totally satisfactory results, namely due to sensor imperfections, adverse signal propagation effects, and the hidden PU problem (i.e., a SU does not succeed sensing the activities of PUs it can interfere with). Therefore, cooperative approaches have been proposed in order to improve PU detection efficiency (see Section 2.5.2). The main idea consists in combining the sensing outputs of various SUs, taking advantage of spatial diversity. In centralized CR networks, the fusion process is performed by a central entity, while in distributed CR networks each SU acts as both a sensor and a fusion centre. For this purpose, a SU collects sensing outcomes from its neighbours. For example, in the work of Timmers et al. [2010], a SU cannot access a channel that at least one of the SUs in the network declares as being busy, i.e., when the so-called OR fusion rule is globally applied to the network.

Even when local or cooperative sensing is perfect, it remains possible that, during data transmission, a PU appears on a channel that has been sensed idle before the access phase. To address the appearance of PU activity during data channel access time, some authors assume that sensing and communication can be performed simultaneously and that a SU leaves a channel as soon as a PU appears. However, these assumptions are not compatible with many practical approaches such as using half-duplex transceivers, which are either in transmission or reception mode at any time, and energy-based detection, the currently simplest and most popular sensing scheme (see Section 2.5.2). Other proposals are based on ideal assumptions that are hardly found in real deployments. For instance, the solution proposed by Zhao et al. [2007] was designed based on the assumption that the SUs can obtain information from the PUs, which does not comply with the rule that CR does not imply modifications to the PUs. Hassan et al. [2011] assume in their work that the SUs are location-aware and know the locations of all the incumbent transmitters and receivers (i.e., PUs), which might be unpractical. Some authors also consider that the PUs can tolerate interferences that do not exceed a certain amount of time [Xiang et al., 2010; Zhao et al., 2007]. In this case, the protection of PUs is achieved by defining an appropriate maximum transmission time on data channels.

Another approach that has high potential to avoid harmful interferences to PUs during data transmission consists in probabilistically determining busy and idle periods on the targeted data channels. This approach is mostly based on learning through past experience and observation, which is a core issue in CR (see Section 2.7). Basically, existing proposals try to efficiently exploit PU behaviour over time for each channel. Several research works have indicated that channel occupancy and traffic patterns can be statistically modelled, which makes prediction based on learning feasible [Wang et al., 2010b]. With such dynamic prediction capabilities, the SUs are able to take optimized spectrum decisions, i.e., to select a channel that will probably be sensed idle and won't experience any PU activity during transmission time. This approach is particularly interesting when the SUs are not capable of detecting PU activities during transmission time and PUs do not tolerate any level of interference, which is the case in many real scenarios. Usually, PU traffic patterns are stochastic phenomena (i.e., non-deterministic) and, therefore, prediction techniques are not able to deliver fully accurate results (see Section 2.7).

Power control strategies have been widely studied in the context of underlay CR networks [Chen et al., 2008c; Xu et al., 2011; Xu et al., 2012], which consist in another CR approach for enabling the coexistence of SUs and PUs on licensed channels. On the contrary of opportunistic CR, which has received much more attention from the research community and we simply designate as CR (see Chapter 2), underlay CR is not based on dynamic spectrum access and on the detection of spectrum opportunities. It aims at enabling the SUs to access the channels simultaneously with the respective PUs without any interruption of service or spectrum handover procedure. With underlay CR, also designated as interference-tolerant CR, a SU maintains transmission power below the noise floor of PUs. Therefore, the key elements are power control and power management instead of spectrum sensing and spectrum mobility. Various resource allocation and power control schemes have been studied and proposed with the primary goal of limiting SU interference to PUs [Lu et al., 2012; Ansari et al., 2013]. For example, the solution proposed by Salameh et al. [2009] dynamically adjusts transmission power in order to guarantee that the outage probability of PUs satisfies a pre-defined threshold. The work of Salameh et al. [2010] defines a maximal transmission power level and does not use spectrum sensing.

Regarding spectrum sharing in distributed CR networks, the type of CR approach we target in this thesis, several research works that consider varying the transmission power of the SUs also exist. Their objectives consist in increasing the protection of PUs as well as improving the performance of SUs. The latter results from a higher spatial reuse of the spectrum enabled by lower transmission power and, consequently, inferior interference ranges. Hassan et al. [2011] review some of these works. Power control has also potential to help users saving energy [Ren et al., 2012] and depends directly on the availability of accurate signal propagation models that establish dependence between transmission distance and transmission power. Xiang et al. [2010] consider that the majority of existing studies on power control in CR are theoretical and that there is a lack of detailed MAC solutions designed with power control features.

The proposals of Qu et al. [2010], Pirmoradian et al. [2012], and Hassan et al. [2011] are examples that include power control features. However, they are not jointly specified with any MAC solution and make a few ideal assumptions (e.g., a priori knowing the information on the side of the PUs). The work of Wang et al. [2010c] uses power control to increase spatial reuse efficiency and to support concurrent transmissions. However, it follows a time-slotted access approach, which is distinct from the type of CR MAC protocol we target in this thesis. Dependence between signal propagation model and transmission distance can also be exploited without the aim of dynamically varying transmission power. For example, the distributed asynchronous CR MAC protocol proposed by Salameh et al. [2010] exploits this dependence as well as traffic characteristics for assigning channels with lower SINR (Signal to Interference plus Noise Ratio) to shorter distances. The preference of a channel in the selection process is, therefore, influenced by the distance between the transmitter and the receiver.

The solutions the current chapter defines jointly support the following features in OOB handshake-based distributed CR scenarios: improved spatial reuse of the spectrum; utilization of power control based on distance estimation; avoidance of the exposed SU problem (i.e., a SU is denied access to a channel that is in use by neighbours despite it cannot interfere with the corresponding receivers); and reduction in the number of transmitted control frames through what we designate as late replies. To the best of our knowledge, no other OOB handshake-based distributed CR MAC solution includes algorithms such as transmitting late control frames or addressing the exposed SU problem jointly with transmission power control based on distance estimation. In fact, Salameh et al. [2010] argue that most exiting CR MAC proposals were developed without exploiting transmission distance and are limited to the analytical aspects of MAC design, with no complete operational details. The current chapter also accounts for the possibility of the OOB handshake-based distributed CR scenarios it targets being enhanced with the solutions proposed in Chapter 3, Chapter 4, and Chapter 5. That is, it also provides an integrated vision of all the contributions provided in this thesis.

6.3 PEL strategy

This section describes the solutions the current chapter proposes (see Figure 6.1). We designate the joint utilization of the solutions in Figure 6.1 as the PEL strategy. This section is organized in two distinct subsections that are related to improving the spatial reuse of the spectrum and reducing the number of issued control frames, respectively. We specifically target distributed CR MAC protocols that are OOB handshake-based (see Section 5.3.1 and Figure 5.2). This type of commonly used solution consists in performing signalling over a dedicated CCC and on a data frame basis, and optionally includes sensing in handshake (i.e., it optionally follows a sense-before-transmit approach). When sensing is considered, there is an additional phase, designated as decision phase in Figure 5.2, which serves to fuse the sensing results of the transmitter and receiver, and to conclude about the availability of the channel selected during the selection phase. COSBET-MAC, the CR MAC protocol Chapter 3 proposes, is illustrative of such approach. We also note that this thesis includes some assumptions, such as the availability of techniques for controlling transmission power and making automated distance estimation, with details that are out of its scope.

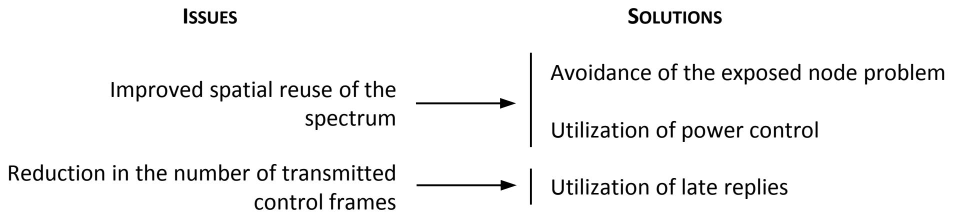


Figure 6.1. Issues to be addressed and proposed solutions

Before presenting the specific contributions of the current chapter, we briefly recall some of the characteristics of OOB handshake (see Section 5.3.1 for additional details). The first control frame of a handshake process, which we designate as initial control (IC) frame, is issued on the

CCC through a contention-based scheme similar to CSMA/CA. The broadcast nature and permanent operation of the dedicated CCC enables the SUs to passively learn the status and actions of their neighbours and channels, even during data channel access time. Inspecting the control frames that are overheard on the CCC is the only action required for this purpose. The control frames can purposely include supplementary information in order to let the neighbours know any relevant information about the ongoing negotiation and use it if needed. For instance, a CCC reservation time field enables the neighbours of a given transmitter-receiver pair to refrain themselves from accessing the CCC until handshake concludes, which enables the control frames that follow the IC frame to be issued directly without any contention-based scheme.

The last frame of a handshake process carries a zero reservation time value that releases the CCC and gives awaiting SUs the opportunity to access it. With OOB handshake, the channel to be sensed is usually selected by the receiver. For this purpose, it runs a selection algorithm (e.g., uniform random selection) on the set of channels that are available at both sides of the communication link. Therefore, the information on the transmitter's side is provided to the receiver through IC frames. The neighbours of the negotiating pair overhear the final decision on the CCC and record its details (i.e., allocated channel, allocation duration, transmitter, and receiver).

6.3.1 Improved spatial utilization of the spectrum

In real CR scenarios, it is expected that there are less spectrum opportunities than SUs needing to transmit data frames at some instant. The higher is the density of SUs and transmission load, the higher is this concern. Therefore, it is crucial to spatially use the spectrum efficiently in order to enable the same channels to be reused simultaneously in distinct areas of the network. However, existing OOB handshake-based solutions do not fully achieve this goal since they do not adjust transmission power to admissible minimum values, i.e., taking into account the distance between the transmitter and the receiver. This subsection discusses this issue and proposes solutions to address it (see Figure 6.1).

6.3.1.1 Avoiding the exposed node problem

When a CR MAC protocol includes a retransmission scheme, the receiver of a unicast data frame replies with an acknowledgment frame over the selected data channel. In this case, the two sides of a communicating pair act as both transmitters and receivers independently of the direction data flows. However, it is legitimate and feasible to consider that data retransmission is not handled by MAC entities and that, consequently, no acknowledgment frames are issued on data channels upon data frame receptions. In this case, the source of the data frame is the sole SU that transmits a signal, which opens a new way to further improve the spatial utilization of the radio spectrum in CR scenarios. That is, a given transmitter-receiver pair starts being allowed to select a channel that is already in use in its vicinity if the following two conditions are jointly met: (1) all the receivers in the neighbourhood are out of the interference range of the transmitter; and (2) the receiver in the pair is out of the interference ranges of the transmitters in the neighbourhood. For instance, with this approach, transmitters C and E in Figure 6.2 can select the same channel simultaneously since none of them affects each other's receiver. Basically, we aim at addressing the so-called exposed node problem on the data channels. This problem consists in a SU being prevented from accessing a data channel due to ongoing neighbouring transmission, despite it cannot actually interfere with any receiver.

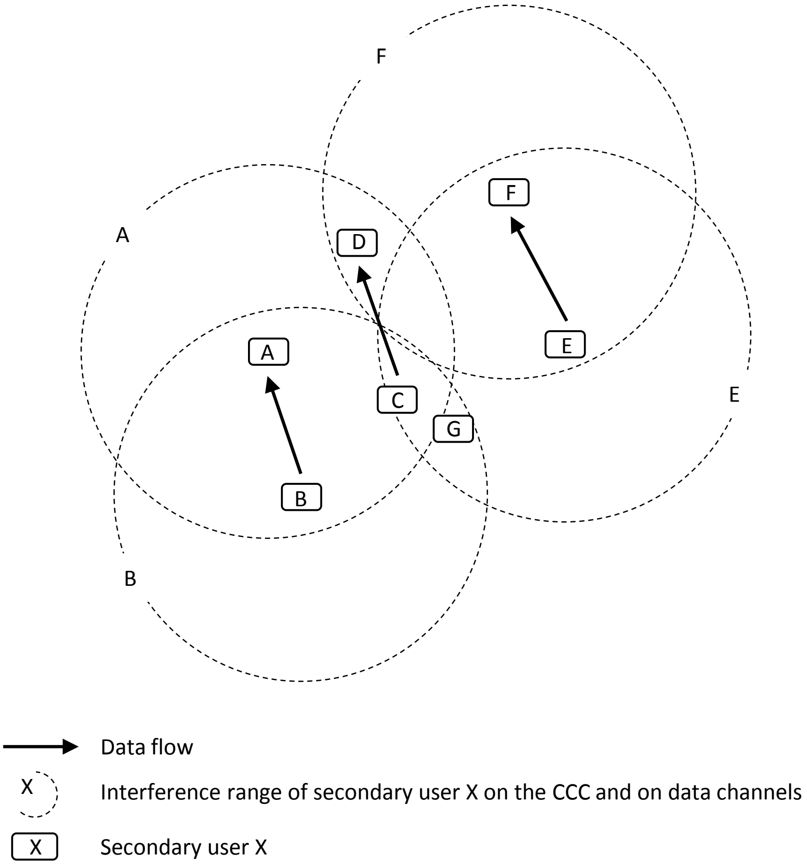


Figure 6.2. Spatial reuse of the spectrum

The interference range of a SU is the range within which a transmitted signal has enough strength to interfere with the correct reception of legitimate frames. Additionally, the transmission and sensing ranges are the distances within which the transmitted frames can, respectively, be received correctly and sensed by other SUs with high probability [Xu et al., 2003]. With OOB handshake, a SU decides if there is a risk of mutual interference with neighbours on a given data channel based on passive learning, i.e., on the information it extracts from correctly received and overheard control frames. That is, in this thesis we use transmission range instead of interference range, being the former lower than the latter. Therefore, in multi-hop scenarios, there is still the possibility of mutual interference when two distinct transmitter-receiver pairs that are out of the transmission ranges of each other select the same data channel. This issue, which is a kind of hidden SU problem that results from the difference between transmission and interference ranges, is not addressed by most existing protocols and has already been discussed in Section 3.3.3. Even mechanisms that are designed to handle the hidden node problem, such as “Request To Send/Clear To Send” handshake in IEEE 802.11, cannot totally prevent it [Xu et al., 2003]. Nevertheless, if a SU selects a channel it believes to be unused by neighbours and detects some activity during the sensing phase (i.e., it is in the interference and/or sensing ranges of neighbouring transmitters, but not in their transmission ranges), the channel ends up not being accessed.

With OOB handshake, a SU records the selections that nearby transmitter-receiver pairs make. The recorded information includes channel identification, reservation time, and the MAC addresses of the respective transmitter and receiver. A SU extracts this information from the control frames it overhears on the CCC during the decision phase or, if sensing is not included in handshake, throughout the selection phase. We globally designate them as the decision control frames. Since the SUs always go through a handshake process over the CCC prior accessing a given data channel, if a SU has not heard any control frame from the destination of an overheard decision frame in the past, then, it can conclude that it is out of the transmission range of that SU on the CCC. Without any loss of generality, in this thesis we consider that transmission range on data channels is the same for all the SUs and it is equal to the transmission range on the CCC, i.e., neighbourhood is the same on the CCC and on data channels (see Chapter 3). Therefore, a SU assumes that it is out of the transmission range of another SU on the data channels if it did not hear any control frame from it in the past. When scenarios are prone to mobility or have dynamic characteristics, a forgetting mechanism must be applied concerning the neighbours that have been dynamically learnt.

Algorithm 6.1 is the algorithm that a SU runs to determine if it can use a given channel. It accounts for the possibility of not using acknowledgment frames on the data channels and, therefore, of addressing the exposed node problem as described in previous paragraphs. The set of channels that successfully pass the verification test of Algorithm 6.1 includes the channels that are eligible for selection (i.e., the candidate channels). Since OOB handshake-based solutions simply consider the set of channels that are not reserved in the vicinity (e.g., see expression $C_s \cap C_r$ in Algorithm 3.1), they do not address the exposed node problem for performance optimization. On the other hand, a SU that is already using a given data channel and overhears a control frame belonging to the selection phase with the same channel selected runs Algorithm 6.2 to determine if there is any conflict with itself. When there is any conflict, the SU can notify the transmitter-receiver pair through a control frame sent over the CCC during the sensing phase, which corresponds to a quiet period on the CCC (see the cooperation of neighbours as defined in Chapter 3). Algorithm 6.1 and Algorithm 6.2 also assume the possibility of using transmission power control based on distance estimation, which is discussed in the next section and, consequently, is omitted in the current discussion.

Inputs:

- a, the state of the SU that runs the algorithm (i.e., receiver or transmitter);
- c, the channel to be evaluated;
- n, the number of reservations currently registered for channel c in the neighbourhood of the SU;
- t_i, the transmitter of the i^{th} known reservation of channel c;
- r_i, the receiver of the i^{th} known reservation of channel c;
- tr_i, the transmission range as defined in the i^{th} reservation of channel c;
- k(x), determines if secondary user x is a known neighbour;
- p, the communicating peer;
- d(x), the estimated distance to secondary x (if any control frame that includes it as transmitter or receiver was heard in the past);
- [x], expression x applies only when distance estimation and power control capabilities are available.

Output: *true* if channel c can be accessed without conflicting with neighbours and *false* otherwise.

```
if not use acknowledgement frames on data channels then
    for $i \leftarrow 1$ to $n$ do
        if $a$ = receiver and k($t_i$) = true [and $tr_i \geq$ d($t_i$)] then return false
        if $a$ = transmitter and k($r_i$) = true [and d($p$) $\geq$ d($r_i$)] then return false
    end for
else
    for $i \leftarrow 1$ to $n$ do
        if k($t_i$) = true [and (d($p$) $\geq$ d($t_i$) or d($t_i$) $\leq tr_i$)] then return false
        if k($r_i$) = true [and (d($p$) $\geq$ d($r_i$) or d($r_i$) $\leq tr_i$)] then return false
    end for
end if
return true
```

Algorithm 6.1. Verification made by a SU to determine if it can utilize a given data channel

Inputs:

- k(*x*), [*x*], d(*x*), *a*, *p*: see Algorithm 6.1;
- *t*, the transmitter of the overheard control frame;
- *r*, the receiver of the overheard control frame;
- *c*, the channel selected in the overheard control frame;
- *tr*, the transmission range to be used by the neighbouring pair.

Output: *true* if the selected channel might result in a conflict with the channel currently in usage and *false* otherwise.

```
if $c$ = channel currently in use then
    if not use acknowledgement frames on data channels then
        if $a$ = receiver and k($t$) = true [and d($t$) ≤ $tr$] then return true
        if $a$ = transmitter and k($r$) = true [and d($p$) ≥ d($r$)] then return true
    else
        if k($t$) = true [and (d($t$) ≤ $tr$ or d($t$) ≤ d($p$))] then return true
        if k($t$) = true [and (d($r$) ≤ $tr$ or d($r$) ≤ d($p$))] then return true
    end if
end if
return false
```

Algorithm 6.2. Verification made by a SU that is already accessing a data channel and that overhears a control frame indicating the selection of a channel

6.3.1.2 Utilization of transmission power control

CR enables a SU to dynamically adjust its transmission parameters in order to improve its communication performance, while protecting PUs from interferences (see Chapter 2). Therefore, dynamic reconfiguration is not limited to the selection of the operating channel and might concern other parameters. For example, it makes sense to envisage a transmitter that dynamically selects the lowest transmission power that enables the receiver to get a signal with enough quality (e.g., signal-to-interference-plus-noise-ratio over a defined critical threshold). Figure 6.3, which omits some of the fixed transmission ranges on the CCC for a matter of intelligibility, illustrates a scenario with such possibility. When compared to the utilization of fixed transmission power, dynamic transmission power control might result in a reduction of the transmission and interference ranges. Consequently, the spatial reuse of the spectrum increases and the number of interfered PUs potentially decreases. Energy preservation is another relevant gain we expect to obtain from power control.

Power control-based approaches require the availability of practical mechanisms for a transmitter to be able to: (1) dynamically determine or a priori know the distance to the receiver; and (2) compute the appropriate transmission power for achieving the minimum required transmission range. COSBET-MAC, the OOB handshake-based distributed CR MAC protocol Chapter 3 defines, already applies power control in order to keep transmission range on the data channels constant and similar to the one achieved on the CCC, independently of the centre frequency in use. With the power control approach we describe next being applied to COSBET-MAC, transmission range on the CCC becomes the upper limit for transmission range on data channels.

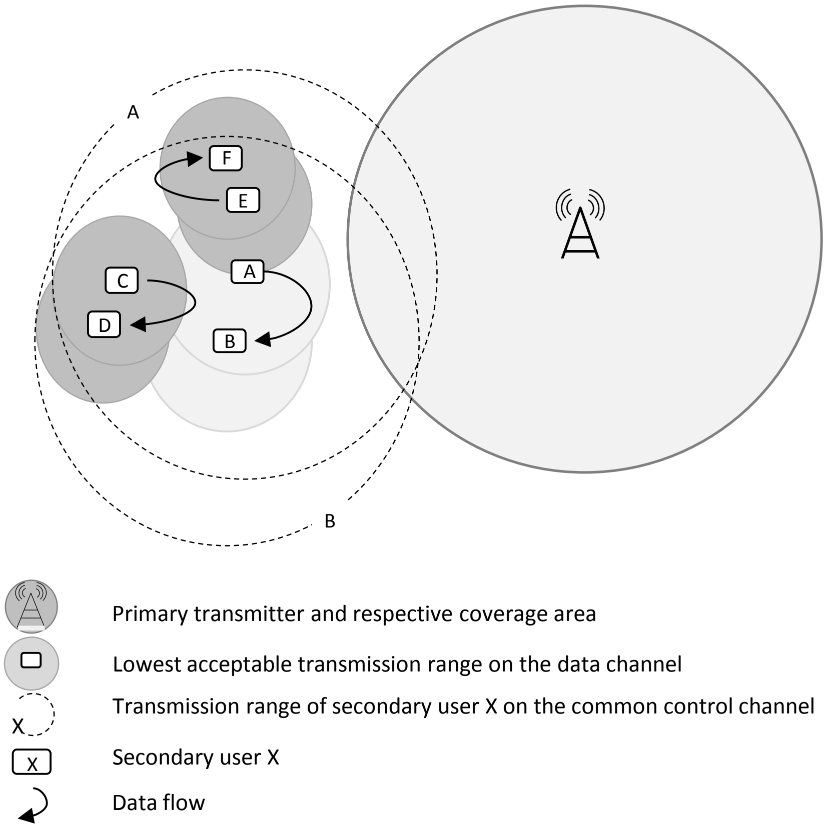


Figure 6.3. Minimum transmission range based on distance to receivers

There are different kinds of practical approaches that enable a SU to estimate the distance to its neighbours. For instance, we can consider that every SU is equipped with a GPS (Global Position System) device and that it piggybacks its coordinates in the control frames it transmits over the CCC. However, this approach suffers from inefficiency in terms of energy consumption, results in additional costs, and cannot work indoor [Franceschini et al., 2009; Xiao et al., 2007]. Currently, the most commonly used solution consists in determining the distance to a neighbouring node based on received signal strength indicator (RSSI). RSSI is usually modelled as a random variable with the mean related to the distance between the transmitter and the receiver. Using it for distance measurements requires knowing the emitter's transmission power, an accurate propagation loss model, and a statistical model of phenomena such as background noise [Yang et al., 2010; Clouqueur et al., 2001].

RSSI is also sensitive to several interference problems (e.g., obstacles) and adverse factors (e.g., multi-path fading). Hence, distance estimation based on RSSI is limited in terms of accuracy [Niculescu, 2004]. However and despite other approaches are possible for automated distance determination, RSSI is still the prime candidate for range measurements, mainly due to its simplicity and low cost [Savarese et al., 2001; Franceschini et al., 2009; Niculescu, 2004]. Other possible approaches include, for instance, having the nodes equipped with arrays of directional antennas that enable determining the angles of arrival (AoA) of the received signals using principals of trigonometry [Savarese et al., 2001]. When compared to the use of RSSI, this approach has the advantage of not requiring any a priori knowledge of the transmission power of the transmitters and being more precise.

Based on the previous discussion, we enable a SU to dynamically adjust its transmission power to a level that results in a transmission range that coincides with the distance to the receiver (see Figure 6.3). Without loss of generality or practicality, we assume that every SU estimates the distances to its neighbours based on the RSSI of the frames it receives and overhears on the CCC. With this approach, a SU dynamically estimates and records the distance to a given neighbour any time it receives or overhears a control frame from it on the CCC. The SUs must also apply an aging mechanism to account for the possibility of mobility or time-varying characteristics in the CR scenario.

Since the transmission parameters on the CCC are fixed and each SU a priori knows them, the utilization of RSSI over that channel can be considered feasible in practical terms. The same assumption cannot be applied to the reconfigurable radios as their transmission parameters (e.g., operating frequency, transmission power) vary dynamically over time. Each SU must take into account RSSI-based distance estimation imprecision when adjusting its transmission power. The reason is as follows: if the required power is underestimated, the transmitter stops being able to reach the intended receiver and a temporarily connection loss occurs. A possible approach for addressing this issue consists in adding a safety margin to the estimated distance. If some of the statistical characteristics of distance estimation errors are known (e.g., lower and upper bound limits), then, the safety margin can be objectively defined.

Algorithm 6.1 and Algorithm 6.2 already consider the possibility of integrating power control based on distance estimation with OOB handshake-based distributed CR MAC protocols. A SU runs Algorithm 6.1 to determine if it can use a channel, either as transmitter or receiver, without going into conflict with known neighbours. Algorithm 6.2 is the algorithm that enables a SU that overhears a control frame during a selection phase (see Figure 5.2) to determine if there is any conflict with itself. When underlying distance estimation and power control capabilities are available to the SUs, these two algorithms take into account the transmission ranges that neighbouring transmitter-receiver pairs are planning to use or are already using. This information is provided in the control frames that are exchanged and overheard over the CCC. The transmitter of a control frame sets the corresponding field with the distance it estimates to the destination or an invalid value when distance estimation is not available.

Globally, Algorithm 6.1 and Algorithm 6.2 jointly enable a SU to determine if it can interfere with and be interfered by any neighbouring pair. The higher efficiency in terms of spatial reuse of the spectrum is expected to be achieved when addressing the exposed node problem, i.e., when not using acknowledgement frames on the data channels, and applying transmission power control. For instance, the three pairs in Figure 6.3 are allowed to use the same channel simultaneously with this approach. On the contrary, if acknowledgement frames are replied over the data channels upon the reception of data frames, pairs A-B and E-F in Figure 6.3 are denied access to the same channels simultaneously since there is no distinction between transmitters and receivers in decision making. As signalling is achieved through the CCC, it is not affected by power control on the data channels (e.g., in Figure 6.3, all the pairs remain able to share signalling information with each other over the dedicated CCC).

6.3.2 Reduction in the number of transmitted control frames

Negotiation between two SUs that follow the OOB handshake approach starts with the transmitter issuing an IC frame to the receiver over the CCC through a contention-based approach similar to IEEE 802.11 DCF (Distributed Coordination Function). If the transmitter receives a reply back, then, negotiation proceeds. Additionally, overhearing control frames on the CCC enables the neighbours of a transmitter-receiver pair to set the CCC as being reserved for the specified amount of time and to refrain themselves from accessing it. On the other hand, if a transmitter does not receive a reply back after a defined timeout period or receives it with no channel selected, it backs-off for a random period before issuing another IC frame. After a predefined maximum number of tries, the data frame awaiting to be transmitted is discarded from the MAC output queue. In this section, we discuss and propose a solution that contributes to decrease the number of uselessly transmitted control frames and, therefore, reduces the number of data frames discarded due to exceeded number of attempts (see Figure 6.1). We designate it as late reply.

The problem we address through late replies is as follows. The control frames that are sent over the CCC include a reservation time for that channel and are overheard by all the neighbours of the transmitter. During reservation time, these neighbours suspend the counting of any ongoing back-off period and, therefore, refrain themselves from accessing the CCC. However, there is the possibility that a SU in a given multi-hop CR network considers the CCC to be idle while the SU it wants to transmit a data frame to does not. For instance, that is always the case of SU A in Figure 6.4 since it is out of the transmission ranges of all the active SUs in the network except SU B (i.e., the SU it targets). If we assume that SU B does not have to handshake with any other SU in the network, SU A never sets the CCC as being reserved and, therefore, issues an IC frame any time it has data to transmit and concludes backing-off. However, SU B, the destination of SU A in Figure 6.4, might have the CCC set as reserved due to neighbouring activities and, therefore, remains silent even when it is idle and correctly receives an IC frame from SU A.

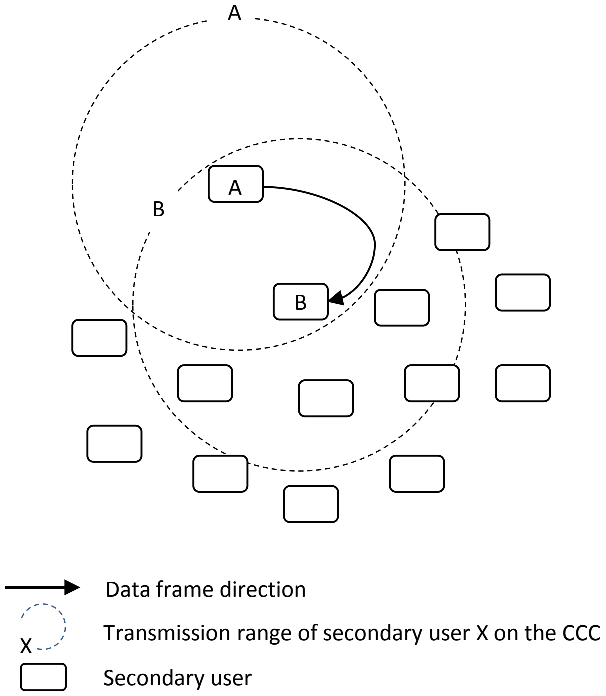


Figure 6.4. A scenario prone to ignored initial control frames

Since during a sensing phase there are no activities on a reserved CCC, a control frame sent by SU A in Figure 6.4 might be appropriately received by SU B, i.e., with no collisions occurring at its location. Consequently, SU A repeatedly times out, backs-off, and retransmits IC frames up to the defined limit. This issue, which we designate as the ignored IC frame problem, might affect a large extension of consecutive retransmissions. The higher is the load on the network, the more often is the CCC busy and, therefore, the more frequent is the occurrence of this issue that affects SU A in Figure 6.4. Consequently, we might expect SU A to exhibit a higher number of IC frames per transmitted data frame and more exceeded try limits than other SUs in Figure 6.4. We address this issue through late replies, as described next.

OOB handshake-based distributed CR MAC protocols and, globally, other wireless MAC protocols estimate time to receive a reply back after a frame was successfully sent taking into account maximum air propagation time and time required to transmit the reply, and use it to define an appropriate timeout value. We name this approach as regular timeout. The basic idea to address the ignored IC frame problem is as follows. A SU that transmits an IC frame awaits a reply back up to an extended timeout period that is in order of magnitude of a complete OOB handshake process (see Figure 5.2). The CCC reservation time value that IC frames include, such as the other control frames do, is also determined by this extended timeout value. A SU can use an estimated value on start-up for handshake time and, then, continuously adjust it based on the values it observes.

A SU that receives an IC frame and has the CCC set as reserved still remains silent as native OOB handshake-based distributed CR MAC does. However, it records this request as well as its time of reception. If multiple IC frames are received while the CCC is busy, only the last one is recorded. Then, when the CCC goes unreserved, the SU processes the recorded IC frame. If time that has elapsed since its reception is lower than the extended timeout value minus a margin that accounts for several factors such as air propagation and transmission times, then, a reply is issued. Otherwise, the recorded IC frame is discarded. With this approach, we are reducing the number of uselessly sent IC frames and also the possibility of exceeding the defined maximum number of IC tries per data frame.

Despite effectively addressing the problem that consists in a receiver ignoring IC frames addressed to it due to the busy status of the CCC, the approach we define and designate as late reply has a negative side effect when a missed reply does not result from this type of issue (e.g., it results from a collision or bit errors affecting the IC frame or the corresponding reply frame). In this case, as there is no possibility for the transmitter to ever receive the expected reply back, the use of extended timeouts and extended CCC reservation times is a waste of time that slows down the recovery process and has a negative impact on performance when compared to the utilization of regular timeouts. The neighbours of the transmitter of an IC frame are also affected since they set the CCC as being reserved for a longer time. With regular timeouts, a new attempt is made as soon as possible. On the contrary, extended timeouts account for the time required to exchange additional control frames plus sensing time (see Figure 5.2). Therefore, when an ignored IC is not the cause of a missed reply, the most appropriate solution remains using regular timeouts.

We address the aforementioned issue through a hybrid approach in which, for a given data frame awaiting transmission, a SU uses a regular timeout on the first IC frame transmission attempt and the late reply approach for any subsequent attempt (see Algorithm 6.3 for a global description).

Inputs:

- *r*, the number of initial control frames already sent;
- *c*, the number of initial control frames sent since the last time a frame was received/overheard on the CCC;
- *n*, an established threshold for *c* and above which the late reply approach is to be used;
- *ts*, timeout strategy (use_short_timeout or use_extended_timeout).

Output: *true* if an initial control frame/reply frame exchange was effectively completed for the data frame awaiting transmission in the MAC output queue and *false* otherwise.

```
$r \leftarrow 0$
$c \leftarrow 0$
while $r$ < maximum number of attempts per data frame do
    back-off for a random period
    if any control frame was received/overheard on the CCC during back-off period
        then $c \leftarrow 0$
    $r \leftarrow r + 1$
    $c \leftarrow c + 1$
    if $c <= n$ then
        $ts$ = use_regular_timeout
    else
        $ts$ = use_extended_timeout
    end if
    transmit the initial control frame piggybacking $ts$
    wait for the reply frame up to the timeout value defined by $ts$
    if reply received then return true
    if any control frame was received/overheard on the CCC while waiting for a reply
        then $c \leftarrow 0$
end while
return false
```

Algorithm 6.3. Transmission of initial control frames based on the use of regular and extended timeouts

For a matter of generalization, Algorithm 6.3 uses parameter *n*, i.e., it applies late reply and extended timeout after *n* consecutive regular timeouts instead of just one. This parameter can assume any integer value between zero and the maximum number of IC tries allowed per data frame. The lowest and highest values are two limits that correspond to always and never using late replies, respectively. Any time a new data frame starts being processed or a control frame from any source is correctly received or overheard on the CCC, a SU resets the counting of consecutive missed replies. That is, parameter *c* in Algorithm 6.3 is set to zero (see steps 2, 5, and 16 in Algorithm 6.3). In this case, we assume that the problem we address through late replies is not affecting the SU. That is, the SU does not incorrectly consider the CCC as being always idle and, consequently, does not issue IC frames in vain and at disproportionate rates. We recall that control frames carry a CCC reservation time. Therefore, the SUs that overhear them suspend any back-off counting process during the specified period. With the hybrid approach we propose, the destination of an IC frame must be informed about the timeout strategy the transmitter is using. The straightforward approach consists in including an additional control bit in IC frames.

Table 6.1 summarizes the characteristics of the PEL strategy. It also makes a reference to the respective algorithms and describes any additional field that is required for the control frames to support it. We observe that the PEL strategy results in minimal additional control overhead.

Table 6.1: PEL strategy

			Fields included in some of the control frames		Frames of the selection phase		Frames of the decision phase
Aim	Component	Algorithm	Field	Size (bits)	IC	Reply	
Improved spatial reuse of the spectrum	Power control	1 and 2	*tr* - transmission range to be used on the selected data channel	*m* [a]		yes	yes
	Avoidance of the exposed node problem	1 and 2					
Reduction in the number of transmitted control frames	Late reply	3	*ts* - timeout strategy (regular or extended)	1	yes		

[a] Large enough to represent the maximum allowed transmission range with the intended precision.

6.4 Performance evaluation

This section evaluates, through simulation, the PEL strategy that the current chapter proposes and that aims at improving OOB handshake-based distributed CR protocols in terms of the performance that is delivered to the SUs. It also analyses its effect on the protection of PUs, a major concern of CR. In order to produce results that enable supporting the discussion and draw appropriate conclusions, the same simulation experiments are repeated using different combinations of the three components included in the PEL strategy (see Table 6.1). Power control, one of the PEL components, depends on the availability of automated distance estimation mechanisms and accurate propagation models. Such requirements might not be met on real deployments. Therefore and for a matter of practicality, it is relevant to provide results that omit this component. For a comparison basis, we provide results for IEEE 802.11, which is representative of commonly used single-channel access protocols. The aim is evaluating the gains that can result from making a shift to CR in ad-hoc networks as well as if the PEL strategy is able to further improve it.

The previous chapters also provide optimization solutions for OOB handshake-based distributed opportunistic CR scenarios. Therefore, we also take them into account. That is, the current section also evaluates the overall MAC-level contributions of this thesis regarding the communication performance of SUs and the protection of PUs. These solutions, which we consider beyond the PEL strategy, are: the cooperative sense-before-transmit approach proposed in Chapter 3; FIBASC, the algorithm defined in Chapter 4 for an effective utilization of prediction capabilities; and CORHYS, the solution specified in Chapter 5 to address the CCC saturation problem. We recall that the first two solutions aim at addressing issues that arise in scenarios that suffer from the hidden PU problem. Consequently, when such problem does not exist, using them has no relevant effects.

6.4.1 Simulation setup

Such as in previous chapters, we use the OMNeT++/MiXiM platform [OMNeT++ Network Simulation Framework, 2010; MiXiM, 2010] to implement the simulation model of the PEL strategy. We also utilize the implementation of COSBET-MAC, the CR MAC protocol that Chapter 3 describes and evaluates, as our OOB handshake-based CR MAC solution. Therefore, we implement the PEL strategy on top of it. The cooperation of idle neighbours, a specific characteristic of COSBET-MAC, is inhibited by default. The simulation scenario is the one in Figure 6.5 and the most relevant settings are listed in Table 6.2. Globally, the simulation scenario in Figure 6.5 aims at including representative adverse and challenging characteristics. For example, we can mention that the number of channels is considerably lower than the number of SUs in the network and the hidden PU and hidden SU problems are a concern. As discussed in Section 6.3.1.2, we assume that each SU uses the RSSI of control frames received and overheard on the CCC to estimate its distance to neighbours.

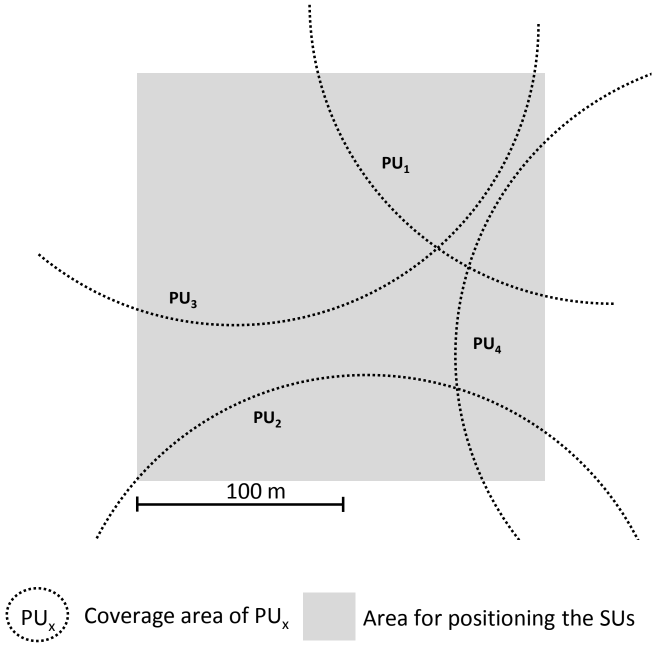


Figure 6.5. Simulation scenario

The simulation scenario includes four PUs with each one having a specific channel licensed to it. PU activities are characterized by alternating idle and busy periods exponentially distributed with means 0.1 and 0.01 seconds, respectively, such as in the work of Issariyakul et al. [2009]. The SUs opportunistically use the four licensed channels for data transmission. Mean load per transmitter varies up to 2 Mbit/s. Data frame payload length is set to 16 Kbit and time between arrivals is exponentially distributed with the parameter adjusted according to the targeted mean load. In some of the experiments, we use IEEE 802.11 as a comparison basis. Therefore, for fair comparison, the maximum number of IC frame tries per data frame is set to seven, which is similar to default IEEE 802.11 short retry count. For the same reason and since the MAC-level CR solutions we evaluate do not consider the retransmission of data frames, IEEE 802.11 long try count is set to one. We use the default simple path loss model of MiXiM and transmission power is set such that the transmission range is 100 meters on the CCC, on data channels, and for IEEE 802.11 nodes, independently of the respective operating frequencies. Some experiments use variations of the specified simulation settings. We specify them at the time they are used. The presented results are averaged over 15 runs of 300 seconds simulated time and with different seeds.

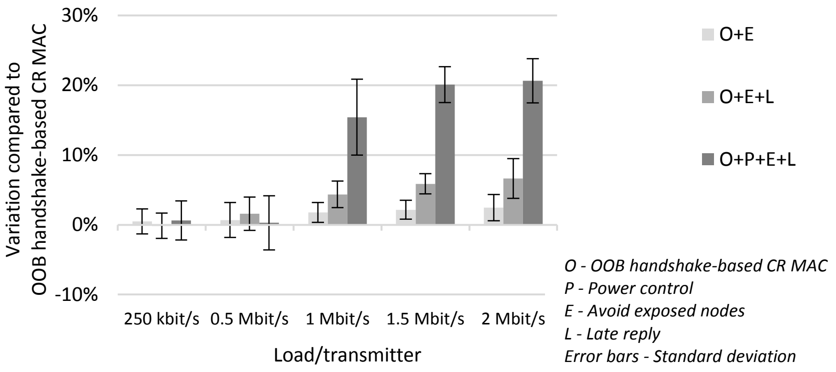
Table 6.2: Simulation settings

Parameter	Value	Remark
Size of the simulation area	200 meters x 200 meters	
Number of secondary users	32	
Number of transmitter-receiver pairs	16	
Positioning of the SUs	Uniform random	
Simulation time	300 s	
Runs	15	
Maximum distance between transmitter and receiver	100 meters	
Number of channels	4	
Bit rate on the data channels	2 Mbit/s	
Maximum transfer unit	18432 bits	Similar to IEEE 802.11.
IC frame retry limit per data frame	7	Same value as default IEEE 802.11 short retry count.
Channel switching time	10^{-4} seconds	Such as in the work of Jia and Zhang [2009].
Sensing time	0.5 milliseconds	Fast sensing recommended to be under one millisecond [IEEE 802.22 Working Group on Wireless Regional Area Networks, 2013].
Bit rate on the CCC	2 Mbit/s	
Transmission range on the CCC, data channels, and IEEE 802.11	100 meters	
IEEE 802.11 long try count	1	Default value is 4.
IEEE 802.11 RTS-threshold	400 bits	
MAC queue size	50 frames	

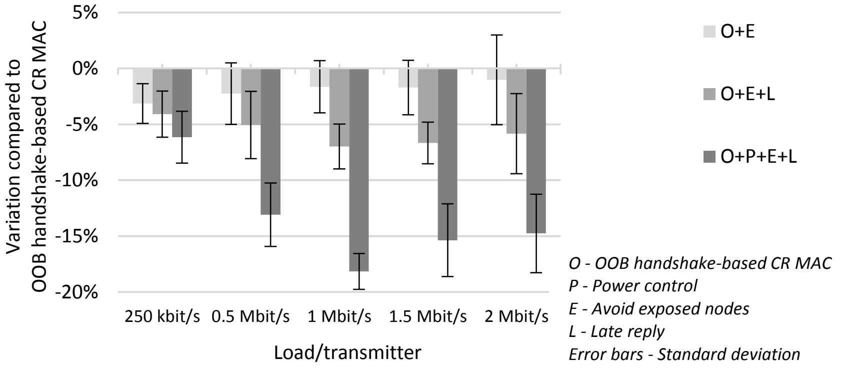
6.4.2 *Effectiveness of the PEL strategy*

We first assess if the PEL strategy effectively improves the performance of SUs when applying the default simulation settings specified in the previous section. We use aggregate throughput and the average number of IC frames per transmitted data frame as evaluation metrics. Comparison is established with the results obtained with the OOB handshake-based CR MAC we use (i.e., COSBET-MAC without cooperation of neighbours).

Figure 6.6 presents the obtained results when applying the three components of the PEL strategy (see Table 6.1), individually and jointly, to OOB handshake-based CR MAC. The error bars show the standard deviation between the 15 runs. From these results, we conclude that all the PEL components provide effective gains concerning the two metrics under analysis. Power control is the component that contributes the most for performance improvement since it allows a higher number of transmitters to use the same channel simultaneously. It is followed by late reply. Addressing the exposed node problem results in relatively modest gains since this issue concerns a limited number of transmitter-receiver pairs in the simulation scenario in use. If we ignore the possibility of power control based on distance estimation, the single component of the PEL strategy that might not be feasible in some real deployments, we observe that OOB handshake-based distributed CR MAC protocols still benefit from using the two other components.



a) Variation of aggregate throughput when compared to OOB handshake-based CR MAC



b) Variation in the number of initial control frames transmitted per data frame when compared to OOB handshake-based CR MAC

Figure 6.6. Gains provided by the PEL strategy

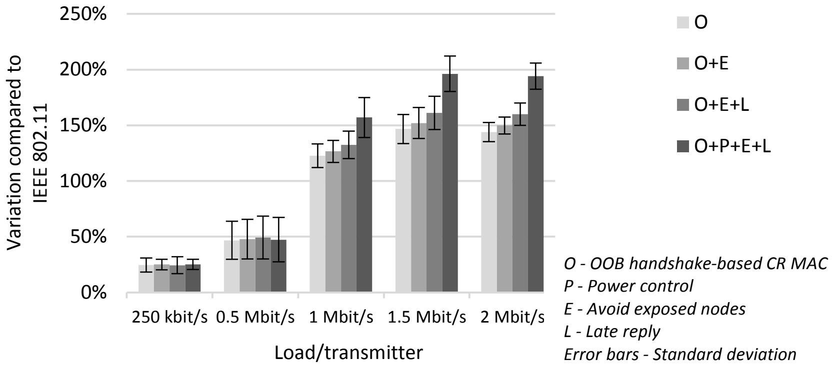
We observe in Figure 6.6 that the standard deviation between runs associated with each data point is significant. The main reason is as follows. Since the locations of the SUs in the simulation scenario are randomly defined (with a uniform distribution), their relative positions to each other and to the PUs varies over the different simulation runs. Consequently, the level of occurrence of the issues that the PEL strategy aims at addressing also varies over the runs. For example, the exposed node problem might affect several transmitter-receiver pairs in a given run and no pairs in another run. Therefore, addressing the exposed node problem has results that vary significantly between runs. Nevertheless, based on the obtained results, we can state that the late reply and power control components of the PEL strategy provide effective gains regarding the number of IC frames transmitted per data frame and the throughput of SUs when load per transmitter exceeds 0.5 Mbit/s (i.e., when the MAC output queues start filling up due to saturation), although results vary over the runs due to the mentioned randomness of the simulation scenario. On the other hand, addressing the exposed node problem does not result in effective gains for several runs (i.e., simulation scenarios) despite the obtained values are positive on the average both concerning the throughput of SUs and the number of IC frames transmitted per data frame.

6.4.3 Comparison with single-channel access approach

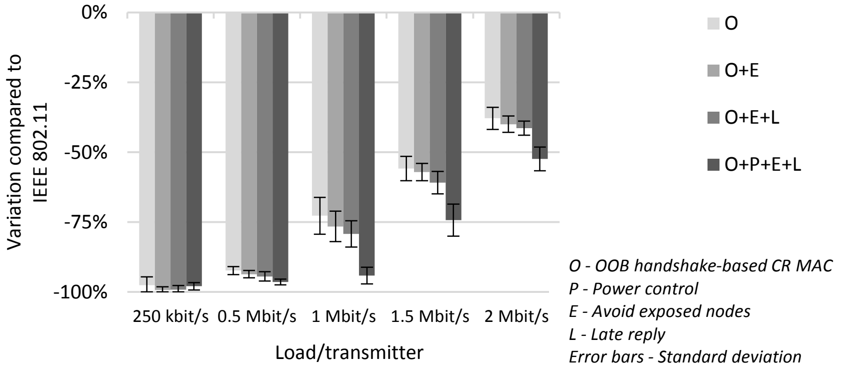
We now compare the performance of OOB handshake-based distributed CR MAC protocols optimized through the PEL strategy with a single-channel access approach, i.e., IEEE 802.11, using the same simulation settings as defined in Section 6.4.1. The aim is evaluating the improvement that results from a shift to CR and from the utilization of the PEL strategy, which is not CR specific.

Figure 6.7 and Figure 6.8 present the obtained results with error bars that show the standard deviation between the runs. Beyond aggregate throughput, we also consider three other performance metrics that are particularly relevant for applications with QoS requirements. One of them is the percentage of lost frames (see Figure 6.7), i.e., transmission requests received by the MAC entity and that do not result in data frames reaching destination due to diverse factors such as bit errors and MAC queue overflows. Packet loss is a major performance parameter for many applications with QoS requirements. Additionally, some applications are sensitive to latency (i.e., transmission delay from source to destination) and jitter (i.e., variation between the latency of two consecutive frames). Therefore, we also consider these parameters and present the obtained results in Figure 6.8. For example, video-phony, which is an example of an application with both audio and video data, requires minimum delay and minimum jitter. On the contrary, video-on-demand applications are more sensitive to jitter [Chen et al., 2004; Clouqueur et al., 2001]. With real-time services, packet loss and jitter are preferred over extra delays since large delays result in new data overriding old data and, consequently, in packet loss [Zhang et al., 2009].

Based on the results depicted in Figure 6.7 and Figure 6.8, we conclude that distributed opportunistic CR effectively improves the four performance metrics under analysis when compared to single-channel access. We also conclude that the PEL strategy has the ability to further improve it. The main reason for the observed standard deviation between runs, which is particularly significant for the variation of data frame latency (see Figure 6.8), consists in the randomness of the simulation scenario (e.g., locations of the SUs, PU traffic, SU traffic), as already discussed in section 6.4.2. When not applying power control based on distance estimation, which might be the considered due to practical limitations, there is an expected degradation of performance. Nevertheless, results still remain positive and the remaining PEL components still contribute to increase the four performance metrics we consider in Figure 6.7 and Figure 6.8. The effect of the PEL strategy, particularly of its power control component, is more visible for loads over 0.5 Mbit/s per transmitter, i.e., when saturation starts occurring and, consequently, the MAC output queues start filling up. In this case, we also observe that the late reply component slightly affects latency as expected.



a) Variation of aggregate throughput when compared to IEEE 802.11

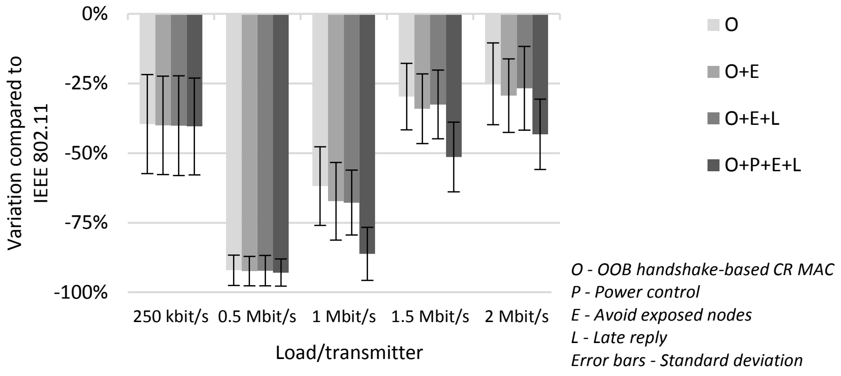


b) Variation in the rate of data frame loss when compared to IEEE 802.11

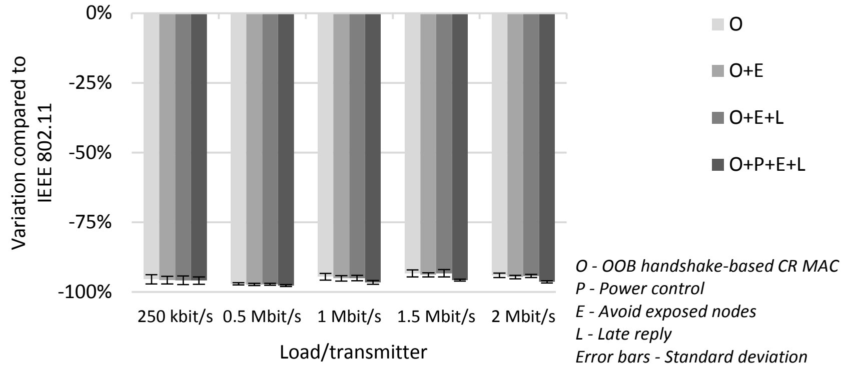
Figure 6.7. Comparison with IEEE 802.11 (aggregate throughput and data frame loss)

6.4.4 Protection of primary users

PU protection is a key concern of CR and there is often a trade-off between it and the performance that is delivered to the SUs. That is, in many situations, the higher is the protection of PUs the lower is the expected performance of SUs since the number of false spectrum opportunities the SUs access decreases, and vice-versa. Furthermore, it is not acceptable to improve communication performance at the expense of PU protection degradation. The current section evaluates the impact of the PEL strategy on PU protection. With this purpose, we also take into account the possibility of jointly using the mechanisms proposed in Chapter 3 and Chapter 4 for higher PU protection in distributed CR scenarios with hidden PUs. They are the cooperation of idle neighbours in sensing (see Chapter 3) and FIBASC (see Chapter 4), respectively. We recall that Chapter 4 states that the utilization of FIBASC (or any other solution with the same objective) is mandatory in distributed scenarios with hidden PUs when the SUs have prediction capabilities based on learning through local observation and past experience.



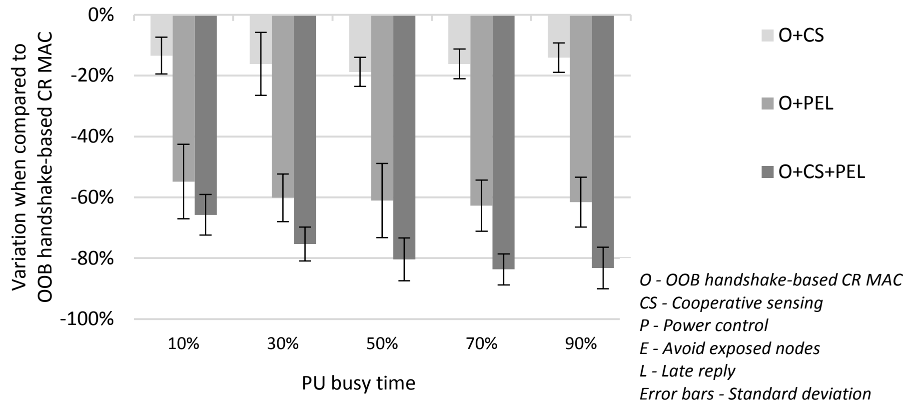
a) Variation of data frame latency when compared to IEEE 802.11



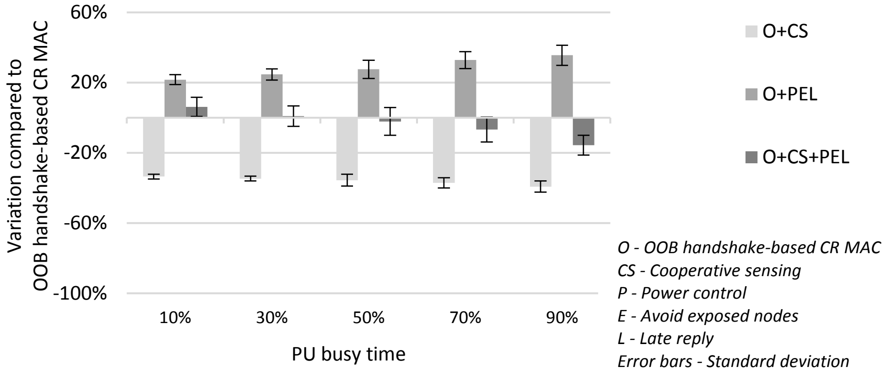
b) Variation of data frame jitter when compared to IEEE 802.11

Figure 6.8. Comparison with IEEE 802.11 (latency and jitter)

The evaluation metrics we use are the variation in the ratio of interfered PU activities to transmitted data frames and the variation of aggregate throughput when compared to OOB handshake-based CR MAC. We use the ratio to the number of transmitted data frames rather than absolute values in order to normalize the results and enable comparison across different runs and configurations. Figure 6.9 and Figure 6.10 depict the obtained results with error bars that show the standard deviation between runs.



a) Variation in the rate of interfered primary user activities when compared to OOB handshake-based CR MAC

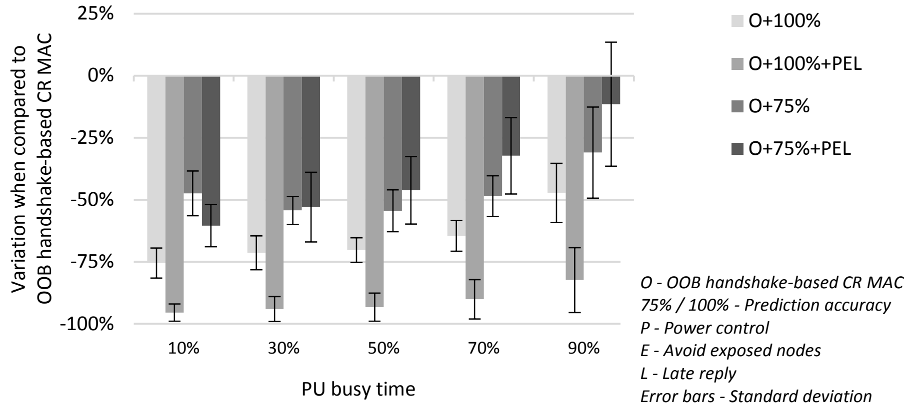


b) Variation of aggregate throughput when compared to OOB handshake-based CR MAC

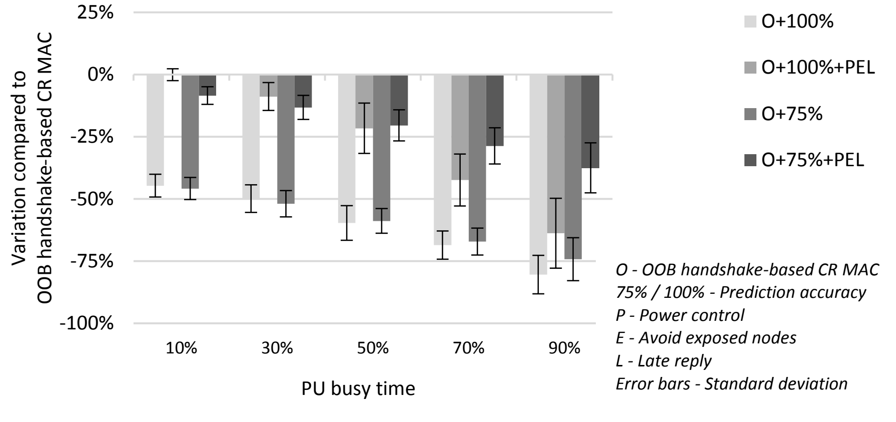
Figure 6.9. Protection of PUs and communication performance without prediction capabilities (2 Mbit/s load per transmitter)

In order to obtain the results depicted in Figure 6.9 and Figure 6.10, we use distinct PU activity characteristics. For this purpose, we consider that every data channel has PU activities characterized by alternating idle and busy periods exponentially distributed with parameters λ_i and λ_b, respectively, being the sum of the respective means equal to 0.1 seconds (i.e., $1/\lambda_i + 1/\lambda_b = 0.1$). Load per transmitter is set to 2 Mbit/s, i.e., beyond saturation point for all the configurations, and PU busy time varies from 10% to 90%. The other simulation settings are the same as specified in Section 6.4.1 and Table 6.2. Regarding FIBASC, we use its two-hop approach form and consider 100% and 75% prediction precisions. That is, we make an ideal and a more realistic assumption, respectively, about prediction accuracy in scenarios with non-deterministic PU traffic (see Section 2.7).

In Figure 6.9 and Figure 6.10, we observe that the PEL strategy increases the protection of PUs, even with idle neighbours cooperating in sensing or two-hop FIBASC being applied with 100% prediction accuracy. The observed standard deviation is primarily due to the already mentioned randomness of the simulation scenario (e.g., locations of the SUs, level of occurrence of the issues the PEL strategy aims at addressing, PU traffic, SU traffic). Nevertheless, the observed gains remain meaningful even though they vary with the simulation runs and, therefore, with the particular characteristics of targeted scenarios. In fact, the power control component of the PEL strategy is solely responsible for this result since it limits the transmission ranges of the SUs and, therefore, their interference ranges.



a) Variation in the rate of interfered primary user activities when compared to OOB



b) Variation of aggregate throughput when compared to OOB handshake-base CR MAC

Figure 6.10. Protection of PUs and communication performance with prediction capabilities and 2-hop FIBASC (2 Mbit/s load per transmitter)

On its own, power control increases the protection of PUs more significantly than cooperative sensing (see Figure 6.9). As expected, power control also enables improving the communication performance that is delivered to the SUs (Figure 6.9 and Figure 6.10). That is, it both increases the protection of PUs and reduces the negative impact of higher PU protection on the communication performance of SUs. The only exception occurs when FIBASC is used with imperfect prediction (i.e., 75% accuracy), which is a practical assumption (see Figure 6.10). In this case, we observe that power control results in poorer PU protection with higher PU busy times. The main reason is that it amplifies the effect of missed predictions since it allows more accesses in the simulation scenario at the same time, i.e., it improves spatial reuse of the spectrum.

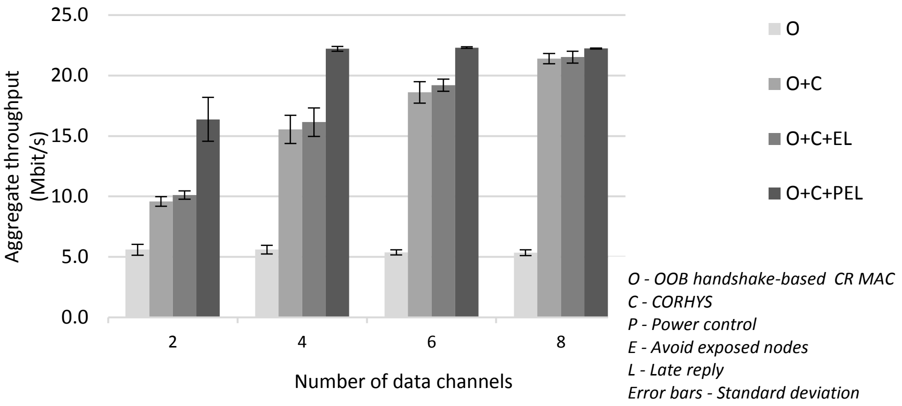
In Figure 6.10, we observe that applying two-hop FIBASC with fully accurate prediction never completely eliminates the interferences to PUs. The reason is as follows. With two-hop FIBASC, if a transmitter-receiver pair gets an empty set of candidate channels, the one-hop approach, which is less efficient concerning the protection of hidden PUs, is applied. If the same situation still occurs, then, filtering ends up not being applied to the channels (see Figure 4.6 in Chapter 4). Some of the transmitter-receiver pairs in the simulation scenario are, therefore, affected by this issue.

6.4.5 Joint utilization of the PEL strategy with CORHYS

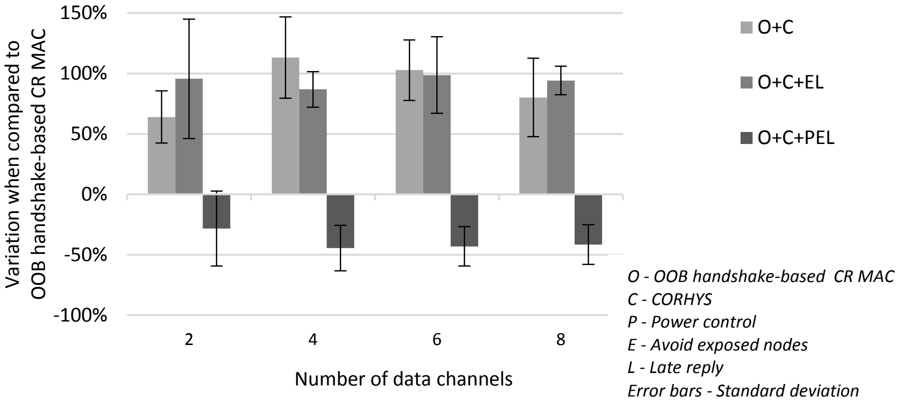
Chapter 5 discusses the CCC saturation problem that affects OOB handshake-based distributed CR MAC protocols. This issue limits the number of channels that can be effectively utilized at the same time in a CR network and, consequently, the number of SUs that are allowed to transmit data frames simultaneously. This limit depends on channel access time to handshake time ratio. The higher is access time the higher is the number of data channels that can be effectively accessed simultaneously through CR. Chapter 5 also proposes CORHYS, a solution that addresses this issue.

The current section aims at evaluating the PEL strategy when CORHYS applies, i.e., when the targeted CR MAC solution does not strictly follow OOB handshake on a single data frame basis and, consequently, is less affected by the CCC saturation problem. With the concern of taking into account the mechanisms for higher hidden PU protection proposed in Chapter 3 and Chapter 4, i.e., two of the contributions this thesis makes, we provide three distinct sets of results: when not using the mechanisms that target higher PU protection (see results in Figure 6.11); when idle neighbours cooperate in sensing (see results in Figure 6.12 and discussion in Chapter 3); and when two-hop FIBASC is used with fully accurate prediction accuracy (see results in Figure 6.13 and discussion in Chapter 4).

The evaluation metrics we use are the observed variation in the ratio of interfered PU activities to transmitted data frames when compared to OOB handshake-based CR MAC and aggregate throughput. We use the ratio to the number of transmitted data frames rather than absolute values in order to normalize the results and enable comparison across different runs and configurations. In order to obtain the results that Figure 6.11, Figure 6.12, and Figure 6.13 depict, we make the number of available channels vary from 2 to 8. This variation enables evaluating the channel utilization efficiency and, therefore, the impact of the solutions under analysis on the CCC saturation problem. The error bars show the standard deviation between the runs. Load per transmitter is set to 2 Mbit/s per transmitter, i.e., beyond saturation point for all the configurations, and data frame payload length is set to 4 Kbit. The other simulation settings are the same as specified in Section 6.4.1 and Table 6.2. The observed standard deviation, which is particularly significant regarding the variation in the rate of interfered PUs, is due to the randomness of the simulation scenario (e.g., PU traffic, locations of the SUs), as already discussed.



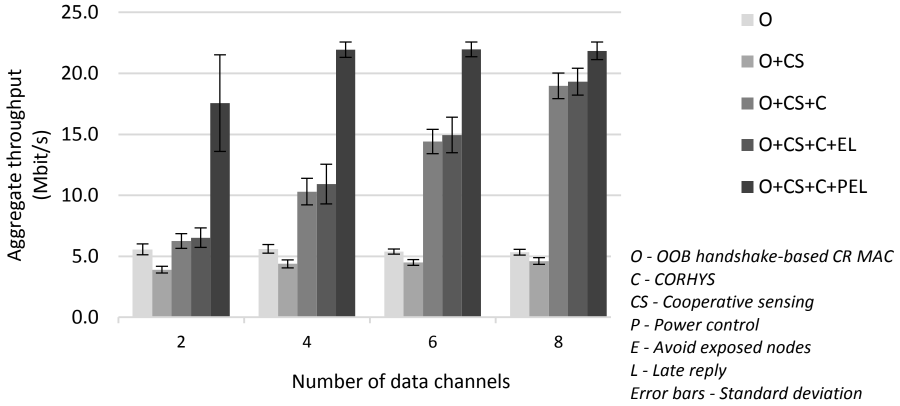
a) Aggregate throughput



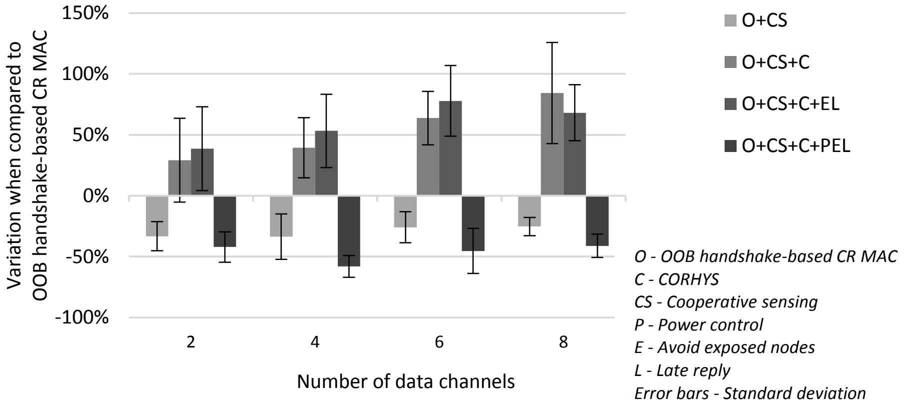
b) Variation in the rate of interfered primary user activities when compared to OOB handshake-based CR MAC

Figure 6.11. Integration with CORHYS (2 Mbit/s load per transmitter)

With 4 Kbit data frame payload length, the number of channels that the OOB handshake-based CR MAC simulation model we use (i.e., COSBET-MAC without cooperation of neighbours) can effectively utilize is limited to two, i.e., data channel access time to handshake time ratio is lower or equal to two and greater than one (see Table 5.4 and Table 5.5 in Chapter 5). Therefore and as depicted in Figure 6.11, Figure 6.12, and Figure 6.13, increasing the number of existing channels beyond two does not result in any throughput improvement due to the already mentioned CCC saturation problem. On the contrary, the obtained results show that applying CORHYS enables throughput to grow as the number of channels increases. That is, CORHYS successfully addresses the CCC saturation problem. We can also conclude that the PEL strategy can further improve performance, even when CORHYS applies, essentially due to its power control component that succeeds improving the spatial reuse of the spectrum.



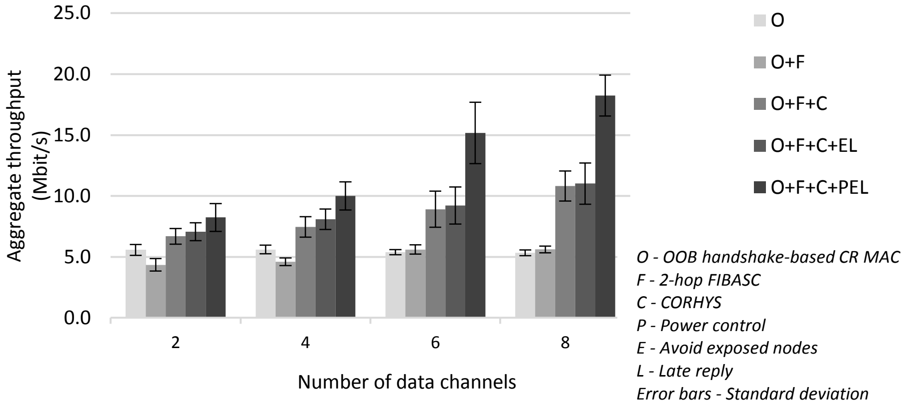
a) Aggregate throughput



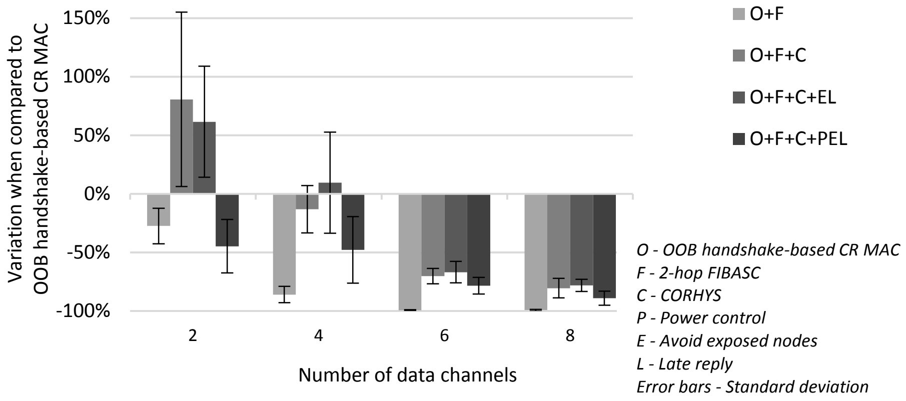
b) Variation in the rate of interfered primary user activities when compared to OOB handshake-based CR MAC

Figure 6.12. Integration with CORHYS and cooperation of idle neighbours in sensing (2 Mbit/s load per transmitter)

As expected from results in Chapter 3 and Chapter 4, we observe in Figure 6.12 and Figure 6.13 that using OOB handshake-based CR MAC with idle neighbours cooperating in sensing or FIBASC, respectively, improves the protection of PUs. Simultaneously, we also observe that these solutions result in a slight degradation of the throughput of the SUs since they reduce the number of accesses to false spectrum opportunities. That is, the cooperation of idle neighbours and FIBASC only target a higher protection of PUs. Results depicted in Figure 6.11, Figure 6.12, and Figure 6.13 also show that CORHYS lowers the protection of PUs since it allows more data channels to be accessed at the same time by distinct SUs and larger access times, and, therefore, more PUs to be interfered simultaneously (i.e., CORHYS only aims at improving the performance of SUs). Applying the power control component of the PEL strategy enables inverting the situation concerning the protection of PUs, even when including the cooperation of idle neighbours in sensing (see Figure 6.12) or FIBASC (see Figure 6.13), since it limits the interference ranges of the SUs.



a) Aggregate throughput



b) Variation in the rate of interfered primary user activities when compared to OOB handshake-based CR MAC

Figure 6.13. Integration with CORHYS, two-hop FIBASC, and 100% prediction precision (2 Mbit/s load per transmitter)

In Figure 6.13, we observe that almost all the interferences to PUs are eliminated (i.e., the observed reduction is over 99%) when solely applying two-hop FIBASC with fully accurate prediction and using more than four channels. The reason is that, in such circumstances, two-hop

FIBASC does not result in empty channel sets for any of the transmitter-receiver pairs in the simulation scenario and, therefore, there are no transmitter-receiver pairs that turn out following the one-hop approach or avoiding any channel filtering process (see related discussion in Section 6.4.4). For the same reason, we also observe, in Figure 6.13, that the obtained results remain more consistent between different simulation runs, i.e., less prone to the specific characteristics of the targeted scenarios, when using more than four channels. Using CORHYS, decreases the protection level of PUs due to the previously mentioned reason.

6.5 Summary

Opportunistic CR aims at increasing spectrum utilization efficiency by allowing the SUs to dynamically locate and access frequency bands that are vacant. In cooperative distributed CR networks, the SUs take their own spectrum decisions based on local observation and information exchanged with neighbours, being the utilization of a dedicated CCC a common practice for OOB (Out-of-Band Handshake) signalling. The current chapter proposed and evaluated a MAC-level strategy, named PEL (Power control, avoidance of the Exposed node problem, and Late reply), which further improves the performance that is delivered to the SUs in OOB handshake-based distributed CR networks, increasing the spatial reuse of the spectrum and reducing control traffic. The components of the PEL strategy consist in addressing the exposed node problem, applying power control, and using late replies. The current chapter also provided a summary of the overall contributions this thesis makes since it also took into account the contributions of previous chapters when evaluating the PEL strategy.

The obtained simulation results show that the solutions we proposed in current and previous chapters, and which are exclusively based on observation and cooperation, are capable of providing effective gains in OOB handshake-based distributed CR networks. The PEL strategy and CORHYS, defined in current chapter and in Chapter 5, respectively, increase the performance of SUs. Using them jointly results in a performance improvement greater than using them individually. Concerning PU protection, a CR key issue, power control, one of the components of the PEL strategy, significantly improves it except when using FIBASC (see Chapter 4) with imperfect prediction accuracy. Since power control improves both the protection of PUs and the communication performance of SUs in most situations, using it does not require making a trade-off between these two objectives. However, power control is challenging in practical terms since it requires the availability of accurate propagation models and automated distance estimation features.

Chapter 7

Conclusions and future work

CR (Cognitive Radio) has emerged as a promising technology to address the spectrum scarcity problem. In this thesis, which specifically targets distributed opportunistic CR networks, we have studied issues that limit the protection of PUs (Primary Users) and the communication performance of SUs (Secondary Users), which are the two main concerns of CR. We have also proposed innovative MAC (Medium Access Control) level solutions to address them. These contributions resulted in a cooperative distributed CR MAC protocol that jointly: avoids complicated architectures with stringent synchronization requirements; copes with the hidden PU and hidden SU problems; enables the cooperation of idle neighbours in spectrum sensing and spectrum decision on a non-mandatory basis; includes a solution that enables tracking hidden PUs; enables the SUs to effectively use prediction features based on observation and past experience in scenarios with hidden PUs; performs signalling through a hybrid approach that mitigates the CCC saturation problem; uses power control and distance estimation, and addresses the exposed node problem in order to improve the efficiency of spectrum utilization; and reduces control traffic through an approach we named late reply.

The remainder of this chapter, which concludes this thesis, is organized as follows: Section 7.1 summarizes the main contributions provided in this work and Section 7.2 recommends issues that need to be addressed as future work.

7.1 Conclusions

The first chapter of this thesis provided a brief introduction to the work it describes, stressing its main motivation, objectives, and contributions. Then, Chapter 2 presented a literature survey on the CR area, focusing on related technologies, standardization activities, architectural approaches, relevant issues, communication protocols, and learning through observation and past experience. Our findings in the literature enabled us to identify CR issues that still needed further research at the starting point of this thesis. It also motivated us to specifically investigate

MAC-level solutions for an effective protection of PUs and an efficient utilization of spectrum opportunities in distributed CR networks with hidden PUs and hidden SUs.

COSBET-MAC (Cooperative Sense-Before-Transmit), a cooperative CR MAC protocol that specifically targets fully distributed CR networks, was defined and evaluated through simulation in Chapter 3. It includes a novel cooperative sense-before-transmit feature that increases the protection of PUs, based on a non-mandatory participation of idle SUs. The obtained evaluation results confirmed that COSBET-MAC can result in relevant gains, both in terms of the communication performance of SUs and the protection of PUs, under various operating parameters (i.e., sensing time, PU traffic characteristics, and data frame payload size) and taking into account the imperfect nature of sensors, which inherently have missed detection and false alarm probabilities.

Sensing is not sufficient to entirely eliminate all the interferences to PUs in CR scenarios, even when it produces fully accurate results, since PU activities can appear on a channel sensed idle before access time. Therefore, CR also expects the SUs to have learning capabilities that enable them to predict busy and idle times on the targeted channels. In fully distributed CR scenarios, these capabilities are intended to result from learning based on past experience and observation. In selection processes that follow a sense-before-transmit approach, such as with COSBET-MAC, priority must thus be given to channels that are likely to be vacant during the entire sensing and transmission times.

Chapter 4 firstly showed that, in a CR scenarios with hidden PUs, having SUs with prediction capabilities based on learning through observation and past experience does not necessarily result in the expected gains concerning the protection of PUs. Then, it defined a novel solution that addresses this problem and was named FIBASC (Filtering Based on Suspicious Channels). This solution consists in identifying and filtering, based on the sensing and learning outcomes of SUs, channels that probably suffer from the hidden PU problem. FIBASC was also integrated with COSBET-MAC based on a distributed and passive learning approach, and evaluated through simulation. The obtained results showed that it effectively enables the SUs to mitigate the negative effect of hidden PUs on the gains that result from learning through observation and past experience regarding the protection of PUs.

Results obtained in Chapter 3 showed that data frame payload size has great impact on the communication performance of distributed CR schemes that perform handshake over a dedicated CCC on a data frame basis. It was specifically observed that channel utilization efficiency decreases as payload size decreases and that it might even degenerate to single-channel, i.e., non-CR, access. In Chapter 5, we further analysed this issue and concluded that the efficiency of dedicated CCC-based solutions in utilizing all the available channels depends on the ratio between channel allocation time and handshake time. Additionally, Chapter 5 proposed and evaluated, through simulation, a solution that addresses this issue. CORHYS (Cognitive Radio Hybrid Signalling), as it was named, allows more vacant channels to be simultaneously accessed on distributed opportunistic CR networks and, consequently, improves the communication performance of SUs mitigating the CCC saturation problem.

Being defined two solutions to improve the protection of PUs in CR scenarios with hidden PUs (i.e., COSBET-MAC and FIBASC) and a solution to increase the communication performance of cooperative distributed CR MAC protocols that are based on a CCC and perform handshake on a data channel access basis (i.e., CORHYS), Chapter 6 was dedicated to define and evaluate a strategy that enables further increasing the performance of SUs. This MAC-level strategy, which we called PEL (Power control, avoidance of the Exposed node problem, and Late reply), aims at both increasing the spatial reuse of the spectrum and reducing control traffic. It is the last contribution of this thesis. The components of the PEL strategy, which are not CR specific in terms of applicability, consist in addressing the exposed node problem, applying power control, and using late replies. The innovative characteristic of Chapter 6 was essentially motivated by its late reply component and by the integration of all its components with each other and with the remainder contributions of this thesis, which resulted in an optimized distributed CR MAC protocol.

An evaluation of the impact of all the contributions in this thesis, when utilized individually and jointly, was also provided through simulation in Chapter 6. The obtained results show that there is usually a trade-off between the communication performance of SUs and the protection of PUs in CR. We also concluded that power control based on destination estimation, one of the three components of the PEL strategy, is an exception since it enables improving both aspects without requiring the mentioned compromise. However, this component might not be always feasible in real deployments since it requires the availability of accurate propagation models and automated distance estimation features.

7.2 Future work

We start mentioning that the solutions this thesis proposed lack validation on real deployments or experimental platforms due to time and other resource restrictions. Therefore, it should be considered as future work. CR testbeds already exist and the following were discussed in Chapter 2: ORBIT (Open-Access Research Testbed for Next-Generation Wireless Networks);

CORNET (Cognitive Radio Network); Emulab; CorteXlab (Cognitive Radio Testbed Experimentation Lab); CREW (Cognitive Radio Experimentation World); and CORE+ (Cognitive Radio Trial Environment+).

The contributions in this thesis were not defined or evaluated taking into account applications with specific requirements (e.g., real-time, quality of service, and quality of experience), which should be considered as future work. When defining FIBASC and the PEL strategy, in Chapter 4 and Chapter 6, respectively, we suggested that the SUs must apply a time-out or forgetting mechanism (e.g., regarding activities sensed in the past and the classification of data channels as suspicious channels), in order to account for scenarios with mobility or time-varying conditions. However, the contributions in this work were not validated under such circumstances, which must thus be analysed with more detail as future work and should possibly include the development of other adaptive strategies.

Since in this thesis we assume and simulate the availability of underlying prediction capabilities based on learning through past experience and observation, we must also consider the utilization of specific learning solutions. The same remark applies concerning the utilization of power control, which requires the availability of accurate propagation models and automated distance estimation features, particularly when using real deployments or experimental platforms. Finally, we mention that it is worth analysing the applicability and adaptation of the contributions in this thesis to other types of scenarios (e.g., centralized CR networks).

References

[Ahmed et al., 2013] Ahmed, A., Bakar, K. A., Channa, M. I., and Qureshi, K. N. (2013). A simulation based study of well known routing protocols for delay tolerant network. *World Applied Sciences Journal, 28*(3), 353-360.

[Akyildiz and Wang, 2005] Akyildiz, I. and Wang, X. (2005). A survey on wireless mesh networks. *Communications Magazine, 43*(9), S23-S30.

[Akyildiz et al., 2006] Akyildiz, I., Lee, W., Vuran, M., and Mohanty, S. (2006). NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey. *Computer Networks, 50*(13), 2127-2159.

[Akyildiz et al., 2008] Akyildiz, I., Lee, W., Vuran, M., and Mohanty, S. (2008). A survey on spectrum management in cognitive radio networks. *Communications Magazine, 46*(4), 40-48.

[Akyildiz et al., 2009] Akyildiz, I., Lee, W., and Chowdhury, K. (2009). CRAHNs: Cognitive radio ad hoc networks. *Ad Hoc Networks, 7*(5), 810-836.

[Akyildiz et al., 2011] Akyildiz, I., Lo, B., and Balakrishnan, R. (2011). Cooperative spectrum sensing in cognitive radio networks: A survey. *Physical Communication, 4*(1), 40-62.

[Al-Karaki and Chang, 2004] Al-Karaki, J. and Chang, J. (2004). Quality of service support in IEEE 802.11 wireless ad hoc networks. *Ad Hoc Networks, 2*(3), 265-281.

[Amanna and Reed, 2010] Amanna, A. and Reed, J. (2010). Survey of cognitive radio architectures. *Proceedings of the IEEE SoutheastCon 2010* (pp. 292-297). IEEE.

[Anastasi et al., 2003] Anastasi, G., Borgia, E., Conti, M., and Gregori, E. (2003). IEEE 802.11 ad hoc networks: performance measurements. *23rd International Conference on Distributed Computing Systems Workshops, 2003* (pp. 758-763). IEEE.

[Ansari et al., 2013] Ansari, J., Zhang, X., and Mähönen, P. (2013). A decentralized MAC protocol for opportunistic spectrum access in cognitive wireless networks. *Computer Communications, 36*(13), 1399-1410.

[Araujo et al., 2012] Araujo, A., Blesa, J., Romero, E., and Villanueva, D. (2012). Security in cognitive wireless sensor networks. Challenges and open problems. *EURASIP Journal on Wireless Communications and Networking, 2012*(48). doi:10.1186/1687-1499-2012-48

[Atakli et al., 2008] Atakli, I. M., Hu, H., Chen, Y., Ku, W. S., and Su, Z. (2008). Malicious node detection in wireless sensor networks using weighted trust evaluation. *Proceedings of the 2008 Spring Simulation Multiconference, 2008* (pp. 836–843). Society for Computer Simulation International.

[Baddour et al., 2011] Baddour, K., Üreten, O., and Willink, T. (2011). A Distributed Message-passing Approach for Clustering Cognitive Radio Networks. *Wireless Personal Communications, 57*(1), 119-133.

[Bahl et al., 2004] Bahl, P., Chandra, R., and Dunagan, J. (2004). SSCH: slotted seeded channel hopping for capacity improvement in IEEE 802.11 ad-hoc wireless networks. *10th annual international conference on Mobile computing and networking* (pp. 216–230). ACM.

[Bao and Fujii, 2011] Bao, S. and Fujii, T. (2011). Q-learning based p-pesistent csma mac protcol for secondary user of cognitive radio networks. *2011 Third International Conference on Intelligent Networking and Collaborative Systems (INCoS)* (pp. 336-337). IEEE.

[Beltrán et al., 2010] Beltrán, F., Gutiérrez, J., and Melús, J. (2010). Technology and Market Conditions Towards a new Competitive Landscape in the Wireless access Market. *Communications Magazine, 48*(6), 46-52.

[Bhushan and Murthy, 2013] Bhushan, B. and Murthy, B. (2013). Analysis of Throughput in WLANS considering Aggregation scheme using Mathematical modeling (MATLAB). *International Journal of Computer Networks and Wireless Communications, 3*(6).

[Biaz and Wu, 2008] Biaz, S. and Wu, S. (2008). OTLR: Opportunistic transmission with loss recovery for WLANs. *IEEE Wireless Communications and Networking Conference, 2008. WCNC 2008*. (pp. 1541-1546). IEEE.

[Bicen et al., 2012] Bicen, A. O., Gungor, V. C., and Akan, O. B. (2012). Delay-sensitive and multimedia communication in cognitive radio sensor networks. *Ad Hoc Networks, 10*(5), 816-830.

[Blesa et al., 2013] Blesa, J., Romero, E., Rozas, A., and Araujo, A. (2013). PUE attack detection in CWSNs using anomaly detection techniques. *EURASIP Journal on Wireless Communications and Networking, 2013*(1), 1-13.

[Brik et al., 2005] Brik, V., Rozner, E., Banerjee, S., and Bahl, P. (2005). DSAP: a protocol for coordinated spectrum access. *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.* (pp. 611-614). IEEE.

[Brown and Sethi, 2008] Brown, T. and Sethi, A. (2008). Potential Cognitive Radio Denial-of-Service Vulnerabilities and Protection Countermeasures: a Multi-dimensional Analysis and Assessment. *Mobile Networks and Applications, 13*(5), 516-532.

[Celebi and Arslan, 2007] Celebi, H. and Arslan, H. (2007). Utilization of Location Information in Cognitive Wireless Networks. *Wireless Communications, 14*(4), 6 – 13.

[Chang et al., 2014] Chang, C. Y., Wang, T. L., and Lin, C. Y. (2014). A MAC protocol by applying staggered channel model for cognitive radio networks. *Wireless Networks, 20*(7), 1873-1888.

[Chen and Park, 2006] Chen, R. and Park, J. (2006). Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks. *1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks. SDR '06*. (pp. 110 –119). IEEE.

[Chen et al., 2004] Chen, Y., Farley, T., and Ye, N. (2004). QoS requirements of network applications on the Internet. *Information Knowledge Systems Management, 4*(1), 55-76.

[Chen et al., 2008a] Chen, R., Park, J., and Reed, J. (2008a). Defense against Primary User Emulation Attacks in Cognitive Radio Networks. *IEEE Journal on Selected Areas in Communications, 26*(1), 25–37.

[Chen et al., 2008b] Chen, T., Zhang, H., Matinmikko, M., and Katz, M. (2008b). CogMesh: Cognitive Wireless Mesh Networks. *GLOBECOM Workshops, 2008* (pp. 1-6). IEEE.

[Chen et al., 2008c] Chen, Y., Yu, G., Zhang, Z., Chen, H. H., and Qiu, P. (2008c). On cognitive radio networks with opportunistic power control strategies in fading channels. *IEEE Transactions on Wireless Communications, 7*(7), 2752-2761.

[Chen et al., 2012a] Chen, C. Y., Chou, Y. H., Chao, H. C., and Lo, C. H. (2012a). Secure centralized spectrum sensing for cognitive radio networks. *Wireless Networks, 18*(6), 667–677.

[Chen et al., 2012b] Chen, C., Song, M., Xin, C., and Alam, M. (2012b). A robust malicious user detection scheme in cooperative spectrum sensing. *2012 IEEE Global Communications Conference (GLOBECOM)* (pp. 4856–4861). IEEE.

[Chen et al., 2013] Chen, J., Jiao, L., Wu, J., and Wang, X. (2013). Compressive spectrum sensing in the cognitive radio networks by exploiting the sparsity of active radios. *Wireless Networks, 19*(5), 661-671.

[Chen et al., 2014] Chen, C., Song, M., and Xin, C. (2014). CoPD: a conjugate prior based detection scheme to countermeasure spectrum sensing data falsification attacks in cognitive radio networks. *Wireless Networks, 20*(8), 2521-2528.

[Choi and Nettles, 2005] Choi, S. H. and Nettles, S. M. (2005). An overhead controlled MAC protocol for high data-rate wireless networks. *2005 IEEE 62nd Vehicular Technology Conference. VTC-2005-Fall*. (pp. 675-679). IEEE.

[Choi et al., 2003] Choi, S., Prado, J., Shankar, N., and Mangold, S. (2003). IEEE 802.11e contention-based channel access (EDCF) performance evaluation. *IEEE International Conference on Communications. ICC'03*. (pp. 1151-1156). IEEE.

[Choi et al., 2006] Choi, N., Patel, M., and Venkatesan, S. (2006). A Full Duplex Multi-channel MAC Protocol for Multi-hop Cognitive Radio Networks. *1st International Conference on Cognitive Radio Oriented Wireless Networks and Communications* (pp. 1-5). IEEE.

[Chowdhury and Akyildiz, 2008] Chowdhury, K. and Akyildiz, I. (2008). Cognitive Wireless Mesh Networks with Dynamic Spectrum Access. *IEEE Journal on Selected Areas in Communications, 26*(1), 168–181.

[Chowdhury and Felice, 2009] Chowdhury, K. and Felice, M. (2009). Search: A routing protocol for mobile cognitive radio ad-hoc networks. *Computer Communications, 32*(18), 1983-1997.

[Chowdhury and Melodia, 2010] Chowdhury, K. and Melodia, T. (2010). Platforms and testbeds for experimental evaluation of cognitive ad hoc networks. *Communications Magazine, 48*(9), 96-104.

[Clancy and Goergen, 2008] Clancy, T. C. and Goergen, N. (2008). Security in Cognitive Radio Networks: Threats and Mitigation. *3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications. CrownCom 2008*. (pp. 1-8). IEEE.

[Clancy et al., 2007] Clancy, C., Hecker, J., Stuntebeck, E., and O'Shea, T. (2007). Applications of Machine Learning to Cognitive Radio Networks. *Wireless Communications, 14*(4), 47-52.

[Clouqueur et al., 2001] Clouqueur, T., Ramanathan, P., Saluja, K., and Wang, K. (2001). Value-fusion versus decision-fusion for fault-tolerance in collaborative target detection in sensor networks. *Proceedings of Fourth International Conference on Information Fusion*.

[Cormio and Chowdhury, 2009] Cormio, C. and Chowdhury, K. (2009). A Survey on MAC Protocols for Cognitive Radio Networks. *Ad Hoc Networks, 7*(7), 1315-1329.

[Cormio and Chowdhury, 2010] Cormio, C. and Chowdhury, K. (2010). Common control channel design for cognitive radio wireless ad hoc networks using adaptive frequency hopping. *Ad Hoc Networks, 8*(4), 430-438.

[CREW Project, 2015] CREW Project. (2015). Retrieved Mar. 22, 2015, from http://www.crew-project.eu/

[De Domenico et al., 2012] De Domenico, A., Strinati, E. C., and Di Benedetto, M. (2012). A Survey on MAC Strategies for Cognitive Radio Networks. *Communications Surveys & Tutorials, 14*(1), 21-44.

[Eljack et al., 2009] Eljack, S., Huang, B., Tu, L., and Zhang, P. (2009). Synchronized Multi-Channel Cognitive MAC Protocol with Efficient Solutions for Second Spectrum Access. *Ubiquitous, Symposia and Workshops on Autonomic and Trusted Computing, 2009. UIC-ATC '09*. (pp. 477-48). IEEE.

[Fatemieh et al., 2010] Fatemieh, O., Chandra, R., and Gunter, C. A. (2010). Secure Collaborative Sensing for Crowd Sourcing Spectrum Data in White Space Networks. *IEEE Symposium on New Frontiers in Dynamic Spectrum* (pp. 1-12). IEEE.

[FCC Spectrum Policy Task Force, 2002] FCC Spectrum Policy Task Force. (2002). *Report of the spectrum efficiency working group*.

[Ferré et al., 2008] Ferré, P., Doufexi, A., Chung-How, J., Nix, A., and Bull, D. (2008). Robust video transmission over wireless LANs. IEEE Transactions on Vehicular Technology, 57(4), 2596-2602.

[Filin et al., 2011] Filin, S., Murakami, H., Harada, H., Yoshino, H., Kashiki, K., and Shibata, T. (2011). ITU-R standardization activities on Cognitive Radio Systems. *2011 Sixth International ICST Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)* (pp. 116-120). IEEE.

[FIT/CorteXlab - Cognitive Radio Testbed, 2015] *FIT/CorteXlab - Cognitive Radio Testbed*. (2015). Retrieved Mar. 22, 2015, from http://www.cortexlab.fr/

[Fragkiadakis et al., 2013] Fragkiadakis, A., Tragos, E., and Askoxylakis, I. (2013). A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks. *Communications Surveys & Tutorials, 15*(1), 428–445.

[Franceschini et al., 2009] Franceschini, F., Galetto, M., Maisano, D., and Mastrogiacomo, L. (2009). A review of localization algorithms for distributed wireless sensor networks in manufacturing. *International Journal of Computer Integrated Manufacturing, 22*(7), 698-716.

[Ghaboosi et al., 2008] Ghaboosi, K., Latva-aho, M., and Xiao, Y. (2008). A Distributed Multi-channel Cognitive MAC Protocol for IEEE 802.11s Wireless Mesh Networks. *3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008*. (pp. 1-8). IEEE.

[Ghaboosi et al., 2009] Ghaboosi, K., MacKenzie, A., DaSilva, L., Abdallah, A., and Latva-Aho, M. (2009). A Channel Selection Mechanism based on Incumbent Appearance Expectation for Cognitive Networks. *Wireless Communications and Networking Conference, 2009. WCNC 2009*. IEEE.

[Grace et al., 2009] Grace, D., Chen, J., Jiang, T., and Mitchell, P. (2009). Using cognitive radio to deliver 'Green' communications. *4th International Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2009. CROWNCOM '09*. (pp. 1-6). IEEE.

[Guan et al., 2010] Guan, Q., Yu, F., Jiang, S., and Wei, G. (2010). Prediction-Based Topology Control and Routing in Cognitive Radio Mobile Ad Hoc Networks. *IEEE Transactions on Vehicular Technology, 59*(9), 4443-4452.

[Hamdaoui and Shin, 2008] Hamdaoui, B. and Shin, K. (2008). OS-MAC: An Efficient MAC Protocol for Spectrum-Agile Wireless Networks. *IEEE Transactions on Mobile Computing, 7*(8), 915-930.

[Hassan et al., 2011] Hassan, M. R., Karmakar, G., and Kamruzzaman, J. (2011). Maximizing the concurrent transmissions in cognitive radio ad hoc networks. *7th International Wireless Communications and Mobile Computing Conference (IWCMC)* (pp. 466-471). IEEE.

[He et al., 2014] He, Z., Mao, S., and Kompella, S. (2014). QoE driven video streaming in cognitive radio networks: The case of single channel access. *2014 IEEE Global Communications Conference (GLOBECOM)* (pp. 1388-1393). IEEE.

[Höyhtyä et al., 2008] Höyhtyä, M., Pollin, S., and Mammela, A. (2008). Performance improvement with predictive channel selection for cognitive radios. *First International Workshop on Cognitive Radio and Advanced Spectrum Management, 2008. CogART 2008*. (pp. 1-5). IEEE.

[Hsieh et al., 2008] Hsieh, H., Liu, T., Liao, W., and Ho, T. (2008). Moving toward higher speed WLANs through dynamic spectrum access in the unlicensed band. *European Conference on Wireless Technology, 2008. EuWiT 2008*. (pp. 111-114). IEEE.

[Hsu et al., 2007] Hsu, A., Weit, D., and Kuo, C. (2007). A Cognitive MAC Protocol Using Statistical Channel Allocation for Wireless Ad-Hoc Networks. *IEEE Wireless Communications and Networking Conference, 2007. WCNC 2007*. (pp. 105-110). IEEE.

[Huang et al., 2014] Huang, X. L., Wang, G., Hu, F., Kumar, S., and Wu, J. (2014). Multimedia over cognitive radio networks: Towards a cross-layer scheduling under Bayesian traffic learning. *Computer Communications, 51*, 48-59.

[Hussein et al., 2013] Hussein, H., Elsayed, H. A., and Elramly, S. (2013). Performance evaluation of Cognitive Radio Network Predictive MAC (P-MAC) access algorithm and its enhancement. *2013 International Conference on Information Networking (ICOIN)* (pp. 434-439). IEEE.

[Idoudi et al., 2014] Idoudi, H., Daimi, K., and Saed, M. (2014). Security Challenges in Cognitive Radio Networks. *World Congress on Engineering*. IAENG.

[IEEE 802.21, 2012] *IEEE 802.21*. (2012). Retrieved July 16, 2012, from http://www.ieee802.org/21

[IEEE 802.22 Working Group on Wireless Regional Area Networks, 2013] *IEEE 802.22 Working Group on Wireless Regional Area Networks*. (2013). Retrieved Dec. 12, 2013, from http://www.ieee802.org/22/

[Issariyakul et al., 2009] Issariyakul, T., Pillutla, L., and Krishnamurthy, V. (2009). Tuning Radio resource in an Overlay Cognitive Radio Network for TCP: Greed Isn't Good. *Communications Magazine, 47*(7), 57-63.

[Jain et al., 1984] Jain, R., Chiu, D., and Hawe, W. (1984). A quantitative measure of fairness and discrimination for resource allocation in shared computer system. *Digital Equipment Corporation, Maynard, Mass, USA*.

[Jeon et al., 2012] Jeon, W. S., Han, J. A., and Jeong, D. G. (2012). A Novel MAC Scheme for Multichannel Cognitive Radio Ad Hoc Networks. *IEEE Transactions on Mobile Computing, 11*(6), 922–934.

[Ji and Liu, 2007] Ji, Z. and Liu, K. (2007). Cognitive Radios for Dynamic Spectrum Access - Dynamic Spectrum Sharing: A Game Theoretical Overview. *Communications Magazine, 45*(5), 88-94.

[Jia and Zhang, 2009] Jia, J. and Zhang, Q. (2009). A Testbed Development Framework for Cognitive Radio Networks. *IEEE International Conference on Communications, 2009. ICC '09*. (pp. 1-5). IEEE.

[Jia et al., 2008] Jia, J., Zhang, Q., and Shen, X. (2008). HC-MAC: A Hardware-Constrained Cognitive MAC for Efficient Spectrum Management. *IEEE Journal on Selected Areas in Communications, 26*(1), 106-117.

[Jiang et al., 2008a] Jiang, T., Grace, D., and Liu, Y. (2008a). Cognitive radio spectrum sharing schemes with reduced spectrum sensing requirements. *2008 IET Seminar on Cognitive Radio and Software Defined Radios: Technologies and Techniques* (pp. 1-5). IET.

[Jiang et al., 2008b] Jiang, T., Grace, D., and Liu, Y. (2008b). Performance of cognitive radio reinforcement spectrum sharing using different weighting factors. *Third International Conference on Communications and Networking in China, 2008. ChinaCom 2008*. (pp. 1195-1199). IEEE.

[Jin et al., 2009] Jin, Z., Anand, S., and Subbalakshmi, K. P. (2009). Mitigating Primary User Emulation Attacks in Dynamic Spectrum Access Networks using Hypothesis Testing. *ACM SIGMOBILE Mobile Computing and Communications Review, 13*(2), 74-85.

[Jing et al., 2012] Jing, M. A., Sekiya, H., Nagasaki, A., Komuro, N., and Sakata, S. (2012). MAC protocol for ad hoc networks using smart antennas for mitigating hidden and deafness problems. *IEICE transactions on communications, 95*(11), 3545-3555.

[Jo et al., 2009] Jo, O., Choi, H., and Cho, D. (2009). Seamless spectrum handover improving cell outage in cognitive radio systems. *4th International Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2009. CROWNCOM '09*. (pp. 1-6). IEEE.

[Joe and Son, 2008] Joe, I. and Son, S. (2008). Dynamic Spectrum Allocation MAC Protocol Based on Cognitive Radio for QoS Support. *Japan-China Joint Workshop on Frontier of Computer Science and Technology, 2008. FCST '08*. (pp. 24-29). IEEE.

[Kai et al., 2014] Kai, P., Fanzi, Z., and Qingguang, Z. (2014). A New Method to Detect Primary User Emulation Attacks in Cognitive Radio Networks. *3rd International Conference on Computer Science and Service System. CSSS 2014*. (pp. 674-677). Atlantis Press.

[Khaleghi et al., 2013] Khaleghi, B., Khamis, A., Karray, F. O., and Razavi, S. N. (2013). Multisensor data fusion: A review of the state-of-the-art. *Information Fusion, 14*(1), 28-44.

[Kim and Shin, 2008] Kim, H. and Shin, K. G. (2008). Efficient Discovery of Spectrum Opportunities with MAC-Layer Sensing in Cognitive Radio Networks. *IEEE Transactions on Mobile Computing, 7*(5), 533-545.

[Kim et al., 2012] Kim, M., Chung, M. Y., and Choo, H. (2012). VeriEST: verification via primary user emulation signal-based test for secure distributed spectrum sensing in cognitive radio networks. *Security and Communication Networks, 5*(7), 776–788.

[Ko et al., 2010] Ko, G., Franklin, A., You, S., Pak, J., Song, M., and Kim, C. (2010). Channel management in IEEE 802.22 WRAN systems. *IEEE Communications Magazine, 48*(9), 88-94.

[Kondareddy and Agrawal, 2008] Kondareddy, Y. and Agrawal, P. (2008). Synchronized MAC Protocol For Multi-Hop Cognitive Radio Networks. *IEEE International Conference on Communications, 2008. ICC '08*. (pp. 3198-3202). IEEE.

[Kumar and Shin, 2012a] Kumar, A. and Shin, K. G. (2012a). DSASync: managing end-to-end connections in dynamic spectrum access wireless LANs. *IEEE/ACM Transactions on Networking (TON), 20*(4), 1068-1081.

[Kumar and Shin, 2012b] Kumar, A. and Shin, K. G. (2012b). Application-aware dynamic spectrum access. *Wireless Networks, 18*(3), 257-275.

[Le and Hossain, 2008] Le, L. and Hossain, E. (2008). A MAC Protocol for Opportunistic Spectrum Access in Cognitive Radio Networks. *Wireless Communications and Networking Conference, 2008. WCNC 2008*. (pp. 1426-1430). IEEE.

[Lee and Kim, 2012] Lee, Y. H. and Kim, D. (2012). A slow hopping MAC protocol for coordinator-based cognitive radio network. *2012 IEEE Consumer Communications and Networking Conference (CCNC)* (pp. 854-858). IEEE.

[Lei et al., 2012] Lei, H., Ren, Z., Gao, C., and Guo, Y. (2012). A new multi-channel MAC protocol for 802.11-based wireless mesh networks. *2012 IEEE International Conference on Computer Science and Electronics Engineering (ICCSEE)* (pp. 27-31). IEEE.

[León et al., 2012] León, O., Hernández-Serrano, J., and Soriano, M. (2012). Cooperative detection of primary user emulation attacks in CRNs. *Computer Networks, 56*(14), 3374–3384.

[Li and Zekavat, 2009] Li, X. and Zekavat, S. (2009). Traffic Pattern Prediction Based Spectrum Sharing for Cognitive Radios. In W. Wang (Ed.), *Cognitive Radio Systems* (pp. 77-95). InTech. doi:10.5772/7838

[Liu et al., 2007] Liu, Y., Yu, R., and Xie, S. (2007). Wireless digital home networking based on cognitive radio. *IET Conference on Wireless, Mobile and Sensor Networks, 2007. CCWMSN07*. (pp. 785-788). IET.

[Lo, 2011] Lo, B. (2011). A survey of common control channel design in cognitive radio networks. *Physical Communication, 4*(1), 26-39.

[Lo and Akyildiz, 2013] Lo, B. and Akyildiz, I. (2013). Reinforcement learning for cooperative sensing gain in cognitive radio ad hoc networks. *Wireless Networks, 19*(6), 1237-1250.

[Lopez-Benitez et al., 2009] Lopez-Benitez, M., Umbert, A., and Casadevall, F. (2009). Evaluation of Spectrum Occupancy in Spain for Cognitive Radio Applications. *69th conference on Vehicular Technology, 2009. VTC Spring 2009*. (pp. 1-5). IEEE.

[Lu et al., 2012] Lu, L., Zhou, X., Onunkwo, U., and Li, G. (2012). Ten years of research in spectrum sensing and sharing in cognitive radio. *EURASIP Journal on Wireless Communications and Networking, 2012*(1), 1-16.

[Luo et al., 2009] Luo, T., Motani, M., and Srinivasan, V. (2009). Cooperative Asynchronous Multichannel MAC: Design, Analysis, and Implementation. *IEEE Transactions on Mobile Computing, 8*(3), 338–352.

[Ma et al., 2005] Ma, L., Han, X., and Shen, C. (2005). Dynamic open spectrum sharing MAC protocol for wireless ad hoc networks. *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005*. (pp. 203-213). IEEE.

[Malady and da Silva, 2008] Malady, A. and da Silva, C. (2008). Clustering methods for distributed spectrum sensing in cognitive radio systems. *Military Communications Conference, 2008. MILCOM 2008*. (pp. 1-5). IEEE.

[Marinho and Monteiro, 2012a] Marinho, J. and Monteiro, E. (2012). Cooperative sensing-before-transmit in ad-hoc multi-hop cognitive radio scenarios. *Wired/Wireless Internet Communication. WWIC 2012.* (pp. 186-197). Springer Berlin Heidelberg.

[Marinho and Monteiro, 2012b] Marinho, J. and Monteiro, E. (2012a). Cognitive Radio: Survey on Communication Protocols, Spectrum Decision Issues, and Future Research Directions. *Wireless Networks, 18*(2), 147-164.

[Marinho and Monteiro, 2012c] Marinho, J. and Monteiro, E. (2012b). Enhanced Protection of Hidden Primary Users through Filtering based on Suspect Channels Classification. *2012 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* (pp. 419-426). IEEE.

[Marinho et al., 2015] Marinho, J., Granjal, J., and Monteiro, E. (2015). A Survey on Security Attacks and Countermeasures with Primary User Detection in Cognitive Radio Networks. EURASIP Journal on Information Security, 2015(4), 1-14.

[Masonta et al., 2013] Masonta, M. T., Mzyece, M., and Ntlatlapa, N. (2013). Spectrum decision in cognitive radio networks: A survey. *Communications Surveys & Tutorials, 15*(3), 1088-1107.

[Masri et al., 2010] Masri, A., Chiasserini, C., and Perotti, A. (2010). Control information exchange through UWB in cognitive radio networks. *5th IEEE International Symposium on Wireless Pervasive Computing (ISWPC)* (pp. 110-115). IEEE.

[Min et al., 2009] Min, A. W., Shin, K. G., and Hu, X. (2009). Attack-tolerant distributed sensing for dynamic spectrum access networks. *17th IEEE International Conference on Network Protocols. ICNP 2009*. (pp. 294–303). IEEE.

[Mitola and Maguire, 1999] Mitola, J. and Maguire, G. (1999). Cognitive radio: making software radios more personal. *Personal Communications, 6*(4), 13-18.

[MiXiM, 2010] *MiXiM*. (2010). Retrieved Dec. 10, 2010, from http://mixim.sourceforge.net/

[Mo et al., 2008] Mo, J., So, H.-S., and Walrand, J. (2008). Comparison of Multichannel MAC Protocols. *IEEE Transactions on Mobile Computing, 7*(1), 50-65.

[Mody et al., 2008] Mody, A., Sherman, M., Martinez, R., Reddy, R., and Kiernan, T. (2008). Survey of IEEE standards supporting cognitive radio and dynamic spectrum access. *Military Communications Conference, 2008. MILCOM 2008*. (pp. 1-7). IEEE.

[Mody et al., 2009] Mody, A. N., Reddy, R., Kiernan, T., and Brown, T. X. (2009). Security in cognitive radio networks: An example using the commercial IEEE 802.22 standard. *Military Communications Conference. MILCOM 2009*. (pp. 1-7). IEEE.

[Mueck et al., 2010] Mueck, M., Piipponen, A., Kalliojärvi, K., Dimitrakopoulos, G., Tsagkaris, K., Demestichas, P., . . . Hayar, A. (2010). ETSI reconfigurable radio systems: status and future directions on software defined radio and cognitive radio standards. *Communications Magazine, 48*(9), 78-86.

[Nan et al., 2007] Nan, H., Hyon, T., and Yoo, S. (2007). Distributed Coordinated Spectrum Sharing MAC Protocol for Cognitive Radio. *2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks. DySPAN 2007*. (pp. 240-249). IEEE.

[Nasipuri and Li, 2005] Nasipuri, A. and Li, K. (2005). Collaborative Detection of Spatially Correlated Signals in Sensor Networks. *Proceedings of the 2005 International Conference on Telecommunication Systems Modeling and Analysis*, (pp. 17-20).

[Newman et al., 2010] Newman, T., Hasan, S., Depoy, D., Bose, T., and Reed, J. (2010). Designing and deploying a building-wide cognitive radio network testbed. *IEEE Communications Magazine, 48*(9), 106-112.

[Nezhadal et al., 2012] Nezhadal, S., Berangi, R., and Fathy, M. (2012). Common Control Channel Saturation Detection And Enhancement In Cognitive Radio Networks. *International journal of Distributed and parallel systems, 3*(2).

[Nguyen et al., 2012] Nguyen, V. T., Villain, F., and Guillou, Y. L. (2012). Cognitive radio RF: overview and challenges. *VLSI Design 2012, 1*.

[Niculescu, 2004] Niculescu, D. (2004). Positioning in ad hoc sensor networks. *IEEE Network, 18*(4), 24–29.

[Niyato and Hossain, 2009] Niyato, D. and Hossain, E. (2009). Cognitive radio for next-generation wireless networks: an approach to opportunistic channel selection in ieee 802.11-based wireless mesh. *Wireless Communications, 16*(1), 46-54.

[O'hara and Petrick, 2005] O'hara, B. and Petrick, A. (2005). *IEEE 802.11 handbook: a designer's companion*. IEEE Standards Association.

[OMNeT++ Network Simulation Framework, 2010] *OMNeT++ Network Simulation Framework*. (2010). Retrieved Dec. 10, 2010, from http://www.omnetpp.org/

[Orbit, 2011] *Orbit*. (2011). Retrieved Dec. 4, 2011, from http://www.orbit-lab.org

[Pandit and Singh, 2013] Pandit, S. and Singh, G. (2013). Self-scheduled MAC-layer protocol for spectrum sharing in cognitive radio communication. *2013 Sixth International Conference on Contemporary Computing (IC3)* (pp. 250-255). IEEE.

[Pawelczak et al., 2005] Pawelczak, P., Prasad, R., Xia, L., and Niemegeers, I. (2005). Cognitive radio emergency networks - requirements and design. *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005*. (pp. 601-606). IEEE.

[Phillips et al., 2013] Phillips, C., Sicker, D., and Grunwald, D. (2013). A survey of wireless path loss prediction and coverage mapping methods. *Communications Surveys & Tutorials, 15*(1), 255-270.

[Piri and Pentikousis, 2009] Piri, E. and Pentikousis, K. (2009). IEEE 802.21: Media-Independent Handover Services. *The Internet Protocol Journal, 12*(2), 7-27.

[Pirmoradian et al., 2012] Pirmoradian, M., Adigun, O., and Politis, C. (2012). Adaptive power control scheme for energy efficient cognitive radio networks. *2012 IEEE International Conference on Communications (ICC)* (pp. 6988-6992). IEEE.

[Qu et al., 2010] Qu, X., Zhang, J., and Li, M. (2010). A power allocation algorithm for distributed cognitive radio systems. *2010 International Conference on Wireless Communications and Signal Processing (WCSP)* (pp. 1-4). IEEE.

[Ren et al., 2012] Ren, P., Wang, Y., Du, Q., and Xu, J. (2012). A survey on dynamic spectrum access protocols for distributed cognitive wireless networks. *EURASIP Journal on Wireless Communications and Networking, 2012*(1), 60.

[Ren et al., 2014] Ren, P., Wang, Y., and Du, Q. (2014). CAD-MAC: A Channel-Aggregation Diversity Based MAC Protocol for Spectrum and Energy Efficient Cognitive Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications, 32*(2), 237-250.

[Renk et al., 2008] Renk, T., Kloeck, C., Burgkhardt, D., Jondral, F., Grandblaise, D., Gault, S., and Dunat, J. (2008). Bio-Inspired Algorithms for Dynamic Resource Allocation in Cognitive Wireless Networks. *Mobile Networks and Applications, 13*(5), 431-441.

[Rifà-Pous and Garrigues, 2012] Rifà-Pous, H. and Garrigues, C. (2012). Authenticating hard decision sensing reports in cognitive radio networks. *Computer Networks, 56*(2), 566–576.

[Sadeghi et al., 2005] Sadeghi, B., Kanodia, V., Sabharwal, A., and Knightly, E. (2005). OAR: an opportunistic auto-rate media access protocol for ad hoc networks. *Wireless Networks, 11*(1-2), 39-53.

[Salah-Eldeen et al., 2007] Salah-Eldeen, S., Elnahas, A., and Ghoniemy, S. (2007). A hybrid distributed channel allocation algorithm using traffic prediction. *ITI 5th International Conference on Information and Communications Technology, 2007. ICICT 2007*. (pp. 115-121). IEEE.

[Salameh et al., 2009] Salameh, H. A., Krunz, M. M., and Younis, O. (2009). MAC Protocol for Opportunistic Cognitive Radio Networks with Soft Guarantees. *IEEE Transactions on Mobile Computing, 8*(10), 1339-1352.

[Salameh et al., 2010] Salameh, H. A., Krunz, M., and Younis, O. (2010). Cooperative Adaptive Spectrum Sharing in Cognitive Radio Networks. *IEEE/ACM Transactions on Networking, 18*(4), 1181–1194.

[Saleem and Rehmani, 2014] Saleem, Y. and Rehmani, M. H. (2014). Primary radio user activity models for cognitive radio networks: A survey. *Journal of Network and Computer Applications, 43*, 1-16.

[Sam and Raj, 2014] Sam, D. and Raj, V. C. (2014). A Time Synchronized Hybrid Vehicular Ad Hoc Network of Roadside Sensors and Vehicles for Safe Driving. *Journal of Computer Science, 10*(9), 1617-1627.

[Savarese et al., 2001] Savarese, C., Rabaey, J. M., and Beutel, J. (2001). Location in distributed ad-hoc wireless sensor networks. *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'01)* (pp. 2037-2040). IEEE.

[Shah et al., 2011] Shah, M. A., Safdar, G. A., and Maple, C. (2011). DDH-MAC: A novel Dynamic De-Centralized Hybrid MAC protocol for Cognitive Radio Networks. *2011 10th Roedunet International Conference (RoEduNet)* (pp. 1-6). IEEE.

[Sharma and Belding, 2008] Sharma, A. and Belding, E. (2008). FreeMAC: framework for multi-channel mac development on 802.11 hardware. *Proceedings of the ACM workshop on Programmable routers for extensible services of tomorrow* (pp. 69-74). ACM.

[Sherman et al., 2008] Sherman, M., Mody, A., Martinez, R., Rodriguez, C., and Reddy, R. (2008). IEEE Standards Supporting Cognitive Radio and Networks, Dynamic Spectrum Access, and Coexistence. *Communications Magazine, 46*(7), 72-79.

[Shu et al., 2014] Shu, Z., Qian, Y., Yang, Y., and Sharif, H. (2014). A cross-layer study for application-aware multi-hop cognitive radio networks. *Wireless Communications and Mobile Computing*. doi:10.1002/wcm.2557

[So and Vaidya, 2004] So, J. and Vaidya, N. (2004). Multi-Channel MAC for Ad Hoc Networks: Handling Multi-Channel Hidden Terminals Using a Single Transceiver. *5th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc)* (pp. 222-233). ACM.

[Su and Zhang, 2008] Su, H. and Zhang, X. (2008). Cross-Layer Based Opportunistic MAC Protocols for QoS Provisionings Over Cognitive Radio Wireless Networks. *IEEE Journal on Selected Areas in Communications, 26*(1), 118-129.

[Suen and Yasinsac, 2005] Suen, T. and Yasinsac, A. (2005). Peer identification in wireless and sensor networks using signal properties. *IEEE International Conference on Mobile Adhoc and Sensor Systems*. IEEE.

[Sutton et al., 2010] Sutton, P., Fahmy, S., Nolan, K., Özgul, B., Rondeau, T., Noguera, J., and Doyle, L. (2010). Iris: an architecture for cognitive radio networking testbeds. *IEEE Communications Magazine, 48*(9), 114-122.

[Suzuki et al., 2006] Suzuki, T., Noguchi, A., and Tasaka, S. (2006). Effect of TXOP-bursting and transmission error on application-level and user-level QoS in audio-video transmission with IEEE 802.11e EDCA. *2006 IEEE 17th International Symposium on Personal, Indoor and Mobile Radio* (pp. 1-7). IEEE.

[The CORE+ project, 2015] *The CORE+ project*. (2015). Retrieved Mar. 22, 2015, from http://core.willab.fi/

[Tian et al., 2014] Tian, J., Tian, X., and Qian, L. (2014). Second Users Operation Strategies Based on Primary Users Activities. *Scientific Journal of Information Engineering, 4*(1).

[Timmers et al., 2010] Timmers, M., Pollin, S., Dejonghe, A., Van der Perre, L., and Catthoor, F. (2010). A Distributed Multichannel MAC Protocol for Multihop Cognitive Radio Networks. *IEEE Transactions on Vehicular Technology, 59*(1), 446-459.

[Tingting and Feng, 2013] Tingting, L. and Feng, S. (2013). Research on hidden malicious user detection problem. *Security and Communication Networks, 7*(6), 958-963.

[Tsagkaris et al., 2008] Tsagkaris, K., Katidiotis, A., and Demestichas, P. (2008). Neural network-based learning schemes for cognitive radio systems. *Computer Communications, 31*(14), 3394-3404.

[Tung et al., 2013] Tung, L. C., Mena, J., Gerla, M., and Sommer, C. (2013). A cluster based architecture for intersection collision avoidance using heterogeneous networks. *2013 12th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET)* (pp. 82-88). IEEE.

[U.S. Patent No. 8,204,005, 2012] Liu, C., Stephens, A. P., and Akhmetov, D. V. (2012). *U.S. Patent No. 8,204,005*.

[Vuran and Akyildiz, 2007] Vuran, N. and Akyildiz, I. (2007). A-MAC: adaptive medium access control for next generation wireless terminals. *IEEE/ACM Transactions on Networking (TON), 15*(3), 574-587.

[Wang and Chen, 2014] Wang, J. and Chen, I. R. (2014). Trust-based data fusion mechanism design in cognitive radio networks. *2014 IEEE Conference on Communications and Network Security (CNS)* (pp. 53-59). IEEE.

[Wang and Garcia-Luna-Aceves, 2011] Wang, X. and Garcia-Luna-Aceves, J. (2011). Collaborative Routing, Scheduling and Frequency Assignment for Wireless Ad Hoc Networks Using Spectrum-Agile Radios. *Wireless Networks, 17*(1), 167-181.

[Wang and Salous, 2008] Wang, Z. and Salous, S. (2008). Time series arima model of spectrum occupancy for cognitive radio. *2008 IET Seminar on Cognitive Radio and Software Defined Radios: Technologies and Techniques* (pp. 1-4). IET.

[Wang et al., 2007] Wang, J., Abolhasan, M., Safaei, F., and Franklin, D. (2007). A survey on control separation techniques in multi-radio multi-channel MAC protocols. *International Symposium on Communications and Information Technologies, 2007. ISCIT '07*. (pp. 854-859). IEEE.

[Wang et al., 2008] Wang, H., Qin, H., and Zhu, L. (2008). A Survey on MAC Protocols for Opportunistic Spectrum Access in Cognitive Radio Networks. *2008 International Conference on Computer Science and Software Engineering* (pp. 214-218). IEEE.

[Wang et al., 2010a] Wang, W., Li, H., Sun, Y., and Han, Z. (2010a). Securing collaborative spectrum sensing against untrustworthy secondary users in cognitive radio networks. *EURASIP Journal on Advances in Signal Processing, 4*.

[Wang et al., 2010b] Wang, X., Wong, A., and Ho, P. (2010b). Dynamically optimized spatiotemporal prioritization for spectrum sensing in cooperative cognitive radio. *Wireless Networks, 16*(4), 889-901.

[Wang et al., 2010c] Wang, Y., Ren, P., and Wu, G. (2010c). A Throughput-Aimed MAC Protocol with QoS Provision for Cognitive Ad Hoc Networks. *IEICE TRANSACTIONS on Communications, 93*(6), 1426-1429.

[Wang et al., 2011a] Wang, X. Y., Wong, A., and Ho, P. H. (2011a). Stochastic Medium Access for Cognitive Radio Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications, 29*(4), 770–783.

[Wang et al., 2011b] Wang, X., Zhang, X., Zhang, Q., and Tang, C. (2011b). Common control channel model on MAC protocols in cognitive radio networks. *2011 International Conference on Computer Science and Network Technology (ICCSNT). 4*, pp. 2230–2234. IEEE.

[Wang et al., 2014] Wang, J., Huang, A., Wang, W., Zhang, Z., and Lau, V. K. (2014). On the transmission opportunity and TCP throughput in cognitive radio networks. *International Journal of Communication Systems, 27*(2), 303-321.

[Wellens and Mähönen, 2010] Wellens, M. and Mähönen, P. (2010). Lessons Learned from an Extensive Spectrum Occupancy Measurement Campaign and a Stochastic Duty Cycle Model. *Mobile Networks and Applications, 15*(3), 461-474.

[Wellens et al., 2010] Wellens, M., Riihijarvi, J., and Mähönen, P. (2010). Evaluation of adaptive MAC-layer sensing in realistic spectrum occupancy scenarios. *IEEE Symposium on New Frontiers in Dynamic Spectrum, 2010* (pp. 1-12). IEEE.

[Xiang et al., 2010] Xiang, J., Zhang, Y., and Skeie, T. (2010). Medium access control protocols in cognitive radio networks. *Wireless Communications and Mobile Computing, 10*(1), 31-49.

[Xiao et al., 2007] Xiao, B., Chen, H., and Zhou, S. (2007). A walking beacon-assisted localization in wireless sensor networks. *IEEE International Conference on Communications. ICC'07*. (pp. 3070–3075). IEEE.

[Xiao Y. , 2004] Xiao, Y. (2004). Concatenation and piggyback mechanisms for the IEEE 802.11 MAC. *IEEE Wireless Communications and Networking Conference, 2004. IEEE WCNC 2004*. (pp. 1642–1647). IEEE.

[Xin and Song, 2014] Xin, C. and Song, M. (2014). Detection of PUE Attacks in Cognitive Radio Networks Based on Signal Activity Pattern. *IEEE Transactions on Mobile Computing, 13*(5), 1022-1034.

[Xiukui and Zekavat, 2008] Xiukui, L. and Zekavat, S. (2008). Traffic Pattern Prediction and Performance Investigation for Cognitive Radio Systems. *IEEE Conference on Wireless Communications and Networking, 2008. WCNC 2008*. (pp. 894-899). IEEE.

[Xu et al., 2003] Xu, K., Gerla, M., and Bae, S. (2003). Effectiveness of RTS/CTS handshake in IEEE 802.11 based ad hoc networks. *Ad Hoc Networks, 1*(1), 107-123.

[Xu et al., 2011] Xu, D., Feng, Z., Li, Y., and Zhang, P. (2011). Optimal Power Control of Cognitive Radio under SINR Constraint with Primary User's Cooperation. *IEICE TRANSACTIONS on Communications, 94*(9), 2685-2689.

[Xu et al., 2012] Xu, D., Feng, Z., and Zhang, P. (2012). Protecting Primary Users in Cognitive Radio Networks with Effective Capacity Loss Constraint. *IEICE TRANSACTIONS on Communications, 95*(1), 349-353.

[Yang et al., 2010] Yang, Y., Liu, Y., Zhang, Q., and Ni, L. (2010). Cooperative boundary detection for spectrum sensing using dedicated wireless sensor networks. *29th IEEE International Conference on Computer Communications. INFOCOM 2010*. (pp. 1-9). IEEE.

[Yau et al., 2008] Yau, A., Komisarczuk, P., and Teal, P. (2008). On Multi-Channel MAC Protocols in Cognitive Radio Networks. *Australasian Telecommunication Networks and Applications Conference, 2008. ATNAC 2008*. (pp. 300-305). IEEE.

[Yu et al., 2009] Yu, F., Tang, H., Huang, M., Li, Z., and Mason, P. (2009). Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios. *Military Communications Conference. MILCOM 2009*. (pp. 1-7). IEEE.

[Yu et al., 2011] Yu, F., Sun, B., Krishnamurthy, V., and Ali, S. (2011). Application layer QoS optimization for multimedia transmission over cognitive radio networks. *Wireless Networks, 17*(2), 371-383.

[Yuan et al., 2007] Yuan, Y., Bahl, P., Chandra, R., Chou, P., Ferrell, J., Moscibroda, T., . . . Wu, Y. (2007). KNOWS: Cognitive Radio Networks Over White Spaces. *2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks. DySPAN 2007*. (pp. 416-427). IEEE.

[Yuan et al., 2012] Yuan, Z., Niyato, D., Li, H., Song, J. B., and Han, Z. (2012). Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks. *IEEE Journal on Selected Areas in Communications, 30*(10), 1850-1860.

[Yucek and Arslan, 2009] Yucek, T. and Arslan, H. (2009). A survey of spectrum sensing algorithms for cognitive radio applications. *Communications Surveys & Tutorials, 11*(1), 116-130.

[Zeng et al., 2010] Zeng, K., Paweczak, P., and Cabric, D. (2010). Reputation-based cooperative spectrum sensing with trusted nodes assistance. *IEEE Communications Letters, 14*(3), 226–228.

[Zhang and Lazos, 2013] Zhang, Y. and Lazos, L. (2013). Vulnerabilities of cognitive radio MAC protocols and countermeasures. *IEEE Network, 27*(3), 40-45.

[Zhang and Su, 2011] Zhang, X. and Su, H. (2011). CREAM-MAC: Cognitive Radio-EnAbled Multi-Channel MAC Protocol Over Dynamic Spectrum Access Networks. *IEEE Journal of Selected Topics in Signal Processing, 5*(1), 110–123.

[Zhang et al., 2008] Zhang, Q., Fitzek, F., and Iversen, V. (2008). Cognitive radio MAC protocol for WLAN. *IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communication 2008. PIMRC 2008*. (pp. 1-6). IEEE.

[Zhang et al., 2009] Zhang, C., Wang, X., Guan, X., and Chen, H.-H. (2009). Quality-of-Service in Cognitive Radio Networks with Collaborative Sensing. *IEEE Global Telecommunications Conference. GLOBECOM 2009*. (pp. 1-5). IEEE.

[Zhang et al., 2010] Zhang, Y., Meratnia, N., and Havinga, P. (2010). Outlier detection techniques for wireless sensor networks: A survey. *Communications Surveys & Tutorials, 12*(2), 159–170.

[Zhao and Sadler, 2007] Zhao, Q. and Sadler, B. (2007). A Survey of Dynamic Spectrum Access. *Signal Processing Magazine, 24*(3), 79-89.

[Zhao and Swami, 2007] Zhao, Q. and Swami, A. (2007). A Survey of Dynamic Spectrum Access: Signal Processing and Networking Perspectives. *IEEE International Conference on Acoustics, Speech and Signal Processing, 2007. ICASSP 2007*. (pp. IV-1349-IV-1352.). IEEE.

[Zhao et al., 2005] Zhao, J., Zheng, H., and Yang, G.-H. (2005). Distributed coordination in dynamic spectrum allocation networks. *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005*. (pp. 259–268). IEEE.

[Zhao et al., 2007] Zhao, Q., Tong, L., Swami, A., and Chen, Y. (2007). Decentralized cognitive MAC for opportunistic spectrum access in ad hoc networks: a POMDP framework. *IEEE Journal on Selected Areas in Communications, 25*(3), 589-600.