A Novel MAC Protocol for Cognitive Radio Networks

Munam Ali Shah

Student Number: 0922012

In Partial Fulfilment of the Requirements for the Degree

Doctor of Philosophy

from the

University of Bedfordshire

Department of Computer Science & Technology

Institute for Research in Applicable Computing

University of Bedfordshire

Luton, Bedfordshire, LU1 3JU, UK

April 2013

Supervised by: Dr. Sijing Zhang

Co-supervisor: Prof. Carsten Maple

Advisor: Dr. Yue Zhang

I declare that this dissertation is my own work and that the work of others is acknowledged and indicated by explicit references.

Munam A. Shah

April 2013

ABSTRACT

The scarcity of bandwidth in the radio spectrum has become more vital since the demand for wireless applications has increased. Most of the spectrum bands have been allocated although many studies have shown that these bands are significantly underutilized most of the time. The problem of unavailability of spectrum bands and the inefficiency in their utilization have been smartly addressed by the cognitive radio (CR) technology which is an opportunistic network that senses the environment, observes the network changes, and then uses knowledge gained from the prior interaction with the network to make intelligent decisions by dynamically adapting transmission characteristics. In this thesis, recent research and survey about the advances in theory and applications of cognitive radio technology has been reviewed. The thesis starts with the essential background on cognitive radio techniques and systems and discusses those characteristics of CR technology, such as standards, applications and challenges that all can help make software radio more personal. It then presents advanced level material by extensively reviewing the work done so far in the area of cognitive radio networks and more specifically in medium access control (MAC) protocol of CR. The list of references will be useful to both researchers and practitioners in this area. Also, it can be adopted as a graduate-level textbook for an advanced course on wireless communication networks.

The development of new technologies such as Wi-Fi, cellular phones, Bluetooth, TV broadcasts and satellite has created immense demand for radio spectrum which is a limited natural resource ranging from 30KHz to 300GHz. For every wireless application, some portion of the radio spectrum needs to be purchased, and the Federal Communication Commission (FCC) allocates the spectrum for some fee for such services. This static allocation of the radio spectrum has led to various problems such as saturation in some bands, scarcity, and lack of radio resources to new wireless applications. Most of the frequencies in the radio spectrum have been allocated although many studies have shown that the allocated bands are not being used efficiently. The CR technology is one of the effective solutions to the shortage of spectrum and the inefficiency of its utilization.

In this thesis, a detailed investigation on issues related to the protocol design for cognitive radio networks with particular emphasis on the MAC layer is presented. A novel Dynamic and Decentralized and Hybrid MAC (DDH-MAC) protocol that lies between the CR MAC protocol families of globally available common control channel (GCCC) and local control channel (non-GCCC). First, a multi-access channel MAC protocol, which integrates the best features of both GCCC and non-GCCC, is proposed. Second, an enhancement to the protocol is proposed by enabling it to access more than one control channel at the same time. The cognitive users/secondary users (SUs) always have access to one control channel and they can identify and exploit the vacant channels by dynamically switching across the different control channels. Third, rapid and efficient exchange of CR control information has been proposed to reduce delays due to the opportunistic nature of CR. We have calculated the pre-transmission time for CR and investigate how this time can have a significant effect on nodes holding a delay sensitive data. Fourth, an analytical model, including a Markov chain model, has been proposed. This analytical model will rigorously analyse the performance of our proposed DDH-MAC protocol in terms of aggregate throughput, access delay, and spectrum opportunities in both the saturated and non-saturated networks. Fifth, we develop a simulation model for the DDH-MAC protocol using OPNET Modeler and investigate its performance for queuing delays, bit error rates, backoff slots and throughput. It could be observed from both the numerical and simulation results that when compared with existing CR MAC protocols our proposed MAC protocol can significantly improve the spectrum utilization efficiency of wireless networks. Finally, we optimize the performance of our proposed MAC protocol by incorporating multi-level security and making it energy efficient.

Dedicated to my late father and my mother

ACKNOWLEDGEMENTS

I am very grateful to my Director of Studies Dr. Sijing Zhang, for his valuable guidance and continuous support. Sijing has always supported and encouraged me for new achievements in research. I would also like to express my thanks to Professor Carsten Maple, my co-supervisor, who has always been there to guide me and get the best out of me. I would like to thank my study advisor Dr. Yue Zhang for helping me in final stages of my studies. I am thankful to my ex-supervisor Dr. Ghazanfar Safdar for his great help and guidance during preliminary stages of my PhD.

I should also state my gratitude to the Institute for Research in Applicable Computing, University of Bedfordshire, for their support, without which, all this would not have been possible. Special thanks have to be given to Professor Edmond Parakash, Head of the Institute for Research in Applicable Computing, and Professor Ben Allen, Head of the Centre of Wireless Research, University of Bedfordshire, for their generous help. I am thankful to my colleagues Faisal Qureshi, Muhammad Nabeel Asghar and Muhammad Kamran Abbasi for their suggestions and wishes and they deserve acknowledgements for their suggestions. I am also very thankful to Dr. Jon Hitchcock for proof reading the thesis.

I would like to acknowledge the financial support that has been given to me by my employer COMSATS Institute of Information Technology (CIIT), Islamabad, Pakistan who has trusted in me and invested in me to complete my degree.

Lastly, my greatest thanks to my family in back home, especially to my wife Dania and my boy Abdul Muhaimin who all have provided full support to the accomplishment of this task. It would have not been possible without their compromise on my availability.

PUBLICATIONS

Award and Honour

The best student paper award in the 18th International Conference on Automation and Computing (ICAC'12), 8 September 2012, Loughborough University, Leicestershire, UK

Journals

1. M. A. Shah, S. Zhang, and C. Maple, "An analysis on decentralized adaptive MAC protocols for Cognitive Radio networks," *International Journal on Automation and Computing (IJAC)*, vol. 10, no. 1, pp. 46-52, February 2013.
2. M. A. Shah, S. Zhang, and C. Maple, "Efficient discovery and recovery of common control channel in cognitive radio wireless ad-hoc networks," *Journal of Green Engineering*. Accepted, April 2013.

Conferences

1. M. A. Shah, S. Zhang, and C. Maple, "An analysis on decentralized adaptive MAC protocols for Cognitive Radio networks," *18th International Conference on Automation and Computing (ICAC'12)*, 2012, pp. 1–5. Loughborough, UK.
2. M. A. Shah, S. Zhang, and C. Maple, "A novel multi-fold security framework for cognitive radio wireless ad-hoc networks," *18th International Conference on Automation and Computing,* 2012, pp. 1–6, Loughborough, UK
3. M. A. Shah, S. Zhang, and C. Maple, "An efficient and robust decentralized control channel access mechanism for cognitive radio networks," *Proceedings of the 7th International Conference on Broadband Communications (IB2COM'12)*, Nov. 5-8, 2012, pp. 20-25. Sydney, Australia.
4. M. A. Shah, S. Zhang, and C. Maple, "A Novel Dynamic MAC Protocol for Cognitive Radio networks." *First International Conference on Smart Wireless Communications (SWICOM)*, Manchester, UK. 2012.
5. O. Shah, M. A. Shah, and S. Zhang, "A Novel Authentication Mechanism for Secure Communication in Cognitive Radio Mobile Ad-hoc Networks," *Proceedings of the 7th International Conference on Broadband Communications (IB2COM'12)*, Nov. 5-8, 2012, pp. 142-146. Sydney, Australia.

6. M. A. Shah, G. Safdar, C. Maple, "DDH-MAC: A novel dynamic decentralized hybrid MAC protocol for cognitive radio networks," *IEEE 10th RoEduNet International Conference (RoEduNet)*, pp. no. 1-6, 2011, Iasi, Romania.
7. M. A. Shah, S. Zhang, and C. Maple, "Cognitive radio: Challenges and Issues to make software radios more personal" *International Conference on Smart Wireless Communications (SWICOM)*, UK. 2013.

Under Review

1. M. A. Shah, S. Zhang, and C. Maple, "A Performance Evaluation for Multi-Channel Multi-Access MAC Protocol for Cognitive Radio Wireless Ad-hoc Networks." *IEEE transactions on Broadcasting* 2013.
2. M. A. Shah, S. Zhang, and C. Maple, "Control Channel Etiquettes: Implementation and Evaluation of a Hybrid Approach for Cognitive Radio Networks." *IEEE 24th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2013.

CONTENTS

LIST of FIGURES

LIST of TABLES

ABBREVIATIONS

API	Application Programming Interface
ASAP	Automatic Spectrum Adaptation Protocol
BCCH	Backup Control Channel
BF	Beacon Frame
CCC	Common Control Channel
CR	Cognitive Radio
CRN	Cognitive Radio Network
CSMA/CA	Carrier Sense Multiple Access With Collision Avoidance
CST	Channel-State-Table
CTS	Clear-to-Send
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
DT	D-Transceiver
DSA	Dynamic Spectrum Access
FCC	Federal Communication Commission
FCL	Free Channel List
FDM	Frequency Division Multiplexing
FER	Frame Error Rate
FET	Field Effect Transistor
FPGA	Field-Programmable Gate Array
ICCL	Indexed Common Channel List
ICL	Indexed Channel List
ISM	Industrial Scientific and Medical
ITU	International Telecommunication Union
OODA	Observe, Orient, Decide And Act
OSA	Opportunistic Spectrum Access
PAN	Personal Area Network
PCCH	Primary Control Channel
POMDP	Partially Observable Markov Decision Processes
PU	Primary User

RKRL	Radio Knowledge Representation Language
RTS	Ready-to-Send
SCaN	Space Communication and Navigation
SNR	Signal-to-noise Ratio
SU	Secondary User
SDR	Software-defined Radio
WANN	Wireless Adaptable Node Network
WLAN	Wireless Local Area Network
WRAN	Wireless Regional Area Networks

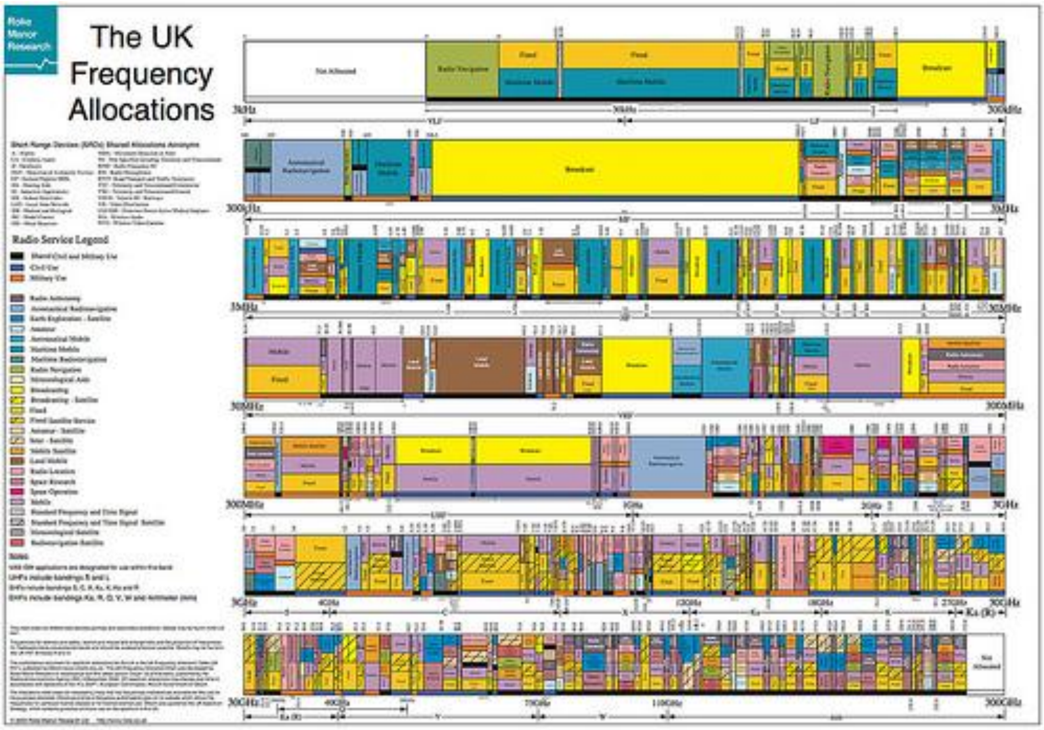
Chapter 1: Introduction

1.1. Spectrum and Frequency Allocation

The wireless technology has become an integral part of everyday life. Broadband wireless access, mobile TV and local TV programme services are just some of the newly-developed services which need spectrum. High definition TV and new developments in digital radio broadcasting are being offered to the public. Some of the other proliferations of spectrum use are broadcasts, remote controllers, mobile phones, garage door openers, satellite transmission, and PDA's. The electromagnetic spectrum which is used as a medium of transmission for wireless communication is a natural resource. Thanks to the German physicist Heinrich Hertz whose discovery of electromagnetic waves led to the development of radio [1][2]. All wireless communication uses some portion of the radio spectrum that needs to be purchased, and the Federal Communication Commission (FCC) provides the service of allocating the spectrum (ranging from 30KHz to 300GHz) for a fee [3][4].

1.1.1. Static and Dynamic Frequency Allocation

A portion of the spectrum can either be statically assigned or dynamically allocated for certain wireless applications. For example, Wi-Fi always uses 2.4GHz band, aeronautical radio navigation operates within the band 190-535 kHz and 100GHz-102GHz is allocated for mobile space-research [5]. Figure 1.1 shows the complete allocation chart of UK frequencies for year the 2012. The second spectrum allocation approach, i.e., dynamic spectrum allocation (DSA), was first discussed in the European DRiVE project [6]. This project aimed to improve spectrum efficiency by dynamically allocating the spectrum to different services. This means that, to introduce flexibility and to improve spectrum efficiency, certain spectrum bands can be allocated to different services for exclusive use. Dynamic spectrum allocation also allows the licensed users of the spectrum to sell and lease their spectrum and to freely choose technology. In this way, DSA enables the industry to make best use of spectrum by allowing the licensed user of the spectrum to either freely use or share their spectrum with unlicensed wireless services.



[1]Figure 1.1. The UK frequency allocation chart [7].

1.1.2. Advantages and Disadvantages of Fixed/Dynamic Frequency Allocation

The major advantage of static allocation of the frequencies in a spectrum band like the Industrial Scientific and Medical (ISM) band (e.g. 2.4 GHz) is that it facilitates development of those wireless applications that can be used globally. It is the static allocation of the ISM spectrum band that helps us connect to the internet regardless of the type and location of the device. However, this has caused severe inefficiency of spectrum utilization which is discussed in more detail in the following section.

1.1.3. Problems in Spectrum Allocation

With the rapid development of wireless applications and more demand for spectrum, the existing spectrum policies have appeared to be longstanding and outmoded. Some of the factors that have forced the policy makers to think beyond the traditional spectrum allocation methods are: demand for increased efficiency of wireless services; development of versatile wireless devices, advances in technology

[1] Courtesy: http://topdf.info/owners-manual/the-uk-frequency-allocations-pdf.pdf

and installation of more and more wireless local area networks (WLANs) in homes and small businesses. Some of the potential problems caused by the classical ways of spectrum allocation have been summarised below.

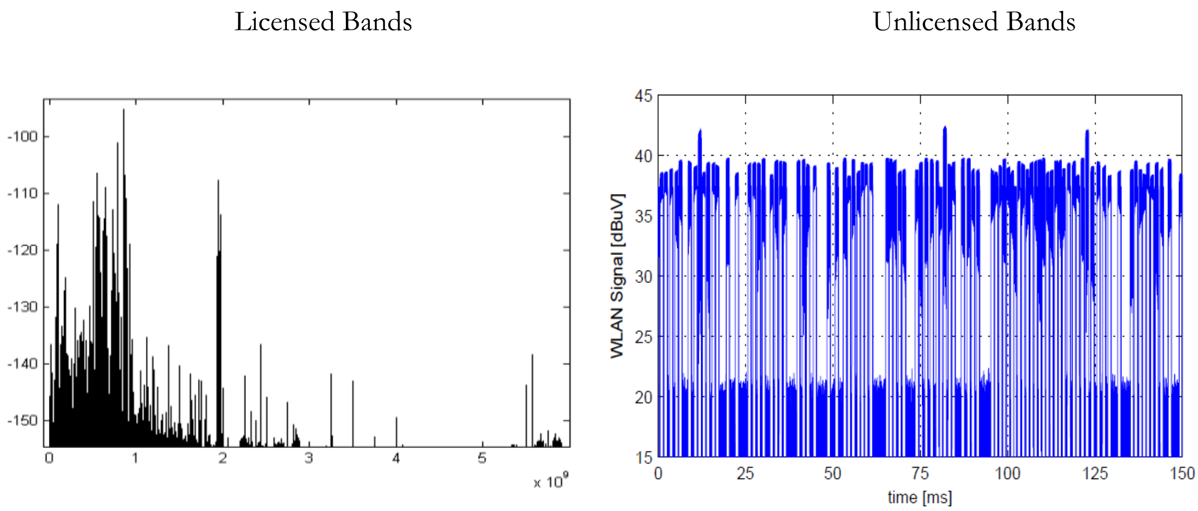
1- Congestion on some of the spectrum bands, e.g., the ISM band.

2- Inefficiency of spectrum utilization in other spectrum bands, e.g., the TV band in rural areas [3][4].

3- Scarcity of spectrum for new wireless applications.

4- Lack of radio resource for those who are more appropriate and needy.

Figure 1.2 shows the inefficiency of spectrum usage in certain spectrum bands.



[2]Figure 1.2. Today's wireless spectrum [8].

1.1.4. Solutions to the Spectrum Scarcity

Technological advancements have enabled the reforms and changes in spectrum policies. Different solutions have emerged to solve the spectrum scarcity issues and to create possibilities for radio systems to use spectrum more rigorously and more efficiently. A few of these solutions are discussed below:

[2] Obtained from D. Cabric et al., "Implementation Issues in Spectrum Sensing for Cognitive Radio."

a) Increased Spectrum Access

The development of new wireless applications and devices has made the spectrum a more scarce resource. Many of the prime spectrum bands have already been allocated to one or more parties, and it is becoming ever more difficult to find spectrum or to expand existing bands for new services. Increased spectrum access allows the licensed users to access the spectrum with more flexibility and more leasing options [9].

b) Opportunistic/ Dynamic Spectrum Access

The concept of opportunistic spectrum access (OSA) has recently emerged as a way to improve spectrum utilization. The basic idea is to first sense the spectrum, which a device wishes to access, and then determine the presence of primary users (if any). Based on that information and regulatory policies, the device can identify transmission opportunities and can utilize the free spectrum if the device imposes no interference or disruption of services to the primary users. The basic components of OSA are: spectrum opportunity identification; spectrum opportunity exploitation; and regulatory policies. OSA allows a higher spectrum utilization and radios can opportunistically retarget their services to a new portion of the spectrum as needed [10][11].

Dynamic Spectrum Access (DSA) improves spectrum utilization by allowing radios to transmit on spectrum bands when they are not in use by the primary owners. The basic components of DSA are: spectrum property rights; dynamic spectrum allocation; and spectrum underlay. The network of radios with the primary rights to transmit in a particular band is the primary network and a radio in this network is a primary radio. The radios that do not have primary rights to transmit in the band are referred to as secondary radios. In DSA, the devices always examine the unoccupied spectrum prior to any data transmission. If the spectrum band is sensed vacant, radio devices can opportunistically use the primary users' spectrum. However, the unlicensed radios must vacate the channel whenever a licensed user's activity is sensed. In order to minimise the interference with the licensed user, spectrum bands are repeatedly scanned by the unlicensed user to avoid any conflict [12].

c) Software-Defined Radios

In response to the reforming of spectrum policy, various new technologies emerged to address the spectrum scarcity issue for efficient radio communication in the 21st century. Among them the technology of *Software-Defined Radio* (SDR)[13] has attracted most attention. SDR aims to perform adaptive and extensive radio signal processing which are not supported in the traditional radio [14]. Based on the same radio hardware, different transmitter/receiver algorithms are implemented in software [15][16][17]. A basic architecture for software-defined radio has been presented in Figure 1.3. This SDR technology has become an integral architectural component of cognitive radio networks.

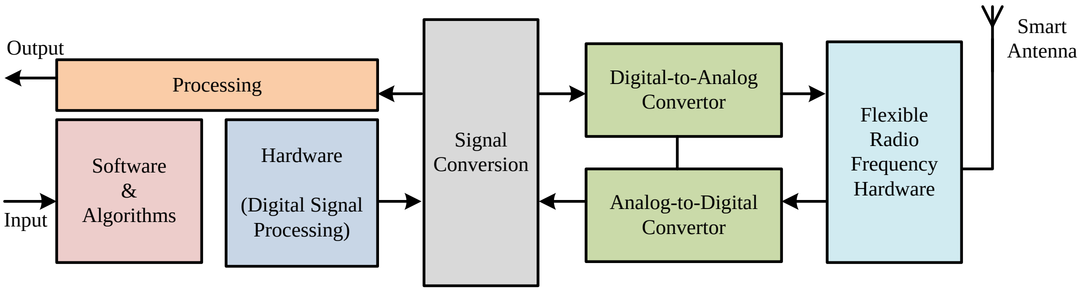


Figure 1.3. Basic architecture for software-defined radio.

The standard features and functions of a software-defined radio have been defined by the International Telecommunication Union (ITU) as follow [18]:

> **Definition 1.1**: Software-Defined Radio
> "*Software-Defined radio (SDR): A radio transmitter and/or receiver employing a technology that allows the RF operating parameters including, but not limited to, frequency range, modulation type, or output power to be set or altered by software, excluding changes to operating parameters which occur during the normal pre-installed and predetermined operation of a radio according to a system specification or standard.*"

d) Cognitive Radios

Advancements in signal processing, radio frequency (RF) technology, and software have led to a rapid evolution of the software-defined radio technology since the term "software radio" was coined by Joe Mitola in 1999 [13][19]. SDR is an essential part of the US military's Joint Tactical Networking Center (JTNC) [20]. Beyond the military applications, commercial standards are being developed and implemented in software (802.16m [21]) and commercial base stations are being implemented as software radios. The Institute of Electrical and Electronics Engineers (IEEE) has also taken initiatives in the potential of software radio and is extensively researching the process of standardization of different networking technologies (802.21[22]). Consider a radio that senses and makes use of an unoccupied spectrum to increase the transmission rate of a data file. Suppose this same radio has the capability to remember the locations where your mobile calls drop and this radio arranges alternate mobile services by different service providers for those locations. This is perhaps the most interesting and motivating idea towards the development of *cognitive radio* (CR) [13]. In fact, a cognitive radio is a software radio which makes use of the knowledge learnt and performs intelligent processing towards users' end goals. Cognitive radio has the capability to learn from its environment and can tune its transmissions parameters to improve reliability, coverage and capacity [23]. Also the use of spectrum in a smart way by cognitive radio can overcome the deficiencies of inexpensive analog components and can offer the deployment of low price cognitive radios [23].

1.2. Defining Cognitive Radio

The simplest way a cognitive radio could be defined is "a radio that is cognitive" or "a radio that thinks". Some of the more prominently offered definitions of cognitive radio are provided below. In the paper published in 1999 which first coined the term "cognitive radio", Joseph Mitola defines a cognitive radio as [13]:

> "*A radio that employs model based reasoning to achieve a specified level of competence in radio-related domains*."

Simon Haykin defines a cognitive radio in his highly cited paper as [24]:

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

The FCC has defined a cognitive radio as [25]:

> "*A radio that can change its transmitter parameters based on interaction with the environment in which it operates.*"

The National Telecommunications and Information Administration (NTIA) [26], adopted the following definition of cognitive radio that focuses on some of the applications of cognitive radio:

> *"A radio or system that senses its operational electromagnetic environment and can dynamically and autonomously adjust its radio operating parameters to modify system operation, such as maximize throughput, mitigate interference, facilitate interoperability, and access secondary markets."*

The International Telecommunication Union (ITU) has defined a cognitive radio system as [18]:

> *"Cognitive radio system (CRS): A radio system employing technology that allows the system to obtain knowledge of its operational and geographical environment, established policies and its internal state; to dynamically and autonomously adjust its operational parameters and protocols according to its obtained knowledge in order to achieve predefined objectives; and to learn from the results obtained."*

IEEE USA offered the following definition[27]:

> *"A radio frequency transmitter/receiver that is designed to intelligently detect whether a particular segment of the radio spectrum is currently in use, and to jump into (and out of, as necessary) the temporarily-unused spectrum very rapidly, without interfering with the transmissions of other authorized users."*

The IEEE 1900.1 group to define cognitive radio has the following working definition [28]:

> *"A type of radio that can sense and autonomously reason about its environment and adapt accordingly. This radio could employ knowledge representation, automated reasoning and machine learning mechanisms in establishing, conducting, or terminating communication or networking functions with other radios. Cognitive radios can be trained to dynamically and autonomously adjust its operating parameters."*

Virginia Tech Cognitive Radio Working Group has adopted the following capability-focused definition of cognitive radio [29]:

"An adaptive radio that is capable of the following:

- *awareness of its environment and its own capabilities,*
- *goal driven autonomous operation,*
- *understanding or learning how its actions impact its goal,*
- *recalling and correlating past actions, environments, and performance."*

Finally, the author of this dissertation has defined cognitive radio as [30][31][32][33]:

"CR nodes are intelligent wireless devices that sense the environment, observe the network changes, and then use knowledge learnt from the previous interaction with the network, to make intelligent decisions to seize the opportunities to transmit. This process of scanning the spectrum (S), exchanging control information (E), agreeing upon white space (A) and transmitting data (T) on the network is repeated continuously in a cycle called SEAT cycle."

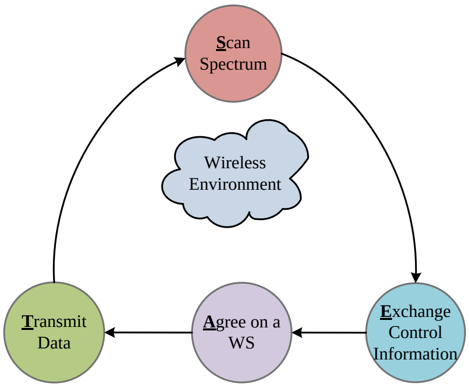


Figure 1.4. Cognitive radio SEAT cycle.

It is possible that these definitions may not be harmonized. However, the following are some general capabilities (see Figure 1.5) found in all of the definitions:

a) Intelligence/Awareness – the radio is capable of applying information towards a purposeful goal.
b) Adaptivity – the radio is capable of changing its waveform.
c) Reconfigurable – the radio is capable of tuning its transmission parameters such as wavelength.
d) Convenient – whether directly or indirectly, the radio is capable of acquiring information about its operating environment.

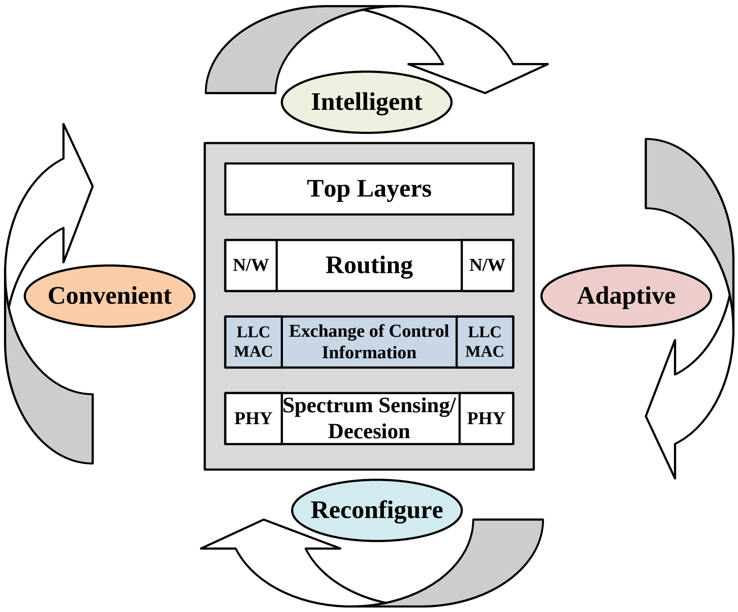


Figure 1.5: Generic capabilities of cognitive radio networks.

Table 1.1 presents the definition matrix for cognitive radio.

Table 1.1 Definition Matrix for Cognitive Radio (adapted from [34]).

Defined by	Adaptivity	Capability Of Environment Sensing	Transceiving Capabilities	Context Aware	Goal Driven	Environment Learning Capability	Negotiate Waveform	Reconfigurability	Tuning Of Transmission Parameters	Process Repetition
Mitola [13]	✓	✓	✓	✓	✓	✓	✓	✓		
IEEE 1900.1[28]	✓	✓	✓	✓	✓	✓		✓		
ITU [18]	✓	✓	✓	✓	✓	✓		✓		
Author [30-33]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

By using common features of all these definitions we arrive at the definition of cognitive radio given in Definition 1.2.

> **Definition 1.2**: Cognitive Radio
> *CR nodes are intelligent wireless devices that sense the environment, observe the network changes, and then use knowledge learnt from the previous interaction with the network, to make intelligent decisions to seize the opportunities to transmit. This process of scanning the spectrum (S), exchanging control information (E), agreeing upon white space (A) and transmitting data (T) on the network is repeated continuously in a cycle called SEAT cycle*.

CR has emerged as promising technology to address spectrum scarcity issues. However, there are some issues related to CR. For example, how can we assure that cognitive radios will not behave inconsistently and the opportunistic spectrum access will not result in overall a poor network performance? Also, how can we verify that the radio will behave as intended and there will be collaboration and cooperation amongst cognitive radios to seize spectrum opportunities?

The work presented in this thesis concentrates on this last problem – the interaction and convergence of cognitive radios in distributed radio environment by developing techniques for modelling and analysing adaptive algorithms for cooperative communication to determine convergence, coordination and cooperation that yield good performance for the cognitive radio network.

Beyond cognitive radio, the techniques developed and presented in this thesis can also be extended to the modelling, analysis and design of cooperative communication in a distributed radio environment. This chapter focuses on the concept, implementation, and applications of cognitive radio and is organized as follows: Section 1.1 discusses the spectrum scarcity issues which gave birth to the concept of cognitive radios. Section 1.2 formally defines cognitive radio. Section 1.3 discusses CR evolution. Related terminologies are discussed in Section 1.4. Section 1.5 discusses some of the regularization issues in CR. Section 1.6 presents existing standards for CR. Section 1.7 briefly reviews the applications of CR. Issues and challenges currently being faced by CR are presented in Section 1.8. Section 1.9

provides some solutions to the existing problem in CR. And lastly, our problem statement, objectives and motivations are discussed in Section 1.10.

1.3. Cognitive Radio Evolution

Cognitive radio has been continuously evolving over the past 15 years. Cognitive radio is in fact an enhanced version of software radio. The idea of software radio was first introduced by Joseph Mitola in the early 1990s [35]. In his dissertation published in 2000, Mitola took the SDR concept one step further, coining the term of cognitive radio [19]. In short, CRs are basically SDRs with the additional feature of artificial intelligence. This feature makes the CR capable of sensing and reacting to its environment. Figure 1.6 differentiates traditional with cognitive radio.

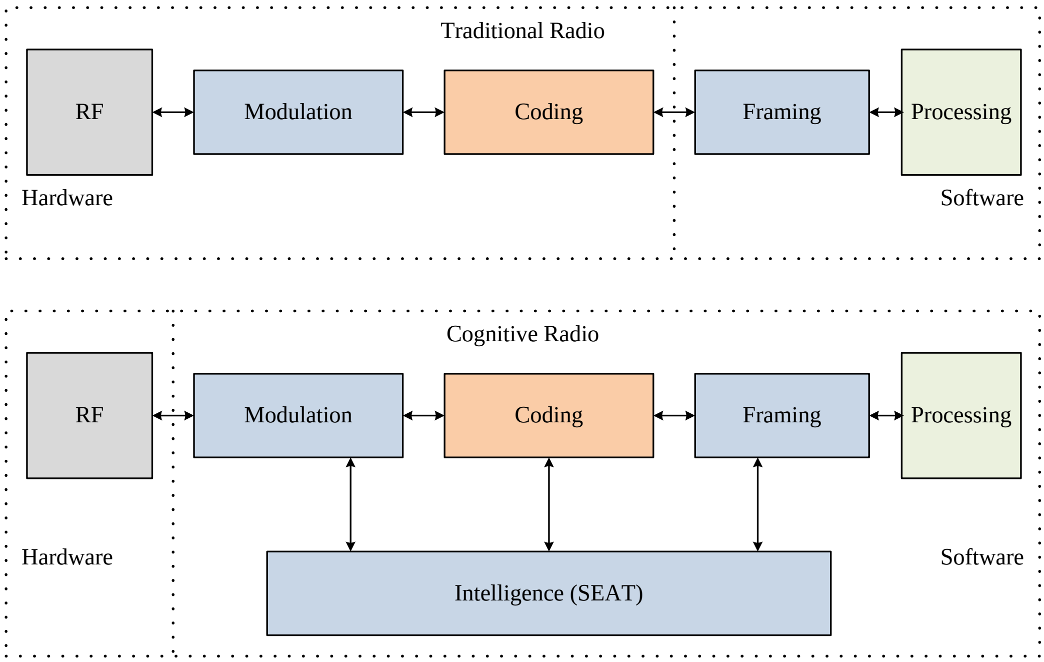


Figure 1.6. Evolution of radio technology.

Based on their adaptability and applicability, cognitive radios have also been defined as: “a military radio that can sense the urgency in the operator's voice, and can guarantee QoS”. Another example is “a mobile phone that could make a mobile call and establish the necessary cell tower handoffs” [13]. CR can also be considered as a reasoning engine with learning and decision making capabilities. Figure 1.7 shows that in addition to a simple policy-based engine, a learning engine is required to observe the radio's behaviour and resulting performance. The facts in the knowledge base are used to form judgements.

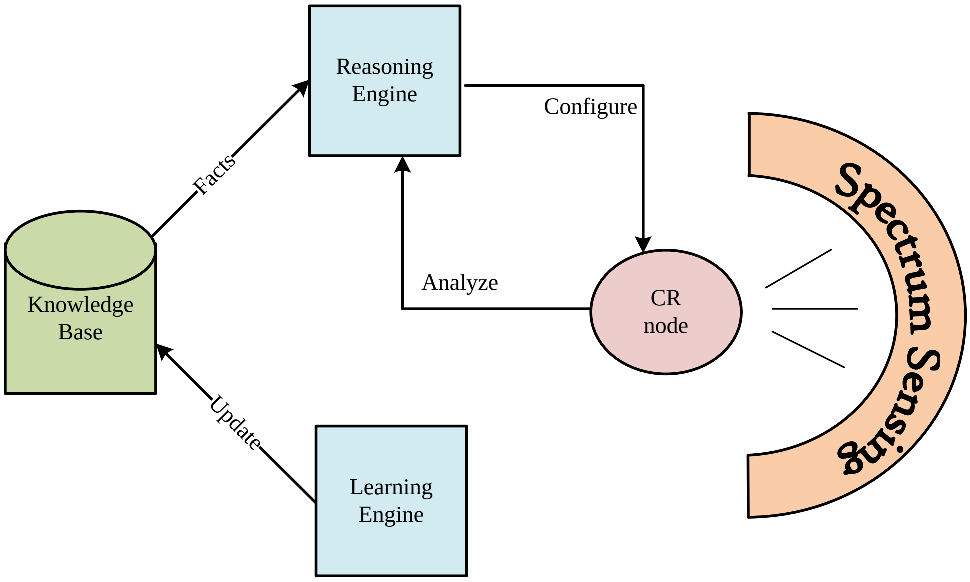


Figure 1.7. Learning and reasoning capabilities of a cognitive radio.

The FCC has shown interest in researching ways in which CRs could be allowed to use licensed bands, if they do not interfere with existing licensed users. A document has been recently approved and adopted by the FCC [36], which allows cognitive radios to operate in certain frequency bands.

1.4. Related Terminology

This subsection describes some terminology, including *Primary User*, *Secondary User*, *White Space* and *Common Control Channel*.

1.4.1. Primary User

The licensed users or primary users (PUs) of the frequency band are those wireless applications who purchased portion of radio spectrum from FCC for some fee [12][19][32][37][38][39][40].

There are three types of frequency bands allocation [41]:

1- No one may transmit, e.g., frequencies reserved for radio astronomy to avoid interference at radio telescopes

2- Anyone may transmit, as long as they respect certain transmission power and other limits, e.g., open spectrum bands such as the unlicensed ISM bands and the unlicensed ultra-wideband band, and the somewhat more regulated amateur radio frequency allocations.

3- Only the licensed user (PU) of that band may transmit

Some of the examples of spectrum primary user wireless applications are

FM Radio Band II = 88MHz - 108MHz

TV Band I (Channels 2 - 6) = 54MHz - 88MHz

GSM primary mobile communication bands = 850MHz and 1.900GHz

Wi-Max Spectrum Band = 3.5GHz and 5.8 GHz

1.4.2. Unlicensed/Secondary/Cognitive User

The secondary users (SUs) are those wireless applications which utilize the unoccupied licensed spectrum opportunistically for communication with the condition that there would be no interference to PUs [19][37][38][42]. Spectrum opportunity [10][39][40][43][44][45] deals with the usage of free/unoccupied spectrum that is part of radio spectrum and not currently being used by PUs.

1.4.3. Spectrum Holes

PUs, when not transmitting in the licensed spectrum, create free channels in the spectrum. These free channels, also called white spaces (WS) or spectrum holes, are used by SUs opportunistically [30][32]. Figure 1.8 shows the spectrum usage by PUs and the formation of free channels. These free channels are in fact the opportunities for SUs to transmit.

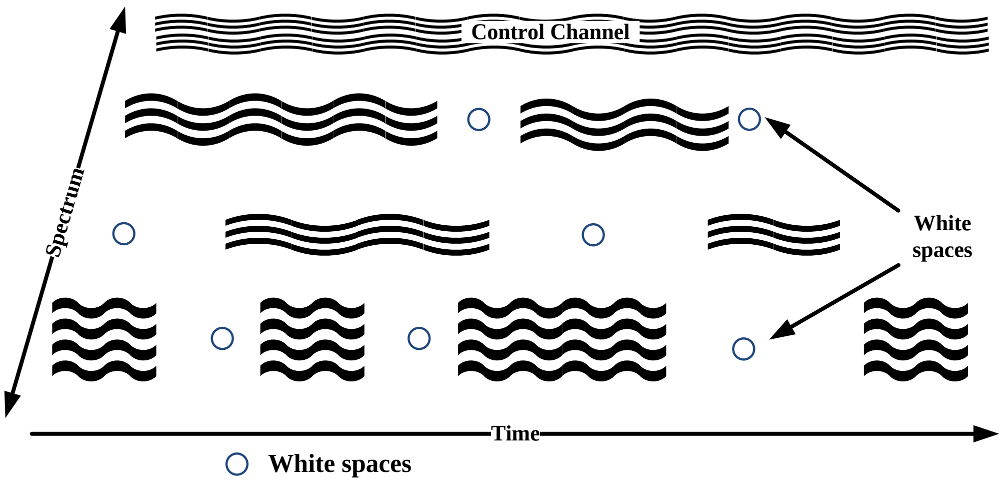


Figure 1.8. Spectrum usage by PUs and the formation of white spaces.

1.4.4. Common Control Channel

A Common Control Channel (CCC) is a free channel required by cognitive devices to exchange the free channel list (FCL) and to initialize communication among co-operating cognitive nodes. Before a pair of SUs start sending and receiving actual data, first they have to coordinate and decide by communicating on the CCC about the chosen white space(s) for subsequent transmission. The pair of SUs exchanges initial information such as how to send the FCL requests, which white spaces to be used and how long the communication will last, etc. This information could also include exchange of Ready-To-Send (RTS) and Clear-To-Send (CTS) control frames, mostly used by cognitive radio devices for exchange of control information [32][47–50][51].

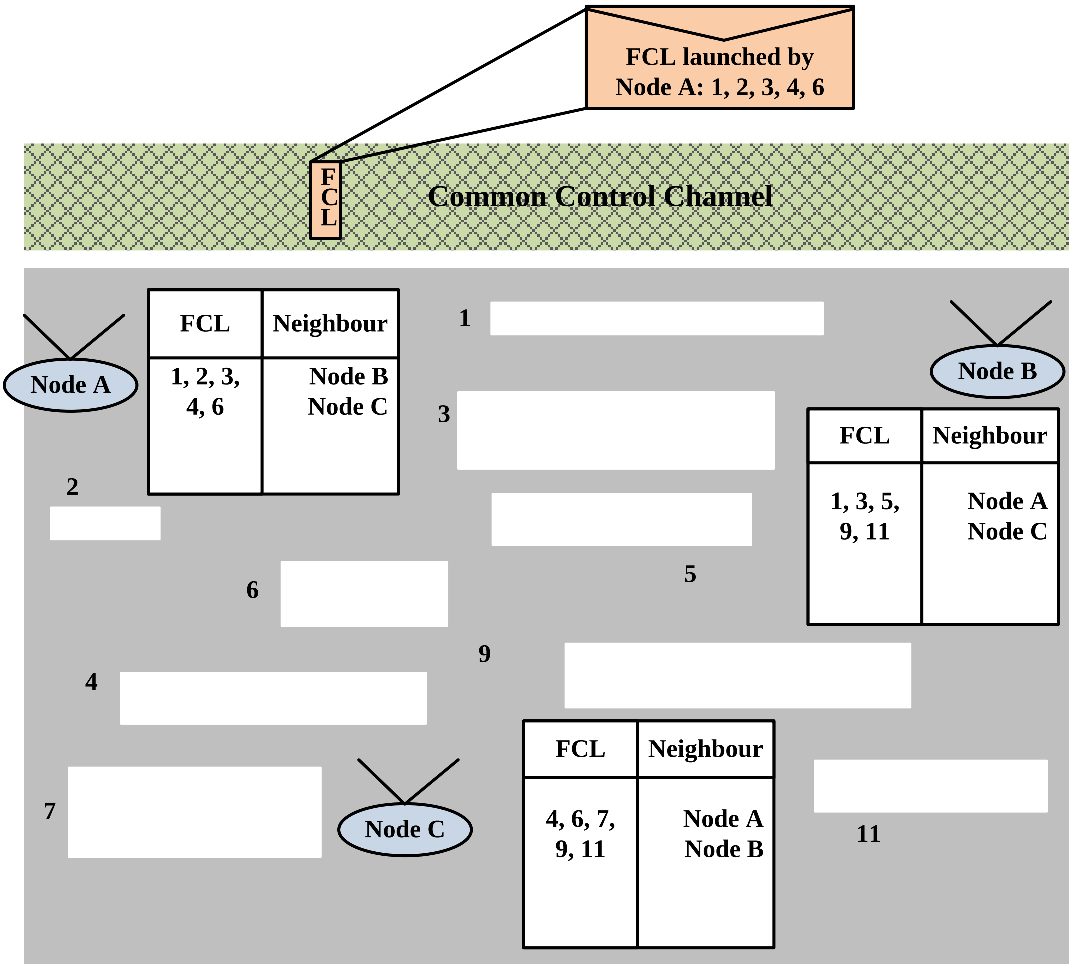


Figure 1.9. Existence of common control channel to exchange the FCL between CR nodes.

The SUs, also called CR users, scan the spectrum for the unused bands (channels) from time to time and create the FCL. The FCL generated by one CR user could be different from the other. The existence of a common control channel between the CR users is the core component in a cognitive radio network (CRN) through which FCLs could be exchanged amongst CR nodes. For communication to occur in a CRN, there must be at least one white space common in their FCLs. The CCC provides a mechanism for nodes in CRN to control access to the spectrum and to exchange the FCL.

1.5. Cognitive Radio Regularisation

Joseph Mitola [52] considers the nine levels of increasing cognitive radio functionality shown in Table 1.2, ranging from software radio to complex self-aware radio.

Table 1.2 Levels of Cognitive Radio Functionality (adapted from [52]).

Level	Characteristic	Comment
1	Pre-programmed	A software radio
2	Goal driven	Chooses waveform according to goal. Environment aware.
3	Context aware	Knowledge of what user is trying to achieve
4	Radio aware	Knowledge of radio and network components
5	Capable of planning	Analyze situation
6	Negotiates	Settle on plan with another radio
7	Environment learning	Determines environment
8	Adapts plan	Generates new goals
9	Adapts protocols	Proposes and negotiates mew protocols

The learning process in a cognitive radio is repeated in a cycle which can make a CR more complex and more artificial intelligence dependent. Some researchers expect lower levels of functionality in their cognitive radio. For instance, in his remarks at the 2005 MPRG Technical Symposium, Bruce Fette, Chief Scientist at General Dynamics Decision Systems, comments that the learning cycle in cognitive radio should be primarily based on an "OODA" (Observe, Orient, Decide and Act) loop. However, [52] suggests that apart from learning capabilities obtained through an OODA loop, there must be additional planning capabilities based on previous network interactions in a cognitive radio.

Based on the existing concept of the OODA cycle, we have developed a loop model specifically for cognitive radio networks. We have called this loop the *SEAT cycle* and have already shown it in Section 1.2, Figure 1.4. All cognitive radios are most likely to make use of the SEAT cycle.

The CR technology is being researched extensively. Different regulatory steps have been put forward to make CR more regularized and applicable. Based on CR functionality and adaptive features, many organizations have implemented cognitive radios in different ways. Some examples of implemented cognitive radio are: CR1 [52]; DARPA's xG program [28]; the biologically inspired cognitive radio [53][54]; CoRTekS (Cognitive Radio Tektronix System) [55]; and Adapt4 [56].

1.6. Cognitive Standards

Since the inception of this technology, lots of efforts have already been made and quite a few are underway to develop cognitive radios as a standardized technology. A generalized policy-based radio suitable for cognitive radio is being developed by DARPA under the xG program using XML based policy descriptive language [57][58]. The IEEE 802 community is currently developing two standards directly related to cognitive radio – IEEE 802.22 and IEEE 802.11h [59][60][61]. Table 1.3 below compares various IEEE standards which incorporate cognitive, dynamic spectrum access, and coexistence technologies.

Table 1.3 Comparison of various IEEE standards [62].

Standard	Scope
IEEE 802.22 Initiation: 9/2004 Completion: 9/2009	This standard specifies the air interface, including MAC and PHY layers, of fixed point-to-multipoint wire-less regional area networks operating in the VHF/UHF TV broadcast bands between 54 MHz and 862 MHz.

802.19 Initiation: 3/2006 Completion: 9/2008	This describes methods for assessing coexistence of CR with wireless networks. The document defines recommended coexistence metrics and methods of computing these coexistence metrics. The focus of the document is on IEEE 802 wireless networks, though the methods developed may be applicable to other standards development organizations and development communities.
IEEE 802.16h Initiation: 12/2004 Completion: 9/2008	This amendment to the 802.16 standard specify improved mechanisms (as policies and medium access control enhancements) to enable coexistence among license-exempt systems based on IEEE standard 802.16 and to facilitate the coexistence of such systems with primary users.
IEEE 802.16m Initiation: 12/2006 Completion: 12/2009	This amendment to the 802.16 standard provides an advanced air interface for operation in licensed bands. It meets the cellular layer requirements of IMT-advanced next-generation mobile networks while providing continuing support for legacy Wireless MAN-OFDMA equipment. It is possible cognitive technology may be introduced in this amendment.
IEEE 802.11y Initiation: 3/2006 Completion:12/2009	This amendment to the 802.11 standard allows application of 802.11-based systems to the 3650–3700MHz band in the U.S. It standardizes the mechanisms required to allow shared 802.11 operations with other users. Likely required mechanisms include: specification of new regulatory classes (extending 802.11j), sensing of other transmitters (extending 802.11a), transmit power control (extending 802.11h), dynamic frequency selection (extending 802.11h).

Apart from initial deployments of cognitive radios, several institutes such as DARPA [23][58][63], the SDR forum [58], NASA's SCaN [64], FCC [65], Winlab, [66] and IEEE 1900 group [28][67][68] have started widely acknowledged initiatives.

1.7. Cognitive Radio Applications

Despite the fact that cognitive radio technology is in its infancy and there is not any concrete example of fully functional and operational cognitive radio, there is a lot of potential applicability of cognitive radio because of its compelling, affordable and unique features. Also, cognitive radio is a promising technology to enhance the existing SDR techniques. In this section we will review cognitive radio applications.

1.7.1. Commercial Applications

The CR technology can be deployed for a number of commercial applications.

- Switching of TV channels from analog to digital has vacated a large amount of TV band [69]. This released TV band could now be used for provision of different commercial wireless applications. Wireless broadband could be one commercial example of a CR technology.
- The requirement for a higher bandwidth for achieving maximum throughput in downlinks in Advanced Long-Term Evolution (LTE-Advanced) systems is another factor contributing towards spectrum scarcity. An LTE-advanced system could seek the opportunities in the DVB (digital video broadcasting) band by using spectrum sensing and sharing methods. A cognitive based spectrum sharing scheme can be employed for spectrum sharing between the DVB and LTE-Advanced systems, which leads to efficient spectrum usage [70].
- Femtocells are widely deployed in homes and buildings due to its attractive benefits for both subscribers and operators, to improve indoor coverage and system capacity. However, some unique features present a challenge in interference mitigation in femtocells. Cognitive radio technology could be deployed to mitigate both cross-tier (nodes in the same tier) and intra-tier (nodes in different tiers) interferences. The potential of applying cognitive radio yields limited complexity and imposes no impact on the state-of-the-art architecture of femtocells [71].

1.7.2. Spectrum Sensing and Access Applications

CR systems are able to sense and observe the local spectrum utilization. The information could then be passed on to the centralized management of a CR system to create increased spectrum access opportunities. This will also avoid interference between two CR systems. By estimating the other uses and monitoring for interference, two CR systems may converge on an unoccupied spectrum band and can communicate [72]. Since spectrum is dispersed, continuous monitoring is required, and cooperative and distributed coordination is needed. A centralized control channel could be used to govern the cognitive function and spectrum occupancy amongst CR users.

1.7.3. Free Mobile Calls with Improved Link Quality

A daily life example that could directly benefit a mobile user is 'free mobile calls'. Consider your mobile device as a CR functionality enabled which has the capability to detect white spaces, and the moment some free channels are detected/sensed by the CR mobile device, the user could be given an option to switch a GSM call over a CR call for free conversation. Or switching from a GSM network to a CR network could also be performed to improve call quality and achieve better coverage, e.g., inside a lift or a building where the reception of GSM signals is week.

1.7.4. Public Safety and Disaster Management Applications

It has been identified that there is a severe lack of interoperability amongst emergency service providers. Responders are unable to establish coordination in an emergency response [73]. Spectrum band which has been dedicated for public safety sometimes interleaves with the frequencies designated for business, industrial, and transportation users and non-military federal users [73]. A cognitive radio could be an efficient solution for the congestion in the traditional radio bands. Policy-based cognitive radio systems could be deployed which can operate and cooperate in a timely manner.

1.7.5. CR Applications for Authentication

Mostly cell phones are equipped with digital cameras with facial recognition software to authenticate an owner. A cognitive radio could also be equipped with such a mechanism that helps learning the identity of its owner and can authentication the legitimate cognitive user. The unauthorised users which try to become part of the CR network could be denied access by running an authenticate application either locally on a cognitive radio device or it can access a remote cognitive radio authentication server. Voice or image recognition could also be used to prevent unauthorized users from becoming part of the CR network.

1.7.6. License Free

For any wireless application, some portion of the spectrum needs to be purchased from FCC. Due to the nature of this technology, CR applications do not have to pay any licensing fee and do not require any permission to use the unoccupied spectrum (as long as they operate within the restricted bands). This feature makes a CR technology less expensive as compared with Wi-MAX and other mobile services.

1.7.7. Radio Resource Management

Tuning the radio parameters after deployment of a wireless network, to adjust call drop thresholds, antenna patterns, antenna power and timing to get the most out of a network, is a challenging task for engineers. Cognitive radio networks could take over the task of post-deployment tuning and automatically update the radio parameters to improve efficiency in terms of performance and network adaption [74]. Cognitive radio should be able to reduce the demand for post-deployment engineering. Such a CR application would have a significant impact on rapidly deployed networks, for example, home WLANs, and certain networks in fixed commercial infrastructure.

1.7.8. Cognitive Radio and Online Multi-user Gaming

With the increasing number of online gamers, the games market is investing a lot to increase revenue potentialities. Online gaming becomes more interesting and challenging for ad-hoc networks where gamers change their location quickly and frequently. The communication amongst vehicular ad-hoc networks is not new and some schemes to reduce number of hops and decrease the delay for ad-hoc vehicular networks have been proposed [75][76]. The cognitive radio technology could make online gaming more interesting, versatile and appealing. CR users can search for available CR gamers in the vicinity and can utilize the available spectrum to play games in real time. It is believed that due to the searching and striving nature of CR, games such as chess are more appropriate candidates for online gaming amongst CR users.

1.8. Deployment of Cognitive Radios: Issues and Challenges

There are a number of issues that should be addressed prior to deployment of this technology on a wide scale. These key issues and challenges could be related to regularization, timely coordination, complicated decision processing and hardware constraints.

1.8.1. Regulatory Issues and Legal Values

Regularization and standardization have been a vibrant point of conflict that needs to be addressed on urgent basis. If cognitive radios are to use the licensed spectrum, what would be the legal value for this usage? No wireless application would allow access to the proprietary spectrum for free as this may cause inconvenience, security vulnerability, and disruption in the services to the primary/licensed user. On the other hand, if cognitive radio is to use the ISM band than there is no need to be a cognitive radio, as unlicensed band could be used by any wireless application anytime. There should be a simple and widely acceptable regulation that could ensure proper and predictable operation of cognitive radios, but at the moment there is no such regulation.

1.8.2. Sensing Abilities

Cognitive radios must be capable of detecting and classifying the signals in the vicinity to exploit spectrum opportunistically and to respond to the changes in environment in an efficient way. The classification between the licensed user signal and the unlicensed signal is the key challenging task. Additionally, presence of multiple licensed users with a variety of signals in the same band imposes additional challenges. Researchers are now actively exploring the issue of signal detection and classification to extract signal information [77]. Even with the best sensing capabilities, there exists the possibility of failing to find the active primary devices (false positive). For example, in the UHF bands in the US which have been suggested for initial cognitive radio deployments, there are currently three primary signals that must be protected - analog TV, digital TV, and wireless microphones – with the possibility of many more to come in the future. The IEEE 802.22 standardization committee is currently considering requiring the maintenance of spectrum usage tables as a part of its standard [78].

1.8.3. Knowledge Representation

The capability of CR to intelligently reason about the environment is subject to the representation of the knowledge that the radio has learnt about its environment. A challenging task is how to represent this knowledge. Mitola [19], has proposed the use of a Radio Knowledge Representation Language (RKRL) to describe the information learnt by a CR device. The xG program has developed an XML-based language for representing in a declarative manner the policies that govern a cognitive radio's actions [79]. Baclawski *et al* [80], has also proposed a language for representing radio knowledge in a declarative manner, but primarily for the purpose of supporting knowledge queries between radios. A Web-based Ontology Language has been proposed in [80]. However, it is uncertain how these languages will interoperate with each other to provide a basis for implementation of CR reasoning capabilities.

1.8.4. Software Radio Issues

As cognitive radio is just an evolution of the SDR, all software radio issues will remain issues for cognitive radio. This includes improving frequency flexibility and agility, enhancing data converter technologies and careful software architecting. The use of field effect transistors (FETs) to implement reconfigurable antennas for cognitive radios has been proposed by Aberle *et al* [81] and Domalapally *et al* [82]. Data converter technologies could also be used to address software issues [83]. Developing techniques for CR are extensively being researched but no generalizable technique has been developed yet.

1.8.5. Negative Impact on Network Performance

Due to the striving nature of CR, a concern has been raised that cognitive radios may negatively impact network performance. While the way that a cognitive radio can negatively impact network performance may not be immediately apparent from SEAT cycle shown in Figure 1.4, CR is preliminary designed to react and respond to an outside world whose state is jointly determined by the adaptations of several cognitive radios, the existence of licensed users, and the sensing powers of a CR, which can make the decision-making of a CR more challenging, ultimately effecting the overall network performance. Consider a centralized CR network where nodes have tuned their transmission parameters to listen to the centralized CR device which governs the cognitive functionality. CR nodes are receiving the information about spectrum opportunities from the centralized CR device. Suppose that a pair of CR nodes have decided to use a spectrum hole whose availability was confirmed from the central CR device. When nodes are about to start transmission, the central CR device updated its information about the availability spectrum. Nodes in this case have to roll back any transaction and will revert to the previous state. The network performance in this scenario will be heavily degraded as CR devices holding delay sensitive data have to wait for longer and renegotiations for transmission parameters could cost time and mobile energy.

1.8.6. Synchronization Amongst CR Nodes

Cooperative communication is the main objective in cognitive radio networks. The CR nodes must be aware of other CR nodes in the distributed environment, and the services they can provide to each other. Once CR nodes learn about other CR nodes they can start data communication. However, network convergence and synchronization amongst CR nodes is the most challenging task. If there is no timely coordination in the CR network, nodes can miss the rare opportunity to transmit.

1.8.7. Security Concerns

The cognitive radio technology has appeared to be an efficient solution for heterogeneous networks. However, this leads to security issues because the same security standards could not be applied in all heterogeneous networks [33]. In GSM [84], WiMAX [85], WCDMA [86] and WCDMA2000 [87], the legality of terminals and users is controlled by a strict authentication process from the base station and the SIM card authentication. The differences between technologies used for cognitive radio and for existing wireless networks make the security incorporation a veiled question. The adaptive nature of cognitive radio technology imposes additional complications and introduces new challenges. For example, an attacker may pretend to be a secondary user and can intercept, without authentication, the FCL by a false claim of being an SU.

1.8.8. Which Spectrum Band to Transmit

Ideally, the cognitive radio should be capable of sensing and exploiting any transmission opportunities in the available spectrum band ranging from 30 KHz to

300GHz. However, due to their sensitive nature, police, medical and military bands are excluded from being sensed and cannot be used by CR. If the rest of the spectrum band is available to be sensed and scanned for transmission opportunities, then it will lead to issues such as regulatory issues, allowance from the primary user, and antenna constraints.

1.8.9. Hardware Constraints

Cognitive radios require hardware design. To make the CR capable of sensing and scanning most of the available spectrum bands, there are certain hardware constraints that need to be addressed. For example, a CR antenna capable of sensing and scanning unoccupied spectrum at 410MHz would be different from an antenna designed for 2.4GHz. The different antenna sizes and transmission power rates, make the CR technology more hardware constrained.

1.9. Addressing Challenges in Cognitive Radios

Cognitive radio has emerged as a promising technology to address spectrum scarcity and its inefficient utilizations. Extensive research is being carried out to make this technology more practical. Some of the solutions for the challenges discussed above are provided below:

- ✓ Currently, FCC and other organizations such as IEEE are working towards the standardization of the CR technology. A first draft for centralized CR networks has already been proposed [88].
- ✓ It is believed that a spectrum band with more transmission potential and less regulatory issues should be considered as a candidate for CR. One example could be the TV band which has become widely available after the TV channels have switched from analog to digital transmission.
- ✓ Security in wireless ad-hoc networks has been extensively researched. The existing security frameworks [33][89] could be deployed to incorporate the security into cognitive radio networks.
- ✓ Adapt4 [56] has developed its SRT (Spectral Reuse Transceiver) technology to facilitate an efficient and non-interfering method of using otherwise idle radio spectrum. It allows all XG1 cognitive radios within a network to monitor the

activities of other users in a specified band and identify unused bandwidth. The network generates a set of parallel carriers and transmits on these channels while they are not in use. When another licensed user is sensed, the network stops using that frequency until it again becomes dormant.

- ✓ Different solutions have been proposed to enhance the spectrum sensing capabilities of CR. This includes spectrum usage tables, sharing spectrum occupancy information amongst CR devices, network assisted detection, and using beacons when primary license devices become active [78]. The IEEE 802.22 standardization committee is currently considering the maintenance of spectrum usage tables as a required part of its standard.
- ✓ The spectrum sensing range could be improved by the deployment of multiband antennas [90][91] in CR devices. This unique feature will enhance the cognition and adaptive capabilities of CR devices.

1.10. Problem Statement

This section refines the problem addressed by this work, and describes the contributions made as part of this work

1.10.1. Research Challenges, Motivations and Problem Statement

One of the most important aspects of cognitive radio networks is how to exchange the control information amongst CR nodes for subsequent communication? Tackling this issue requires us to handle the following three challenges:

- How do the CR nodes interact with each other for cooperative communication, and how do nodes know which CR nodes exist in the vicinity?
- How are the CR nodes synchronized with the same information?
- How do we model/analyse/design an interactive, cooperative and synchronized cognitive radio network?

In order to address these challenges, we develop a novel CR MAC protocol that establishes cooperative communication amongst CR nodes by exchanging control information on a common control channel which is known to all CR nodes in the vicinity. This common control channel helps all the CR nodes to get synchronized with the same information about the network and about the other CR nodes. Our research contribution is to model CR functionality of the MAC layer and then analyse the structure and characteristics of the behaviours of CR network through mathematical modelling and simulation modelling.

a) Modelling Cooperative Communication

The communication could only take place amongst CR nodes if there is some cooperation in the CR network. The existing methods to exchange control information could not be applied as they use either the ISM band which is heavily congested and prone to security threats, or one of the free spaces as common control channel, but no clear model has been identified for CR nodes to converge on a common control channel.

b) Synchronization Amongst CR Nodes

Timely coordination is a key challenge in CR networks. Nodes must efficiently utilize the unoccupied spectrum before it is claimed back by licensed users. Not all the nodes share the same information about the surrounding environment. There must be a centralized point which is accessible and readily available to all CR nodes all the time. Also, the centralized point must serve as an information sharing highway and must not be affected by the PU occupancy.

c) Analysis and Design of a CR Network

While analysing and designing an interactive, cooperative, and synchronized CR network we wish to answer following questions:

1- How to anticipate the performance of a CR network in the presence of network adaptations that can change the state of the network?

2- How to ensure the convergence of nodes in the case that the network state is changed?

3- What would be the effect of wireless medium and unpredictable PU occupancy?

We would answer these questions by mathematically analysing the structure and characteristics of the adaptive behaviour of CR network. Our goal is to model the CR network and analyse interactions amongst CR nodes.

1.10.2. Research Contributions

A novel MAC protocol for cognitive radio networks is proposed in this research. The proposed protocol for cooperative cognitive radio networks enables the CR nodes to quickly and efficiently converge on a common control channel which is available to all CR nodes. The existing MAC protocols either use an ISM band for exchange of control information for subsequent data transmission which is more prone to congestions and security vulnerabilities, or assume that nodes are already converged. Our model is based on the MAC layer which is robust to the PU claims and takes into account all possible network states. Unlike other CR MAC protocols, nodes deploying our MAC scheme have self-reconfiguring capability and always remain in the state of having confidence that there is a channel available to exchange the control information. The mathematical analysis and simulation results show that our MAC protocol outperforms the existing schemes and can work best in all possible scenarios that can occur in a CR environment.

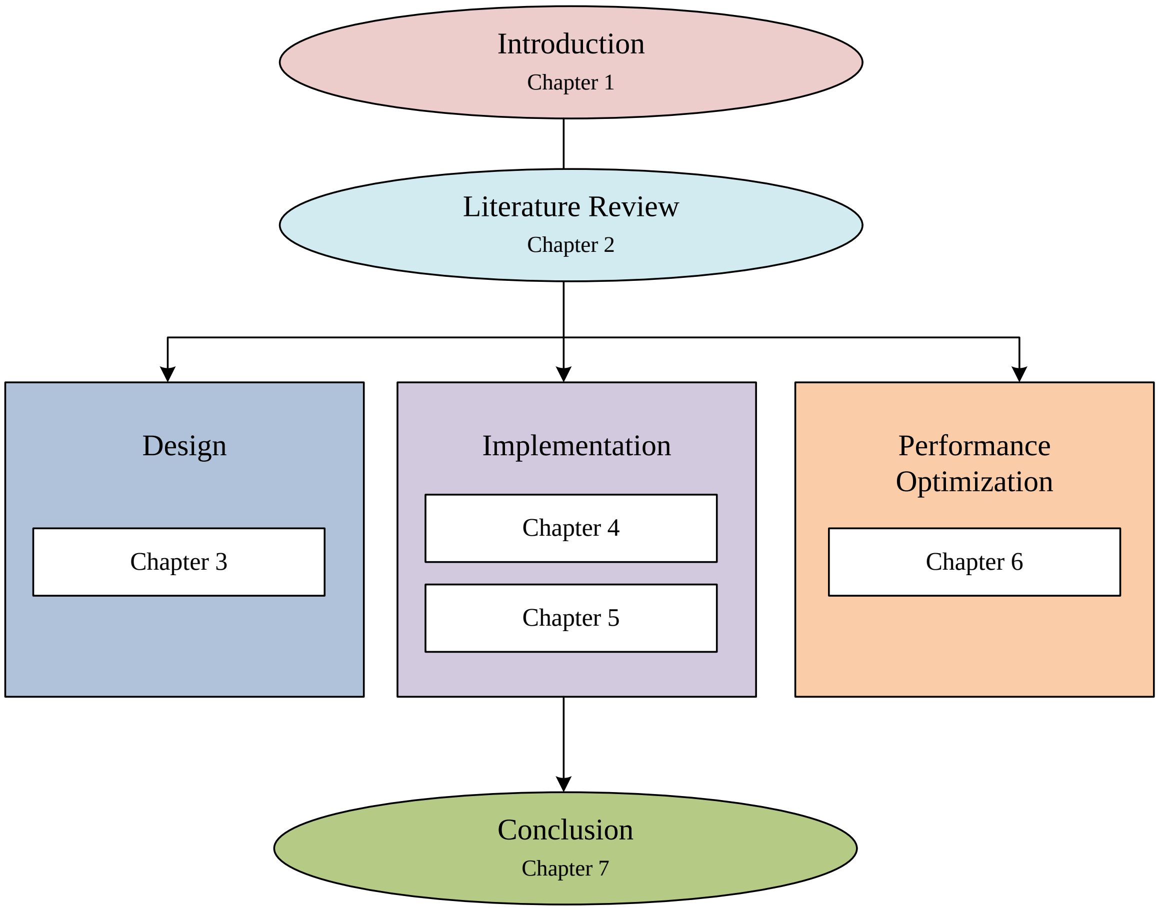


Figure 1.10. Overview of the thesis.

1.10.3. Outline of the Thesis

The outline of the thesis is organized as presented in Figure 1.10.

Chapter 2: This chapter presents a thorough review of the existing work. We have classified the existing CR MAC protocols into different categories and have discussed pros and cons of each of the category. This has given us the motivation to draw a novel MAC protocol which combines the best features of each category and also overcomes their problems.

Chapter 3: This chapter presents a novel MAC protocol developed as part of this work, which is suitable for modelling cooperative communication amongst cognitive radio nodes. The detailed architecture for our scheme has been presented. The pre-transmission time that heavily impacts the performance of a CR MAC protocol has been computed and compared for different case scenarios.

Chapter 4: This chapter covers an analytical model, including a Markov chain model, for the performance of our MAC protocol and discusses the performance evaluation and comparison for different parameters such as throughput, load and delay. The state diagram, DDH-MAC algorithm, and access mechanism used to model our proposed protocol have also been discussed in this chapter.

Chapter 5: This chapter introduces the tools and techniques that have been used to simulate our protocol. The implementation of the DDH-MAC protocol and the performance evaluation and comparison for parameters such as throughput, delay, and load are presented in this chapter.

Chapter 6: This chapter describes the performance optimization of our MAC protocol. Security has been a major challenge in wireless ad-hoc networks. We have incorporated security in our MAC protocol and a

	4-tier security model is presented in this chapter. Also, the efficiency of our protocol in terms of energy-efficiency has been discussed.
Chapter 7:	Based on the modelling and analysis covered in the preceding chapters, this chapter draws conclusions on the design and implementation of cognitive radio network MAC protocols, summarizes the results of this dissertation, and propose directions for future work.

The research contributions made in this PhD study are covered in detail in most of the chapters of this dissertation. Chapters 3, 4, 5 and 6 show main areas of novel contributions. First two chapters present the basic theory for application and implementation of cognitive radio networks. Table 1.4 lists major and novel contributions to the analytical modelling and design of cognitive radio networks.

Table 1.4 Research Contribution in Each Chapter

Chapter	Research Contribution
Chapter 1	Compilation of definitions, discussion about standardization, regularization, applications and challenges for cognitive radio networks
Chapter 2	Intensive research review on existing MAC protocols for cognitive radio networks. Provision of a classification model for CR MAC protocols.
Chapter 3	Provision of a novel secure QoS-aware adaptive MAC protocol for CR networks.
Chapter 4	Analytical Model for Cognitive Radio Network using a Markov chain model
Chapter 5	Simulation experiments to evaluate the performance of the proposed protocol for KPIs such as throughput.
Chapter 6	Performance enhancement of the proposed MAC protocol by incorporating security and making it energy-efficient.
Chapter 7	Conclusions and provision of future work on CR MAC protocols.

Chapter 2: Related Work

Cognitive radio networks serve as a framework for accessing the spectrum allocation dynamically where the vacant channel can be accessed by sensing the spectrum. To exploit spectrum opportunities in a licensed band, cognitive radio devices are equipped with sensor(s) which help them to create the FCL after scanning the spectrum. PUs, when not transmitting creates free channels in the spectrum, these free channels are used by SUs opportunistically. SUs, which are by nature not licensed, are responsible for avoiding interference to PUs. When a PU is detected, SUs should immediately react by changing transmission parameters such as power, and rate, etc. because their transmissions should not degrade primary users' transmissions. Moreover, SUs should coordinate their access between different cognitive radios to avoid collisions on the available spectrum channels.

2.1. Types of Cognitive Radio Networks

A cognitive radio network has the capability to self-organize and self-configure to utilize an unoccupied band and to transmit based on the available spectrum resources. A cognitive radio can form its own network or it can coexist with other existing wireless networks. Due to its ability to coexist with other wireless networks, a CR network structure is heterogeneous. A cognitive radio network can adapt one of the following three different network architectures.

2.2.1 Infrastructure CR Networks

This type of CR network has a base station which usually governs the cognitive functions in the network. Like other Infrastructure wireless networks, the base station is responsible for providing information about available spectrum, security management and cooperation amongst CR nodes in the infrastructure network (Figure 2.1). Cordeiro *et al* [59] has presented the first worldwide wireless standard IEEE 802.22 for cognitive radios. The applicability and market of IEEE 802.22 is restricted to remote and rural areas and the TV channel bandwidths of 6, 7 and 8 MHz have been specified as the most appropriate spectrum band for unlicensed users to transmit. Further enhancements on IEEE 802.22 has been presented by Carl *et al* [92]. Their article presents a high-level overview of the IEEE 802.22 standard for cognitive wireless regional area networks (WRANs) that is under development in the IEEE 802 LAN/MAN Standards Committee.

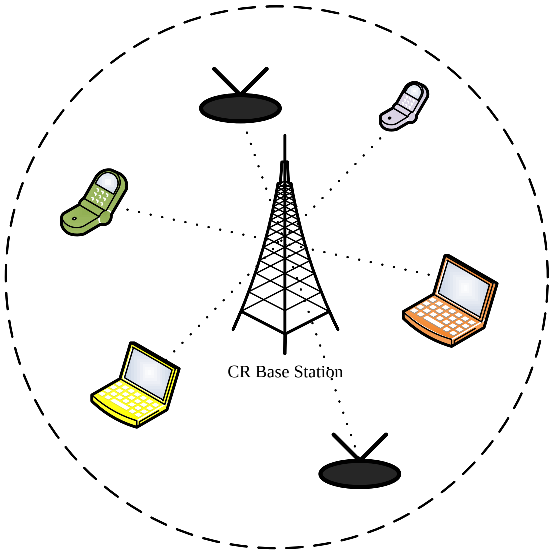


Figure 2.1. An infrastructure-based CR network.

A dynamic spectrum access (DSA) protocol (DSAP) has been presented in [93] which makes use of DSAP server and DSAP relay which are centralized entities that coordinate spectrum access requests and allow multi-hop communication between DSAP clients. The server accepts spectrum lease requests from clients and assigns the spectrum resources with certain constraints such as a time for lease. Like the dynamic host configuration protocol (DHCP), DSAP also makes use of a channel-discover request which is responded to by a channel offer message and a channel request message. Both these messages contain the channel details and lease criteria. A channel ACK is sent by the DSAP server to either accept or decline clients' requests for lease. In the case that there is PU occupancy, a channel reclaim message is sent to the client, forcing it to terminate or reassign clients' lease. In spite of the dedicated central entity that is in DSAP, the exchange of five control frames as control information, prior to any data transmission, imposes a high computational cost and pre-transmission overheads. We suggest that the channel-discover, channel-offer and channel-request messages could be replaced by channel broadcast message containing the FCL. DSAP clients can receive a channel broadcast message and can start their data transmission with other DSAP clients.

Bolivar *et al* [94] present an infrastructure-based cognitive radio network and use frequency-division multiplexing to divide the spectrum into predetermined frequency slots in which SUs communicate. The time-division multiplexing scheme is additionally used to determine if a PU has accessed the channel. This scheme also exchanges multiple control frames that consume network bandwidth. Like DSAP [93], no specification has been made on which spectrum band will be used by the server and clients to dialogue control information. Islam *et al* [95] consider a point-to-multipoint CR network that shares a set of channels with a primary network. A base station controls and supports a set of fixed-location wireless subscribers. Two-phase mixed distributed/centralized control algorithms that require minimal cooperation between cognitive and primary devices are developed. In the first phase, a distributed power updating process is employed at the cognitive and primary nodes to maximize the coverage of the cognitive network while always maintaining the constrained signal-to-interference-plus-noise ratio of primary transmissions. In the second phase, the centralized channel assignment is carried out within the cognitive network to maximize its throughput. We believe that in presence of a centralized CR, the transmission overheads should be optimized in all possible ways.

2.2.2 Ad-hoc CR Networks

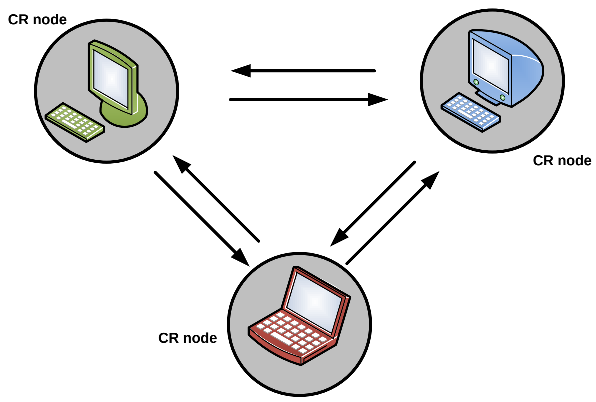


Figure 2.2. An infrastructure-less CR network.

Unlike infrastructure-based CR networks, the CR nodes in the ad-hoc network are responsible for all cognitive operations and functionality. CR nodes can communicate directly with other CR nodes without involvement of a central entity like the base station (see Figure 2.2). Nodes can join and leave the network at any time, and exchanging control information amongst CR nodes without the presence of a centralized station is a key challenge in CR ad-hoc networks. Extensive research has been carried out for this category and different protocols have been presented for ad-hoc CR networks which address issues such as synchronization of nodes, authentication mechanisms for new nodes to join the network, and access mechanisms to dialogue control information on the common control channel. Ad-hoc CR networks are further categorized based on whether they use the ISM band global common control channel (GCCC) or not. Our research is based on infrastructure-less CR networks and is a hybrid between GCCC and non GCCC. More details about GCCC and non-GCCC will be provided in the next section.

2.2.3 Mesh CR Networks

Mesh networks for cognitive radio merge the architectures of infrastructure CR networks and ad-hoc CR networks into one. It uses the mesh topology where different base stations are connected to form a single backbone. The challenge for route selection and spectrum decision could be efficiently addressed by mesh CR networks [96][97]. Figure 2.3 shows the topological design for Mesh CR network.

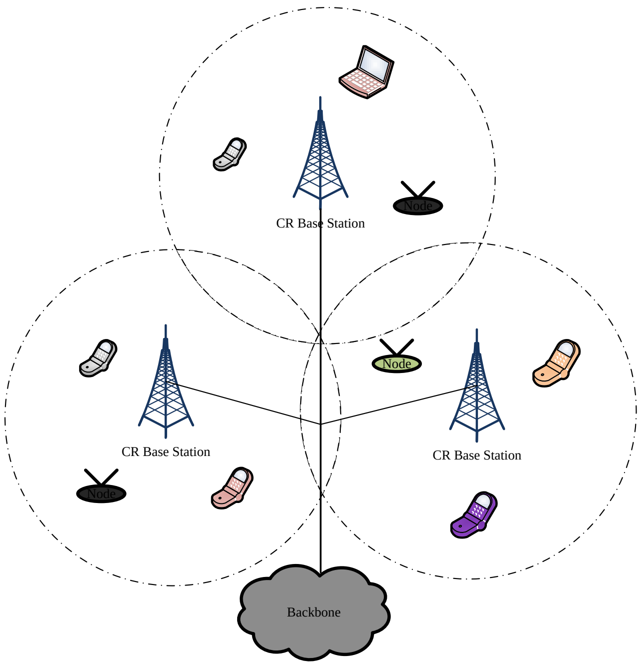


Figure 2.3. Mesh CR network architecture.

The medium access control plays an important role in several cognitive radio functions: spectrum mobility, channel sensing, resource allocation, and spectrum sharing [43][48][98]. Spectrum mobility allows a secondary user to vacate its channel, when a primary user is detected, and to access an idle band where it can re-establish the communication link. Channel sensing is the ability of a cognitive user to collect information about spectrum usage, and to maintain a dynamic picture of available channels. Resource allocation is employed to opportunistically assign available channels to cognitive users according to QoS requests. Spectrum access deals with contentions between heterogeneous primary and secondary users in order to avoid any harmful interference. Multi-channel MAC protocols for ad-hoc wireless networks have represented a first step in the development of MAC protocols for cognitive radio in unlicensed scenarios. These protocols address similar problems; operating in a multichannel context and facing the multiple channel hidden terminal problem [99]. A cognitive radio may exploit, however, increased sophisticated sensing functionalities; it distinguishes between primary and secondary users, and provides protection to licensed transmissions. The number of channels available to each user is fixed in a multi-channel network, while it varies with time and space in a cognitive network. Furthermore, the time-scale in which a cognitive radio operates is very different from that of an ad-hoc radio in that secondary users must exploit periodical sensing to be aware of the wireless environment evolution and must rapidly adapt their behaviour to reach QoS and comply with interference constraints.

2.2. Types of Common Control Channel

As previously discussed in Section 1.4.4, a common control channel is a free channel required by cognitive devices to exchange a FCL and to initialize communication among co-operating cognitive nodes. Before a pair of SUs start to send and receive actual data, they have to coordinate and decide by communicating on the CCC about the chosen white space(s) for subsequent transmission. A common control channel is only required by infrastructure-less CR nodes where they dialogue control information.

2.2.1. GCCC and non-GCCC

The selection criteria for the CCC could be *Static* or *Dynamic* under the static case, SUs use the ISM band provided by the FCC for exchange of control information. CCC in this case would be called a global/universal common control channel. We denote this global CCC as 'GCCC'. In the dynamic case, the control channel is one of the empty spaces from the list of unoccupied spectrum bands or a channel from the FCL. This type of control channel is also called local control channel and is denoted as non-GCCC. Synchronization amongst CR nodes using a non-GCCC is one of the most challenging tasks as nodes are not aware of other nodes in the vicinity initially and nodes may have disparity in deciding a channel in FCL as non-GCCC.

2.2.2. Advantages and Disadvantages of GCCC

Using GCCC for control information has advantages and disadvantages.

a) Advantages of GCCC

- CCC is available 24X7. Since GCCC can be any band specified in ISM, it is always available and can be used by any type of wireless applications.
- There is no need to purchase a license to use the GCCC. The GCCC is within the ISM band so the users do not need to pay any licensing fee or ask for permission to use the GCCC.
- The pair of SUs can find the best channel based on the policy of channel selection and agree on transmission parameters to transmit data; this will lead to zero or minimum interference with the PU. Using the GCCC to exchange RTS/CTS decreases to zero the probability of interfering with the PUs [100].
- The multichannel hidden terminal problem in the cognitive network environment [101] is solved by having a GCCC. The communicating nodes get updated from neighbouring nodes about any hidden terminals in their vicinity through GCCC.

b) Drawbacks of GCCC

Some of the major drawbacks of using GCCC include:

- There is no traffic differentiation, with the First Come First Served (FCFS) mechanism to access the GCCC.
- The higher the saturation of GCCC, the higher will be the computational cost and back-off algorithm to access it, leading to a lower probability of availability of GCCC, which can subsequently have serious effects on the QoS requirements of CR devices.

- The increased number of wireless applications has created huge demand for more radio spectrum; and in these circumstances, having a dedicated band for all wireless applications causes congestion.
- An adversary can impose a denial of service (DoS) attack on a well-known dedicated GCCC by intentionally flooding it, thus creating a major security flaw [102].

2.2.3. Medium Access Control Mechanism in CR networks

In order for CR nodes to communicate with each other, they must exchange the control information and spectrum information through a common control channel. This CCC must be known and available to all CR nodes for subsequent transmission to take place. The medium access control (MAC) protocols help CR nodes to access the CCC and to access available white spaces without interfering with the licensed users. MAC protocols also help CR nodes with addressing and channel access control mechanisms that make it possible for nodes in the CR network to communicate within a multiple access network that employs a shared medium. MAC protocols for CR networks are especially designed to enable reconfiguration and adaptation based on spectrum sensing functions. CR MAC protocols could be classified on the basis of channel access mechanism, use of GCCC or non-GCCC, in-band or out-of-band CCC, overlay and underlay, synchronous and asynchronous CRN, direct access based and dynamic spectrum allocation based, centralized and decentralized CR networks, and whether they are based on cooperative or non-cooperative CR MAC protocols. A single CR MAC protocol can belong to different categories at the same time. For example, a MAC protocol presented in [32] is non-GCCC, decentralized, overlay and cooperative at the same time. More detail about each category will be provided in the oncoming sections of this chapter.

2.3. Design Constraints of Channel Accessing for CR users

To borrow unoccupied channels, CR users must have the ability to identify a channel's characteristics and its availabilities. Since PUs can come back to use the spectrum anytime, CR users should be able to detect the presence of PUs in time and vacate the occupied bands immediately to prevent or reduce the interference to PUs.

Therefore, spectrum sensing and spectrum accessing/vacating are two crucial tasks to realize this technique. Spectrum sensing is the task for CR users to collect information about the spectrum usage and the existence of PUs, and it is mostly the job of the physical layer; while spectrum accessing and vacating are the task for CR users to transmit data packets on unoccupied channels and release these channels to PUs as quickly as possible. We examine the design constraints of channel access for CR users, including the efficiency of control channel, the efficiency of data channel and the efficiency of vacating a channel.

2.3.1. Efficiency of Control Channel

This is reflected by the time required for CR nodes to discover a common control channel. Subsequent communication amongst CR nodes could not occur until CR nodes are aware of a channel that is available for all CR nodes. The control channel efficiency depends on the selection criteria for the control channel. The control channel could be either a well-known and publicly available channel, commonly called the GCCC or it could be one of the most reliable and available white spaces (non-GCCC). The former category suffers from the drawbacks such as saturation of the GCCC, no traffic differentiation (QoS unaware) and security attacks like denial-of-service (DoS). The latter category of control channel has worse searching efficiency, but once the control channel is discovered by all CR nodes in the vicinity, nodes spend less time in exchanging control information and quickly get ready to transmit data.

2.3.2. Efficiency of Data Channel

Data channel efficiency is defined as the time required for two CR nodes to conclude transmission on a data channel. In high traffic loads of PUs, CR users send only one data frame and then vacate the channel. However, when the chances of PUs interferences are low and CR nodes still have data to send, more than one data frame will be transmitted in one transaction. The data channel efficiency could be increased by using more than one data channel simultaneously [103][104]. On the other hand, determining the length of a spectrum hole could also help increase data channel efficiency.

2.3.3. Efficiency of Vacating a Channel

CR users must vacate the occupied channel when the PU claims it in order to minimize the interference. The majority of the CR MAC protocols found in the literature assume that nodes are automatically aware of the presence of PUs [105–112]. However, the unrealistic assumption is criticized because CR nodes cannot sense the PU presence when transmitting and PUs cannot generate interruptive signals to SUs on occupied channels. The performance of both PUs and SUs largely depends on whether or not the PU activity can be sensed in a timely manner. Equipping CR nodes with sensors in conjunction with transceivers could help alleviate the assumption and is less costly than transceivers [38].

2.4. CR MAC Protocols Classification Process.

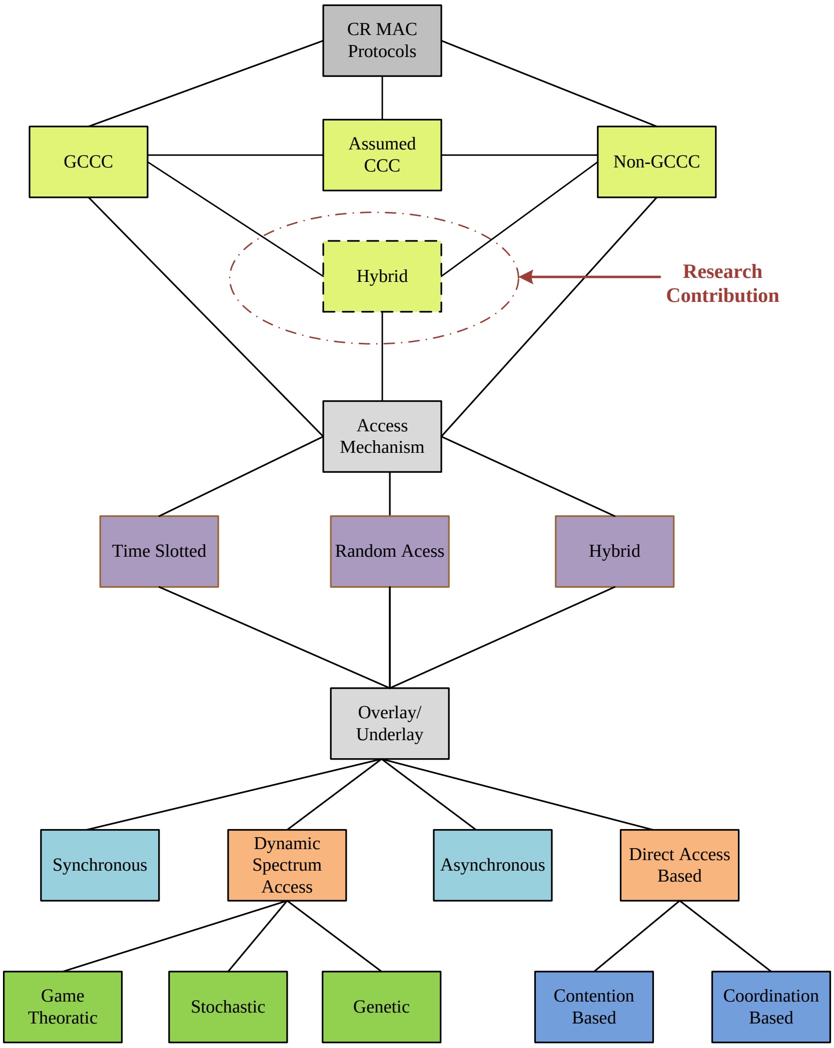


Figure 2.4. Classification model for cognitive radio MAC protocols.

As previously discussed, MAC protocols for CR networks are especially designed to enable reconfiguration and adaptation due to their dependence on spectrum sensing functions. Numerous protocols for CR networks have been designed and developed. A thorough review has enabled us to classify CR MAC protocols as presented in Figure 2.4.

2.4.1. Classification Based On Access Mechanisms

Due to the classical wireless nature of cognitive radio, existing channel access mechanisms (e.g. random, time slotted and hybrid, a combination of random and time slotted) could be applied. The classification of CR MAC protocols based on different channel access mechanisms is further described below.

a) Time-slotted CR MAC protocols

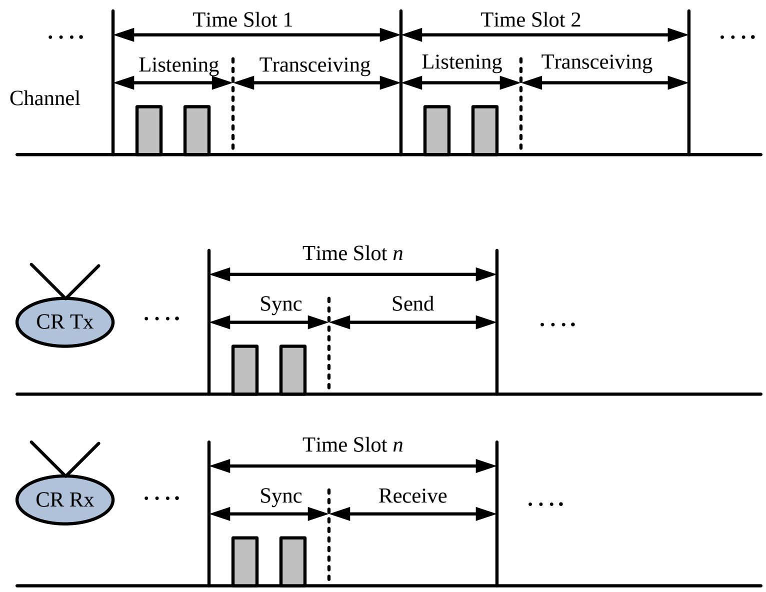


Figure 2.5. Structure of time slotted CR MAC protocols.

The MAC protocols in this category divide the control channel into time slots of fixed length. Each time slot represents one CR node, and nodes can only communicate in their respective time slots. Each time slot has a listening period and a transceiving period. All CR nodes are synchronized in the listening period of each time slot. The time division multiple access (TDMA) algorithm is used to access the common control channel to exchange the FCL or to transmit data in data channels. The protocols presented in [113][114][115] and [100] logically divide the channel into slots, each of which, in turn, includes a slotted listening period where nodes exchange information, negotiate channel usage and get synchronized, and a transceiving period where the actual data transmission takes place (see Figure 2.5). Each node transmits/receives a beacon in a listening period of its designated time slot, which helps deal with hidden nodes, medium reservations, and mobility. The limitation of this category of CR MAC protocols is that a centralized entity is required for the network-wide synchronization.

b) Random Access CR MAC Protocols

The main principle used by the CR MAC protocols in this category is carrier sense multiple access with collision avoidance (CSMA/CA). Each CR node contends for the medium to dialogue control information and then switches to a common channel in the FCL for subsequent data transmission. No time synchronization amongst CR nodes is required in this category but there is always starvation of the control channel. The protocols designed in [116][117][118][119][120] use traditional listen-before-transmission phenomenon. Each node shall sense the carrier before transmission. If the channel is sensed idle, then the CR node that wants to transmit packets sends a RTS message on the common control channel. If the corresponding CTS message is received successfully, then both the sender and receiver switches to the data channel that was found as common during the initial RTS/CTS dialogue. Data packets can be transmitted on the data channel followed by an acknowledgement (ACK) message.

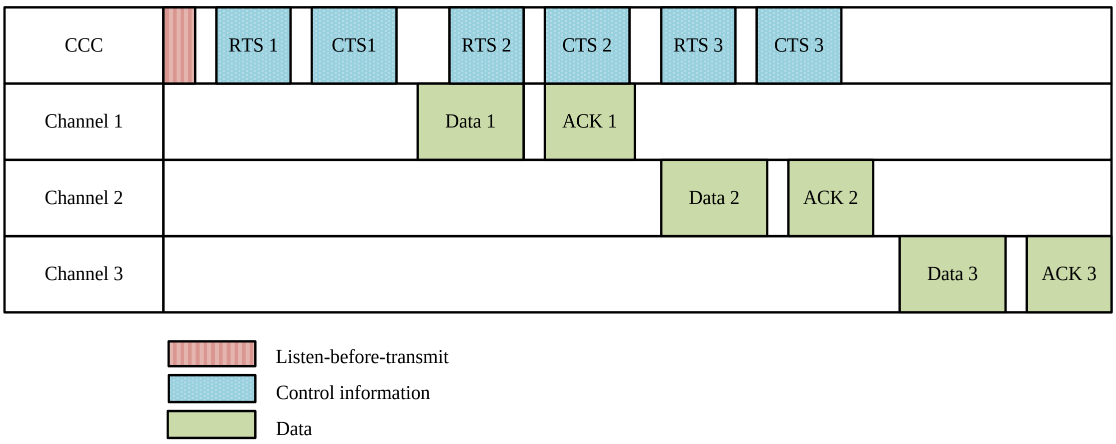


Figure 2.6. The behaviour of random access CR MAC protocols.

c) Hybrid Access MAC

The protocols in this category make use of an approach lying between random access and time-slotted access mechanism. Control signals are synchronized amongst nodes in the CR network through time slots, and actual data transmission occurs following the random channel access mechanism. The OS-MAC protocol for cognitive wireless networks [121] dedicates one channel as a CCC, where inter-channel control traffic takes place. In OS-MAC, devices are only required to be equipped with a half-duplex transceiver. OS-MAC significantly improves the spectrum access efficiency by balancing the traffic load over all spectrum bands, and it fairly treats all users by assuring them to receive an equal access time share or throughput share. Synchronizing amongst nodes is established by locating and switching nodes to the best spectrum band (which is, less loaded, and less noisy). Another hybrid access CR MAC protocol which has been developed is the SYN-MAC protocol [122], which divides the network time into frames. Every frame includes three intervals: the contention interval, the hidden-station elimination interval and the data interval. These intervals help achieve a shorter synchronization time, and nodes within one collision domain agree on a close-enough time point for transmission. The major design flaw in both the OS-MAC and SYN-MAC protocols is the fixed duration of time-slot. The length of time-slot should vary as more nodes join and leave the network.

2.4.2. Classification Based on Proactive and Reactive Approaches

In the proactive approaches, a CR user periodically searches for unoccupied channels, and maintains a table to record the characteristics of sensed channels (such as signal-to-noise ratio, and channel occupancy), even though it has no data to send immediately. A statistical channel allocation MAC protocol is proposed in [103], where all CR users sense the spectrum periodically. The potential transmission opportunities are determined by CR receivers. CR pairs tune their transceivers to agreed-upon channels for data transmissions. A CR user can utilize multiple continuously unoccupied channels to transmit data, and thus the total transmission time is reduced. This approach requires more message exchanges when designated spectrum holes are not available for CR senders. Instead of dedicating a channel for control message exchanges, the mechanism proposed in [100] assumes that each CR user equips two transceivers to do channel sensing (named listening radio) and data transmission (named data radio). For each CR user, its listening radio keeps sensing channels sequentially. When a CR sender wants to send data, it randomly selects a common channel to send control frames at a specified time slot. Global synchronization among CR users is an implementation issue in this approach. A sequence-based rendezvous scheme was proposed in [123]. Two non-synchronized radios looking for each other will eventually be searching on the same channel through the use of non-orthogonal channel hopping sequences. The paper did not describe how to detect the presence of PUs.

In the reactive approaches, a CR user searches for unoccupied channels only when it has data frames to transmit. In HC-MAC [110] time is divided into beacon intervals, and each beacon interval is further divided into three phases: *channel selection*, *sensing*, and *data transmission*. In the channel selection phase, a CR user informs its intended receiver of the selected data channel. In the sensing phase, a CR pair sense the availability of the selected data channel. When the selected data channel is sensed idle, the CR sender starts to transmit data packets. In the data transmission phase, CR users can transmit packets on not only data channels but also the control channel. Therefore, CR users still have opportunities to send data when all data channels are utilized by PUs. Similar to [124], the global synchronization among CR users is a key implementation challenge. Considering limitations of the sensing constraint and the transmission constraint, an optimal stopping problem was formulated in [125] by considering the sensing overhead and the transmission limitation. The derived sensing time helps a potential CR sender to achieve its optimal expected throughput. CR nodes which hear a cognitive-ready to send (C-RTS) or cognitive-clear-to-send (C-CTS) on the control channel are not allowed to send data. As a result, only one CR pair can transmit at a time, and thus the overall throughput of the CRN decreases.

A channel-hopping based cognitive radio MAC mechanism, called CH-MAC in this thesis, was proposed in [109]. In CH-MAC, each CR user has its own channel hopping sequence, which is determined by an unique ID (e.g., MAC address). All CR users share the same hopping-sequence generation function, and thus a potential CR sender can easily obtain the hopping sequence of its intended CR receiver. When a

CR sender has data to send, it follows its receiver's hopping sequence to do negotiation and data transmission. Though this approach does not need a dedicated control channel, how a potential CR sender meets its intended CR receiver on a specific channel efficiently, is not addressed. The sensing mechanism proposed in [123] aimed at exploring the channel hopping sequence to guarantee rendezvous. Indeed, each CR user has a pre-defined channel hopping sequence. The sequences are constructed in such a way to guarantee CR senders rendezvous with their intended CR receivers when they are not synchronized. However, the derived expected time-to-rendezvous is considering a CR pair, and sensing conflict is ignored. The multi-channel cognitive medium access control had been studied in [126]. The authors first formulated the problem of optimal channel sensing order and then proposed a dynamic programming approach to solve the optimization problem. Besides, some special cases are presented to show that the optimal solution does exist. However, the computation complexity is high when some channels cannot be utilized by CR users, and the channel vacating issue has not been addressed.

2.4.3. Classification Based on Common Control Channel

CR MAC protocols dialogue control information on a well-known and well defined control channel. Based on the selection criteria of the control channel, CR MAC protocols could be broadly classified into three categories: GCCC CR MAC protocols, non-GCCC CR MAC protocols and Assumed CCC CR MAC protocols:

a) GCCC MAC Protocols

This category makes use of GCCC in either the ISM band e.g., 2.4GHz, or any other unlicensed band. Cognitive MAC protocol using the statistical channel allocation for wireless ad-hoc networks (SCA-MAC) [103] is a decentralized GCCC-based CR MAC protocol that can speed up the transmission by using more than one channel for data transmission and can wait for some time for a channel with higher bandwidth to become available. A hardware-constrained cognitive MAC (HC-MAC) for efficient spectrum management [117] uses an unlicensed band as control channel and addresses the hardware issues to make CR more practical. A new MAC protocol with control channel auto-discovery for self-deployed cognitive radio networks (DUB-MAC) is presented in [118], which uses a different unlicensed spectrum band other than ISM and employs one frequency band as the control channel and another frequency band to transmit data. These protocols emphasize on data transmission but ignore the pre-transmission overheads such as the time required in dialogue to exchange initial configuration and the time required to converge on the common control channel.

b) Non-GCCC CR MAC Protocols

Protocols in this category either use one of the white spaces as the control channel or use a different band other than ISM to exchange control information before they can actually start communication. The synchronized MAC protocol for multi-hop cognitive radio networks (SYNC-MAC) [100] chooses one of the channels common between itself and neighbours to exchange control signals while other channels are selected to send data. In the opportunistic-cognitive MAC (OC-MAC) [127], initially all nodes reside on a non-GCCC, perform three-way handshakes to select a data channel from the FCL, and confirm the data transmission through an acknowledgement. CR nodes in OC-MAC predict the length of the spectrum hole, but this prediction is strongly criticized because the CR network is an opportunistic network and it is very hard to find the exact duration during which the PU is not utilizing the spectrum so that the length of available spectrum hole could be calculated. The cognitive MAC protocol for multi-channel wireless networks [128] selects the so-called R channel within the white spaces and sets this channel as a control channel and manages the communication on the R channel. The selection criterion for the control channel has not been clearly defined in the above mentioned protocols and most importantly, the clarification about which node will set the control channel and how the rest of nodes will be synchronized is missing.

A distributed cluster-based CR MAC protocol (DCP-MAC) for common control channel selection is proposed in [129]. The CR nodes in DCP-MAC searches for an existing common control channel by scanning all possible channels to receive a CC-BC (Common Channel Beacon) which is broadcasted periodically by a cluster head. A node should listen on one channel to receive CC-BC as well as recording available channels where there are no primary system signals during this scanning time. In the event that a node did not receive any CC-BC during the scanning procedure, it means that either there exists no CCC or the existing CCC is not an available channel at this node. It starts to process the cluster construction by sending a CC-IVT (Common Channel Invite) message to its neighbour nodes using CSMA/CA. Four different types of frames, CC-BC, CC-IVT, common channel report (CC-RPT), and common channel advertisement (CC-ADV), are exchanged amongst CR nodes. Apparently, the network topology based on a cluster is formed by a group of neighbour nodes sharing the same common channels but DCP-MAC has ignored the overheads of exchanging four control frames and has not mentioned the time it will take for all CR nodes to complete the clustering forming process. There are real chances that the channel identified as control channel will be occupied by the time CR nodes in the network form the cluster.

F^2-MAC Protocol [42] presents an efficient channel sensing and access mechanism for an ad-hoc CRN. F^2-MAC uses a five-way handshake to dialog control information. Two types of control frames, similar to traditional RTS and CTS frames, are delivered through a dedicated control channel. Three more control messages, Data Channel Idle (DCI), DCIACK and Ready-To-Vacate (RTV), are delivered through data channels. The proactive channel vacating phenomenon presented in F^2-MAC lets the CR users be reactively aware of the presence of PUs, and the nodes vacate the licensed channel before the PU reclaims. SUs in F^2-MAC sense the data channel, send the RTV frame and then wait for certain time. By transmitting multiple frames on a licensed channel, the throughput in a CR network is improved. However, five control frames and a certain waiting time before transmitting in the F^2-MAC protocol impose the highest overheads. The maximum number of frames exchanged as control information is four for many CR-MAC protocols. Exchanging five control frames will not only consume more mobile energy but also CR nodes may miss the rare opportunity to transmit. Moreover, F^2-MAC does not specify whether the dedicated control channel is GCCC or non-GCCC.

c) Assumed CCC CR MAC Protocols

The protocols [38][42][130][131] in this category do not delve into a control channel setup mechanism and simply assume that a control channel has already been established prior to any data transmission. The Cognitive radio-enabled multi-channel MAC (CREAM-MAC) [38] is a decentralized CR MAC protocol that applies a four-way handshake with communicating nodes on the control channel under the assumption that the control channel is always available and reliable. CREAM-MAC assumes that a CCC has been found and agreed upon by all CR nodes in the vicinity before the CREAM-MAC starts its operation. Further to the assumed existence of a control channel, CREAM-MAC also assumes that the control channel is always reliable and PU-interference free. It is strongly believed that finding a common channel to exchange control information is the primary task of cognitive nodes. Subsequent operations could not take place if the existence of a control channel has not been addressed. So the unrealistic assumption of an available control channel is not a well-built justification. Emphasis has been given to data transmission with complete ignorance of the overheads of determining and agreeing upon the control channel.

Song *et al* [131] have proposed a CR MAC protocol under the property-right model, in which SUs are divided into several non-overlapping groups, and each group uses the proposed auction algorithm to bid for leasing the required channels from the auctioneer appointed by PUs. Based on the distributed environment, secondary users are divided into several non-overlapping groups. Each non-overlapping group has a leader (who is adjusted dynamically), who is responsible for members' management, group channel's management and communication management. Also, an auctioneer, who is appointed by primary users, is used for auctioning vacant channels among leaders through the control channel. The auctioneer checks all bids and allocates the free channels to leader of the group. Though, the proposed MAC protocol claims for efficient spectrum usage but there are numerous pre-transmission overheads, e.g., those made by two different algorithms (an algorithm for joining/leaving the network and another algorithm for free channel allocation to the leaders in each SU group) which are executed prior to any CR transmission. The protocol also does not identify the process of FCL creation.

It is strongly believed that finding a common channel to exchange control information is the primary task of cognitive nodes, and that subsequent operations could not take place if the existence of the control channel has not been well addressed. So the assumption of an available control channel is not a well-built justification.

To summarize, GCCC-based protocols [103][117][118] suffer from the drawbacks discussed previously such as the saturation of GCCC (since it is widely available for anyone, imposing a high computational cost from backing off) and security vulnerabilities. The synchronization of CR nodes on the common control channel is not clearly defined in non-GCCC MAC protocols. The assumption of existence of a control channel is too strong for subsequent data transmission which is heavily dependent on the control channel. Also, CR nodes must release the occupied spectrum to avoid interference with PUs. Most of the protocols discussed above assume that SUs will vacate the spectrum whenever a PU activity is detected. However, this assumption needs to be carefully justified because if SUs are busy transmitting, they cannot detect any activity of PUs and PUs cannot generate signals on busy channels to CR users. Emphasis should be given to the clear methodology for the selection of the control channel rather than on how data transmission amongst two CR nodes will take place (because CR nodes can only switch to actual data transmission once successful and secure FCL transactions have taken place).

2.4.4. MAC Protocols Based on Direct Access

Direct-access based MAC protocols are of two types: *contention based protocols* and *coordination based protocols*. In former category, the CR nodes perform a handshake. This handshake includes classical RTS and CTS frames followed by the FCL. After the exchange of FCL, nodes are able to identify the common white space which they both agree to select as data channel and the subsequent transmission is concluded on the agreed data channel.

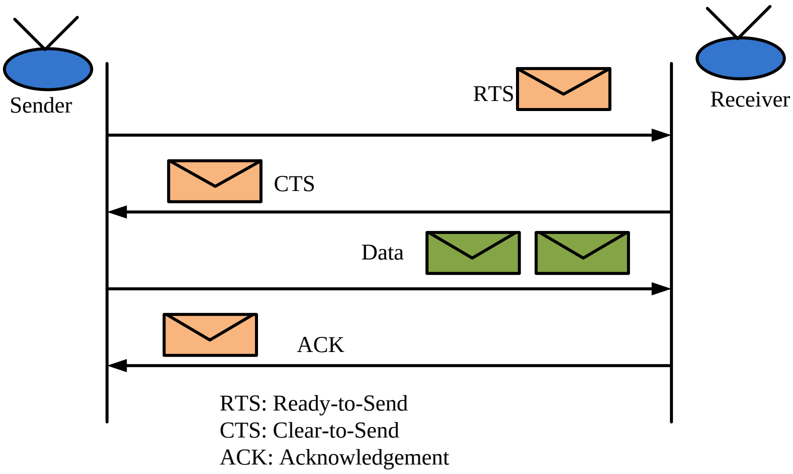


Figure 2.7. Simple handshake process in direct-access based MAC protocols.

Adaptive MAC (A-MAC) [104] is a contention based non-GCCC CR MAC protocol. The A-MAC protocol is distributed in nature and can utilize the backup channel when higher throughput is required. A-MAC needs an always-available control channel to exchange control information amongst CR nodes. Each secondary user senses the licensed spectrum for a period of time. The number of channels sensed by each CR device is subject to a hardware constraint, i.e., the number of sensors per SU. When free channels are sensed, an indexed channel list (ICL) is created. The ICL must be renewed before T_{max} time, where T_{max} is the maximum tolerable time for the primary users to use the licensed channel. Channel indexing is done according to the available bandwidth. The higher the bandwidth of a channel, the higher will be the throughput on that channel. Other parameters that can be used to build a channel rank in A-MAC are SNR, queue length, frame error rate and past history. After the successful four-way handshake, the sender sends data frames in the specified channel and can also use the backup channel if (i) either there is channel occupancy by the PU, or (ii) when improved throughput is required, or (iii) if there are errors occurring in data channel. The important thing to note in A-MAC is the exchange of four control frames. A-MAC, being a contention-based protocol, gives to the contention winning node a chance to occupy the control channel for as long as required. This may cause severe delays to other nodes contending for the medium, especially when any of the control frames is lost and thus has to be retransmitted.

A-MAC is different from the previously discussed protocols as it makes use of a non-GCCC. However the methodology used by CR nodes in the vicinity to converge on a non-GCCC is clearly missing. It is very important for nodes in the CR network to be well aware of the control channel because no subsequent transmission could occur without first finding the control channel. Also more control frames with a larger size for each control frame cause a higher pre-transmission time. Consequently CR nodes will struggle a lot in order to seize the rare opportunity to utilize the white spaces before a PU activity is sensed.

In the coordination-based MAC protocols, each CR node establishes adjacency with its neighbours to improve sensing reliability and improve the system performance. This also helps CR nodes to avoid the hidden terminal problem.

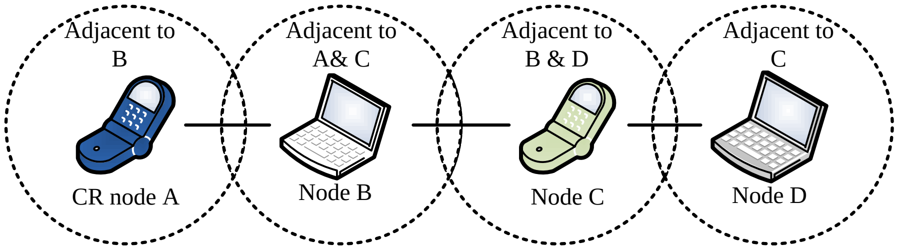


Figure 2.8. Network architecture of a coordination based CR MAC protocol.

The Opportunistic Cognitive MAC (OC-MAC) [127] is a coordination-based MAC protocol that co-exists with a wireless local area network (WLAN). OC-MAC performs the three-way handshake by employing IEEE 802.11 DCF over the dedicated control channel [132][133]. Each secondary user in the OC-MAC protocol maintains a list of all channels available for communication and creates a Channel-State-Table (CST). The physical layer is equipped with sensors. The sensors scan the spectrum and look for the free channels. The statistics for channel utilization and average time of use of channel by the PU are maintained in the CST.

The information contained in the CST is used to estimate the PU traffic and the system busy time. However, there are some vital design flaws in OC-MAC which make it inappropriate for CR nodes. First of all, the operation of OC-MAC is started with the existence of a dedicated control channel which will be used for exchange of RTS/CTS and CRTS, and no description of the dedicated control channel is provided. Secondly, CR nodes in OC-MAC predict the length of a spectrum hole. We strongly criticize this because a CR network is an opportunistic network and it is very hard to find the exact time interval during which the PU will not utilize the spectrum so that the time length of spectrum hole could be calculated. Lastly, the protocol claims to be co-existent with a WLAN, however, the justification for this is neither clearly presented in the paper nor do we believe that CR nodes need to coexist with a WLAN because WLANs use the ISM band (e.g., 2.4GHz) which is already freely available to any user. There is no need to seize the opportunity to transmit in the ISM band, and nodes only need to contend for the ISM band.

The SCA-MAC protocol [103] intelligently senses the spectrum and dynamically accesses the unused or underutilized spectrum with minimum or no interference to PUs. Two basic control parameters are *operating range* and *channel* *aggregation* for SCA-MAC. This protocol also uses the CSMA/CA [134] mechanism to achieve a higher spectrum utilization. SCA-MAC uses a cyclostationery feature detection [8][135] for the continuous and rapid spectrum sensing. This protocol can speed up transmission by using more than one channel for data transmission and can wait for some time for a channel with a higher bandwidth to become available. SCA-MAC is a global decentralized CR protocol which performs a two-way handshake by exchanging frames which contain the information of the best opportunity. SCA-MAC emphasizes the data transmission, and ignores the pre-transmission overheads. Obviously, having more frames exchanged as control information will not only add to the delay for QoS aware data but it will also contribute towards inefficient energy consumption as nodes will have to wait longer before the actual transmission starts.

2.4.5. MAC Protocols Based on Dynamic Spectrum Allocation (DSA)

The DSA-based MAC protocols make use of advanced algorithms to access the available spectrum opportunistically, intelligently, and fairly. The SUs in DSA-based MAC protocols adapt their transmission parameters, such as modulation and coding, power transmission, and antenna configuration, to the changes of the wireless environment, in order to efficiently exploit the available resource. Finding the best transmission opportunities in this category is the most challenging task that requires computational cost and complex calculations to fully understand and learn the status of the CR network. Hence, the MAC protocols in this category suffer from low scalability, negotiation delay and the complexity. In order to reduce complexity in DSA-MAC protocols, several approaches have been considered to model network interactions, such as the localized variation of the island genetic algorithm [136], graph colouring theory [137], [138], game theory [139], [140], stochastic theory [141], genetic algorithms [142], and swarm intelligence algorithms [54].

2.4.6. MAC Protocols for Synchronous Cognitive Radio Networks

The research community has proposed several spectrum sharing based MAC protocols for the synchronous cognitive radio networks. More precisely, Swami *et al* and Zhao *et al* [141][143] developed a cognitive-radio MAC protocol based on the partially observable Markov decision processes (POMDPs) framework. A decentralized cognitive MAC protocol has been proposed in [143]. The protocol allows SUs to autonomously exploit spectrum opportunities without a central entity or a dedicated communication channel.

2.4.7. MAC Protocols for Asynchronous Cognitive Radio Networks

Several asynchronous CR MAC protocols have been proposed that initialize the CR operation in the network after receiving certain signals at certain time intervals [144 – 153]. The performance evaluation for these CR MAC protocols is carried out based on several parameters such as the transmit duration of SUs based on the sensing results to balance the interference caused to PUs and the overall spectrum utilization efficiency, the coexistence with multiple parallel WLANs and providing an innovative solution to the hidden terminal problem by using three sets of radios.

2.4.8. Classification Based on Overlay and Underlay

The CR MAC protocols can also be classified as overlay or underlay. Kim *et al* [154], proposed an underlay spectrum sharing based CR MAC protocol and investigated the dynamic spectrum sharing problem among PUs and SUs. The protocol considered a scenario where PUs exhibited on-off behaviour and SUs dynamically assess the PU arrival patterns. They calculated the SUs' transmission probabilities and developed a framework to maximize the number of admitted SUs for the given fairness constraints.

Elezabi *et al* [155] proposed a scheme for the SUs in underlay cognitive radio networks, which aims to minimize the interference to the PUs. Wang *et al* [156] focused on the CDMA-based underlay cognitive radio systems where the PUs can increase transmission power to counter-balance the harmful interference caused by the SUs. Hoang *et al* proposed a two-phase channel and power allocation scheme for the underlay-based multi-cell cognitive radio networks to improve the system throughput [157]. Zhang *et al* [158] proposed a single input multiple output (SIMO) MAC scheme with joint beam forming and power allocation, which compares PUs' and SUs' power rates and lets the SUs transmit keeping in mind the PUs' power constraints.

Another CR MAC protocol which exploits the underlay approach is COMAC proposed in [159]. COMAC allows SUs to transmit in PUs' spectrum band at low power rates to avoid interference to PUs. The protocol has a major design flaw, i.e., when multiple SUs simultaneously access the common control channel, it causes collisions and furthermore, the multichannel hidden terminal problem is not solved if neighbouring SUs are busy in transmission.

Numerous overlay CR MAC protocols have been proposed that consider unlicensed users (i.e., secondary users) opportunistically exploiting the spectrum holes in licensed frequency bands. In overlay CR networks, secondary users can only transmit on channels if these channels are not being used by primary users. In [160] the overlay access paradigm is investigated and this approach is compared with the classical interweave access. The assumption of the overlay model is that the secondary transmitter has *a priori* knowledge of the primary user's message. Furthermore, all channel gains are known to both transmitter and receiver. Simulation results presented show how the underlay technique can potentially outperform the achievable secondary network. However, as the knowledge of the licensed user message can be available at the cognitive side only if the two transmitters are located in close proximity, the overlay performance gain is strongly affected by this distance. Moreover, complicated pre-coding techniques must be available at the cognitive transmitter, and cooperation between primary and secondary systems is necessary to estimate channel gains between transmitters and receivers.

A MAC protocol for opportunistic spectrum access in cognitive radio networks (OSA-MAC) has been proposed in [161]. The proposed OSA-MAC integrates both sensing and channel access functionalities and works in a multi-channel environment where each SU only accesses at most one channel at any time. The protocol also takes into account issues such as synchronized transmission, contention on the control channel, and the traditional hidden terminal problem. In addition, to avoid the possible collision with PUs, SUs perform sensing frequently besides doing the contention resolution as in a conventional MAC protocol. The protocol assumes that a dedicated control channel is always available for exchange of control information and thus suffers from all the drawbacks mention in Section 2.2.

In [162], a cognitive MAC protocol for QoS provisioning in overlay ad-hoc networks is proposed which establishes a neighbour list to help a CR node recognize the spectrum opportunities. The protocol is different from the legacy CSMA/CA by introducing an algorithm with an improved contention resolution mechanism, consisting of a gating mechanism, a linear backoff algorithm and a stall-avoidance scheme. The proposed protocol maintains three different types of table: a PU information table (PIT), a reservation information table (RIT), and a contention information table. We believe that creating, populating, indexing and searching three different tables at each CR node will not only add processing complexities within the CR nodes but will also make it hardware dependent as nodes have to manage three different tables simultaneously.

2.4.9. Classification Based on Single Radio And Multiple Radio

The cognitive radio MAC protocols could also be categorized based on the number of transceivers/radios used. Here a single radio is used for sending and receiving data with the constraint that when it transmits, it cannot receive and vice versa. Many single-radio based MAC protocols have been proposed [99][114][163] [164].

The single radio adaptive channel (SRAC) algorithm is proposed in [163] and it adaptively combines spectrum bands based on the CR user requirement, called dynamic channelization. In addition, it uses a scheme like frequency division multiplexing (FDM), called cross-channel communication, in which a CR user may transmit packets on one spectrum band but receive messages on another spectrum band. Although, the hardware cost could be reduced by deploying a single radio but it could suffer the traditional hidden terminal problem. Also, the SRAC algorithm makes the strong assumption and claim to be already capable of detecting PU arrival of the licensed spectrum bands.

The Cognitive MAC (C-MAC) protocol proposed in [114] operates over multiple channels. Each channel is logically divided into recurring super frames which, in turn, include a slotted beaconing period (BP) where nodes exchange information and negotiate channel usage. Each node transmits a beacon frame in a designated beacon slot during the BP, which helps in dealing with hidden nodes, medium reservations, and mobility. For coordination amongst nodes in different channels, a rendezvous channel (RC) is employed that is decided dynamically and in a totally distributed fashion. The functionality and the operation of the C-MAC protocol are heavily dependent on the rendezvous channel (RC), which is one of the white spaces in the FCL. If the RC is occupied or reclaimed by the PU, there are no mechanisms for CR nodes in C-MAC to resume the cognitive functionality on some other RC.

Hyoli *et al* [164] propose a MAC-layer sensing scheme in cognitive radio networks. The proposed scheme tries to discover as many utilizable spectrum opportunities as possible and assumes every SU is equipped with a single identical antenna that can be tuned to any combination of consecutive licensed channels. However, equipping each SU with a single antenna will lead to the traditional hidden terminal problem and SUs would not be able to detect claims by PUs in a timely manner.

When multiple transceivers are in place, the task of designing a multi-channel MAC protocol is significantly simplified. Issues related to hidden and exposed terminal problems, connectivity, and channel switching can be overcome almost completely. Here, it is assumed that nodes have multiple transceivers capable of tuning to and accessing different channels simultaneously, which is the key to overcoming the aforementioned challenges. Research here has mostly focused on channel selection strategies. In the Dynamic Private Channel (DPC) protocol introduced in [165] nodes are assumed to be equipped with as many transceivers as the number of channels. As in other protocols, one particular channel is reserved as the default control channel for negotiation purposes. Given that a transceiver is always associated with the control channel, the multi-channel hidden terminal problem is eliminated. Special RTS and reply-to-RTS frames are employed in this control channel in order to select another channel for data communication.

The multi-channel MAC protocol proposed in [166] also assumes that each node has as many transceivers as the number of available channels, but here nodes are capable of listening to all these channels simultaneously. Whenever a node has a packet to send, it selects an idle channel for transmission. In the case of multiple idle channels, the one employed in the last successful data transmission is preferred. This technique is referred to as "soft channel reservation". An enhanced channel selection strategy for this protocol has been presented in [167], and it consists in selecting the best channel based on the power level sensed at the transmitter. On the other hand, the Receiver-Based Channel Selection (RBCS) mechanism in [168] chooses the best channel on the basis of the signal-to-interference and noise ratio (SINR) at the receiver.

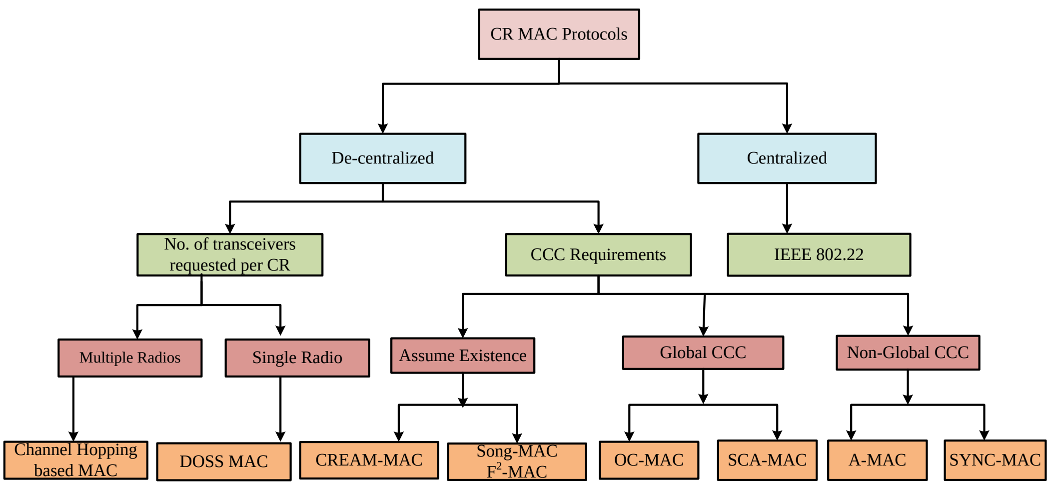
The Dynamic Channel Assignment (DCA) protocol [169] operates similarly to RBCS. It employs a default control channel while other channels may be used for data transmission. A distinctive feature of DCA is that it requires exactly two transceivers, one of which is permanently tuned to the default control channel and the other of which is free to tune to any of the data channels.

The power saving multi-channel MAC protocol (PSM-MMAC) [170] targets the power consumption under reduction of multi-channel operation, which is highly desired due to the fact that some nodes are powered by battery. However, PSM-MMAC focuses only on the one-hop case. It is not straightforward to apply it directly to the multi-hop case. Finally, the Common Spectrum Coordination Channel (CSCC) protocol [171] is an extension of the DCA protocol, allowing different types of wireless devices to share the radio spectrum. This is done via negotiation through the CSCC.

2.5. Summary

Numerous CR MAC protocols have been designed and developed by the research community. There exists different parameters and characteristics that are considered while designing a CR MAC protocol (see Figure 2.4 for different types of CR MAC protocols). These design parameters include the type of infrastructure, the design of the common control channel, the access mechanism on the control channel and the access mechanism on data channels, the number of control frames exchanged as control information, the utilization of free spaces with and without coalition of a PU, the cooperation type, the number of transceivers and the selecting criteria for best channel. There are a few other parameters that are also taken into consideration during the development of a CR network such as signalling methods, spectrum sensing techniques, and certain physical layer parameters.

Not all the CR MAC protocols present a similar design. In our literature review we have focused only on those CR MAC protocols whose design architecture match the design of our proposed DDH-MAC protocol. Other reasons for these protocols being reviewed in Chapter 2 are that these protocols are highly cited and that they are among the newest CR MAC protocols. A broad classification of CR MAC protocols is presented in Figure 2.9.



CCC: Common Control Channel
A-MAC: Adaptive /Cognitive MAC
DOSS: Dynamic Open Spectrum, Sharing
CREAM: Cognitive Radio EnAbled Multi-channel
Song-MAC: A Leasing Oriented MAC Protocol for High Spectrum Usage in CR Network
SCA: Statistical Channel Allocation
OC: Opportunistic Cognitive
SYNC: Synchronized MAC
F^2-MAC: Fast and Fair MAC

Figure 2.9. Classification of CR MAC protocols.

All types of CR MAC protocols exchange control information over the control channel. This control information is a pre-requisite for any subsequent transmission to occur. The control information can include frames such as RTS/CTS/FCL and FCL ACK. The CR nodes intending to transmit to other CR nodes in the vicinity first exchange the control information on a well-known and well-established control channel. The criteria to access the control channel could be either coordination-based or contention-based. Once there is an agreement between a pair of CR nodes about which white space to use for actual data transmission, the CR nodes switch to the data channel and if there is a PU claim on the data channel, then they have to vacate the data channel without interference to PUs. The generic behaviour of CR MAC protocols is described in Figure 2.10.

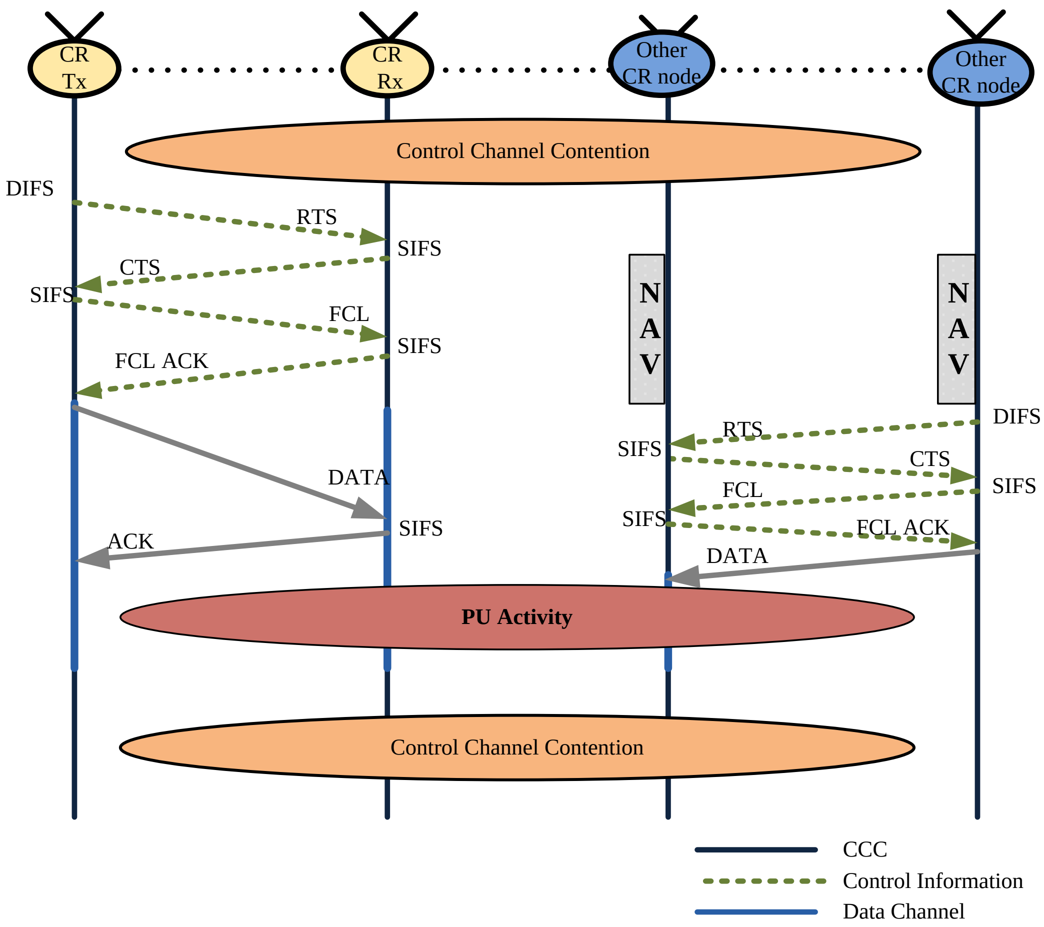


Figure 2. 10. Generic behaviour of CR nodes dialoguing control information on the control channel.

In this literature review we have discussed numerous CR MAC protocols and the parameters considered in their design and development process. We have summarized our review in the following two tables which thoroughly presents different features of CR MAC protocols.

Table 2.1 Comparative evaluation of CR MAC protocols

Features	CREAM	OC-MAC	SCA-MAC	A-MAC	F2-MAC	DNG-MAC
Spectrum Sensing [12][172]	Energy Detection	Not discussed	Cyclo-stationery	Not discussed	Not discussed	Energy Detection
Acknowledgement after Tx	no	✓	✓	no	no	no
Avoidance of multi-channel hidden terminal [118]	no	Not addressed	Not addressed	no	✓	yes
Control Channel	Assumed	Dedicated	GCCC	Non-GCCC	Dedicated	Non-GCCC
Best Channel Criteria	arbitrary	data rate	arbitrary	Channel rank	Not discussed	arbitrary
Multi-Channel MAC [94]	✓	✓	✓	✓	✓	✓
Physical Layer Parameters [40]	[3]DSSS	Not discussed	Not discussed	DSSS	Not discussed	DSSS
Use of backup data channel	no	no	✓	✓	no	no
Spectrum Access	802.11 DCF	802.11 DCF	CSMA/CA	802.11 DCF	CSMA/CA	CSMA/CA
Number of transceivers	Single	single	single	single	multiple	single
Number of Control frames	4	3	4	4	5	2

It is concluded that in order to develop a CR MAC protocol, there are certain parameters that a CR MAC protocol must address. In Table 2.2, we have selected 20 CR MAC protocols and have summarized their design parameters.

[3] DSSS: Direct Sequence Spread Spectrum, A physical layer parameter of IEEE 802.11b

Table 2.2 Characteristics of CR MAC Protocols

	Infrastructure/ Architecture	Common Control channel	Access Mechanism	Direct Access Based	Single/Multi Transceivers	Number of Control channels	Signalling	Quiet period
CREAM-MAC[38]	Decentralized	Assumed	IEEE802.11 DCF	Contention based	Single	1	Not addressed	No
DOSS-MAC[173]	Decentralized	non-GCCC	CSMA/CA	Contention based	Not addressed	n	Out-of-band	Not addressed
SYNC-MAC [100]	Decentralized	Local	IEEE 802.11 DCF	Coordination based	2	1	In-band	No
OS-MAC[121]	Distributed	GCCC	CSMA/CA	Coordination based	single	1	Out-of-band	Not addressed
C-MAC[114]	Distributed	GCCC	Time slotted	Coordination based	single	1	Out-of-band	yes
HC-MAC[117]	Distributed	GCCC	IEEE 802.11 DCF	Contention based	single	1	Out-of-band	yes
DUB-MAC[118]	Decentralized	Non-GCCC	CSMA/CA	Contention based	Not addressed	1	Not addressed	No
CO-MAC[174]	Distributed	GCCC	Not addressed	Contention based	Not addressed	1	Out-of-band	No
OSA-MAC[175]	Decentralized	GCCC	IEEE 802.11 DCF	Contention based	Not addressed	1	Not addressed	No
CogMesh[176]	Distributed	Local	TDMA	Coordination based	single	1	Out-of-band	Yes
IEEE 802.22[92]	Centralized	None	Random	Coordination based	single	none	In-Band	Yes
DC-MAC[177]	Decentralized	Local	Random	Contention based	single	1	Not addressed	no
DCCP-MAC[94]	Centralized	None	Not discussed	Coordination Based	Not addressed	none	Out-of-band	No
CL-MAC[178]	Decentralized	Assumed	CSMA/CA	Coordination Based	2	1	Not addressed	yes
OP-MAC[179]	Decentralized	Local	IEEE 802.11 DCF	Contention based	1	1	Not addressed	No
DCP-MAC[129]	Decentralized	Local	CSMA/CA	Coordination based	Not addressed	1	Not Addressed	No
Sr.-MAC[50]	Decentralized	Global	IEEE 802.11a	Coordination based	2	1	Not addressed	No
Hu.-MAC[130]	Decentralized	Global	Not addressed	Coordination Based	2	1	Not addressed	No
DH-MAC[180]	Decentralized	Assumed	IEEE 802.11 DCF	Contention Base	1	1	Out-of Band	No
NMS-MAC[181]	Decentralized	Global	CSMA/CA	Contention Based	2	1	Not addressed	no

Chapter 3: A Novel Adaptive MAC Protocol for Cognitive Radio Networks

3.1. Introduction

The critical and most important aspect of the cognitive radio network is how to advertise the FCL among the participating cognitive nodes. Some protocols [50][114][121][117][131][161][181] make use of GCCC for the FCL exchange and suffer from all the disadvantages explained in Chapter 2. The other method is to intelligently decide a local control channel (non-GCCC) within the available spectrum holes and advertise this to other nodes. This method which is already used by several proposed protocols [129][179][100][173][118][176], however, lacks a clear methodology of finding the control channel within the white spaces amongst cognitive nodes, especially how the synchronization is established amongst CR nodes, and how nodes are converged on a white space which serves the purpose of a control channel. There is another class of CR MAC protocols [38][178][180][182] that do not delve into common control channel details and simply assume the existence of control channel. It is important to note that no such assumption could be made because finding a control channel is the primary task of a CR MAC protocol and cannot be assumed as it is the fundamental requirement in CR nodes before any subsequent communication can take place. This motivated us to design a CR MAC protocol which is hybrid between GCCC and non-GCCC.

3.2. Design Rationale

It is very important for CR nodes to exchange control information on a control channel which is known and available to all CR nodes in the vicinity. One of the design approaches for the control channel is to use one of the channels in the ISM band, e.g., 2.4GHz. In this case, the control channel would be classified as GCCC because it is globally available. Since the ISM band is freely and widely available, its application as a control channel could be very advantageous as CR nodes can very quickly and effectively transmit the control information on the well-known and always-available control channel. The CR nodes using the GCCC as a control channel will avoid spending time in scanning and sensing for an available control channel. CR nodes only have to contend for the GCCC to transmit the control information. However, the supplementary issues with GCCC cannot be ignored. Two of the main issues associated with using the ISM band as the control channel are: the *saturation problem*; and *security vulnerability*.

The higher the number of applications accessing the ISM band, the higher the computational cost and back-off becomes. The CR nodes holding the control information to transmit on the control channel will have to wait. Also, transmitting the FCL on GCCC will make the CR network more exposed to security threats and vulnerabilities. An adversary can intercept the FCL transaction on the GCCC and could then manipulate the communication.

We have proposed a novel MAC protocol for cognitive radio networks that is a hybrid of GCCC and non-GCCC. The proposed protocol is not only equipped with the best features of the GCCC-based MAC protocols but it also overcomes the saturation problem and certain security issues in GCCC. More details about the proposed protocol are provided in the following sections.

3.3. A Dynamic Decentralized Hybrid Multichannel MAC Protocol

The shortcomings of a GCCC can be avoided by having a dynamic local control channel, i.e., non-GCCC. This has led to our aims to design a *dynamic*, *decentralized*, and *hybrid* medium access control protocol, named DDH-MAC, for overlay ad-hoc cognitive radio wireless ad-hoc networks. The proposed protocol is dynamic because whenever a PU claim happens, CR nodes efficiently agree upon a newly found control channel to maintain the control channel efficiency. The architecture of the protocol is decentralized, not infrastructure-based. DDH-MAC is hybrid in nature, making partial use of both GCCC and non-GCCC families of CR MAC protocols. We have introduced a multi-layer reliability factor and have presented an efficient and robust MAC protocol that emphasizes the control channel efficiency. The CR nodes implementing the proposed mechanism are always in a state where they have access to at least one control channel even after PU interference has been sensed. CR users in the proposed mechanism, without renegotiations, switch to another control channel whenever there is a PU claim. The CR nodes have access to three control channels at the same time. This unique feature smartly and intelligently addresses the problem of the PU channel re-occupancy, and reduces the impact of re-exchange of control information, and leads towards reliable communication in the CRN. We have intelligently avoided shortcomings and have made use of some of the rare advantages of the GCCC for development of our novel CR MAC protocol. Detailed explanation of DDH-MAC is given in the following section.

3.3.1. Design Constraints for DDH-MAC

Design constraints for DDH-MAC include the efficiency of discovering a common control channel, the efficiency of data transmission on a data channel and efficiency of vacating a channel.

a) The Efficiency of Discovering a Common Control Channel

The CR nodes implementing the DDH-MAC protocol require some time to discover a common control channel. Subsequent communication amongst CR nodes will only occur if the CR nodes are aware of a control channel that is available and accessible for all CR nodes to exchange control information amongst the communicating partners. The efficiency of discovering a control channel depends on the selection criteria for the control channel, i.e., GCCC, non-GCCC or assumed. DDH-MAC makes use of both the GCCC and non-GCCC families of CR protocols and uses the GCCC to launch a beacon frame (BF). Making use of both the categories give several advantages to DDH-MAC which other protocols found in the literature cannot have. Launching a BF in GCCC provides the best searching efficiency as GCCC is globally available and is well-known to all CR nodes. No time needs to be spent in discovering a control channel and converging upon a control channel. The BF is broadcast on the GCCC by the first node in DDH-MAC which contains the IDs of the primary control channel (PCCH) and the backup control channel (BCCH). PCCH and BCCH will actually serve the purpose of the control channel in DDH-MAC and control information is exchanged by CR nodes through PCCH or BCCH. The framing structure of PCCH and BCCH is provided in section 3.6.

b) The Efficiency of Transmitting Data

Once the control channel is discovered by all CR nodes in the vicinity, nodes switch to the PCCH and spend less time in exchanging control information and efficiently transmit data on some common white space. Data channel efficiency is defined as the time required for two CR nodes to conclude the transmission on a data channel. In high traffic loads of PUs, the CR users in DDH-MAC can send only one data frame and then vacate the channel. However, when the chances of PU claiming are low and the CR nodes still have data to send, more than one data frame will be transmitted in one transaction. The data channel efficiency in DDH-MAC could also be increased by the length of time a white space would remain unoccupied by the PU.

c) Efficiency of Vacating a Data Channel when PUs Arrive

It is not unusual in cognitive radio networks that a white space is re-claimed by the licensed user. In this case, the CR users must vacate the occupied channel whenever there is PU occupancy to minimize the interference. The majority of the CR MAC protocols found in the literature assume that nodes are aware of the presence of PUs. However, this unrealistic assumption is criticized because CR nodes cannot sense the presence of PUs when transmitting and SUs cannot automatically detect channel occupancy. This SUs' assumption about the awareness of PUs' arrival on a licensed channel is smartly addressed in DDH-MAC. Each CR node in DDH-MAC is equipped with a sensor which detects the PU activity in a timely manner.

3.4. Full Operation of DDH-MAC

In this section we provide in detail the functionality and the operation of DDH-MAC. We first make some assumptions and then describe the DDH-MAC operation with the help of flow chart and timing diagrams.

3.4.1. Assumptions in DDH-MAC Protocol

The protocol makes the following assumptions:

- Each CR node is equipped with two transceivers: G-Transceiver (GT) to continuously and rapidly scan the global control channel, and D-Transceiver (DT) to transmit data [42], [100], [121], [130], [150].
- The CR nodes utilize the CSMA/CA mechanism to access the control channel [71], [118], [121], [173], [181].
- Spectrum has been sensed by the physical layer and the FCL has been populated by each CR node [12], [38], [43], [92], [104], [109], [113–115], [117], [120], [121], [127], [130], [159], [161], [173], [179], [180], [183–197] .
- Each CR node is equipped with a sensor that senses the PU activity on the data channel [38] [198][189].

3.4.2. Levels of selection

DDH-MAC presents a novel design for the cognitive radio MAC protocol which offers two levels of selection.

a) **Level 1**

DDH-MAC makes partial use of GCCC to launch a BF. BF is a control frame containing a small piece of information about sending *node_id*, *PCCH* and *BCCH*. The BF is launched by the first node in the CR network. The BF is a broadcast frame that is received by all CR nodes. Launching the BF in GCCC is the first level of selection and it is used to let other CR nodes in the vicinity know that two local control channels (i.e., PCCH and BCCH) have been established. Primarily the PCCH will be used as a point of contact for all CR nodes and any control information that needs to be exchanged will be transmitted through the PCCH. However, since the PCCH is one of the free channels in the FCL, it is not unusual for a PU to reclaim it. In this case, the CR nodes will simply switch to the BCCH and resume the control information dialogue on the BCCH. The BF is periodically broadcast by the node in the GCCC so that any node that joins or leaves the network has the latest information about PCCH and BCCH.

b) **Level 2**

Once the BF has been received and both PCCH and BCCH have been selected as local control channels, level 2 selection becomes operational where nodes actually start contending for the PCCH to exchange control information. The nodes employ the CSMA/CA mechanism to gain access to the control channel. Multiple frames are exchanged as control information in DDH-MAC of which the detail will be provided in Section 3.6. After the successful exchange of control information, the CR communicating pairs switch to data channels and conclude data transmission. If during the control information dialogue, PU activity has been sensed on both PCCH and BCCH, nodes will eventually switch to GCCC and the level 1 operations will be executed.

3.5. Flow chart

In this section, the full operation of the DDH-MAC is explained with the help of a flow chart drawn in Figure 3.17. At start up, the cognitive nodes are in a steady state and the FCL is already established. Upon initialization, cognitive nodes implementing DDH-MAC use the GT to scan the GCCC for a BF. If the node does not find any BF then the node is responsible for the following three operations:

i) Deciding which white spaces are to be used as PCCH and BCCH

ii) Formation of a BF

iii) Launching the BF in the GCCC.

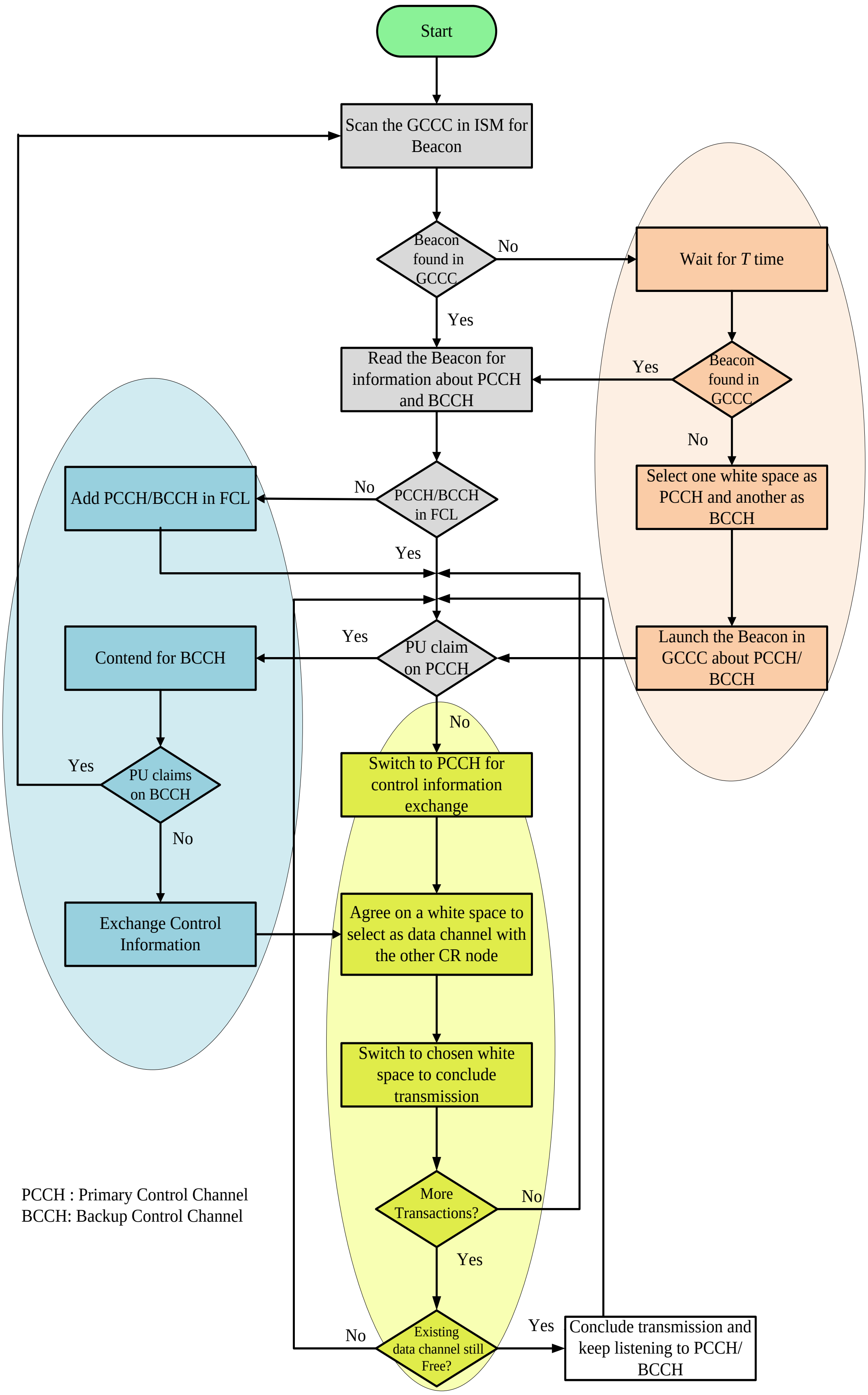


Figure 3.1. Flow chart DDH-MAC.

Any CR node which is going to launch a BF in DDH-MAC must meet the following constraint:

$$\mu > 3 \tag{3.1}$$

where μ is the minimum number of available empty spaces within a CR node. One of the empty spaces will be used as PCCH, another as BCCH, and the last one for the actual data transmission. It is important to note that the BCCH in DDH-MAC protocol is a reserved/secondary control channel and is used only when there is a PU re-claim on the PCCH. Dedicating a white space as BCCH may firstly give an impression of a loss of a white space, but actually it improves the overall network convergence time by simply switching to BCCH if required, and it thus help reduce the computational cost of the protocol and avoids the rescanning of the GCCC which in turn can also help CR nodes conserve energy.

Let N represent a set of cognitive nodes in the network

$$N = \{N_1, N_2, N_3, \dots, N_n\} \tag{3.2a}$$

and C be a set of white spaces within each node

$$C = \{Ch_1, Ch_2, Ch_3, \dots, Ch_m\} \tag{3.2b}$$

then, the FCL which the CR nodes may have can be represented as:

$$\sum_{i=1}^{n} \sum_{j=1}^{m} (N_i, Ch_j) \tag{3.2c}$$

where N_i , Ch_j represents the channel j sensed by node i. The criterion to set one of the channels in the FCL as PCCH or BCCH can be arbitrary or it can satisfy the following equation.

$$P/BCCH \left(\sum_{j=1}^{m} Ch_j\right) = Max_{Ch_{j \in m}} \left\{ fn\ (CHG) \mid \sum_{j=1}^{m} Ch_j \right\} \tag{3.3}$$

where $fn\ (CHG)$ is the function to calculate the channel grade and is defined as:

$$fn\ (CHG) = Max_{AB,\, SNR,\, FER} \{N_iCh_1 + N_iCh_2 + \dots N_iCh_m \mid N_iCh_1 \cap N_iCh_2 \cap \dots N_iCh_m\}_{i=1, 2, \dots, n} \tag{3.4}$$

where AB is the available bandwidth, SNR is the signal-to-noise ratio and FER is the frame error rate. This implies that the Equation 3.4 will be used by a CR node to find the best channel amongst the channels available in its FCL with optimal values for AB, SNR and FER.

Once the node decides about the PCCH and the BCCH, it waits for a time T before launching the BF in the GCCC, where T is the time in micro seconds and is equivalent to the time required by a node to sense at least three white spaces (Equation 3.2). This waiting time of T is there just to avoid doubling of the BF in the GCCC which might be launched by another CR node (see Figure 3.1). If the node finds the BF after scanning the GCCC, it reads the information about PCCH and BCCH, update its FCL and switches to the PCCH for exchange of subsequent control information. Otherwise, it considers itself as the starting node and launches the BF in the GCCC. More discussion on the waiting time which will be called the Pre-Transmission time, denoted as T_{PT} , is given in the Section 3.9.1.

During the initial scanning, if the BF is successfully found by a CR node in the GCCC, it decrypts the information using the relevant decryption scheme to learn about the chosen PCCH and BCCH. Once equipped with this information, the node accordingly updates its FCL by setting the PCCH and BCCH for control information exchange and the rest of the white spaces as data channels for the subsequent data transmission. In addition to the flow chart shown in Figure 3.1 which provides a complete operation of DDH-MAC, the process of BF launch/scanning and the later FCL update by other CR nodes are shown in Figure 3.2. The communicating CR nodes always verify the re-claim of PCCH by the PU before they actually switch to it for further exchange of the FCL. After a successful exchange of the FCL on the chosen PCCH, the CR nodes eventually switch to the agreed empty space to be used as a data channel for the actual data transmission. The CR nodes may come up with a case when there is a re-claim by PU(s) on both PCCH and BCCH; and in this case the nodes have to go to the initial state where they scan the GCCC for a new BF.

Figure 3.1 provides the framework for the DDH-MAC protocol in the form of a flow chart; and Figure 3.2 explains the scenario where three CR nodes are continuously sensing the GCCC for a BF. When the CR nodes find a BF, they read the information about PCCH and BCCH, update their FCL and switch to the newly set-up PCCH for the exchange of control information in the form of RTS and CTS packets with other cooperative communicating nodes. A BCCH has also been reserved to back up cognitive functions because it is not unusual for a PU to interfere on the PCCH.

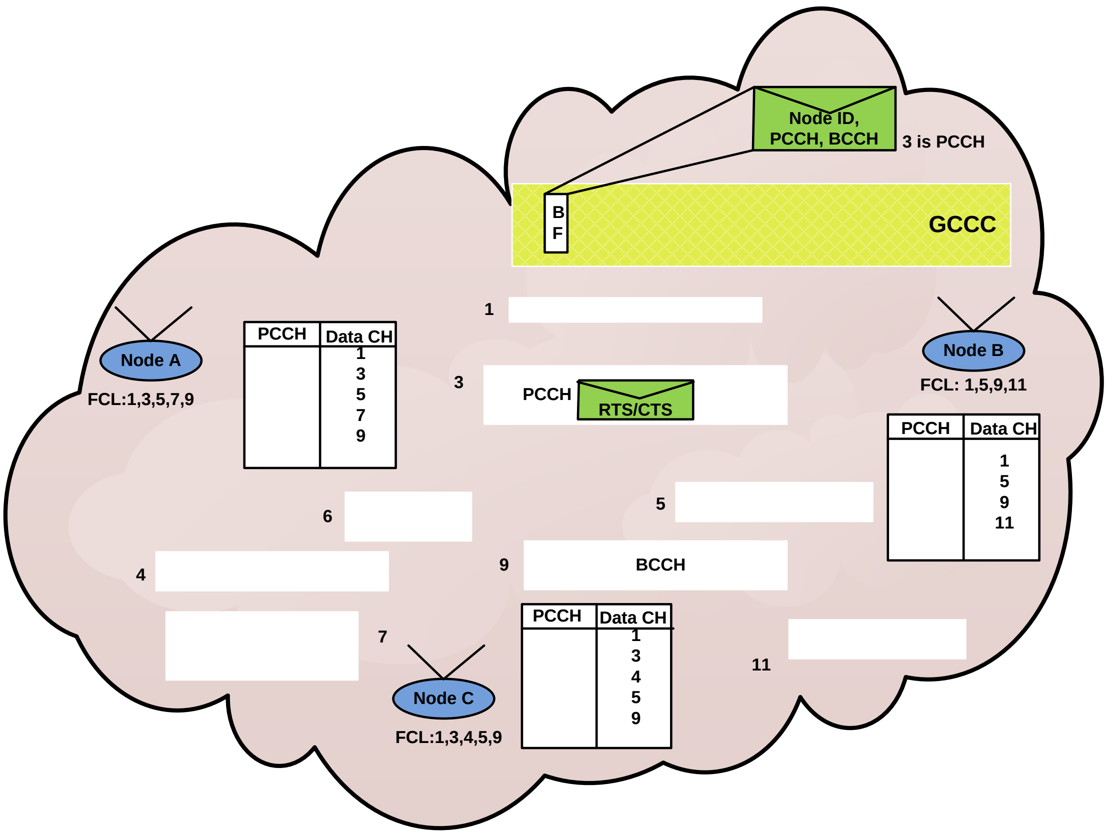


Figure 3.2. The CR nodes in DDH-MAC, receiving the BF in GCCC and switching to PCCH for the subsequent control information dialogue.

In the previous section, the operation of DDH-MAC has been discussed in detail. The next section describes the very important aspect of cognitive radio network, the time CR nodes take to exchange control information, agree on a set of communication rules and start data transmission. This time will be called pre-transmission time and will be denoted as $T_{PT.}$

3.6. Control Frames in DDH-MAC Protocol

Like other CR MAC protocols, DDH-MAC also exchanges control information on the control channel. Four control messages are exchanged in DDH-MAC. One control message (of the BF) is delivered through GCCC.

3.6.1. BF

The BF is launched in the GCCC as a management frame by the first node in the CRN to inform all the other CR nodes about the PCCH and the BCCH. Both PCCH and BCCH use one of the white spaces as a local control channel. Since DDH-MAC will use one of the white spaces as a control channel, it is a non-GCCC. Two parameters are carried in each BF: channel ID of the PCCH and channel ID of the BCCH. Channel IDs are arbitrarily selected by the first CR node, and they refer to the first two channels that the CR node has sensed. The channel ID is a non-negative number,

$$\text{where } 0 \preccurlyeq \text{Channel ID} \prec N$$

The BF is the first frame which is launched by the first node in the DDH-MAC protocol and it gives the primary information about the control channels which will be used in the subsequent exchange of control frames. The BF structure has been derived from IEEE 802.11b. Figure 3.3 shows the structure of a BF.

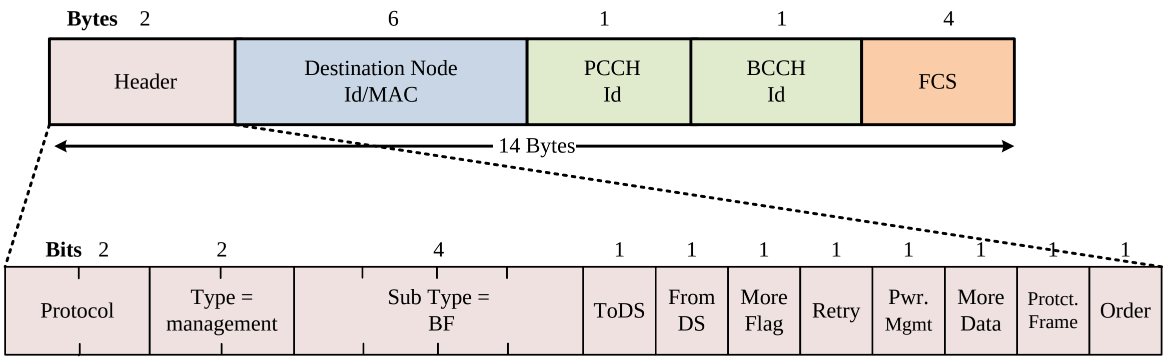


Figure 3.3. The BF in DDH-MAC.

Protocol version

The protocol version is shown as 0 in Figure 3.3 because that is currently the only version. Other versions may exist in the future.

Type

Control frames are assigned the Type Identifier 01. By definition, all control frames use this identifier.

Subtype

This field indicates the subtype of the control frame that is being transmitted.

ToDS and FromDS

Control frames arbitrate access to the wireless medium and thus can only originate from wireless stations. The distribution system does not send or receive control frames, so these bits are always 0.

More Fragments

Control frames are not fragmented in DDH-MAC, so this bit is always set to 0.

Retry

Control frames are not queued for retransmission like management or data frames, so this bit is always 0.

Power Management

This bit is set to indicate the power management state of the sender after conclusion of the current frame exchange.

More Data

The More Data bit is used only in management and data frames, so this bit is set to 0 in control frames.

Protected Frame

Control frames may not be encrypted. Thus, for control frames, the Protected Frame bit is mostly set to 0.

Order

Control frames are used as components of atomic frame exchange operations in DDH-MAC and thus cannot be transmitted out of order. Therefore, this bit is set to 0.

Control frames assist in the delivery of data frames. They administer the access to the wireless medium (but not the medium itself) and provide MAC-layer reliability functions. The local control channel (PCCH or BCCH) delivers three types of control frames: DMCF, FCL, and ACK.

3.6.2. DDH-MAC Control Frame (DMCF)

DMCF is one of the control frames broadcast by a potential CR sender to inform all the CR nodes in the vicinity that it is ready for communication. DMCF acts like a classical RTS frame in wireless networks and which is used by all decentralized CR MAC protocols. DMCF serves two purposes. Initially, it lets the CR nodes know that it is ready for any communication, and secondly, it indicates that the medium has been occupied and the DMCF is followed by another frame, i.e. FCL. The FCL will contain a list of free channels that are available to communicate over. Like other control frames, DMCF is used to gain control of the medium for the transmission. Access to the medium can be reserved only for unicast frames, and broadcast and multicast frames are simply transmitted without reservation. The format of the DMCF frame is shown in Figure 3.4.

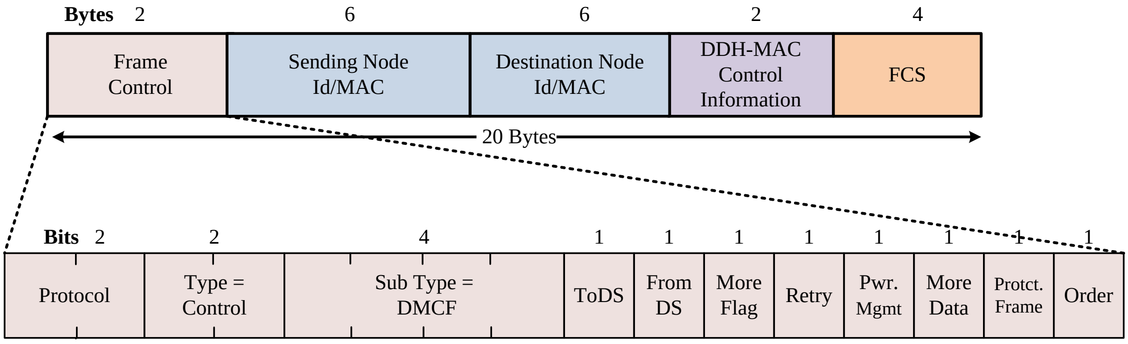


Figure 3.4. DMCF (DDH-MAC Control Frame).

Frame Control

There are two fields that make a header of a DMCF frame different from that of a BF *frame type* and *frame subtype*. The frame type indicates that it is a control frame and the frame subtype is set to 1011 to indicate a DMCF frame. Otherwise, it has all the same fields as fields in a BF frame.

Sending Node Id

The 48-bit (6 bytes) MAC address of the device that is transmitting the DMCF.

Destination Node Id

The MAC address of the station that is the intended recipient of the DMCF. Usually, it is the broadcast address of FF:FF:FF:FF:FF:FF.

DDH-MAC Control Information (DMCI)

This field is specific to the DMCF. It contains the supplementary information about the time that would be required to complete the process of transmitting the DMCF followed by a FCL frame. The sender of the DMCF frame calculates the time needed for the frame exchange sequence after the DMCF frame ends. The entire exchange, which is depicted in Figure 3.5, requires two SIFS periods, the duration of one FCL. Note that the final ACK, plus the time needed to transmit the frame or the first fragment. Fragmentation bursts use subsequent fragments to update the Duration field. The number of microseconds required for the transmission is calculated and placed in the DMCI field. If the result is fractional, it is rounded up to the next microsecond.

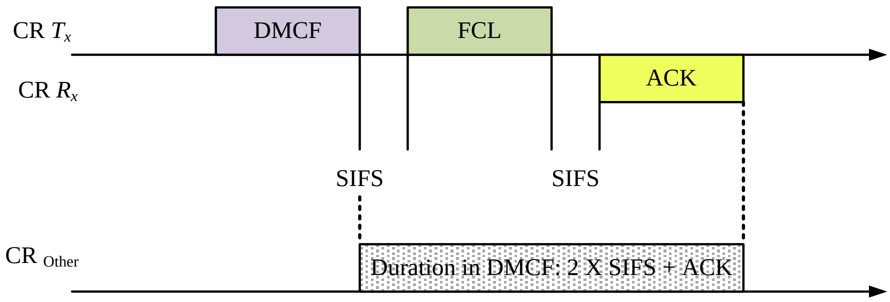


Figure 3.5. Duration in DMCI.

3.6.3. Free Channel List (FCL)

The FCL is another control frame utilized by the same CR sender which recently broadcasted the DMCF. The FCL includes the channel ID of all channels that could possibly be used as data channels for subsequent transmission. The FCL is always sent in conjunction with the DMCF and cannot be sent individually. The FCL also serves the purpose of letting CR nodes be aware that the node which launched the DMCF will be transmitting the FCL, and finishing the transmission of the FCL, it will have no more frames to transmit over the control channel and will be releasing the medium, and lastly, will expect an ACK frame from the CR node which is interested in establishing the communication over the data channel. The pair of DMCF and FCL are also used to avoid the traditional hidden terminal problem in wireless networks. The framing structure for the FCL is provided in Figure 3.6.

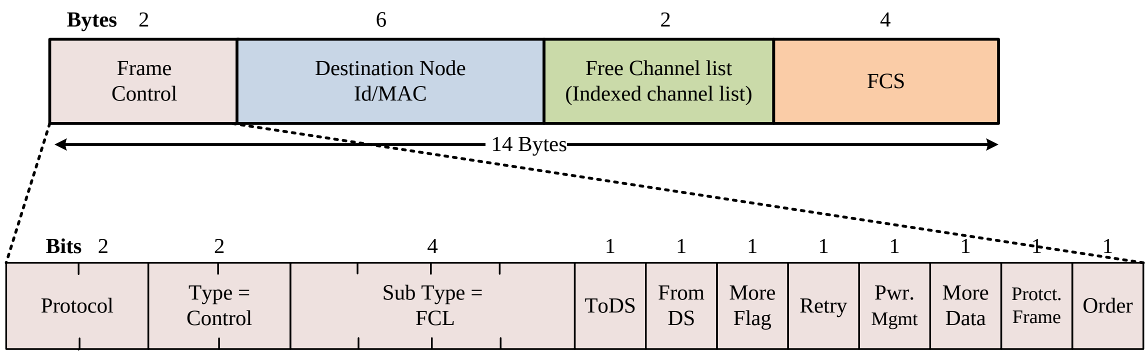


Figure 3.6. Frame structure of an FCL frame.

Frame Control

There is nothing special about the Frame Control field of the FCL. The frame subtype is set to 1100 to indicate an FCL frame, but otherwise, it has all the same fields as other control frames.

Destination Node Id

The FCL is also a broadcast frame. The Destination Node Id will be the broadcast MAC address which will be received by all CR nodes in the vicinity.

Free Channel List

The values in this field are subject to the information provided by the physical layer which senses the spectrum, indexes the channels list and assigns a numeric value to each channel that is sensed empty.

3.6.4. ACK Frame

The ACK frame is utilized by a CR receiver who wins the contention on the PCCH. The receiver replies with its own FCL identifying the channels common between the CR pair for possible data transmission. ACK is used to answer DMCF and FCL frames, and it will never be generated without the preceding DMCF and FCL. The ACK frame format is shown in Figure 3.7. The moment a DMCF is received (Figure 3.5), the nodes set their network allocation vector (NAV) for the duration of the handshake process, and will not attempt to access the PCCH until the end of NAV. The three-way handshake over the PCCH/BCCH in DDH-MAC efficiently avoids the hidden terminal problem in a multi-channel environment. The MAC addresses of the sender and the receiver and their FCLs help avoid any collisions amongst the CR nodes because the nodes which are listening to the PCCH/BCCH learn that the sender will become busy in data transmission. The FCL of the transmitting node is also included in the acknowledgement field of an ACK frame which is overheard by all CR nodes.

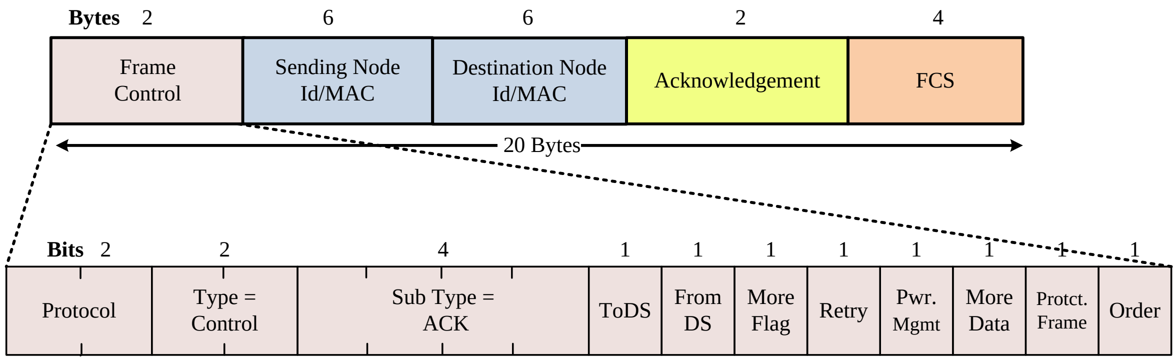


Figure 3.7. Frame structure of an ACK frame.

Frame Control

The frame type is set to control and the subtype is set to 1100 to indicate an ACK frame, and the rest of the fields are similar to the frame control of DMCF and FCL.

Sending Node Id

This is the MAC address of the node which is transmitting the ACK frame.

Destination Node Id

The receiver of a FCL frame is the transmitter of the previous DMCF and FCL frames, so the node which is transmitting the ACK frame copies the Sending Node Id of the DMCF frame into the Destination Node Id of the ACK frame.

3.7. Phase I and Phase II operations

The most important aspect of cognitive radio (CR) network is to search, scan, and access the control channel to advertise the FCL amongst the participating CR nodes. Subsequent communication could not take place until there is an access to a well-known and agreed upon control channel to dialogue the initial configuration. Our proposed DDH-MAC protocol searches, scans, and accesses the control channel in a very efficient and intelligent way. The protocol performs two-phase (Phase I and Phase II) operations, i.e., rapid channel accessing and reliable channel accessing respectively. In rapid channel accessing, nodes quickly and efficiently converge to a newly found control channel. In reliable channel accessing, switching to the backup control channel is performed when necessary. Furthermore, our reliable channel accessing allows CR nodes to access more than one control channel simultaneously.

3.7.1. Phase 1 Operation: Rapid Channel Accessing

When a CR node wants to transmit data, it first scans the GCCC for a BF. There are two possibilities:

1- If any BF is found (Fig. 3.8②), the information about PCCH and BCCH is learnt. This also means that the node has to join an existing CRN and now the PCCH needs to be scanned to learn more about the network.

2- If the CR sender does not find any BF in the GCCC, then this node becomes the first CR node in the CRN and is responsible for three functions: setting one of the white spaces in its FCL as the PCCH and another as the BCCH; forming and launching the BF in the GCCC (Fig. 3.8①); and continuing to transmit copies of the BF at regular intervals (Fig. 3.8③). To make the model traceable we consider that it is not possible for two DDH-MAC nodes to attempt to launch BF at the same time.

In both cases, the CR node starts scanning the PCCH and observes the activities on the local control channel (Fig. 3.8④). The CR sender and the CR receiver then exchange three control information frames through the PCCH. Firstly, DMCF is launched (Fig. 3.8⑤), followed by the transmission of the FCL (Fig. 3.8⑥). DMCF and ACK also serve to avoid the hidden terminal problem which is traditional in ad-hoc networks. The intended recipient checks its FCL to see if a common channel exists. If a common channel is found, a reply with an ACK is sent to the sender (Fig. 3.8⑦). The pair then switch to the identified common data channel and start transmitting data using DT (Fig. 3.8⑧). All the data frames are acknowledged using the data ACK (Fig. 3.8⑨). Other nodes will wait for the PCCH to become idle and will contend to dialogue the control information after it is sensed free. The GT will be used by all the CR nodes in the network to scan the local control channel to have knowledge about all the activities carried out by other CR nodes in the network.

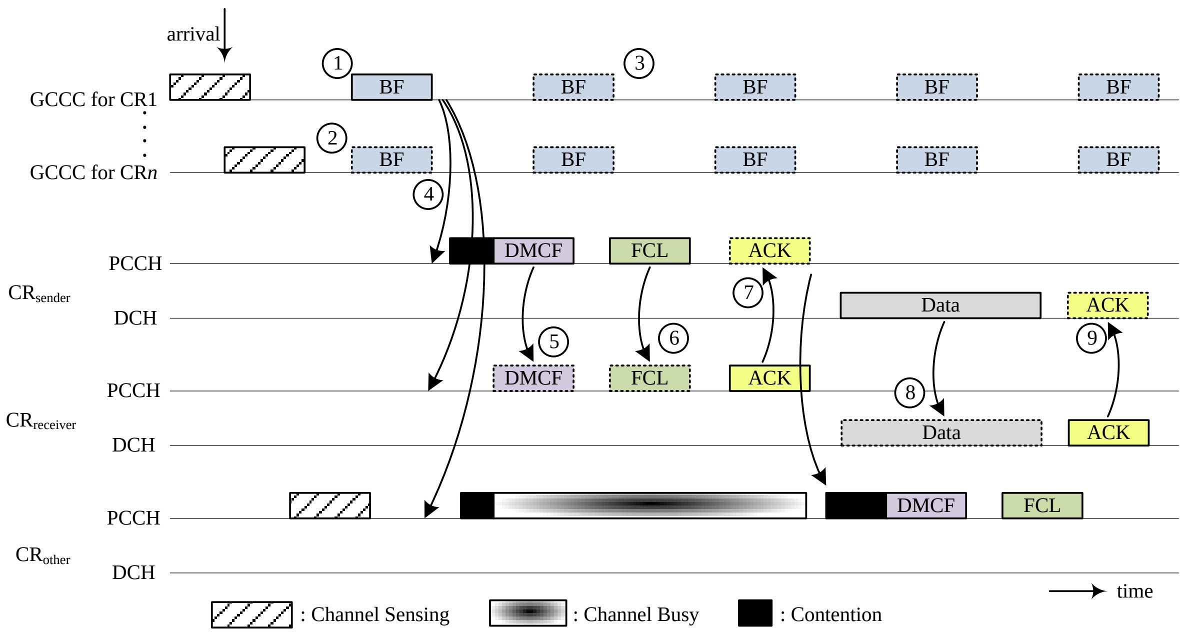


Figure 3.8. An example of Phase I operations.

The CR pair which just finished communication could remain unaware of the status of other CR nodes, and thus continuously scanning the control channel helps track the record of the activities of other CR nodes. This ultimately avoids the hidden terminal problem. In rapid channel accessing, nodes can access the control channel efficiently

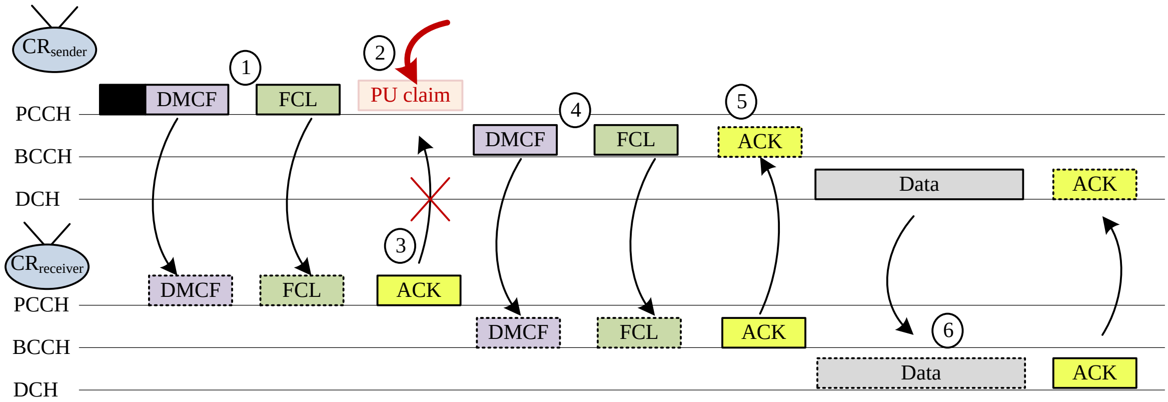


Figure 3.9. An example of Phase II operations.

and rapidly. Any new node joining the network first searches for a BF which could be read for information about the local control channel(s). After this, nodes simply switch to the newly discovered control channel for the most crucial part of communication, i.e., the FCL transactions, which lead to the transmission of data frames.

3.7.2. Phase II Operation: Reliable Channel Accessing

Both the PCCH and the BCCH make use of the most readily available white spaces scanned and setup by a CR user. Unlike when using the GCCC, which is publically available to everyone and thus more prone to security vulnerabilities, the FCL could be exchanged privately and secretly amongst CR nodes through the PCCH after the nodes in the vicinity have converged on this local control channel. Since a PU can claim any occupied channel at any moment of time, the PCCH could also be claimed, and as a result, nodes using the PCCH for exchange of control information would have to either abort the configuration dialogue or renegotiate on other white spaces. The proposed mechanism efficiently deals with this situation by using the BCCH to resume the exchange of control information, if there is a PU claim on the PCCH. Figure 3.9 illustrates an example of Phase 2 operations where the CR sender is transmitting the control information on the PCCH (see Fig. 3.9①) and is awaiting ACK from the recipient. Meanwhile, a PU claim is sensed on the PCCH (see Fig. 3.9②) due to which the ACK could not be delivered (Fig. 3.9③). The CR nodes can switch to the BCCH without re-negotiations and re-searching a control channel, and thus can resume transceiving the control information (see Fig. 3.9④⑤), followed by the data transmission on an agreed data channel (see fig. 3.9⑥). In the worst-case scenario, if the

BCCH is also claimed by the PU, then the CRN will execute operations of Phase 1 and will converge on a new PCCH and a new BCCH. This dynamicity of local control channels provides the nodes an extra security feature. An adversary, planning to attack the PCCH or the BCCH and manipulating the information on the control channel, has to re-compile the attack every time when a new PCCH and a new BCCH are set up. More discussion on security aspects of DDH-MAC is provided in Chapter 6. The reliable channel access gives the CR nodes the assurance that they always have access to three control channels simultaneously and any of these three control channels could be used for subsequent exchange of control information.

3.8. Four Case Scenarios in the Proposed Protocol

In this section, we first discuss different case scenarios and then model the process of rapid channel access and reliable channel access, and finally calculate the time it takes for exchange of the control information. DDH-MAC needs to perform a few operations before the network becomes fully converged. These operations include scanning/sensing the GCCC, exchanging the FCL on PCCH or BCCH (if there is a PU claim on the PCCH), and lastly concluding transmission on the agreed white space(s). Each of the above listed operations requires time for its completion such as the time required to sense/scan a BF in the GCCC, the time required to launch the BF, the time to read BF and the time required to exchange the FCL on PCCH or BCCH. All these operations form part of the pre-transmission time which heavily affects the throughput and the QoS as nodes holding delay-sensitive data will be highly affected through varied values of the pre-transmission time. Let T_X denote the time required for operation X, for one of the above-mentioned operations and $T_{PT}^{DDH-MAC}$ represent the pre-transmission time which is further expressed in Equation 3.5.

$$T_{PT}^{DDH-MAC} = \{ T_{BS}, T_{BF}, T_3, T_{FCL}^{PCCH} T_{FCL}^{BCCH}, T_{DMCF}, T_{ACK} \} \quad (3.5)$$

where T_{BS} is the time required to scan the GCCC for BF, T_{BF} is the time to read the BF or launch the BF in the GCCC, T_3 is the waiting time before a CR node can launch the BF. T_{FCL}^{PCCH} and T_{FCL}^{BCCH} are the amount of time a CR node takes to broadcast its FCL in PCCH or BCCH if there is a PU re-claim. T_{DMCF} and T_{ACK} are control frames similar to RTS/CTS and are used to avoid the traditional hidden terminal problem. They are exchanged between communicating nodes before actual transmission can take place.

Not all the operations are performed by cognitive nodes in DDH-MAC, and the number of operations performed depends on the role of a CR node and the case scenario. There are 4 cases in DDH-MAC.

3.8.1. CASE I: Network Initialization and Launch of a BF

Case I represents the network initialization phase where no control channels have been found and the CR nodes scan the GCCC to search any BF. If a BF is not found then any node which takes the initiative becomes responsible for the following four operations:

i) To decide which white spaces to be used as PCCH and BCCH from the list of channels available in its own FCL.

ii) To create a BF containing the information about the chosen PCCH and BCCH.

iii) To launch the BF in the GCCC.

iv) To transmit copies of BF periodically.

Figure 3.10 presents the first case in DDH-MAC where all the CR nodes initially scan the GCCC using their GT for any BF. Here we consider the scenario where no BF is found and the BF is launched by a node. All the CR nodes, continuously listening to the GCCC, are programmed to receive this BF because the destination address in the MAC header of a BF is a broadcast address. The nodes learn the information about the selected PCCH and BCCH and then switch to the PCCH for subsequent control information exchange.

After switching to the PCCH, nodes use both of their transceivers, i.e., GT and DT. Initially, the GT is used to scan the control channel and to contend to exchange the DMCF followed by the FCL. However, once the control information is exchanged, the node starts using its DT for possible data communication. The GT always keeps scanning the control channel, and in this way, if a CR node is busy in data transmission, all activities are observed and noticed using the GT. So, the probability for hidden terminal collision is efficiently reduced.

We have calculated the pre-transmission (T_{PT}) time for all scenarios in DDH-MAC. The T_{PT}, for this scenario case, is given by

$$T_{PT1}^{DDH-MAC} = \{ T_{BS} + T_3 + T_{BF} + T_{DMCF} + T_{FCL}^{PCCH} + T_{ACK} \} \qquad (3.6)$$

where T_{BS} is time required to scan the GCCC for the BF; T_3 is the waiting time to avoid duplication of the BF by different CR nodes in the same network; and T_{DMCF}, T_{FCL} and T_{ACK} are the time required to transmit the corresponding control frame. Accurate values using IEEE 802.11b as a bench mark have been derived and are shown in Table 3.1.

Table 3.1 The Parameters for the Proposed DDH-MAC Protocol

Parameter	Assigned Value
BF	14Byte
DMCF	20Byte
FCL	20Byte
ACK	14Byte
T_{BS}	10.181µs
T_{BF}	10.181µs
T_{DMCF}	14.545µs
T_{FCL}^{PCCH}	14.545µs
T_{FCL}^{BCCH}	14.545µs
T_3	30.543µs
T_{ACK}	10.181µs
DIFS	50µs
SIFS	20µs

3.8.2. Case II: Receiving the BF

The second DDH-MAC case considers a scenario where the network has already been initialized and both PCCH and BCCH have been established. In this case, the CR nodes will simply receive the BF and switch to the PCCH for possible exchange of control information. The number of operations performed in Case II in DDH-MAC has been derived as Equation 3.7 and is presented in Figure 3.11

$$T_{PT2}^{DDH-MAC} = \{T_{BF} + T_{DMCF} + T_{FCL}^{PCCH} + T_{ACK}\} \quad (3.7)$$

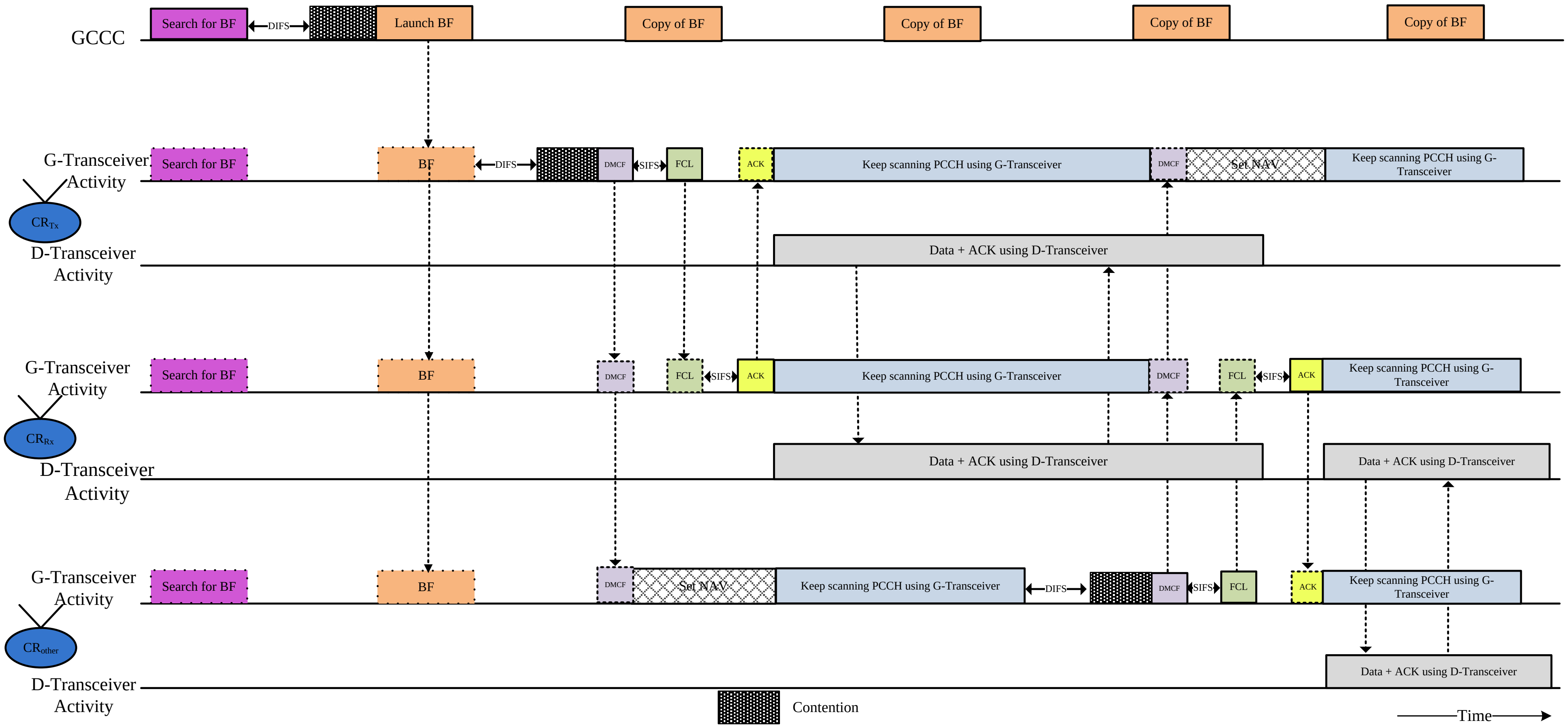


Figure 3.10. Case I of DDH-MAC: Network initialization phase with launch of a BF.

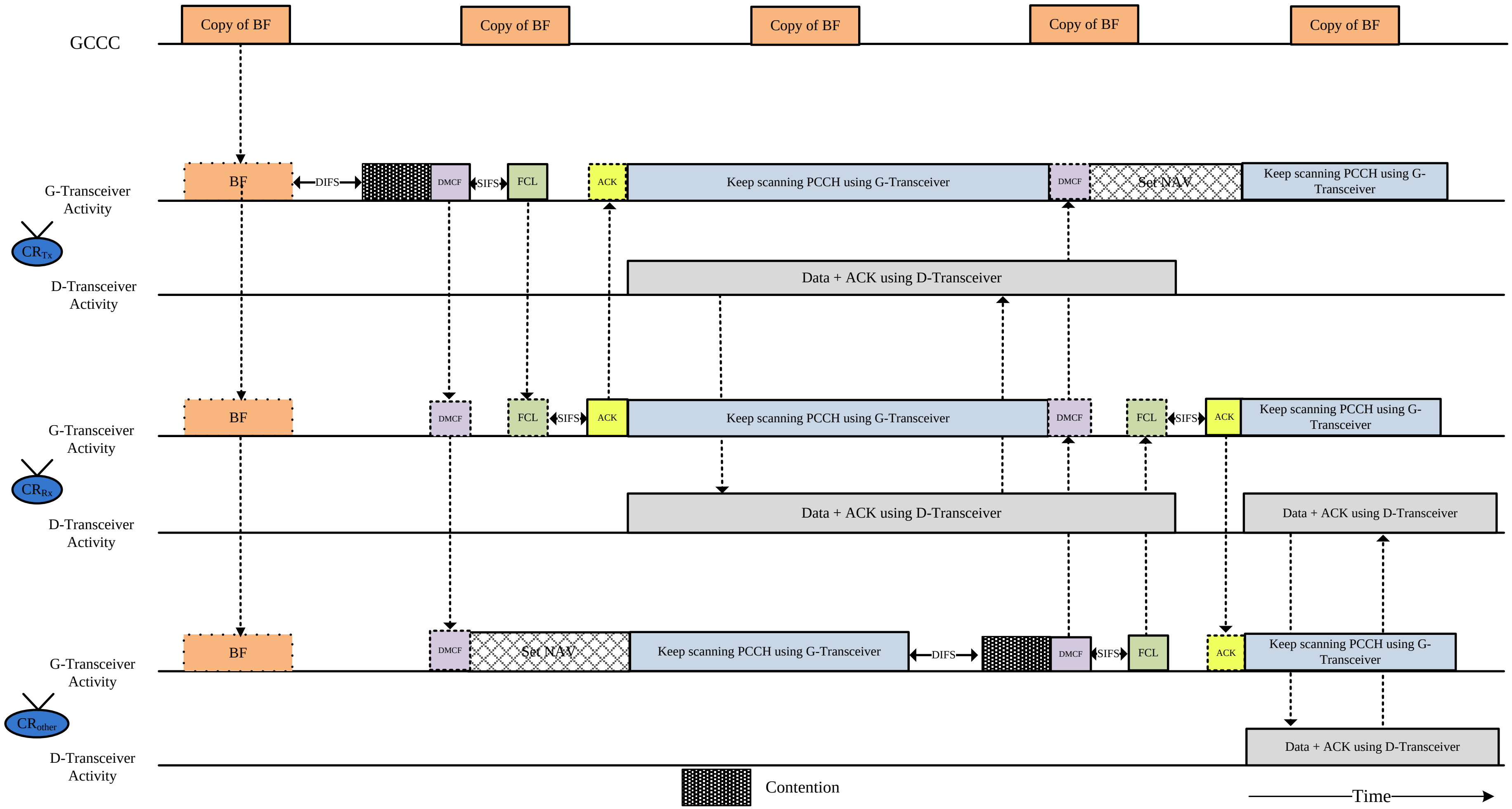


Figure 3.11. Case II of DDH-MAC. After network initialization; the CR nodes receive the BF and then switch to the PCCH for control information.

3.8.3. Case III: Network Initialization, Launch of a BF and Claim on the PCCH

The cognitive radio technology deals with the usage of licensed spectrum when it is not used by a PU with a condition that the spectrum band would be released if the PU claims its channel. In case III of DDH-MAC, we represent the PU occupancy on the PCCH. Usually, the nodes have to search again for some common control channel if one is occupied, but in DDH-MAC, the BCCH is used to resume any control information exchange.

In case III, besides the network initialization phase, we further consider the PU occupancy on the PCCH. Nodes in DDH-MAC are prepared to deal with this situation simply switching to the BCCH and resuming the exchange of control information. Figure 3.12 presents the timing diagram where the first node executes four operations and launches the BF in the GCCC. Other nodes learn the information about the PCCH and the BCCH through the BF and start scanning the PCCH. Consequently, if there is a PU claim on the PCCH then the nodes switch to the BCCH and resume the exchange of control information in BCCH. The operations performed in this case are included in Equation 3.8 and presented in Figure 3.12.

$$T_{PT3}^{DDH-MAC} = \{T_{BS} + T_3 + T_{BF} + T_{DMCF} + T_{FCL}^{PCCH} + T_{ACK} + T_{DMCF} + T_{FCL}^{BCCH} + T_{ACK}\} \quad (3.8)$$

3.8.4. Case IV: Receiving the BF and Claim on the PCCH

This case is an extended version of Case III in DDH-MAC where the PU interference on a local control channel (PCCH) is considered after the network was already initialized. As described earlier, the usual response of CR MAC protocols in this case is to abort transmission, and search and scan another control channel where the control information dialogue could be re-imitated. However, in the proposed scheme, nodes have already had a backup control channel in case the PCCH needs to be vacated. The set of operations performed in Case IV of DDH-MAC are expressed in Equation 3.9 below and the timing diagram is presented in Figure 3.13.

$$T_{PT4}^{DDH-MAC} = \{T_{BF} + T_{DMCF} + T_{FCL}^{PCCH} + T_{ACK} + T_{DMCF} + T_{FCL}^{BCCH} + T_{ACK}\} \quad (3.9)$$

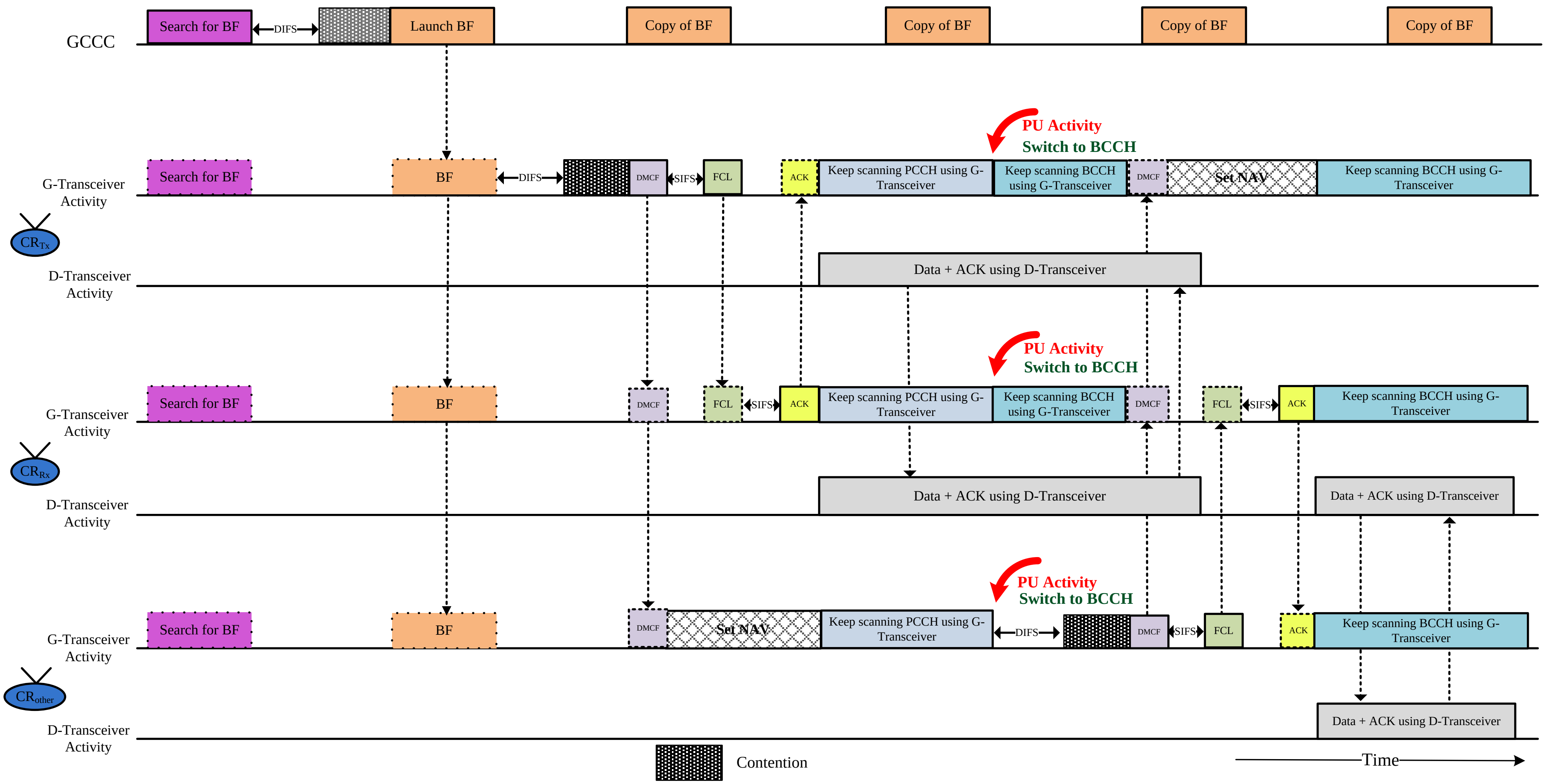


Figure 3.12. Case III Network initialization phase, launch of the BF and the PU claim on the PCCH.

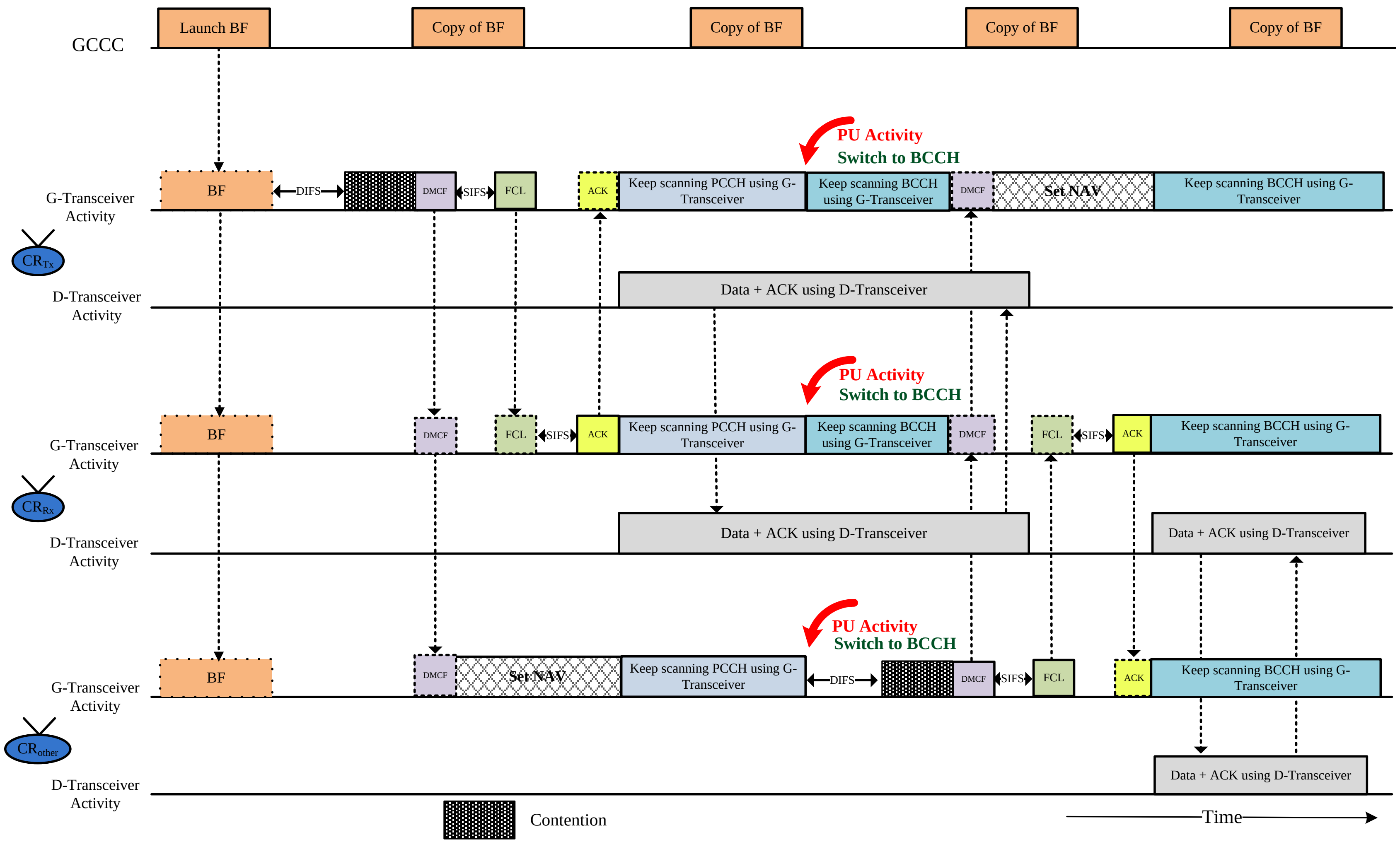


Figure 3.13. Case IV Network initialized, PU Interference on PCCH, and switching to BCCH.

3.9. DDH-MAC Key Performance Indicator

A cognitive radio network is an opportunistic network. Timely coordination amongst the CR nodes is very important to utilize the unoccupied spectrum before there is a PU claim. The CR nodes must exchange control information over the control channel which is a pre-requisite for any subsequent data transmission to occur. However, sometimes the CR nodes take longer in dialogue the control information, and the rare opportunity to transmit may be missed. The time spent over the exchange of control information heavily contributes towards the higher throughput of a CR MAC protocol. We call this amount of time the pre-transmission time (T_{PT}). In this section, we calculate and compute T_{PT} for different cases of DDH-MAC and will compare this time with other CR MAC protocols.

3.9.1. Pre-Transmission Time

Using Equations 3.6 – Equation 3.9, the pre-transmission time for Cases I to IV of DDH-MAC has been computed. We have used IEEE 802.11b [199][200] as a benchmark to calculate values for T_{PT} . For simplicity, we have considered a static size for the contention window, and assume that the channel conditions have been set to ideal. The DIFS and SIFS values are constant for every protocol following the IEEE 802.11b standard i.e., 50µs and 20µs respectively. A total of 124 Bytes, 68 Bytes, 178 Bytes and 122 Bytes are exchanged in Cases I to IV of the proposed protocol respectively which feed the values of T_{PT} in Table 3.2.

3.9.2. Comparison of Pre-Transmission Times

The network convergence in a cognitive radio network is of significant importance as CR nodes holding delay-sensitive data have to quickly start transmission. Fast network convergence is only possible if nodes can access the control channel and quickly exchange the control information. We believe that the pre-transmission time is an overhead, and that CR MAC protocols should be designed in a way to minimize this time as much as possible. Unfortunately, this parameter in a CR network has been largely neglected. The proposed protocol has been designed by aiming to lower the values of pre-transmission time. The pre-transmission time could be efficiently reduced by: i) rapid channel accessing; ii) reliable channel accessing; and iii) reducing the number and size of control frames.

Table 3.2 Pre-Transmission Time for Different Cases in DDH-MAC

DDH-MAC Case I		DDH-MAC Case II		DDH-MAC Case II		DDH-MAC Case II	
T_{BS}	14 Bytes 10.181µs	T_{BS}	14 Bytes 10.181µs	T_{BS}	14Bytes 10.181µs	T_{BS}	14Bytes 10.181µs
T_3	Time length of 3 BF 30.543µs	T_{DMCF}	20 Bytes 14.545µs	T_3	Time length of 3 BF 30.543µs	T_{DMCF}	20Bytes 14.545µs
T_{BF}	14 Bytes 10.181µs	T_{FCL}^{PCCH}	14 Bytes 10.181µs	T_{BF}	14Bytes 10.181µs	T_{FCL}^{PCCH}	14Bytes 10.181µs
T_{DMCF}	20 Bytes 14.545µs	T_{ACK}	20 Bytes 14.545µs	T_{DMCF}	20Bytes 14.545µs	T_{ACK}	20Bytes 14.545µs
T_{FCL}^{PCCH}	14 Bytes 10.181µs			T_{FCL}^{PCCH}	14Bytes 10.181µs	T_{DMCF}	20Bytes 14.545µs
T_{ACK}	20 Bytes 14.545µs			T_{ACK}	20Bytes 14.545µs	T_{FCL}^{BCCH}	14Bytes 10.181µs
				T_{DMCF}	20Bytes 14.545µs	T_{ACK}	20Bytes 14.545µs
				T_{FCL}^{BCCH}	14Bytes 10.181µs		
				T_{ACK}	20Bytes 14.545µs		
$T_{PT1}^{DDH-MAC}$	124 Bytes **90.178µs**	$T_{PT2}^{DDH-MAC}$	68 Bytes **49.454µs**	$T_{PT3}^{DDH-MAC}$	178Bytes **129.447µs**	$T_{PT4}^{DDH-MAC}$	122Bytes **88.727µs**

a) Comparison of Pre-Transmission Time for DDH-MAC in Case I

For the performance evaluation of the proposed DDH-MAC protocol, we have calculated and then compared the pre-transmission time for different CR MAC protocols [38][127][101]. The reasons for selecting these MAC protocols for our comparison are that these protocols are highly cited, that they are the newest CR MAC protocols, and that their design architecture matches the design of our proposed DDH-MAC protocol. Each protocol exchanges specific control information prior to the data transmission. The classical RTS/CTS, FCL and ACK are mostly exchanged by all CR MAC protocols. A few other frames specific to each protocol are also exchanged as control information. For example, CREAM-MAC exchanges four types of packets, namely RTS, CTS, Channel-State-Transmitter (CST) and Channel-State-Receiver (CSR). OC-MAC uses the typical exchange of RTS/CTS, followed by Control-Channel-Request-to-Send (CRTS) and ACK. The four control frames exchanged in A-MAC are indexed-channel-list (ICL), indexed-common-channel-list (ICCL), channel-reservation-control-packet (CRCP) and CRCP-ACK. We first compare the pre-transmission time with the help of timing diagrams (Figure 3.14), then we compute the values for each of the operations performed by these MAC protocols and lastly, we present the results obtained based on our calculations (Table 3.3).

Table 3.3 Pre-Transmission Time Comparison of DDH-MAC for Scenario Case I

DDH-MAC	**CREAM-MAC**	**OC-MAC**	**A-MAC**
T_{BS} 14Bytes 10.181μs	T_{RTS} 20Bytes 14.545μs	T_{BS} : 14Bytes 10.181μs	T_{BS} : 14Bytes 10.181μs
T_{3} time length of 3 BF 30.543μs	T_{CTS} 20Bytes 14.545μs	T_{RTS} : 20Bytes 14.545μs	T_{ICL} : 20Bytes 14.545μs
T_{BF} 14Bytes 10.181μs	T_{CST} 20Bytes 14.545μs	T_{CTS} : 14Bytes 10.181μs	T_{ICCL} : 20Bytes 14.545μs
T_{DMCF} 20Bytes 14.545μs	T_{CSR} 20Bytes 14.545μs	T_{CRTS} : 20ByBytes 14.545μs	T_{CRCP} : 20Bytes 14.545μs
T_{FCL}^{PCCH} 14Bytes 10.181μs		T_{ACK} : 14Bytes 10.181μs	T_{ACK} :14Bytes 10.181μs
T_{ACK} 20Bytes 14.545μs			
$T_{PT1}^{DDH-MAC}$ 124Bytes= 90.178μs	T_{PT1}^{CREAM} 80Bytes=58.18μs	T_{PT1}^{OC-MAC} 82Bytes=59.633μs	T_{PT1}^{A-MAC} 88Bytes=63.997μs

Figure 3.14 below presents the timing structure of the DDH-MAC protocol and compares the behaviour of different CR MAC protocols when the network is initialized.

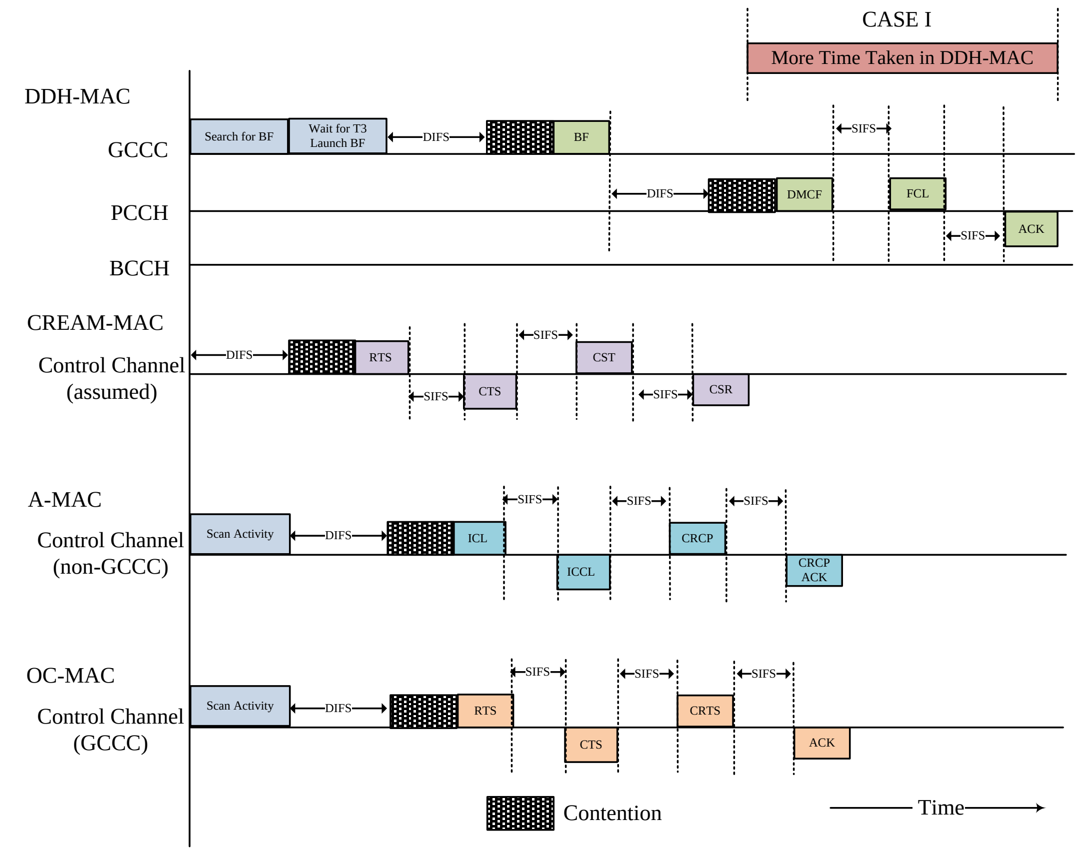


Figure 3.14. Case I- timing diagram comparison with other MAC protocols.

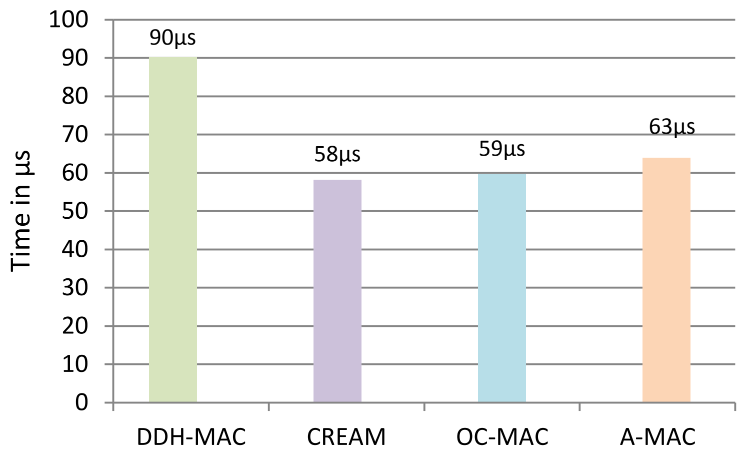


Figure 3.15. Comparison of pre-transmission values for DDH-MAC Case I.

T_{PT} has been calculated for other CR MAC protocols for performance comparison and evaluation. Figure 3.15 shows the T_{PT} in Case I. In this case DDH-MAC protocol has the worst rapid channel accessing. The obvious reason for the high value of T_{PT} is because the network is in the initialization phase and the first CR node has to wait for certain amount of to time to avoid the BF duplication. Since other protocols do not wait to launch a BF and the network is initialized through the scanning activity (or under the assumption of the existence of available control channel) followed by exchange of control frames, T_{PT} is smaller for other protocols in Case I.

b) Comparison of Pre-Transmission Time for DDH-MAC in Case II

Here, we consider the state of a cognitive radio network where a control channel has already been established and CR nodes only have to learn the information about PCCH and BCCH through the BF. The CR nodes scan the GCCC, receive the BF, and eventually switch to the PCCH for subsequent exchange of control information. DDH-MAC Case II has the best rapid channel accessing. In this case, DDH-MAC has the lowest pre-transmission when compared with other CR MAC protocols. It could be observed through the timing diagram in Figure 3.16 that BF is received to learn that the PCCH and the BCCH have been established. Now, nodes simply have to scan the PCCH and contend for the exchange of control information. The pre-transmission time has been computed in Table 3.4.

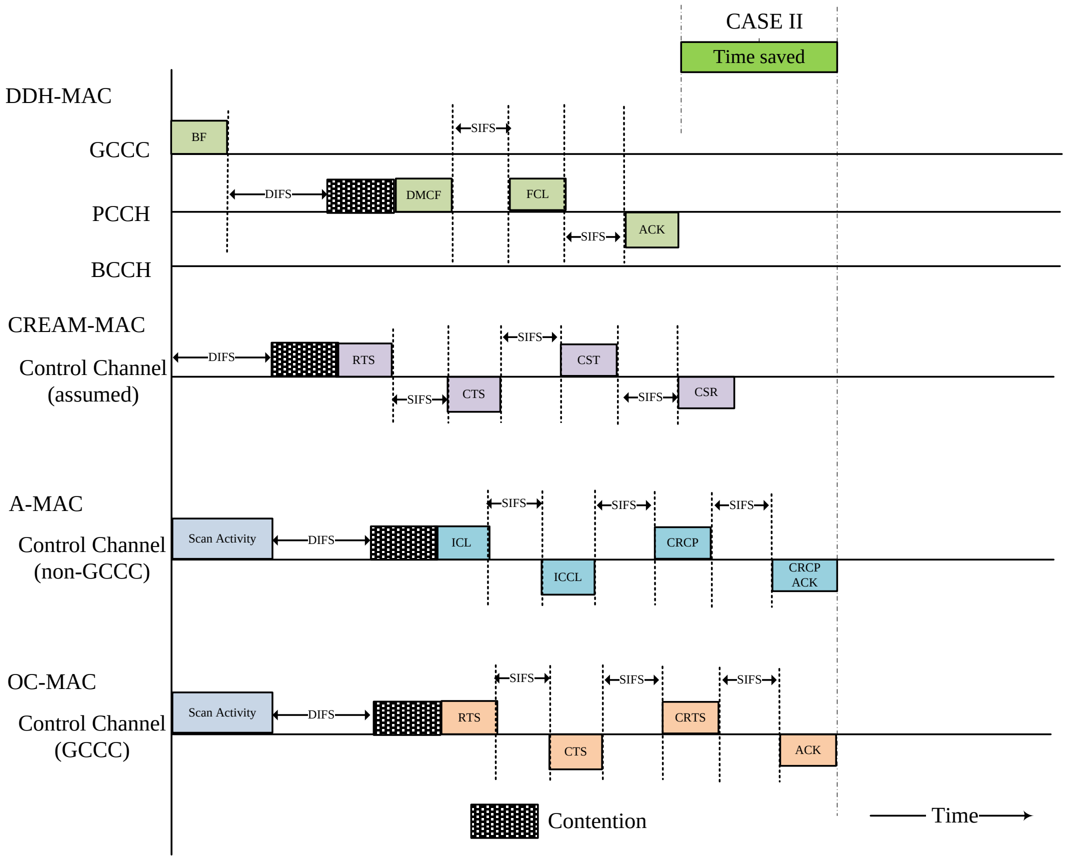


Figure 3.16. Case II- timing diagram comparison with other MAC.

The numerical results obtained for Case II have been plotted in Figure 3.17 which clearly shows that in case of network establishment, DDH-MAC outperforms other MAC protocols.

Table 3.4 Pre-Transmission Time Comparison of DDH-MAC for Case Scenario II

DDH-MAC		**CREAM-MAC**		**OC-MAC**		**A-MAC**	
T_{BF}	14Bytes 10.181µs	T_{RTS}	20Bytes 14.545µs	T_{BF}	14Bytes 10.181µs	T_{BF}	14Bytes 10.181µs
T_{DMCF}	20Bytes 14.545µs	T_{CTS}	20Bytes 14.545µs	T_{RTS}	20Bytes 14.545µs	T_{ICL}	20Bytes 14.545µs
T_{FCL}^{PCCH},	14Bytes 10.181µs	T_{CST}	20Bytes 14.545µs	T_{CTS}	14Bytes 10.181µs	T_{ICCL}	20Bytes 14.545µs
T_{ACK}	20Bytes 14.545µs	T_{CSR}	20Bytes 14.545µs	T_{CRTS}	20Bytes 14.545µs	T_{CRCP}	20Bytes 14.545µs
				T_{ACK}	14Bytes 10.181µs	T_{ACK}	14Bytes 10.181µs
$T_{PT1}^{DDH-MAC}$	: 68Bytes 49.454µs	T_{PT1}^{CREAM}	: 80Bytes 58.18µs	T_{PT1}^{OC-MAC}	: 82Bytes 59.633µs	T_{PT1}^{A-MAC}	: 88Bytes 63.997µs

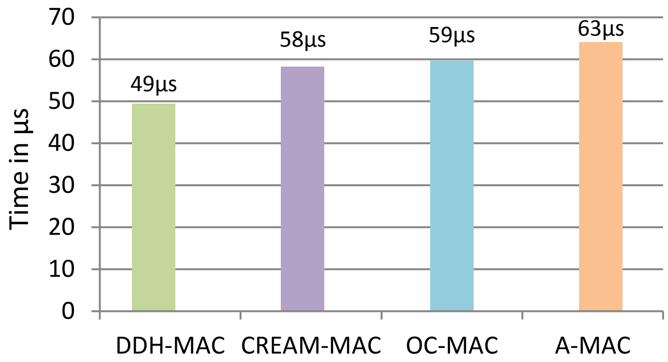


Figure 3.17. Comparison of pre-transmission values for DDH-MAC case II.

c) Comparison of Pre-Transmission Time for DDH-MAC in Case III

The reliability of our scheme is revealed in Cases III and IV. The PU claim on the control channel is efficiently addressed in DDH-MAC by switching to the BCCH and resuming the exchange of control information. Unlike other protocols, the CR nodes in our protocol do not need to search for the control channel, or to re-dialogue the entire configuration whenever the PU occupancy is detected. Table 3.5 shows the efficiency of our scheme in Case III and also reveals that the larger number of control frames exchanged in CREAM-MAC, OC-MAC and A-MAC yield high values of T_{PT} .

Table 3.5 Pre-Transmission Time Comparison of DDH-MAC for Case Scenario III

DDH-MAC	CREAM-MAC	OC-MAC	A-MAC
T_{BS} : 14Bytes 10.181µs	T_{RTS} :20Bytes 14.545µs	T_{BS} : 14Bytes 10.181µs	T_{BS} : 14Bytes= 10.181µs
: time length of 3 BF 30.543µs	T_{CTS} :20Bytes 14.545µs	T_{RTS} : 20Bytes 14.545µs	T_{ICL} : 20Bytes 14.545µs
T_{BF} : 14Bytes 10.181µs	T_{CST} :20Bytes 14.545µs	T_{CTS} : 14Bytes 10.181µs	T_{ICCL} : 20Bytes 14.545µs
: 20Bytes 14.545µs	T_{CSR}:20Bytes 14.545µs	T_{CRTS} : 20Bytes 14.545µs	T_{CRCP} : 20Bytes 14.545µs
T_{FCL}^{PCCH} : 14Bytes 10.181µs	T_{RTS} :20Bytes 14.545µs	T_{ACK} : 14Bytes 10.181µs	T_{ACK} : 14Bytes 10.181µs
T_{ACK} : 20Bytes 14.545µs	T_{CTS} :20Bytes 14.545µs	T_{BS} : 14Bytes 10.181µs	T_{BS} : 14Bytes 10.181µs
T_{FCL}^{BCCH} : 14Bytes 10.181µs	T_{CST} :20Bytes 14.545µs	T_{RTS} : 20Bytes 14.545µs	T_{ICL} : 20Bytes 14.545µs
T_{ACK} : 20Bytes 14.545µs	T_{CSR}:20Bytes 14.545µs	T_{CTS} : 14Bytes 10.181µs	T_{ICCL} : 20Bytes 14.545µs
		T_{CRTS} :20Bytes14.545µs	T_{CRCP} :20Bytes= 14.545µs
		T_{ACK} :14Bytes=10.181µs	T_{ACK} :14Bytes=10.181µs
$T_{PT1}^{DDH-MAC}$: 158Bytes 114.902µs	T_{PT1}^{CREAM} :160Bytes 116.36µs	T_{PT1}^{OC-MAC} : 164Bytes 119.266µs	T_{PT1}^{A-MAC} : 176Bytes 127.994µs

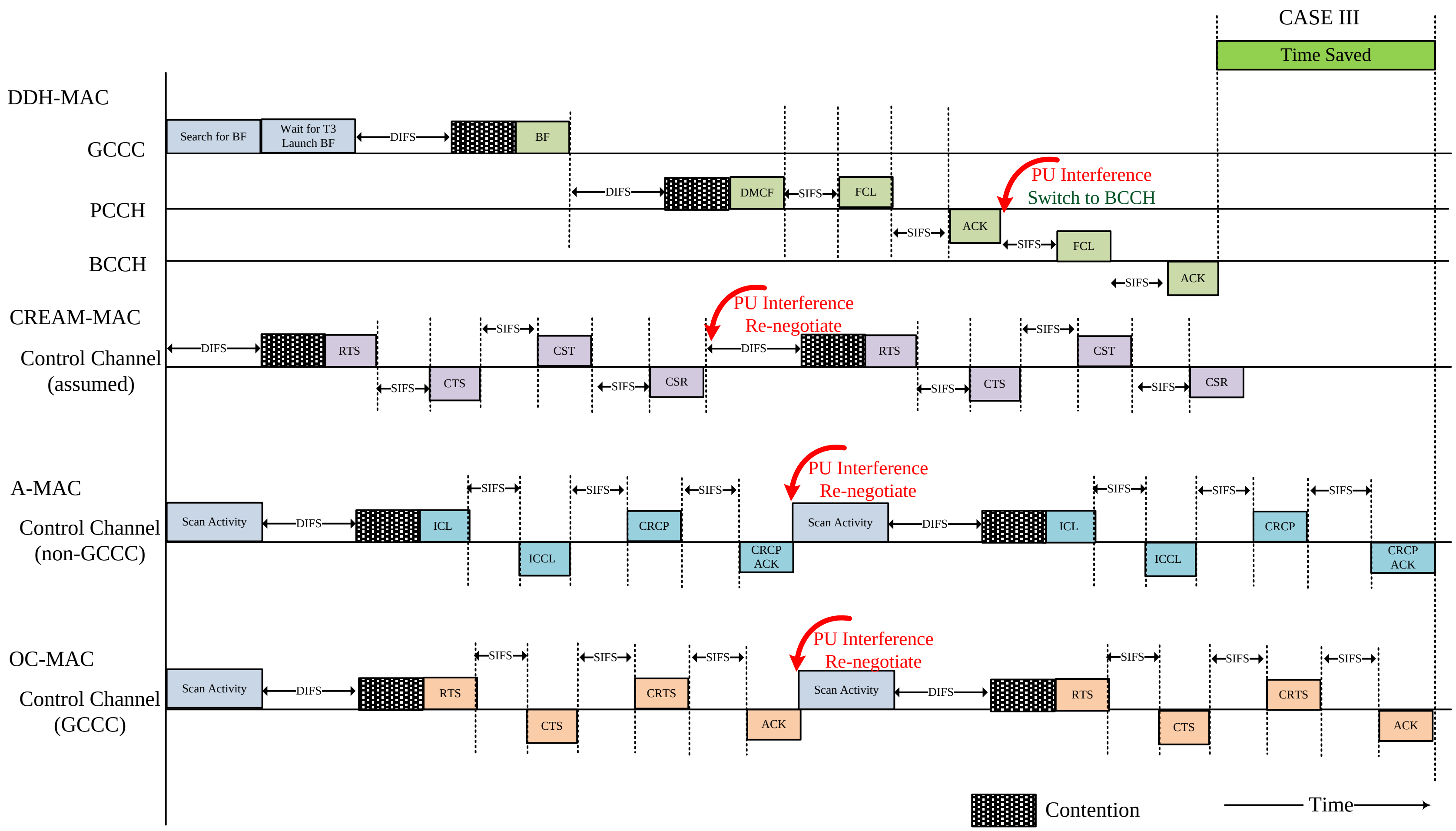


Figure 3.18. Case III- Timing Diagram Comparison with other CR MAC protocols.

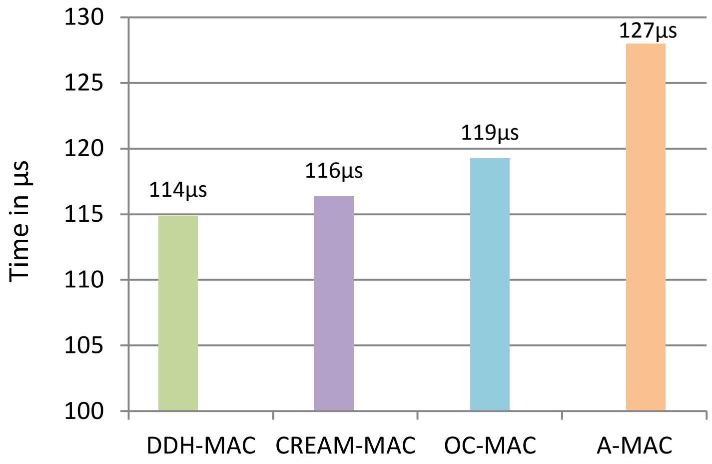


Figure 3.19 Comparison of Pre- transmission values for DDH-MAC case III.

We can see in Figure 3.19 that T_{PT} is significantly lower when compared with other CR MAC protocols and the reason is that reliable channel access mechanism in our protocol gives extra efficiency by avoiding re-transmission of the control information.

d) Comparison of pre-transmission time for DDH-MAC in Case IV

The proposed scheme outperforms other MAC protocols in Case IV and consumes the least amount of time before the nodes finish exchanging control information and start transmitting data on a data channel (see Figure 3.20). The T_{PT} values have been computed in Table 3.6.

Table 3.6 Pre-transmission time comparison of DDH-MAC for case scenario IV

DDH-MAC	CREAM-MAC	OC-MAC	A-MAC
T_{BF} : 14Bytes 10.181µs	T_{RTS} :20Bytes 14.545µs	T_{BS} : 14Bytes 10.181µs	T_{BS} : 14Bytes 10.181µs
T_{DMCF} : 20Bytes 14.545µs	T_{CTS} :20Bytes 14.545µs	T_{RTS} : 20Bytes 14.545µs	T_{ICL} : 20Bytes 14.545µs
T_{FCL}^{PCCH} : 14Bytes 10.181µs	T_{CST} :20Bytes 14.545µs	T_{CTS} : 14Bytes 10.181µs	T_{ICCL} : 20Bytes 14.545µs
T_{ACK} : 20Bytes 14.545µs	T_{CSR}:20Bytes 14.545µs	T_{CRTS} : 20Bytes 14.545µs	T_{CRCP} : 20Bytes 14.545µs
T_{FCL}^{BCCH} : 14Bytes 10.181µs	T_{RTS} :20Bytes 14.545µs	T_{ACK} : 14Bytes 10.181µs	T_{ACK} : 14Bytes 10.181µs
T_{ACK} : 20Bytes 14.545µs	T_{CTS} :20Bytes 14.545µs	T_{BS} : 14Bytes 10.181µs	T_{BS} : 14Bytes 10.181µs
	T_{CST} :20Bytes 14.545µs	T_{RTS} : 20Bytes 14.545µs	T_{ICL} : 20Bytes 14.545µs
	T_{CSR}:20Bytes 14.545µs	T_{CTS} : 14Bytes 10.181µs	T_{ICCL} : 20Bytes 14.545µs
		T_{CRTS} : 20Bytes 14.545µs	T_{CRCP} : 20Bytes 14.545µs
		T_{ACK} : 14Bytes 10.181µs	T_{ACK} :14Bytes 10.181µs
$T_{PT1}^{DDH-MAC}$: 102Bytes 74.178µs	T_{PT1}^{CREAM} :160Bytes 116.36µs	T_{PT1}^{OC-MAC} : 164Bytes 119.266µs	T_{PT1}^{A-MAC} : 176Bytes 127.994µs

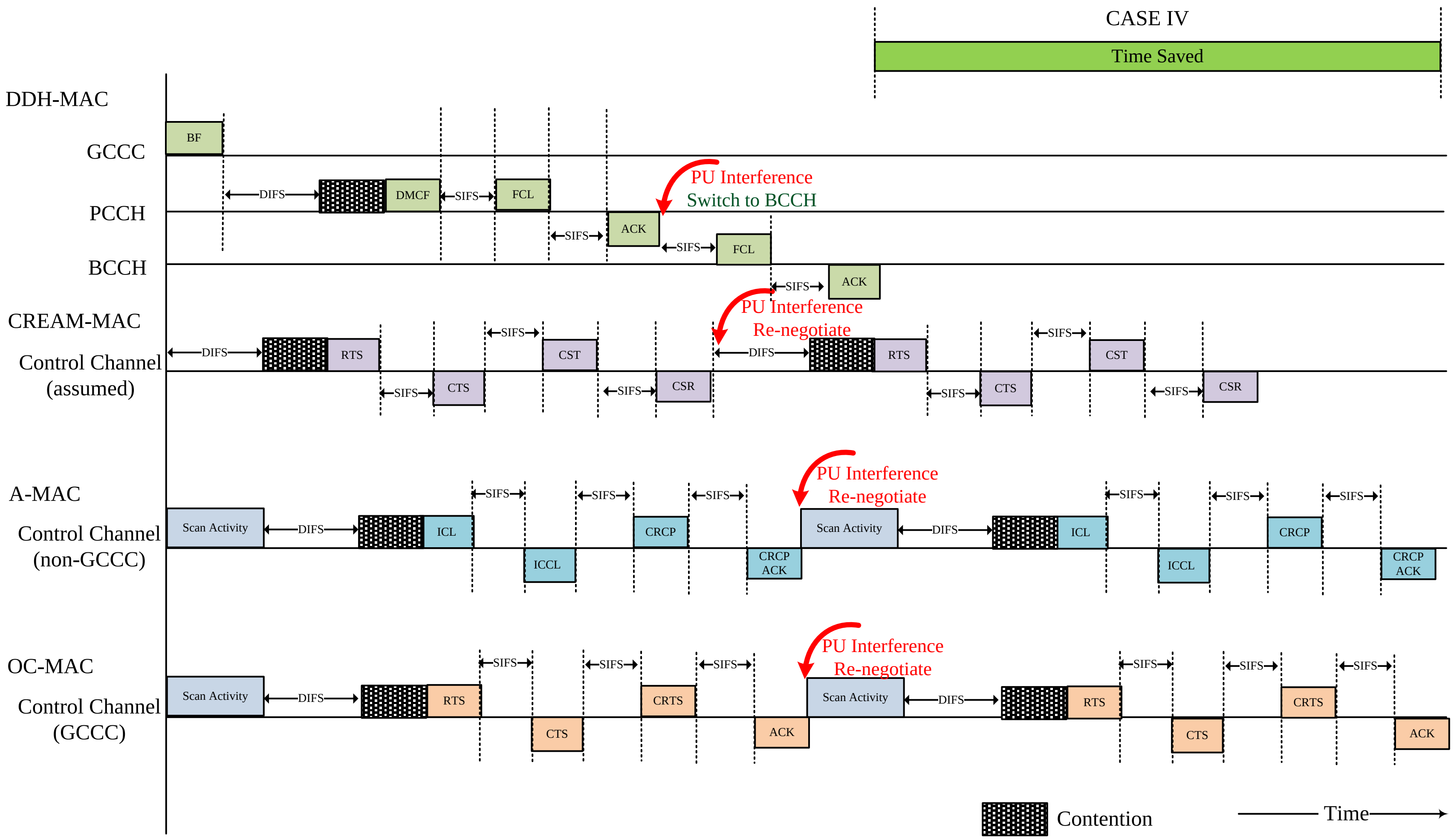


Figure 3.20. Case IV- Timing Diagram Comparison with other CR MAC protocols.

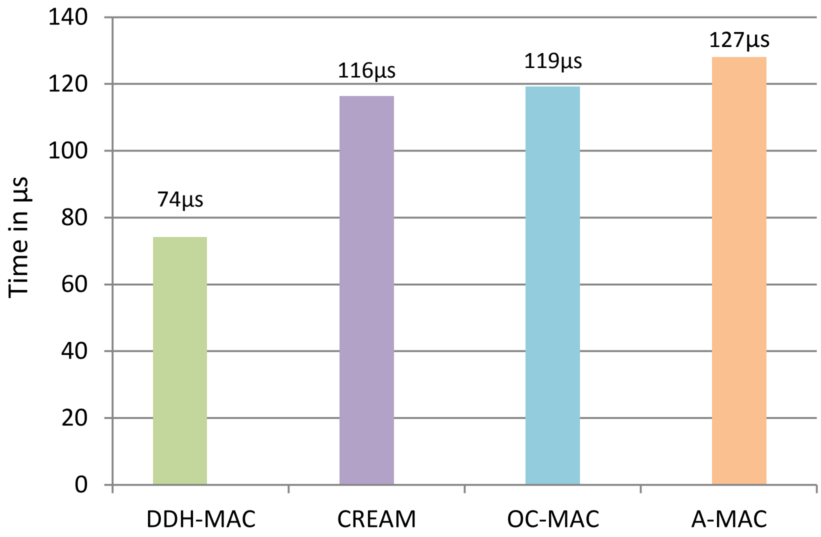


Figure 3.21. Comparison of Pre- transmission values for DDH-MAC case IV.

The numerical values obtained from Table 3.6 have been plotted in Figure 3.21. It can be observed that DDH-MAC saves the maximum of pre-transmission time and performs best even if PU claim has been sensed.

3.9.3. Average Pre-transmission Time

Now we discuss the average pre-transmission time of DDH-MAC when compared with other CR MAC protocols. Rapid channel accessing and reliable channel accessing are the two main features of the DDH-MAC protocol which provides the efficiency and the robustness to the cognitive radio network. The CR nodes implementing the DDH-MAC protocol remain in the state of always keeping access to at least one control channel. The process of exchanging control information over the control channel is always possible through the existence of more than one control channel. The performance of CR MAC protocols can be analysed by observing the behaviours of CR networks with and without PU interference. We provide the behaviours of the DDH-MAC protocol with the aid of time diagrams and framing structures. The pre-transmission time for four cases of DDH-MAC has been derived, computed, plotted and compared in previous sections, and the average pre-transmission time of the different scenario cases is computed in Table 3.6 and compared in Figure 3.22.

Table 3.7. Comparison of average pre-transmission time for all case scenarios

	DDH-MAC	CREAM-MAC	OC-MAC	A-MAC
CASE I	$T_{PT1}^{DDH-MAC}$: 124Bytes 90.178µs	T_{PT1}^{CREAM} : 80Bytes 58.185µs	T_{PT1}^{OC-MAC} : 82Bytes 59.633µs	T_{PT1}^{A-MAC} : 88Bytes 63.997µs
CASE II	$T_{PT2}^{DDH-MAC}$: 68Bytes 49.454µs	T_{PT2}^{CREAM} : 80Bytes 58.185µs	T_{PT2}^{OC-MAC} : 82Bytes 59.633µs	T_{PT2}^{A-MAC} : 88Bytes 63.997µs
CASE III	$T_{PT3}^{DDH-MAC}$: 158Bytes 114.902µs	T_{PT3}^{CREAM} : 160Bytes 116.36µs	T_{PT3}^{OC-MAC} : 164Bytes 119.272µs	T_{PT3}^{A-MAC} : 176Bytes 127.994µs
CASE IV	$T_{PT4}^{DDH-MAC}$: 102Bytes 74.178µs	T_{PT4}^{CREAM} : 160Bytes 116.36µs	T_{PT4}^{OC-MAC} : 164Bytes 119.272µs	T_{PT4}^{A-MAC} : 176Bytes 127.994µs
Average	$T_{AVG}^{DDH-MAC}$: 82.178µs	T_{AVG}^{CREAM} :87.272µs	T_{AVG}^{OC-MAC} : 89.452µs	T_{AVG}^{A-MAC} :95.995µs

It can be seen from Table 3.7 that pre-transmission time for DDH-MAC is better in all cases except Case I. The reason for this higher T_{PT} in Case I is that the network remains in the initialization phase and the first node waits for a time long enough for transmitting 3 BFs in order to avoid duplication of a BF possibly launched by other CR nodes. The detail of this waiting time has already been discussed in Section 3.9. The lower pre-transmission time values in Case II to Case IV of DDH-MAC are because of the number of control and management frames that are exchanged between cognitive nodes and more importantly the mechanism to respond when there is PU interference. CREAM, OC and A-MAC have no mechanism to deal with PU interference during the control information exchange process but to re-exchange all the control and management frames, which increases the pre-transmission time especially in Cases III and IV.

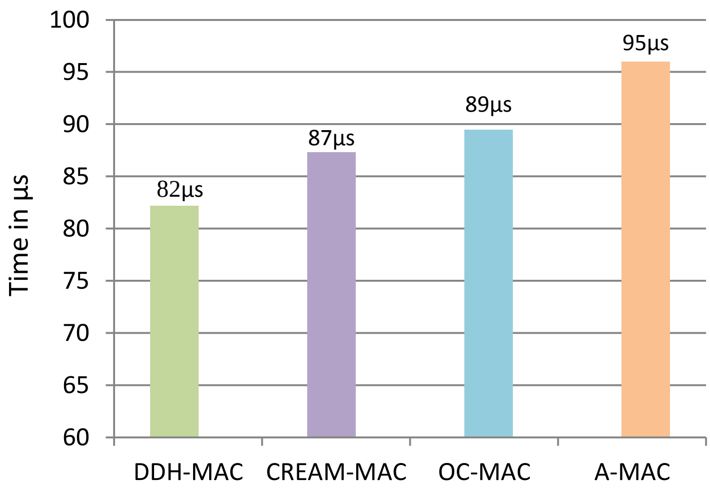


Figure 3.22. Average pre-transmission time for all scenario cases.

3.10. Summary

In this chapter, we provided the framework and detailed architecture of our novel CR MAC protocol. We believe that pre-transmission time plays a very important role in any CR MAC protocol. It is an overhead that each MAC protocol must aim to minimize in all possible ways. The pre-transmission time for different DDH-MAC scenarios has been computed and compared with several other MAC protocols when taking IEEE 802.11b as benchmark. Clearly, the pre-transmission time for DDH-MAC is on average 15% lesser while compared to other MAC protocols. It is important to note that a reduced pre-transmission time not only results in less energy consumption but also helps DDH-MAC to achieve better QoS as CR nodes holding delay-sensitive data will have to wait for less time before the actual communication takes place.

It is worth mentioning that the optimal values of pre-transmission time are subject to a design constraint, i.e., an initial wait time is required prior to launch a BF. This implies that CR nodes deploying DDH-MAC must have at least three white spaces, or else it could not take part into the DDH-MAC operation, and any node launching BF in the start-up must wait for T_3 .

Chapter 4: Mathematical Modelling of the DDH-MAC Protocol

4.1. Communication Model for Cognitive Radio Networks

The cognitive radio network has proven to be the smartest technology in wireless networking to resolve the spectrum scarcity issues. Communication is established after certain operations are performed in a CRN as shown in the communication model in Figure 4.1. Since the inception of CRN, a lot of research has been carried out in this technology which covers a wide range of areas such as spectrum sensing and sharing, and MAC protocols for exchange of free channel list. These are the areas which have been explored extensively while QoS, security and energy efficiency in cognitive radio networks are still challenging tasks that require expertise from researchers.

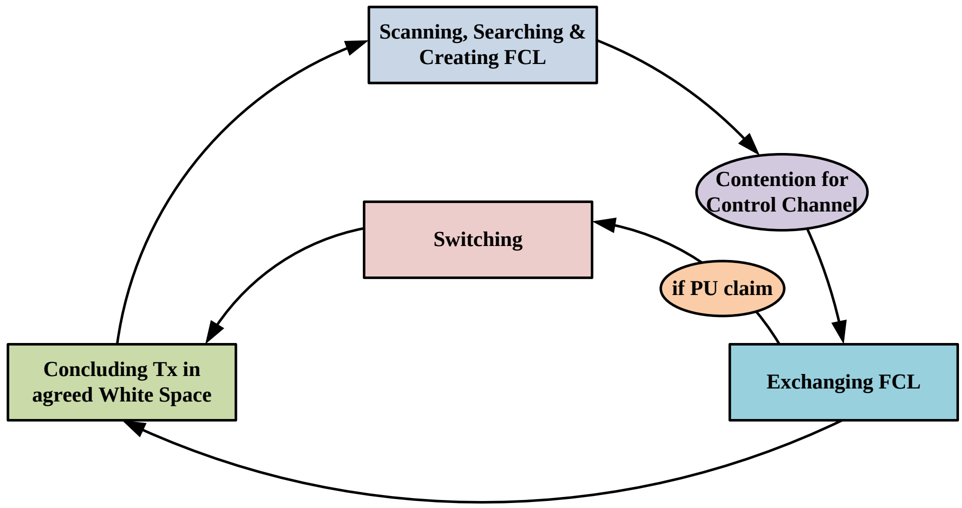


Figure 4.1. Communication model for CR networks.

It is believed that the most important aspect of a cognitive radio network is the exchange of the FCL, because the follow-up communication between two cognitive nodes cannot take place unless and until cognitive nodes have agreed upon white spaces which are common between the communicating partners. Reaching the agreed common white spaces could only be accomplished through the FCL transaction on the control channel. Therefore the primary operation that a CR node must perform prior to any communication is to scan and search its environment to create a list of all available WS, also called the FCL. After all the CR nodes have created their individual FCLs, they contend for exchange of control information on some common medium. This exchange of FCL could take place in two ways: *centralized* if there is a central entity that is responsible for governing the cognitive functionality, e.g., IEEE 802.22 or *decentralized* where it is mandatory to have a common control channel which will be used by all cognitive nodes to setup an initial communication dialogue. After two CR nodes agree upon common white spaces, they conclude transmission and then rescan the environment if changes have occurred. Figure 4.1 shows the generalized communication model for CR networks.

A novel CR MAC protocol has been presented, which makes partial use of GCCC to advertise the information about establishment of a control channel within the white spaces amongst CR nodes. The protocol offers a reliable and secure exchange of control information amongst nodes by making simultaneous use of more than one control channel, i.e., PCCH and BCCH, in case there is a PU claim on the PCCH. Having more than one control channel provides the proposed protocol some unique features such as security, energy efficiency, reliability and time efficiency. In this chapter, we explain the mathematical modelling and evaluate the performance of the DDH-MAC protocol.

4.2. A State Model for DDH-MAC Protocol

DDH-MAC has a novel design of MAC protocol for CRNs which not only benefits from the anytime license-free availability of GCCC but also enjoys the secure communication by privately exchanging the FCL over one of the white spaces. The best features of a decentralized family of MAC protocols have been combined to make the proposed protocol efficient, dynamic, decentralized and hybrid. A detailed explanation in the operations of the protocol including 2 levels of selection has already been presented in Chapter 3. The protocol takes into account four case scenarios in the cognitive radio environment and tunes its parameters efficiently and intelligently according to the current situation of the network, which makes the protocol adaptive, secure and energy efficient. We have defined these case scenarios in the following section and will represent all the states with a 2^n binary function (where n = 2). All the possible states of DDH-MAC are 00, 01, 10 and 11, as specified below:

Network Initialization and launch of BF	*00*
Reading BF and contending for exchange of FCL	*01*
Concluding transmission on agreed WS and scanning PCCH	*10*
Concluding transmission on agreed WS and scanning BCCH	*11*

The operation of the proposed protocol, with the help of state diagram, has been presented in Figure 4.2. As mentioned earlier, the CR nodes implementing DDH-MAC are equipped with 2 transceivers, GT and DT. The GT continuously scan the GCCC for the BF. Periodic copies of BF in GCCC are launched at regular intervals. The DT performs two operations: (1) scanning and sensing the PCCH for control information, and exchanging the FCL; and (2) after successful exchange of the FCL, transmitting data with the partner node over the agreed data channel(s). Like other CR MAC protocols, nodes in DDH-MAC also perform a 3-way handshake in the PCCH. The sender node contends for the PCCH and broadcasts the DMCF followed by the FCL. The receiving nodes update their FCL, find a common data channel and contend to send an ACK in the PCCH. The node which is successful in sending the ACK then switches to the agreed-upon data channel for data transmission and conclusion with the communicating partner.

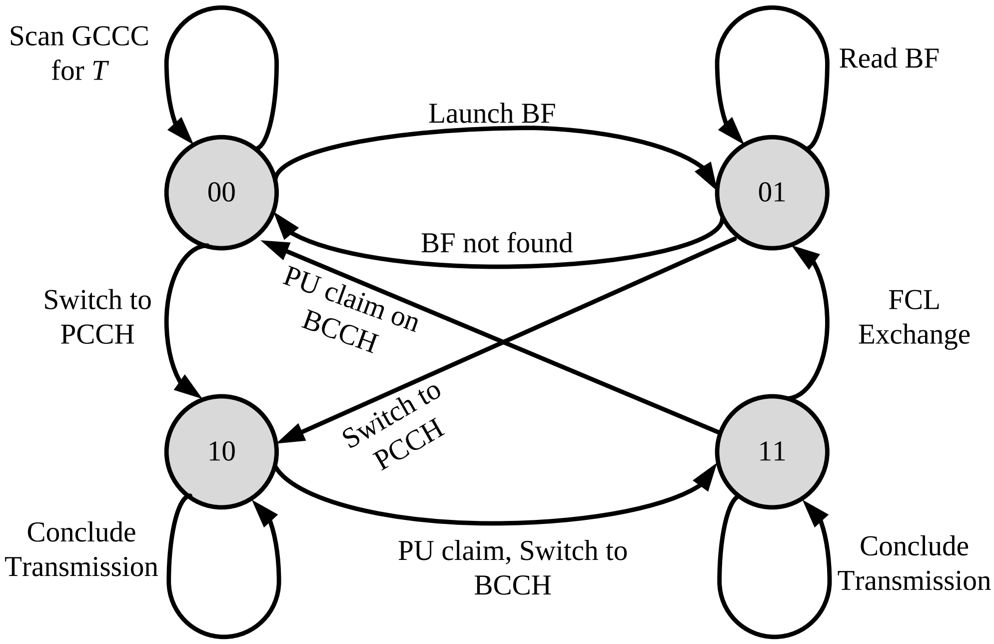


Figure 4.2. States of the DDH-MAC protocol.

Figure 4.2 shows different states of DDH-MAC protocol and the transitions which cause the network to change the states. The CR nodes in DDH-MAC are always certain that they have access to at least one control channel all the time, and thus the exchange of control information would be minimally affected by PU interference. Having more than one control channel gives the DDH-MAC extra reliability. Unlike DDH-MAC, other CR MAC protocols use non-GCCC and thus have to re-negotiate the entire dialogue in the case of PU interference. Whenever PU interference is sensed, nodes in DDH-MAC resume the exchange of control information by simply performing a switch operation. Moreover, the protocol is dynamic because every time there is a PU claim, nodes switch to a newly found and agreed-upon control channel.

To help observe and evaluate the performance of the protocol, a mathematical analysis has been done under a model, which has been developed and is provided in Section 4.3.

4.3. Mathematical Modelling for the Proposed Protocol

Another important key performance indicator of MAC protocols that have been computed by most of the developers in the relevant studies is throughput, which is briefly defined as data transmitted per unit time. However, throughput is heavily affected by multiple factors. Consider an example of calculating the throughput between two CR nodes which have agreed on a common white space to transmit after exchanging their FCL on a common channel. The throughput in this case could only be calculated if all the factors that can affect the communication process have been considered. One of these factors could be the probability that a node will win the contention to exchange the FCL. The other factors could be how many white spaces are common between intended communication partners, the number of other secondary users that are also contending for the control channel, and the time required to setup the initial configuration dialogue. The overall performance of the proposed protocol is also affected by many similar factors. Table 4.1 has been created that lists those parameters and their relationship with throughput, which may bring up or down the performance of DDH-MAC. Some of the factors are co-related with each other. For example, the pre-transmission time is comprised of a number of frames that are exchanged as control information, which ultimately contributes towards delay. The probability that a SU will launch the BF in the GCCC heavily depends upon the congestion which causes an increased size of contention window.

Table 4.1 Factors Influencing Throughput of the DDH-MAC Protocol

Parameter	Notation & Proportionality	Relationship with Throughput
Number of Transceivers	$\propto TR_x$	More no. of transceivers, more rapid sensing and searching, more rapid data transmission
Number of Control Channels	$\propto C_{CH}$	More no. of control channels, more frequent exchange and update of FCL
Number of WS	$\propto$ WS	More no. of WS, more data transmissions
Payload	$\propto$ PL	Larger amount of data to be sent, higher throughput
Number of SUs	$\propto \frac{1}{SU}$	More no. of SUs contending for control channel and white space, less chance to seize the opportunity to transmit
Pre-Transmission Time	$\propto \frac{1}{Pre_{Tx}}$	Less Pre_{Tx} time, faster network convergence, less wait before actual transmission starts
BF Launch Probability	$\propto \mathbb{P}_{BF}$	Higher the probability of successful launch of BF, quicker network initialization
PU Interference Probability	$\propto \frac{1}{P_{PU}}$	Higher PU interference, fewer chances that CR nodes will seize the opportunity to transmit

The mathematical analysis of DDH-MAC is further discussed below:

4.3.1. CCC Access and SU transmission Probabilities

Since the cognitive radio network is an opportunistic technology, the probability to seize the opportunity to transmit heavily effects the performance. There are three types of probabilities that influence the performance of the proposed protocol.

- SU Probability to launch the BF in GCCC, denoted by $\mathbb{P}_{BF}$.
- SU Probability to find and access a white space when PU was in silent mode, denoted by $\mathbb{P}_{PU}$.
- SU probability to be interfered by a PU during an actual transmission also called PU-reclaim probability, denoted by δ.

To calculate $\mathbb{P}_{PU}$, we compute the channel utilization of PU. Figure 4.3 shows two states of a PU, i.e., a PU is in the "On" state when transmitting, or else (when not transmitting), the PU is in the "Off" state. In fact, PU-Off is the state which is opportunistically used by a SU.

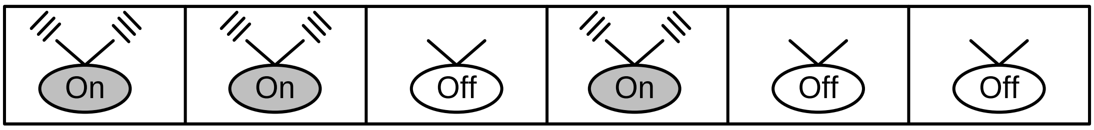


Figure 4.3. Random occupancy of PU in different time intervals.

The Markov chain model for the channel idle-busy periods has been used to find the probability of SUs using a spectrum opportunistically. Let P_α represent the probability that a PU will change its state from On to Off. Then, the probability that a PU will remain in The On state can be expressed by 1- P_α. The probability that SUs can utilize and keep utilizing the white space is shown in Figure 4.4 below:

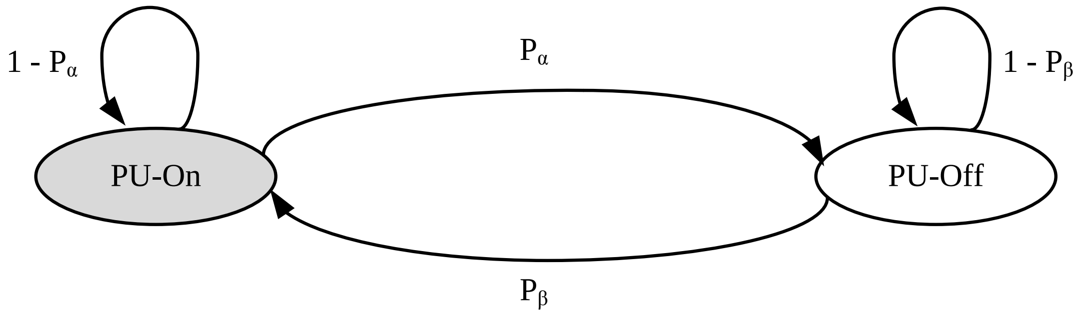


Figure 4.4. Markov chain model of the spectrum opportunity for SUs.

Let Ch = { Ch_1. Ch_2, ... Ch_n} be the set of channels owned by a PU, that could become white spaces, and let SU = {SU_1, SU_2, ... SU_n} be the set of secondary users, then the channel utilization of a PU, denoted as δ, could be derived as:

$$\delta = \frac{(1-P_\alpha)}{(1-P_\alpha)+(1-P_\beta)} \tag{4.1}$$

where $1 \leq i \leq n$. Then the total probability that SU will have white spaces to utilize can be calculated as:

$$P_{WS} = 1 - \frac{(1-P_\alpha)}{(1-P_\alpha)+(1-P_\beta)} \tag{4.2}$$

In a contention-based wireless environment, all nodes use the same medium to transmit. So there is a contest among all the participating nodes to win the medium. The higher the number of users, the higher will be the probability of collision in the network. With DDH-MAC, a node has to contend for GCCC to launch the BF. Since the GCCC is in the ISM band, its free availability to any type of user makes it more saturated. It is uncertain whether or not the CR node will collide with each other when launching BF in the GCCC. We denote this collision probability of launching the BF in the GCCC by, $\mathbb{P}_{CF}$ which has been derived as [201]:

$$P_{CF} = \left(1 - \frac{1}{CW}\right)^{n-1} \tag{4.3}$$

where CW is the size of contention window and CW = {16, 32,…512} and n represents the number of users contending for the control channel in the cognitive radio environment. It is a normal behaviour of nodes in IEEE 802.11 that the more the number of users, the fewer will be the chances to access the medium, which ultimately results in an increased size of contention window up to its maximum possible size, i.e., CW_{max}. If Equation 4.3 represents the probability for nodes not to gain access to GCCC and probably collide with other nodes to launch the BF, then the probability that the nodes may not collide and successfully launch the BF in the GCCC would be represented as:

$$P_{BF} = 1 - \left(\left(1 - \frac{1}{CW}\right)^{n-1}\right) \tag{4.4}$$

4.3.2. Continuous Time Markov Chain (CTMC) Model

In this section, a continuous time Markov chain model (CTMC) [202][203][204] has been used to determine the coalition of a single SU and a single PU (Figure 4.5). Let $\mathbb{P}_{SU}$ represent the probability that only SU will be using the spectrum, then $(1 – \mathbb{P}_{SU})$ will be the probability that the SU will remain in an *Off* state. Let $\mathbb{P}_{PU}$ be the probability that the PU will become *On* after an *Off* state, then $(1 - \mathbb{P}_{PU})$ will be the probability that the PU will remain in the *Off* state. The CTMC model is given in Figure 4.5 and the description of each state is given in Table 4.2.

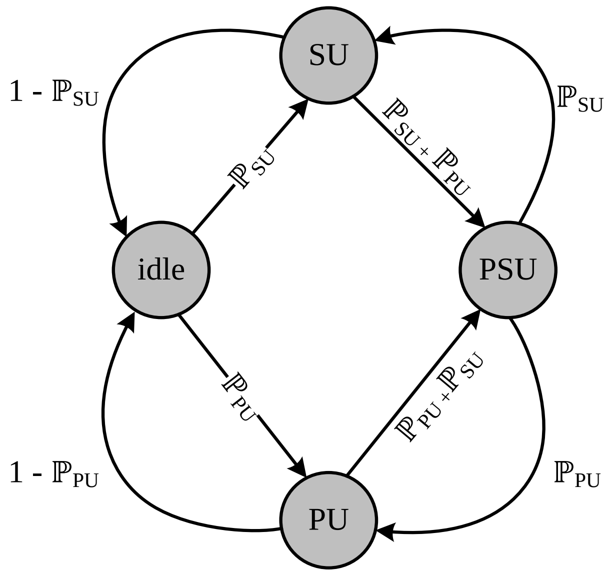


Figure 4.5. A pair of SU and PU CTMC model.

Table 4.2 Description of SU and PU states

States	Description
Idle	No user is accessing the spectrum
SU	A secondary user is accessing the spectrum
PU	A primary user is accessing the spectrum
PSU	Both primary and secondary users are accessing the spectrum

Assume that SU_i is the first CR node to acquire the spectrum, and the CTMC moves from the *idle* state to the *SU* state with the probability $\mathbb{P}_{SU}$. SU_i returns to its *idle* state with probability (1- $\mathbb{P}_{SU}$). Now suppose that a PU arrives and acquires the spectrum, so the CTMC will change its state from *idle* to *PU* state with probability $\mathbb{P}_{PU}$. We further enhance our CTMC by considering the scenario that the spectrum was already in the *PU* state when SU_i arrived, then SU_i seizes any opportunity to share the PU spectrum and the CTMC changes its state to *PSU* with probability ($\mathbb{P}_{SU}$ + $\mathbb{P}_{SU}$), which means that both SU_i and the PU are in coalition. In the negative case where the PU has no spectrum to share, there is no coalition and SU_i has to wait. We will model this scenario in Section 4.5. The CTMC works similarly if SU_i was using the spectrum when the PU arrived, but here, due to the nature of CR network, the SU always shares the spectrum with the PU so that the PU always has access to its own spectrum.

The infinitesimal generator matrix [205][206][207], M, which describes various state transitions of the 1SU and 1PU CTMC model is presented in Figure 4.6

$$
\mathrm{M} = \begin{array}{c} \\ \textit{idle} \\ \textit{SU} \\ \textit{PU} \\ \textit{PSU} \end{array}
\begin{array}{c} \text{States} \\ \\ \\ \\ \\ \end{array}
\begin{array}{cccc}
\textit{idle} & \textit{SU} & \textit{PU} & \textit{PSU} \\
-((1 - \mathbb{P}_{SU}) + (1 - \mathbb{P}_{PU})) & \mathbb{P}_{SU} & \mathbb{P}_{PU} & 1 \\
1 - \mathbb{P}_{SU} & -(\mathbb{P}_{SU} + (1 - \mathbb{P}_{PU})) & ((1 - \mathbb{P}_{SU}) + \mathbb{P}_{PU}) & \mathbb{P}_{SU} + \mathbb{P}_{PU} \\
1 - \mathbb{P}_{PU} & ((1 - \mathbb{P}_{PU}) + \mathbb{P}_{SU}) & -(\mathbb{P}_{PU} + (1 - \mathbb{P}_{SU})) & \mathbb{P}_{PU} + \mathbb{P}_{SU} \\
0 & \mathbb{P}_{SU} & \mathbb{P}_{PU} & -(\mathbb{P}_{SU} + \mathbb{P}_{PU}) + (\mathbb{P}_{PU} + \mathbb{P}_{SU}))
\end{array}
$$

Figure 4.6. One single SU in coalition with one single PU in the CTMC model.

The balance equations with a equalling rate of flow-out are given below:

$$\pi_{idle}\mathrm{P}_{SU} + \pi_{PSU}\ (1 - \mathrm{P}_{PU}) = \pi_i((1 - \mathrm{P}_{SU}) + \mathrm{P}_{PU}) \Rightarrow \pi_{SU} = \frac{\pi_{idle}\mathrm{P}_{SU} + \pi_{PSU}.(1 - \mathrm{P}_{PU})}{(\mathrm{P}_{PU} + (1 - \mathrm{P}_{SU}))} \tag{4.5a}$$

$$\pi_{idle}\mathrm{P}_{PU} + \pi_{PSU}\ (1 - \mathrm{P}_{SU}) = \pi_{PU}(1 - \mathrm{P}_{PU}) + \mathrm{P}_{SU}) \Rightarrow \pi_{PU} = \frac{\pi_{idle}\mathrm{P}_{PU} + \pi_{PSU}.(1 - \mathrm{P}_{SU})}{(\mathrm{P}_{SU} + (1 - \mathrm{P}_{PU}))} \tag{4.5b}$$

$$\pi_{SU}(1 - \mathrm{P}_{SU}) + \pi_{PU}\ (1 - \mathrm{P}_{PU}) = \pi_{idle}(\mathrm{P}_{SU} + \mathrm{P}_{PU}) \Rightarrow \pi_{idle} = \frac{\pi_{SU}(1 - \mathrm{P}_{SU}) + \pi_{PU}.(1 - \mathrm{P}_{PU})}{(\mathrm{P}_{SU} + \mathrm{P}_{PU})} \tag{4.5c}$$

$$\pi_{SU}\mathrm{P}_{PU} + \pi_{PU}\,\mathrm{P}_{SU} = \pi_{PSU}((1 - \mathrm{P}_{SU}) + (1 - \mathrm{P}_{PU})) \Rightarrow \pi_{PSU} = \frac{\pi_{SU}\mathrm{P}_{PU} + \pi_{PU}.\mathrm{P}_{SU}}{((1 - \mathrm{P}_{SU}) + (1 - \mathrm{P}_{PU}))} \tag{4.5d}$$

$$\pi_{idle} + \pi_{SU} + \pi_{PU} + \pi_{PSU} = 1 \tag{4.5e}$$

where π represents the existence in any of the 4 possible states { *idle, SU, PU, PSU* }. Supposing that $\mathbb{P}_{SU} = \mathbb{P}_{PU} = \mathbb{P}$ and $(1 - \mathbb{P}_{SU}) = (1 - \mathbb{P}_{PU}) = (1 - \mathbb{P})$, and solving Equations 4.5a to 4.5e inclusive, we get the following state probabilities:

$$\pi_{idle} = \frac{(1-\mathrm{P})}{\mathrm{P}}\left(\frac{1}{2 + \dfrac{\mathrm{P}}{(1-\mathrm{P})} + \dfrac{(1-\mathrm{P})}{\mathrm{P}}}\right) \tag{4.6a}$$

$$\pi_{SU} = \pi_{PU} = \pi = \frac{1}{2 + \frac{P}{(1-P)} + \frac{(1-P)}{P}} \tag{4.6b}$$

$$\pi_{PSU} = \frac{P}{(1-P)} \left(\frac{1}{2 + \frac{P}{(1-P)} + \frac{(1-P)}{P}} \right) \tag{4.6c}$$

An important performance metric using the CTMC model for access networks is the blocking probability ($\mathbb{P}_{BLK}$). When using one SU in coalition with one PU, the third secondary user is blocked, because the coalition is only possible at maximum between two users, i.e. between a SU and a PU in Figure 4.5. Formally, for a newly arriving secondary user, $\mathbb{P}_{BLK}$ in one pair of SU and PU under CTMC is given by:

$$\mathbb{P}_{BLK\,(1SU\ and\ 1PU)} = \pi_{PSU} \tag{4.7}$$

4.3.3. The CTMC with Multiple SUs Transmitting in Coalition with Multiple PUs

For multiple SUs transmitting in coalition with PUs, a continuous time Markov chain model can be drawn similarly to the case of one single SU and one single PU CTMC. That is, for N SUs and M PUs, we have:

$SU_1 = SU_2 = SU_3 =\ldots..\ SU_K =\ldots..\ SU_{N-1} = SU_N = SU^{s-1}$ and

$PU_1 = PU_2 = PU_3 =\ldots..\ PU_K =\ldots..\ PU_{M-1} = PU_M = PU^{s-1}$, respectively.

where SU^{s-1} and PU^{s-1} represents SU and PU being in any of the possible states respectively.

One SU is required to form a coalition with a PU, and after that several requesting SUs can join the coalition. The requesting SU can interact with multiple SUs (in its neighbourhood) and can form multiple coalitions, simultaneously.

Additionally, let m= {1, 2, 3…….. N} represent the size of a coalition. For example, when m=2, then any Secondary User 1 can form a coalition of size 2 with any other Secondary User k being expressed in the form of (1, k). Similarly, when m=3, then any Secondary User 1 can form a coalition of size 3 with any two other Secondary Users k and o in the form as (1, k, o). This pattern continues until m=N. The number of states (S_N) in multiple SUs, which transmit in coalition with PUs under CTMC at each value of m, follows the pattern given below:

$$S_N = 1 + C_N^1 + C_N^1 + \cdots + C_N^{(m-1)} + C_N^m$$

This implies $S_N = 1 + \sum_{m=1}^{N} C_N^m = 2^N$ (4.8)

where $C_N^m = \dfrac{N!}{((N-m)!*m!)}$

For example, when N=4, by Equation 4.8, we have,

$$S_4 = 1 + C_4^1 + C_4^2 + C_4^3 + C_4^4 = 16$$

Equations 4.5 and Equation 4.6 can be combined to obtain the blocking probabilities for N users [203].

$\mathbb{P}_{BLK\text{ (Multiple SUs and Multiple PUs)}} = \pi(SU_1, PU_1, SU_2, PU_2, \ldots, SU_N, PU_N)$ (4.9)

where $\pi = \{\pi_{idle}, \pi_{SU}, \pi_{PU}, \pi_{PSU}\}$

4.3.4. Single-SU and Single-PU CTMC Model with Queuing

As discussed in Section 4.3.2, we now consider the scenario where a PU has occupied the spectrum and is unable to share the spectrum with SU_i. In this case, SU_i has to wait and temporarily queue the packets [208][209]. A Single-SU and Single-PU CTMC model with queuing for DDH-MAC has been presented in Figure 4.7, and the description of each state is provided in Table 4.3.

Table 4.3 Description of SU and PU States

States	Description
Idle	No user is accessing the spectrum
SU	Secondary User is accessing the spectrum
PU	Primary User is accessing the spectrum
PSU	Both Primary and Secondary users are accessing the spectrum
W_{SU}	SU waiting until spectrum becomes available (does not have spectrum to share)

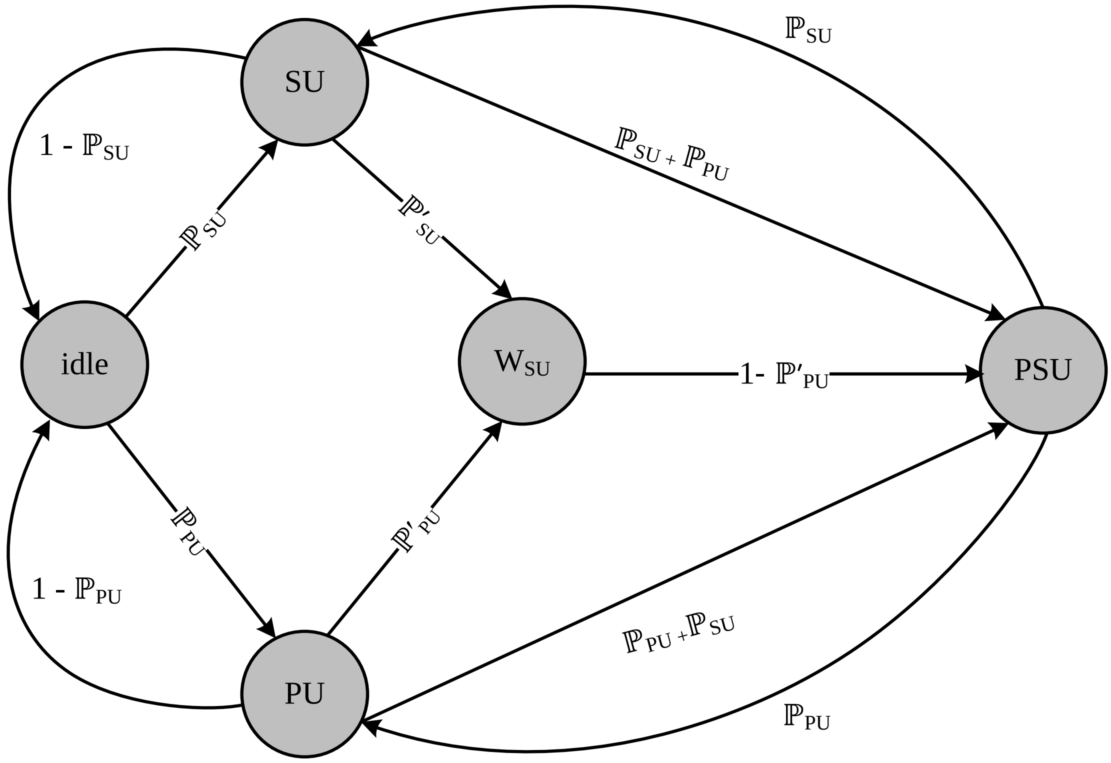


Figure 4.7. A Single-SU and Single-PU CTMC model with queuing.

In Figure 4.7, an additional waiting state for SU_i has been added to represent the scenario where the PU has occupied the spectrum and is unable to share the spectrum with SU_i. In this case, CTMC goes to state W_{SU} with probability P'_{SU} where SU_i has to wait until spectrum becomes available. If the PU vacates the spectrum or is able to share, CTMC moves to the state *PSU* with the probability (1- $\mathbb{P}'_{PU}$), such that (1- P_{SU}) = (1- $\mathbb{P}'_{PU}$) where both the users form a coalition and utilize the spectrum. The infinitesimal generator matrix for the Single-SU and Single-PU CTMC model with queuing is shown in Figure 4.8 below.

$$
M_{queue}\begin{bmatrix}
\text{States} & idle & SU & PU & W_{SU} & PSU \\
idle & -((1-\mathbb{P}_{SU})+(1-\mathbb{P}_{PU})) & \mathbb{P}_{SU} & \mathbb{P}_{PU} & 0 & 1 \\
SU & 1-\mathbb{P}_{SU} & -(\mathbb{P}_{SU}+(1-\mathbb{P}_{PU})) & ((1-\mathbb{P}_{SU})+\mathbb{P}_{PU}) & 0 & \mathbb{P}_{SU}+\mathbb{P}_{PU} \\
PU & 1-\mathbb{P}_{PU} & ((1-\mathbb{P}_{PU})+\mathbb{P}_{SU}) & -(\mathbb{P}_{PU}+(1-\mathbb{P}_{SU})) & \mathbb{P}'_{SU} & \mathbb{P}_{PU}+\mathbb{P}_{SU} \\
W_{SU} & 0 & 1-\mathbb{P}_{PU} & 0 & -\mathbb{P}'_{SU} & 1-\mathbb{P}'_{PU} \\
PSU & 0 & \mathbb{P}_{SU} & \mathbb{P}_{PU} & 0 & -(\mathbb{P}_{SU}+\mathbb{P}_{PU})+(\mathbb{P}_{PU}+\mathbb{P}_{SU})(1-\mathbb{P}'_{SU}))
\end{bmatrix}
$$

Figure 4.8. Single-SU in coalition with Single-PU CTMC model with queuing.

The balance equations with a equalling rate of flow-out are given below:

$$\pi_{idle} = \pi_{SU}(1-P_{SU}) + \pi_{PU}(1-P_{PU}) / (P_{SU} + P_{PU}) \tag{4.10a}$$

$$\pi_{SU} = \pi_{idle} P_{SU} + \pi_{PSU}(1-P_{PU}) + \pi_{WSU}(1-P_{PU}) / (P_{PU} + P'_{PU} + (1-P_{SU})) \tag{4.10b}$$

$$\pi_{PU} = \pi_{idle} P_{PU} + \pi_{PSU}(1-P_{SU}) + (1-P_{SU}) / (P_{SU} + P'_{SU} + (1-P_{PU})) \tag{4.10c}$$

$$\pi_{PSU} = \pi_{SU} P_{PU} + \pi_{PU} P_{SU} + \pi_{WSU}(1-P'_{SU}) + (1-P'_{PU}) / ((1-P_{SU}) + (1-P_{PU})) \tag{4.10d}$$

$$\pi_{WSU} = P'_{SU}\,\pi_{PU} / ((1-P_{PU}) + (1-P'_{PU}) \tag{4.10e}$$

$$\pi_{idle} + \pi_{SU} + \pi_{PU} + \pi_{PSU} + \pi_{WSU} = 1 \tag{4.10f}$$

Solving Equation 4.10a to Equation 4.10f, we get

$$\pi_{idle} = \frac{1-P}{P}\left(\frac{1}{2+\frac{5P}{2(1-P)}+\frac{1-P}{P}}\right) \tag{4.11a}$$

$$\pi_{SU} = \pi_{PU} = \pi = \frac{1}{2+\frac{5P}{2(1-P)}+\frac{1-P}{P}} \tag{4.11b}$$

$$\pi_{WSU} = \pi_{W} = \frac{P}{2(1-P)}\left(\frac{1}{2+\frac{5P}{2(1-P)}+\frac{1-P}{P}}\right) \tag{4.11c}$$

$$\pi_{\text{PSU}} = \frac{3P}{2(1-P)}\left(\frac{1}{2+\frac{5P}{2(1-P)}+\frac{1-P}{P}}\right) \tag{4.11d}$$

The $\mathbb{P}_{BLK}$ in this case could be derived in a similar way to Equation 4.7

$$\mathbb{P}_{BLK\,(1SU\ and\ 1PU)} = \pi_{PSU} \tag{4.12}$$

For multiple SUs transmitting in coalition with multiple PUs with queuing, the CTMC state model, infinitesimal generator matrix and blocking probability can be obtained similarly to the derivation of Equation 4.8 and Equation 4.9.

4.4. Performance Evaluation

For the convenience of presentation, Table 4.4 lists the important parameters for the design and analysis of the proposed DDH-MAC protocol. Let [SU] be the number of secondary users and [WS] be the number of available white spaces in a cognitive radio environment. $\mathbb{P}_{\text{SU}}$ is the probability that the SU will utilize the white spectrum when it is not used by the primary user, and $\mathbb{P}_{\text{BF}}$ is the probability that the initiating node will launch a BF in the GCCC. Clearly $\mathbb{P}_{\text{BF}}$ depends on the level of saturation on the GCCC as derived in Equation 4.4. The aggregated throughput denoted by Ŧ is proportional to multiple factors as mentioned in Table 4.1, Ŧ is derived as:

$$Ŧ \; \alpha \; \frac{\text{TRx } \text{C}_{\text{CH}} \text{ PL } \text{P}_{\text{BF}}}{SU\text{P}_{\text{PU}}\text{Pre}-\text{Tx}} \tag{4.13}$$

$$Ŧ = \frac{\text{TRx } \text{C}_{\text{CH}} \text{ PL } [\check{R}]\, \text{P}_{\text{BF}}}{SU\text{P}_{\text{PU}}\text{Pre}-\text{Tx}} \tag{4.14}$$

where Ř is the data rate of the licensed channel and is set as a constantPre_{Tx}time has been computed in section 3.9 and is given below:

$$Pre-Tx = \left\{\frac{DMCF + FCL + Ack + 2 \times SIFS + DIFS}{[\check{R}]}\right\} \tag{4.15}$$

where DMCF, FCL, and ACK are the control frames sizes 20 Bytes, 14 Bytes and 20 Bytes respectively, exchanged as control information.

4.4.1. Aggregated Throughput

The parameters used to evaluate the DDH-MAC protocol are summarized in Table 4.4. We first investigate the aggregate throughput for the saturated network case where, apart from PU interference probability there is a contention among SUs to launch the BF in GCCC. Let δ be the PU interference probability and $\mathbb{P}_{SU}$ be the probability that SU will utilize white spaces. Assume that the number of transceivers and the number of control channels are both equal to 2 and Ř is set to 11Mbps.

Table 4.4 Parameters for the Proposed Scheme

Parameter	Assigned Value
$[SU]$	Number of secondary users
$[WS]$	Number of white spaces for each SU
$\mathbb{P}_{SU}$	The probability that SU will utilize the white spectrum
$\mathbb{P}_{BF}$	Probability of launching BF
$\mathbb{P}_{CF}$	Probability that SU will utilize WS
Tx	Number of transceivers = 02
C_{CCH}	Number of control channels = 02
Pre_{Tx}	Pre-transmission time
PȽ	Payload = 2000Bytes
Ř	Data Rate of the channel, 11Mbps
CW_{min}	16
CW_{max}	512
δ	PU Interference Probability
BF	14Byte
DMCF	DDH-MAC Control Frame 20Byte
FCL	Free Channel List 14Byte
ACK	20Byte

Using Equation (4.12) we plot the aggregate throughput (Ŧ) against the BF launching probability (Equation 4.3) in Figure 4.9.

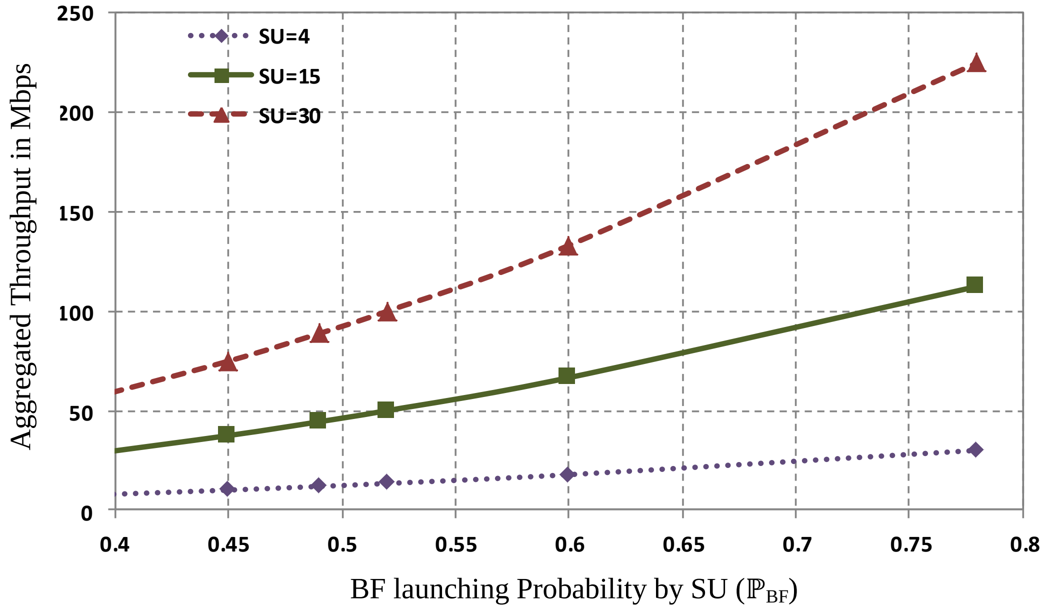


Figure 4.9. The aggregate throughput against the probability ($\mathbb{P}_{BF}$). Note that BF will be launched with the average number of white spaces [WS] for each SU. Pre_{Tx} is 128µs; the number of control channels and the number of transceivers (Tx) are 2.

Figure 4.9 shows that the highest aggregate throughput changes with different numbers of contending secondary users. This is expected because the higher the probability of launching the BF by a secondary user, the higher the aggregate throughput. The aggregate throughput of the DDH-MAC protocol depends on the pre-transmission time which could be different for different case scenarios and on the time to launch BF over the control channel which is ultimately determined by the IEEE 802.11 DCF parameters such as CW_{min} and Ř.

After setting the optimal values for the BF launching probability, the average number of white spaces with each SU and the pre-transmission time, we have used Equation 4.14 to determine the aggregate throughput of the DDH-MAC protocol against the PU interference probability. The numerical values obtained from Equation 4.12 have been plotted in Figure 4.10. It is observed that the aggregate throughput reaches the highest when there is *no* or *minimal* PU interference. Nodes will only have to wait to read/launch the BF in the control channel and with two frames exchanged as control information, nodes will immediately start utilizing white spaces opportunistically. The aggregate throughput decreases and reaches zero as the PU interference probability increases.

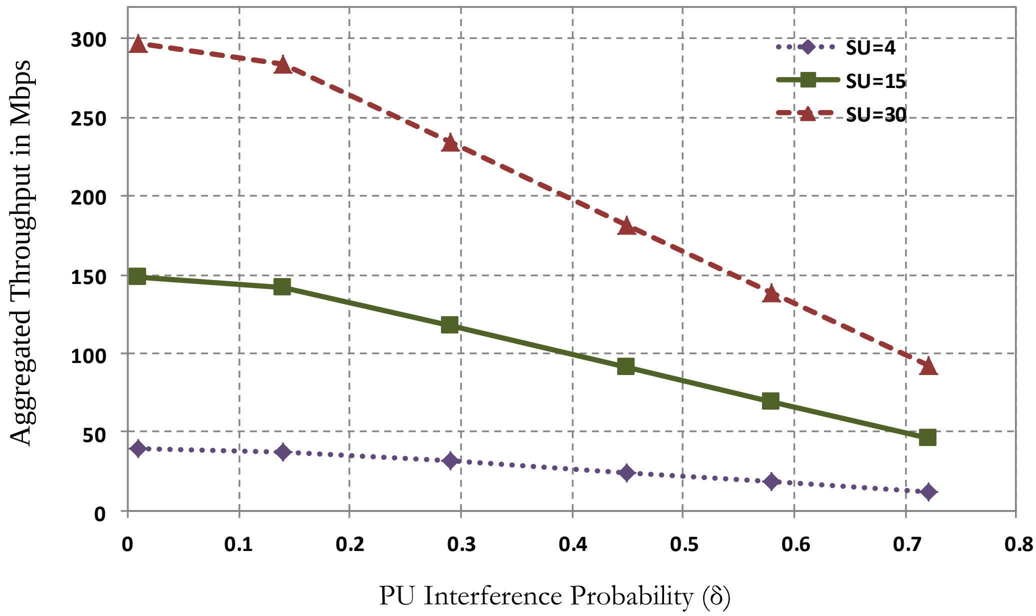


Figure 4.10. The aggregated throughput against the PU interference probability (δ) with the average number of white spaces [WS] for each SU, Pre_{Tx} being 128μs; and the number of control channels and the number of transceivers (Tx) being both 2.

We further proceed to the relationship between throughput and vacant channels. Clearly, the opportunity for the SU to transmit depends heavily on the available white spaces. Fewer white spaces imply lesser opportunity for the transmission. With the average values for the BF-launching probability ($\mathbb{P}_{BF}$) and the PU-interference probability (δ), we again use Equation 4.12 to obtain numerical values which have been plotted in Figure 4.11. It is observed that the aggregate throughput of the CR nodes significantly reaches its highest value when there are maximum available white spaces. The aggregate throughput decreases as the channel utilization of PU increases, which implies that the secondary users get fewer opportunities to transmit their own packets if the primary user utilizes the licensed channels more intensively. Another way to really improve the throughput which has been deployed in the DDH-MAC protocol is, to rigor the hardware cost constraint and use more than one transceiver, and to increase the number of control channels. For example, consider Scenario III of the DDH-MAC protocol where one transceiver is continuously scanning the control channel (PCCH) for control information as well as PU claim, and the other transceiver is used to transmit data. The PU interference is efficiently addressed on the control channel without any network convergence issues by simply switching to the backup control channel (BCCH). Using more than one transceiver and more than one control channel can significantly improve throughput under the DDH-MAC.

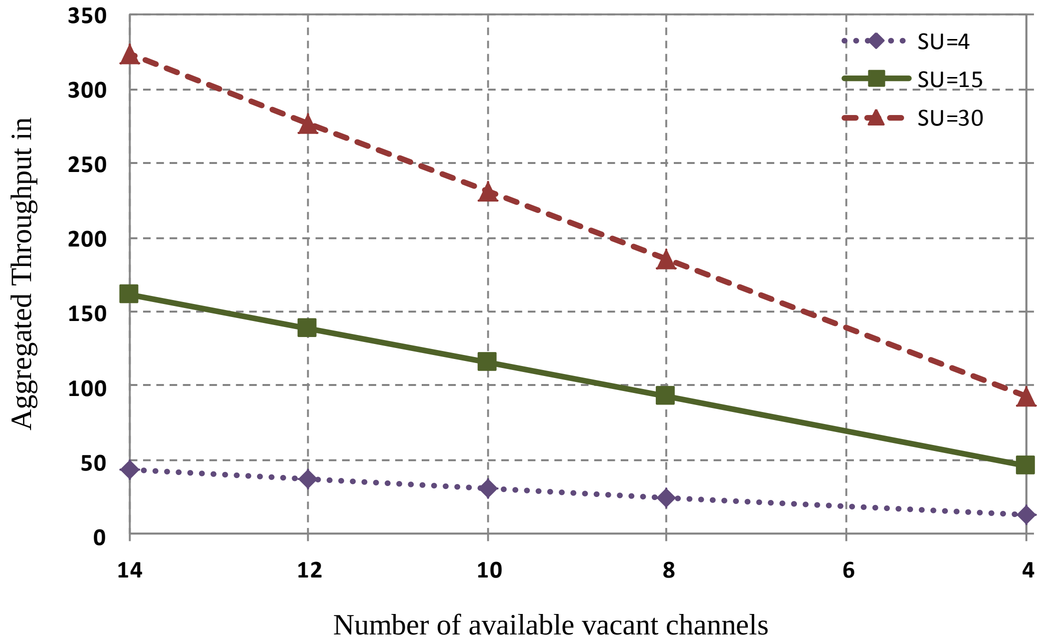


Figure 4.11. The aggregated throughput against the PU interference probability (δ) with the average number of white spaces [WS] for each secondary user. Pre_{Tx} is 128μs; average value of BF transmit probability having been considered, and the number of control channels and the number of transceivers (Tx) are both set to 2.

As shown in Figure 4.11, the aggregate throughput linearly increases as the number of white spaces available to a secondary user increases before reaching the maximum. This is expected by the relationship of throughput and white spaces mentioned in Table 4.1. More precisely, when secondary users can access all the available white spaces simultaneously without any primary user claim, sufficient transmission takes place between secondary users, which ultimately results in higher aggregate throughput.

4.4.2. DDH-MAC Throughput Performance Comparison

In this section we compare the performance of the DDH-MAC protocol with a highly cited CR MAC protocol reported in the literature i.e., CREAM-MAC [38]. For the purpose of comparison, we have considered the same DSSS physical layer parameters for all three protocols. The aggregate throughput for 30 SUs is plotted in Figure 4.12 for the DDH-MAC and CREAM-MAC protocols, against the average value of the probability that SUs will utilize the spectrum, average number of white spaces [WS] available to each SU, and Pre_{Tx} set to 82μs, and 87 μs, for DDH-MAC and CREAM-MAC respectively. The obvious reason for the better throughput of DDH-MAC is the number of control channels used, which significantly reduces the overhead of network convergence, ultimately improving the pre-transmission time spent on the exchange of control information whenever there is a PU activity. We also observe that despite fewer opportunities to use unoccupied spectrum, the aggregated throughput for DDH-MAC is notably higher than the CREAM-MAC protocol. This means that $\mathbb{P}_{PU}$ is affected by the PU claims on data channel. Higher PU claims will imply more re-negotiations, more computational cost and backoff to access control channel, and the exchange of more control frames which will ultimately increase or decrease the aggregated throughput.

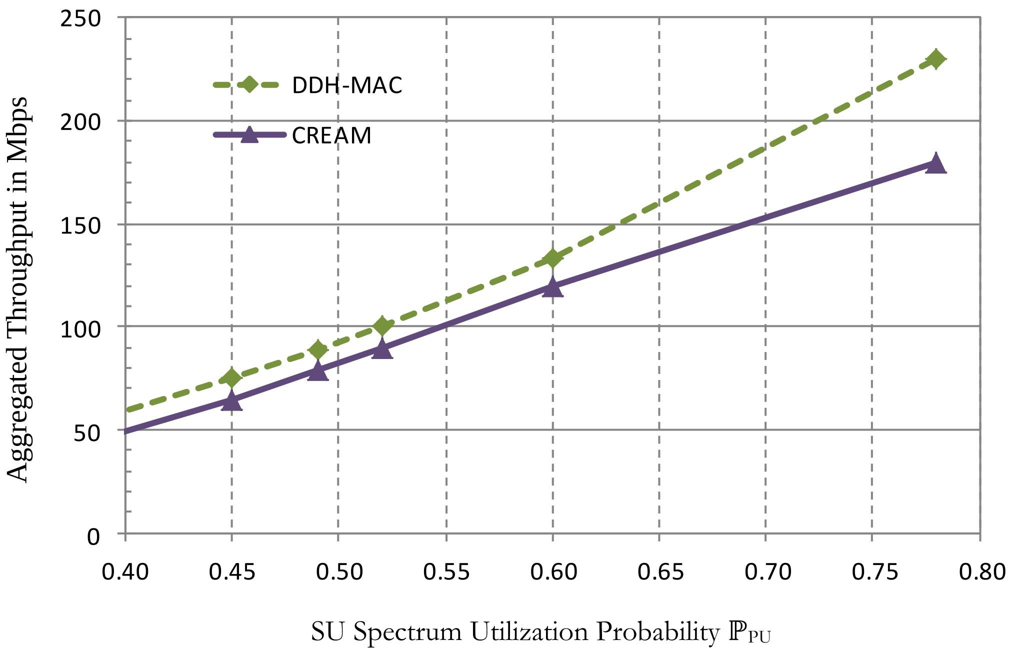


Figure 4.12. The aggregate throughput for SU = 30, against the probability that SU will utilize vacant channel. $\mathbb{P}_{BF}$ has been fixed at 0.5; average number of white spaces [WS] with each SU.

4.5. Summary

The cognitive radio technology has emerged as an effective solution to address the problem of spectrum scarcity. The cognitive nodes adapt the environment and intelligently seize the opportunity to communicate with other CR nodes. Different MAC protocols have been designed to setup an initial configuration dialogue, but unrealistic assumptions or unclear methodology has been used to deal with the very critical part of CR networks, i.e., exchanging the FCL on a common channel. A novel CR MAC protocol has been proposed in this PhD study. To the best of our knowledge, DDH-MAC is the first CR MAC protocol lying between the GCCC and non-GCCC families of protocols, using the GCCC for the BF transmission and intelligently selecting one of the channels as the primary control channel and another as the backup channel. PU claims, which are not unusual in the CR network, are efficiently dealt with by performing a switch channel activity in DDH-MAC. The CR nodes remain always in the state of being able to access at least one control channel. The protocol is dynamic because the CR nodes either switch to the backup channel or find a new channel to exchange control information whenever there is a PU claim. More control channels lead to the exchange of fewer frames for agreeing upon transmission rules. This makes the proposed protocol more time efficient and performs better than any of other CR MAC protocol, especially when a PU activity is sensed (and when this happens, nodes do not need to spend time on finding and synchronizing on a new control channel, they simply switch to backup channels). The results obtained from the mathematical modelling reveal that the proposed protocol performs better in terms of aggregated throughput.

Chapter 5: Simulation of the Proposed Adaptive Multi-access Multi-channel MAC Protocol

5.1. Introduction

Simulation Modelling is the most important method for network performance analysis; and in general, there are two kinds of network modelling: i) *analytical modelling* and ii) *computer simulation* [210]. The first is by mathematical analysis that characterizes a network as a set of mathematical equations. The main disadvantages are a one-dimensional view of the network and an inability to simulate the dynamic nature of a network as nodes join or leave the network. The second type of computer simulator is broadly classified as either a *continuous time simulator (CTS)* or a *discrete event simulator (DES)*. Therefore, the study of a complex system necessarily requires a computer simulation package that is able to compute the time that is associated with real events in a real-life situation

In this chapter, we develop simulation experiments to investigate the system performance of our proposed DDH-MAC protocol. For our simulation experiments we have used OPNET Modeler [211], which is a kind of DES. OPNET provides a comprehensive development environment for the specification, simulation and performance analysis of communication networks. A large range of communication systems from a single LAN to global satellite networks are supported. OPNET Modeler is a powerful tool which evaluates the network efficiently and accurately. OPNET is a new and widely used technology which is equipped with all the features needed to design, model and simulate all types of networks systematically such as home, corporate and wide area networks. OPNET with its unique approach can provide an objective, reliable and quantitative basis for network planning and designing and it could shorten the network construction period, improve the precision of decision making on network building and reduce the risk of network construction investment. Some of the salient features of OPNET are:

- *Modelling and Simulation:* OPNET uses 3 phases for simulating any project, i.e., build model, execute simulation, and analyse results which assists the user in final decision making.

- *Hierarchical Modelling:* OPNET adopts a hierarchical structure to build small and simple to large and complex networks. The bottom layer is 'the process model' which consists of state transition diagrams (STD) that specify a variety of protocols, algorithms and queuing policies. The middle layer is the 'node model' which makes different modules that have pre-defined characteristics and built-in parameters such as packet generators, radio transmitter and receiver etc., and the top layer is the 'network model' which specifies the physical topology of the communication network (e.g., specification of Ethernet, node type).
- *Abundant Communication Network:* OPNET provides abundant network models such as, ATM, x.25, WiMAX, WLAN and Ethernet etc. and also has equipment for different vendors such as CISCO, 3COM and Sun etc. to allow researchers to either modify existing models or develop new communication models of their own.
- *Generation of Statistical Data:* OPNET provides the opportunity for a user to obtain customized statistical data and detailed network performance analysis.

5.2. A Pseudo Code Algorithm for DDH-MAC Protocol

To help fully understand and also to help facilitate the implementation of our proposed DDH-MAC protocol, we summarize our algorithm by providing its pseudo code in Figure 5.1. In Figure 5.1, the BF represents the first management frame that is launched in the GCCC to initialize the network. The size and the structure of the BF have already been described in Section 3.6.1. The algorithm defines two main features of the DDH-MAC protocol, i.e., rapid channel accessing and reliable channel accessing, both of which reflect the efficiency of DDH-MAC in accessing the GCCC. The implementation of DDH-MAC is further described below.

As mentioned earlier, OPNET considers a system as a finite machine which has states and transitions. We first developed the STD (also called the process model) of the DDH-MAC protocol and then developed the node model to incorporate MAC features of DDH-MAC into the node model.

```
DDH-MAC algorithm
//Phase 1: Rapid channel accessing
BF = node_id + PCCH + BCCH;          //fields of a BF
    while
    begin (the action of the secondary user)
    {  case join group:
       listen to GCCC;
      if {
       at least receive a BF in GCCC
       read the BF;
        case 1
        PCCH in FCL                            //white space already known
            If    {
            no claim on PCCH, go to PCCH and exchange control information;
            agree on white space for data transmission;
            conclude transmission with partner node;
            }
//Phase 2: Reliable channel accessing
            else  {
                  if {
                  claim on PCCH AND no claim on BCCH; go to BCCH;
                  exchange control information;
                  agree on white space for data transmission;
                  conclude transmission with partner node;
                      }
                  else
                        {
                        listen to GCCC;
                        }
                  }
       case 2
            PCCH not in FCL:                     //white space not known
            update the FCL;
            go to case 1;
           }
       else {
            if {
                  no. of white spaces ≥ 3 //threshold to make itself 1st node
                  wait till T expires;    //time required to scan 3white spaces
                  create group and make itself first node;//launch BF in GCCC
                  choose PCCH and BCCH;
                  create BF;
                  launch BF in GCCC;
                  the network converges;
                  go to case 1;
               }
            else
                  {
                  listen to GCCC;
                  }
      }
     end while;
```

Figure 5.1. The pseudo code of DDH-MAC.

5.3. Access Mechanism Implementation

Cognitive Radio is a special type of wireless network. The classical features of ad-hoc wireless networks could be deployed. In our research, we have used the distributed coordination function (DCF) which is based on the CSMA/CA mechanism. We have used IEEE 802.11b [212] as a benchmark to implement our protocol. The reasons for using IEEE 802.11b as a benchmark are:

- this model is extensively researched by the research community
- this model is widely deployed and implemented; and it has been widely accepted and used by the industry
- support is available for IEEE 802.11b modelling in many simulation tools such as OPNET [211], ns-2 [213] and OMNeT++ [214].
- most of the existing CR MAC protocols have been developed using the same 802.11b standard [38][191].

5.3.2 Detail of the Network Topology

In our network scenario, we have considered 4 to 30 numbers of SUs. Uniform distribution has been used to place the fixed wireless CR nodes over a simulation area of 150m^2. PU arrival has a Poisson distribution. Figure 5.2 provides the topological network scenario deployed for our proposed DDH-MAC protocol.

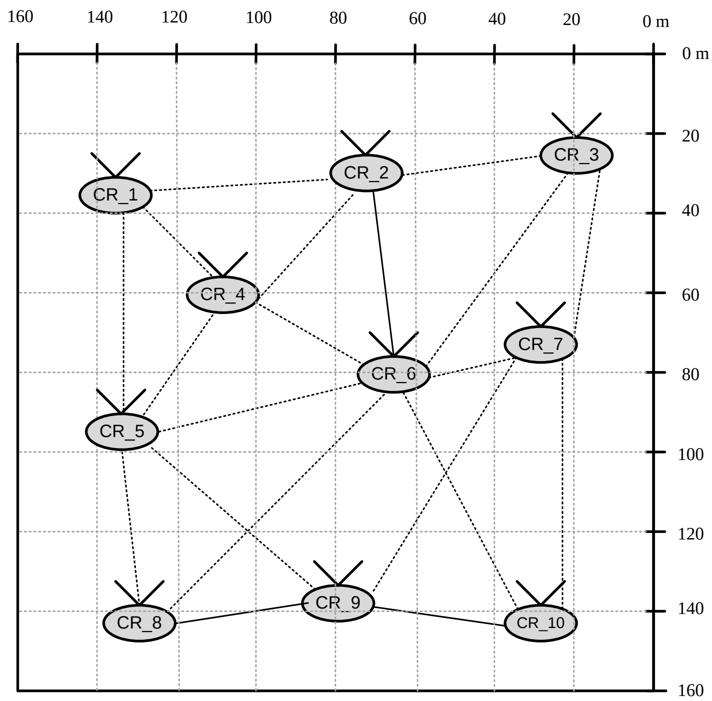


Figure 5.2. A network scenario of DDH-MAC protocol.

5.4. Results and Discussion

Performance is evaluated for the proposed DDH-MAC protocol by simulating a secondary users' session during which a primary signal appears in the band. In our simulation, there are 6 channels in total. Three of them are control channels i.e., GCCC, PCCH and BCCH, and the others are data channels. One of the channels is in the 2.4GHz spectrum band, and thus is not affected by the PU claim and is always available. The remaining data channels are occupied by the primary users with Poisson data arrival distribution. There are 4 pairs of CR nodes which always have data to transmit. A summary of the setting of simulation parameters are given in Table 5.1 below:

Table 5.1 Simulation Parameters for DDH-MAC Protocol.

Parameter	Assigned Value
Number of secondary users	4 - 30
Number of channels available for each SU	6
Payload	2048 Bytes
Channel capacity	11 Mbps
Simulation time	60s
Seed value	128
PHY layer Characteristics	DSSS
PU arrival rate	Poisson distribution
Slot Time	20 μs
SIFS	10 μs
DIFS	2 x slot time + SIFS
Transmission Switch time	$\leq$ 5 μs

In the next section, we discuss the performance evaluation for different parameters such throughput, traffic sent/received per unit time, queuing delay and collisions on the control channel.

5.4.1. Global Statistics

In this section, we discuss simulation experiments to investigate the system throughput of a CR network. The performance of DDH-MAC is dependent on several attributes such as the number of CR nodes, the number of vacant channels to be utilized by CR nodes and the probability of the primary user's claim. We first obtain the global statistics of the average throughput values for a CR network deploying the DDH-MAC protocol.

a) Throughput of DDH-MAC for different numbers of SUs

In our simulation experiment, there are 6 vacant channels available with each CR node. To make the model traceable, we consider the case where the number of vacant channels available with each CR node is greater than or equal to three (Equation 3.1). We further suppose that data packets of SUs arrive as a Poisson process with a mean arrival rate and that the size of each data packet is equal to 2048 Bytes. In the first experiment, we have used 4, 15 and 30 CR nodes. Note that in this case the total number of bits sent by a CR node is dependent on a few parameters. Firstly, the number of common channels available with each CR pair; secondly, the total number of CR users in the vicinity that are candidates for network resources; and lastly, the utilization of vacant channels by SUs in the CR network ($\mathbb{P}_{PU}$). This means that there could be different values of throughput for data transmission among SUs from time to time.

We first obtain the average traffic sent by each CR node for different numbers of available SUs in the vicinity. Figure 5.3 shows that the traffic sent is higher when there are fewer SUs. The average rate of traffic sent degrades when the numbers of SUs become higher. The obvious reason for this is utilization of six vacant channels by 4 SUs and utilization of the same number of vacant channels by 6 and 15 SUs. This implies that there is a contention between SUs which lead them to wait for certain white spaces to become available.

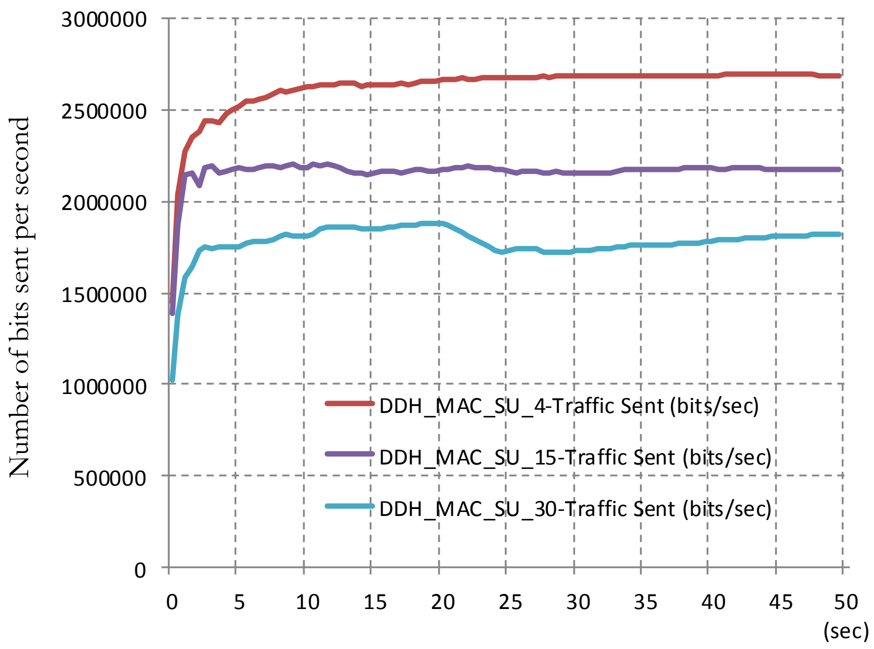


Figure 5.3. Average traffic sent against the simulation time of 50s, under CW_{min}= 32, and $\mathbb{P}_{PU}$ is set to 0.3, and when the number of SUs is set to 4, 15, and 30, the number of available white spaces is 6.

b) Throughput of DDH-MAC for different values of simulation time

In this experiment, we investigate the throughput of a non-saturated network for a fixed number of SUs in different values of simulation time. The parameters used to evaluate the DDH-MAC protocol have been summarized in Table 5.1. Let the number of contending SUs in the CR network be 4 and the number of white spaces with each SU be equal to 6. We then run our simulation for different time periods. The throughput (bits/sec) obtained is plotted in Figure 5.4. Note that throughput increases as the simulation time increases. This shows that with the passage of time the CR network is converged and nodes become aware of the control channel to be utilized. The highest value of throughput is obtained when the simulation is run for the longest period of time. We present the behaviour of this simulation experiment in two different forms of output that are provided by OPNET. These are the output based on average values that are obtained through the total simulation time called 'average', and the output that is drawn as they are retrieved during the simulation time, called 'as-is'. The output in both forms for this simulation experiment is plotted in Figure 5.3 and Figure 5.4 respectively.

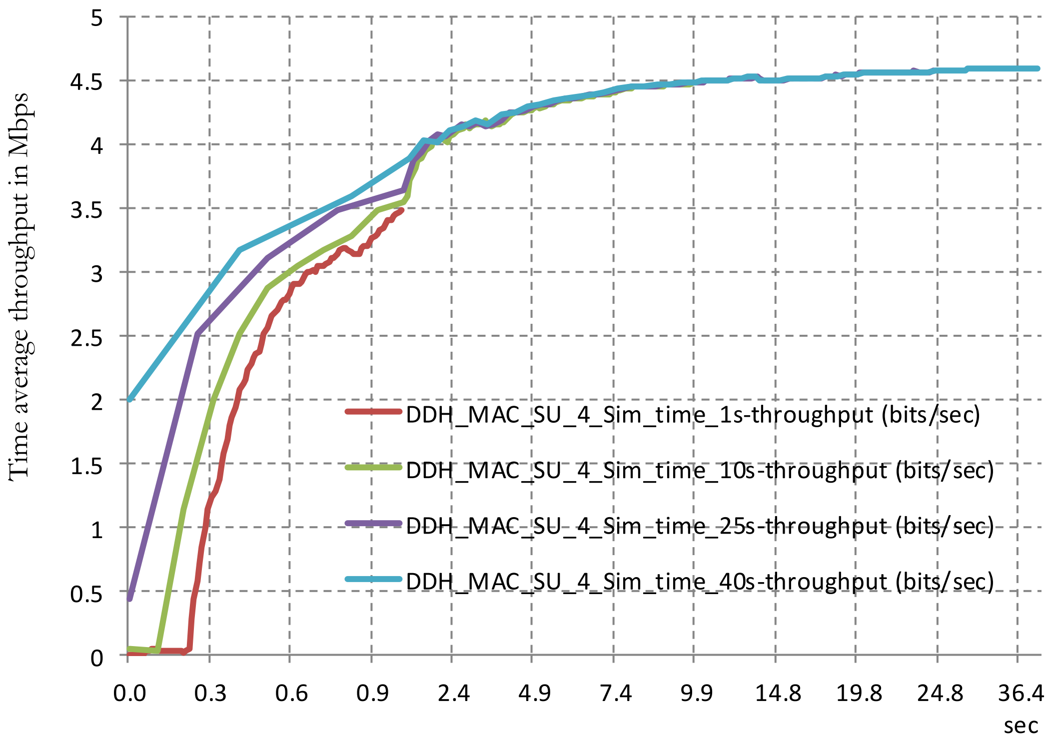


Figure 5.4. Average throughput against different lengths of simulation time, and under CW_{min}= 32, and $\mathbb{P}_{PU}$ is set to 0.5, and when the number of SUs is 4 and the number of white spaces with each SU is 6,

The 'as-is' output for the different lengths of simulation time for a fixed number of SUs and white spaces has been plotted in Figure 5.5 below. It can be observed that when the simulation is run for one second, the CR network is not fully converged and the average throughput varies between 0.5Mbps to 4.4Mbps. This is expected because with the passage of time, CR nodes become aware of the available network resources and the available CR nodes in the range. The throughput is heavily dependent on the time spent on launching the BF and the time spent to accomplish the DMCF/FCL/ACK three-way handshakes over the local control channel. It can be noted that each SU pair of nodes utilize one data channel at the same time, but a simultaneous data transmission on more than one data channel could significantly improve the throughput of the DDH-MAC protocol. However, simultaneous data transmission will require equipping each SU with additional sensors to detect the PU claim and will impose an additional hardware cost.

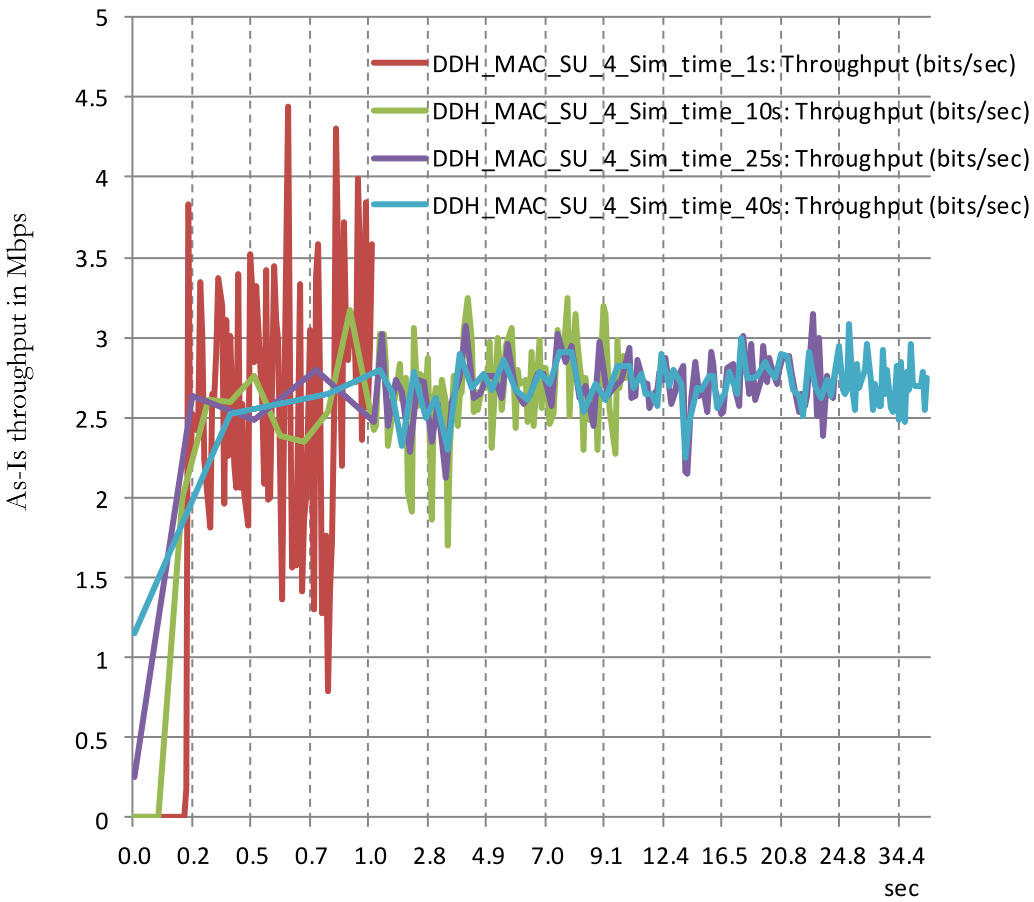


Figure 5.5. As-Is throughput of the DDH-MAC protocol against different lengths of simulation time, when CW_{min}= 32, and $\mathbb{P}_{PU}$ is set to 0.5, the number of SUs is 4 and the number of white spaces with each SU is 6.

5.4.2. Object Statistics

We extend our simulation experiments to investigate the behaviour of SUs when there are many other SUs also contending for network resources. In this experiment we consider two different scenarios for the DDH-MAC network. We first deploy a topology where there are 15 SUs all contending for network resources, and observe the throughput by calculating the average traffic sent during a simulation interval of 50 seconds. We then double the number of SUs to 30 in scenario 2, and all 30 CR nodes in this case are contending for the same network resources. Note that the total number of available white spaces will remain the same. The average throughput values in both scenarios have been plotted in Figure 5.6. It could be observed that the average throughput of a CR node, when there are 30 SUs, is half the average throughput when there are a total of 15 SUs contending in a CR network. This implies that all the CR nodes are resource hungry and are struggling to gain network resources. This also means that the performance of a CR network is not only constrained by the interference from PUs but is also subject to the contending SUs in the vicinity.

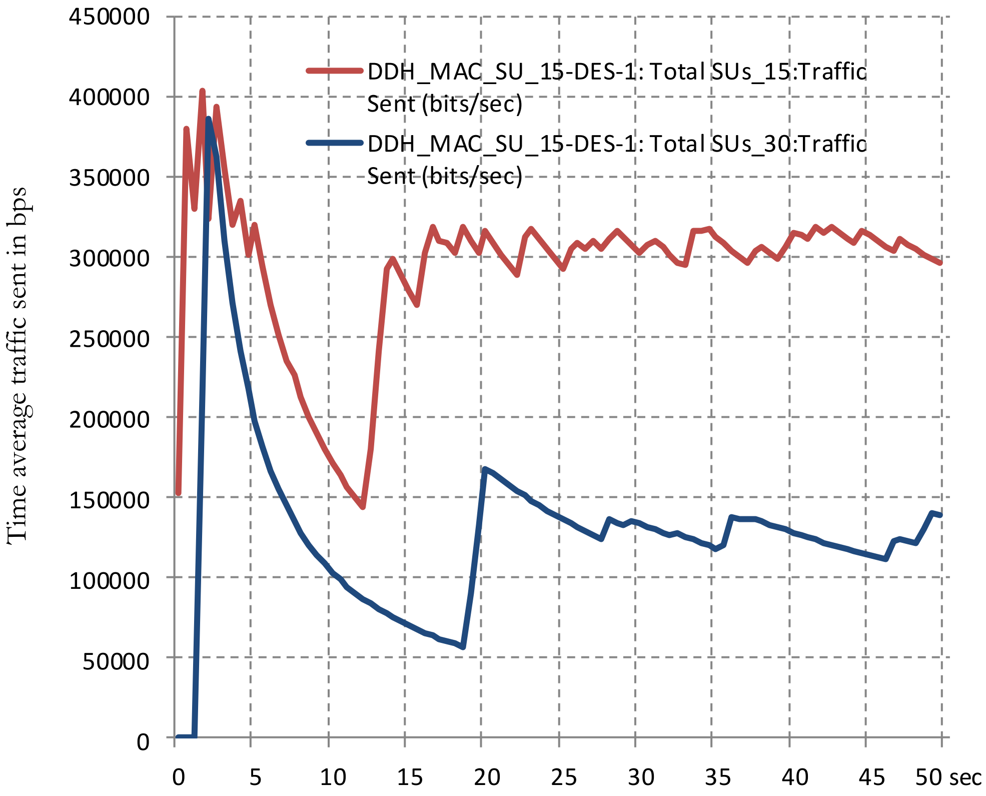


Figure 5.6. Average throughputs in bps of DDH-MAC protocol against two different values of SUs, when there are a fixed number of white spaces.

a) Delay of a Node in the DDH-MAC Protocol

This simulation experiment investigates the performance of the DDH-MAC protocol for queuing delay, for the case where the SUs always have data to transmit and may not have empty queues. After setting the optimal CW_{min} to be 256 for the case where numbers of SUs are 4, 10 and 30 respectively, we investigate the queuing delay. To make the model traceable, we randomly select a node and observe its average delay on a data channel. We observe that the queuing delay is below 25μs when the numbers of SUs are fixed to 4 and 10. For the same network resources when there are 30 SUs, the queuing delay fluctuates to 45μs in first few seconds of the network initialization and then settles to approx. 32μs after the network is converged. This difference on the values of queuing delay is expected because in this experiment we are assuming the saturated network case where there are other SUs contending for network resources. This queuing delay could be minimized if we consider the case where there is no network saturation and congestion, and the primary network resource, i.e. data channels, are available in large number.

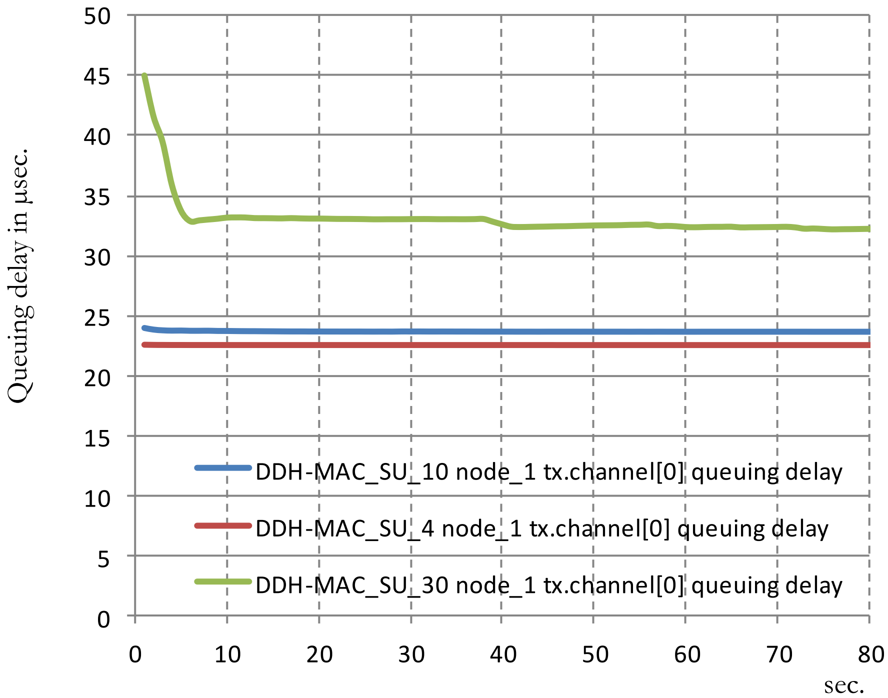


Figure 5.7. Average queuing delay of a node in the DDH-MAC protocol against simulation time, under the assumptions that there are six data channels available, that the network is saturated, that there is congestion amongst SUs, and that the numbers of SUs are set to minimum (4) and maximum (30).

b) The Number of Backoff Slots in DDH-MAC Protocol

We further extend our investigation of the DDH-MAC protocol and observe the behaviour of CR nodes for the average number of backoff slots for different numbers of SUs. We again consider the case of a saturated network where there is a contention for transmission amongst all SUs. The collision amongst SUs to access the local control channel is not unusual in the saturated network case. More precisely, all SUs have the same PCCH to exchange control information for subsequent data transmission to take place. As a result, the PCCH becomes saturated. That is, the more the number of SUs contending for PCCH, the higher will be the number of collisions and higher will be the computational cost and backoff. Figure 5.8 below reveals that the average number of backoff slots remains less than 5 when there are 4 SUs in the range. The number of backoff slots fluctuates between 2 to 23 when there is the maximum number of SUs, and it gradually settles as the simulation proceeds. This is obvious because when the simulation is launched, all SUs are contending for the same PCCH to dialogue control information, causing higher numbers of collisions and backoff slots.

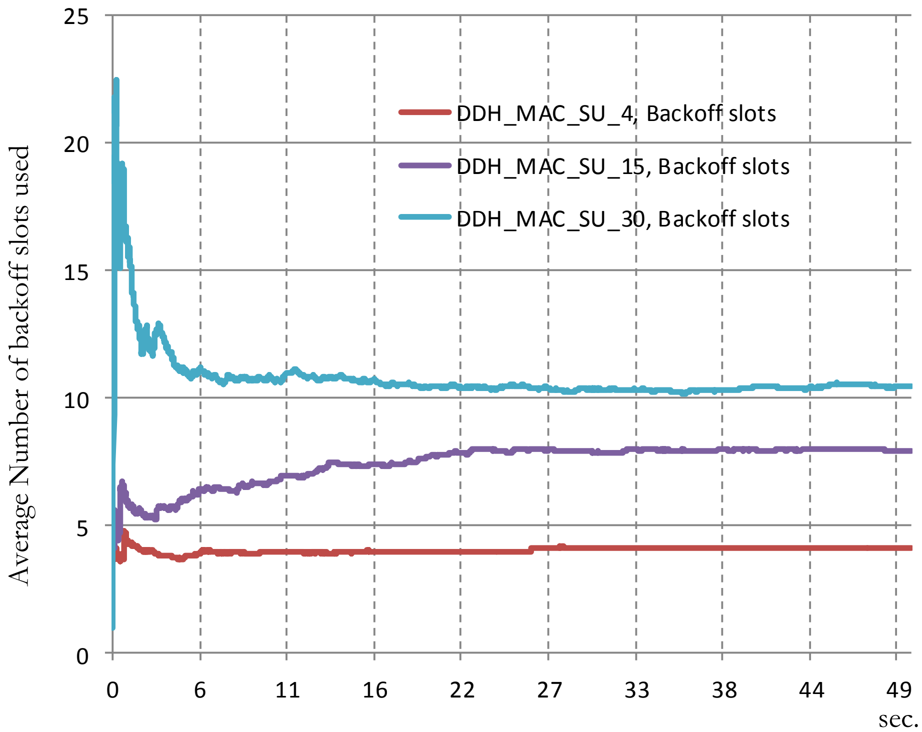


Figure 5.8. The number of backoff slots in the DDH-MAC protocol against the simulation time of 50 sec., there are total of six data channels available., the network is saturated, there is congestion amongst SUs and the numbers of SUs are set to minimum (4) and maximum (30).

c) Signal-to-noise Ratio in the DDH-MAC Protocol

We further proceed to the saturated network case and investigate the signal-to-noise ratio (SNR) on a fixed channel. Note that part 11 of the IEEE 802.11 standard [200] suggests the SNR to be in range of 1db-100db for data frames. Also, the SNR for received beacon frames ranges between 1db-100db. The DDH-MAC protocol launches the BF in the GCCC which is in the ISM band and is saturated by other unlicensed applications. So, a higher value of SNR for BF is expected. Using Equation 5.1 the SNR of the received data frames in db has been computed and plotted in Figure 5.9 for different numbers of SUs.

$$\mathrm{SNR}_{\mathrm{db}} = 10\log_{10}\left(\frac{P_{signal}}{P_{noise}}\right) = P_{\mathrm{signal,db}} - P_{\mathrm{noise,db}} \qquad (5.1)$$

The average values of SNR vary between 73.56db to 75.58db. This is expected because unlike classical wireless networks, if one pair of SUs starts data transmission, it will not stop another SU pair from transmitting data. The data transmission of one SU pair on a certain data channel can cause some interference to another SU pair on some other data channel. Ultimately, more pairs of SUs lead to a slightly higher value of SNR.

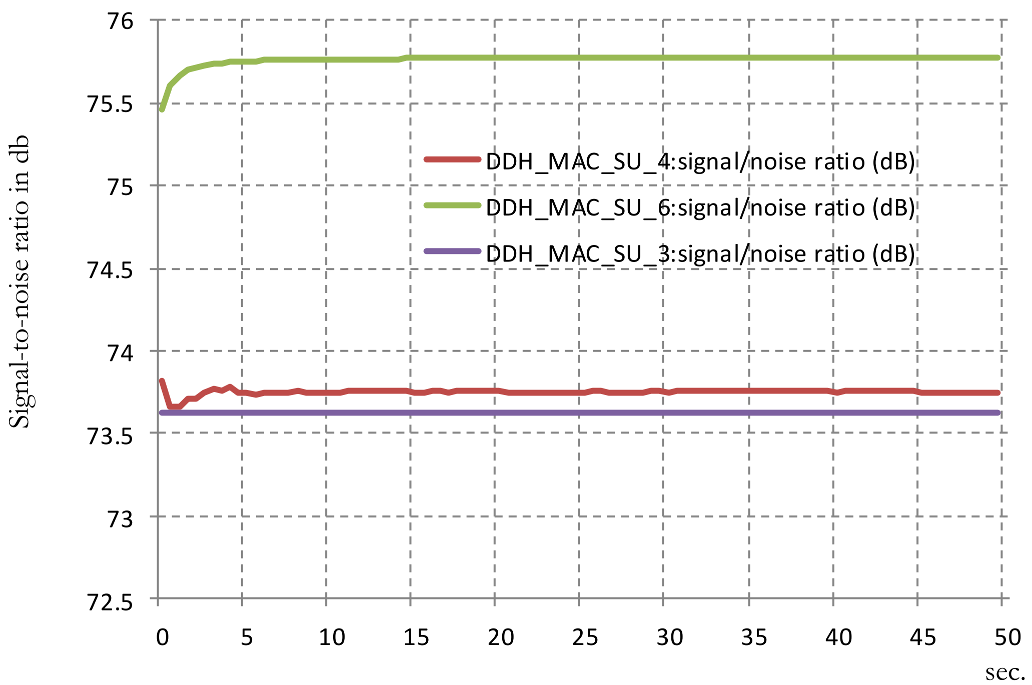


Figure 5.9. Average SNR in the DDH-MAC protocol against the simulation time, over a specific data channel when there are 3, 4 and 6 SUs, and when the data rate is 11Mbps and simulation is run for 50sec.

d) Collisions on the Primary Control Channel

Due to the nature of the CR technology, secondary nodes appear to be always striving for network resources. There is always contention amongst SUs to avail themselves of the transmission opportunities on priority bases. Secondary users always have data to transmit, for which they contend on the control channel. In this experiment, we elaborate this behaviour of SUs and observe the collisions on the control channel. Note that our simulation model is based on the traditional IEEE 802.11 DCF parameters which deploy the CSMA/CA function. Like a traditional wireless network, collisions are expected in DDH-MAC. We consider a network scenario which consists of 6 SUs, all contending to win the PCCH to start to exchange the control information. The scenario has been described in detail in Section 3.8 of Chapter 3. Figure 5.10 shows the collisions on the primary control channel when the network is initialized and all SUs have learnt about the newly established PCCH through the BF. This is expected because all SUs want to access the PCCH to start the exchange of control frames which has led to a few collisions on PCCH.

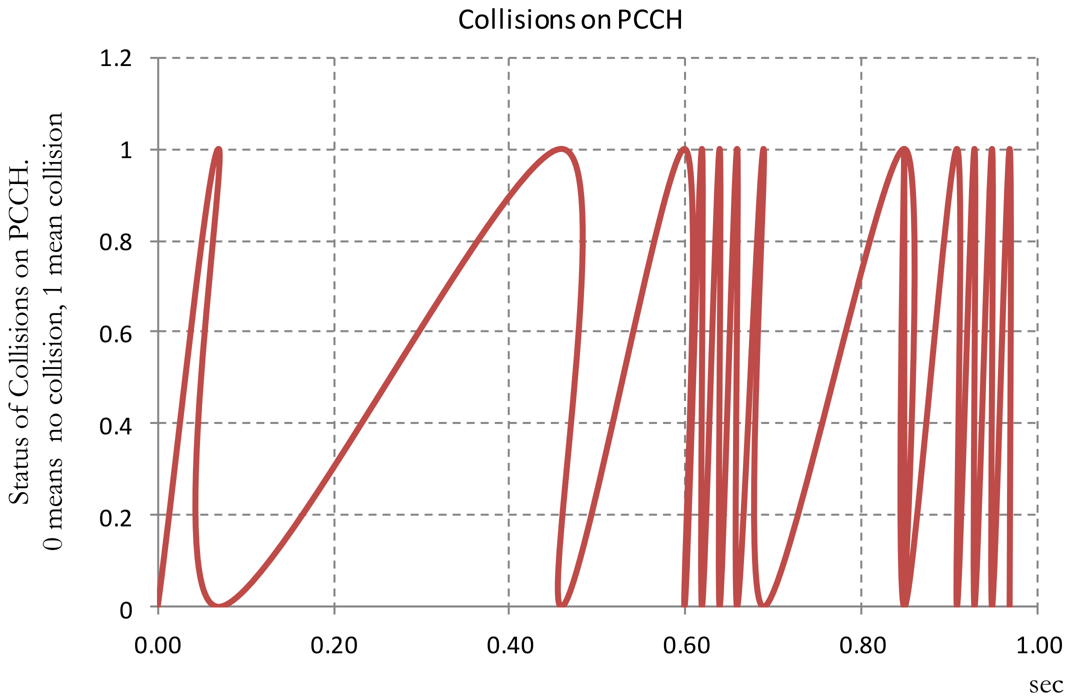


Figure 5.10. Collisions on the primary control channel when there are 6 SUs and the data rate is 11Mbps. Simulation is run for 10sec and the results are captured for the first second.

e) Evaluating DDH-MAC in Noisy Channel Conditions

We have evaluated our proposed DDH-MAC protocol in ideal channel conditions. Now, we extend our simulation and investigate the performance of DDH-MAC in noisy channel conditions. In this experiment we examine the impact of the queuing delay in DDH-MAC with ideal and noisy channel conditions. We simulate the external interference on a specific data channel. In Figure 5.11 we observe that the queuing delays have notably increased as the result of the noisy data channel. It is obvious that the noisy transmission medium causes the loss of data packets and increases the number of retransmissions. SUs holding data in the queue have to wait for slightly longer. The queuing delay in noisy channel conditions could be reduced by transmitting data packets at lower threshold values which can cause minimum interference to the data signal. Another way to minimize the queuing delay due to channel errors could be simultaneous transmission on more than one data channel. However, at this point we do not consider incorporating simultaneous data transmission on more than one data channel.

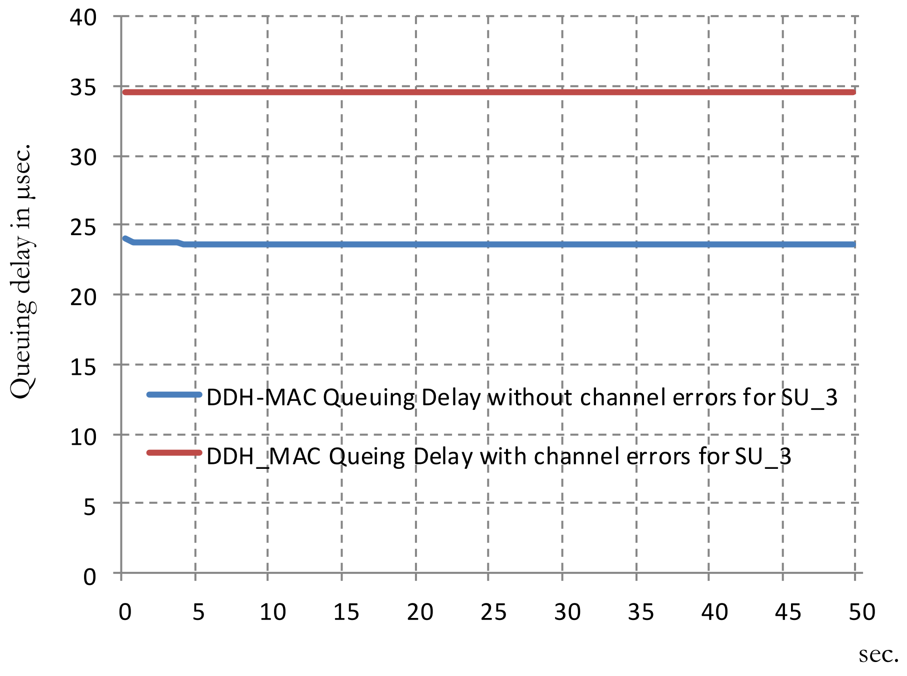


Figure 5.11. Queuing delay in DDH-MAC protocol, with and without channel errors when there are 3 SUs.

5.5. Performance Evaluation and Comparison

In this section, we compare the performance of our proposed DDH-MAC protocol with another CR MAC protocol. For our simulation experiments we compare the DDH-MAC protocol with the CREAM-MAC [38] protocol. This protocol is highly cited and is the latest in the literature. A performance comparison of the DDH-MAC protocol for the pre-transmission time and the analytical aggregated throughput has already been provided in Chapter 3 and Chapter 4 respectively. In this section, we present some simulation experiments to compare the performance of the DDH-MAC protocol for throughput, the number of frames exchanged as control information, and the number of frames exchanged when a PU claim is detected.

We evaluate our proposed DDH-MAC protocol in the saturated network case. Figure 5.11 shows the simulation results for DDH-MAC and CREAM-MAC protocols, given that the number of available data channels is 6 and that the total number of SUs is 10. Figure 5.12 shows the average throughput in bits/sec of a secondary user as the mean of the results of 20 simulations each running for 50 seconds. We observe that the throughput of DDH-MAC is higher and thus better when compared with other CR MAC protocols.

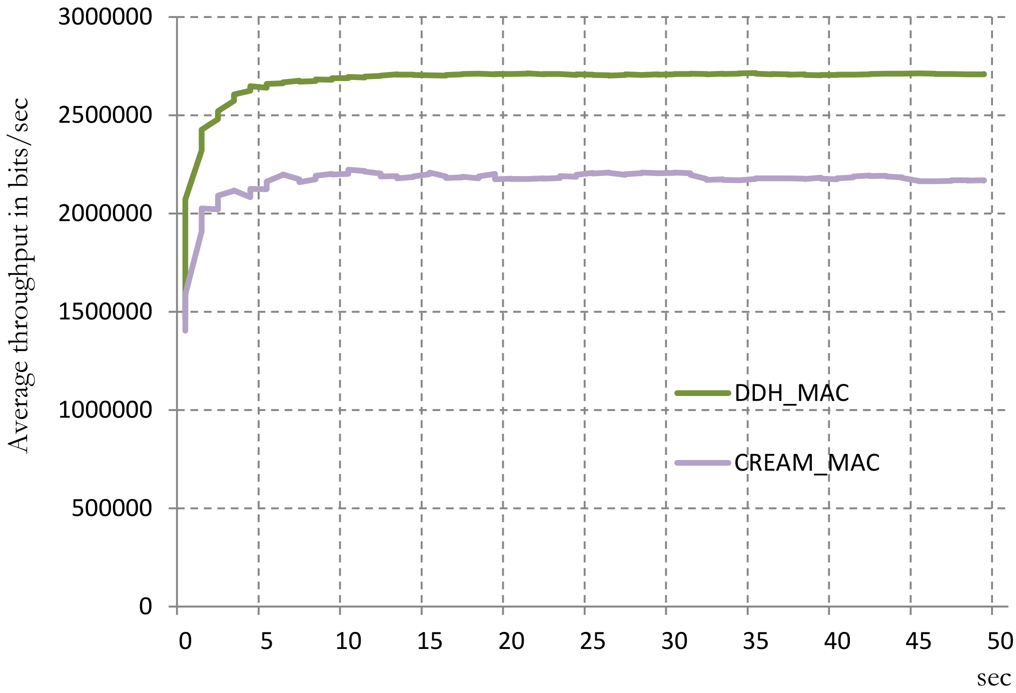


Figure 5.12. Performance comparison between DDH-MAC and CREAM-MAC on the average throughput in bits/sec of an SU pair on a data channel.

The very first reason for a higher throughput value of DDH-MAC is the pre-transmission time which heavily affects the performance of a CR MAC protocol. As discussed in detail in Chapter 3, DDH-MAC has the least amount of the pre-transmission time which is advantageous for DDH-MAC. The pre-transmission time itself depends on several elements. The most important is how easy it is to find and access a control channel.

The second reason for the higher throughput in DDH-MAC is re-dialoguing on control information if the primary control channel becomes unavailable. Nodes deploying the DDH-MAC protocol always have access to a backup control channel and can easily converge on the backup control channel by performing channel-switching. Switching from the primary control channel to the backup control channel consumes a time less than 5μs. However, the other CR protocols have to first find a common control channel, and then disseminate the information about the newly found control channel in the CR network, and last exchange control information.

The third reason for the DDH-MAC to outperform other CR MAC protocols is the number of control frames. Each data transaction amongst any pair of SUs is subject to successful exchange of control frames over the control channel. This control information is an overhead in the CR network and should be minimized in all possible ways. Since, CREAM-MAC protocol exchange 4 control frames for each data transmission, while DDH-MAC only exchanges 3 control frames, the overall throughput in DDH-MAC is greater.

In order to observe the behaviour of the CR MAC protocols while exchanging the control information, we ran another simulation experiment. Figure 5.13 presents the number of frames exchanged as control information on the control channel by DDH-MAC and CREAM-MAC protocols. We strongly believe that a smaller number of frames exchanged as control information can be beneficial in several aspects, e.g., i) it reduces the MAC layer overheads and thus CR nodes can quickly start data transmission; ii) nodes holding delay-sensitive data have to wait less, which will ultimately contribute towards better QoS; and iii) fewer number of control frames exchanged will make the CR network more secure and more energy efficient[4].

[4] We discuss both security and energy efficiency in CR networks in Chapter 6

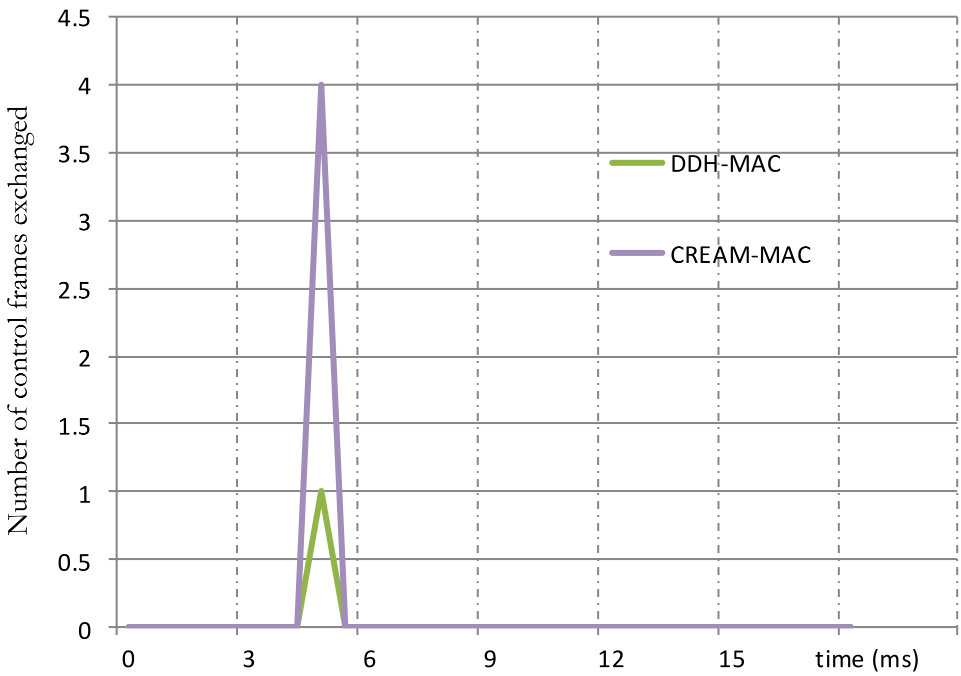


Figure 5.13. Performance comparison of DDH-MAC with CREAM-MAC on the number of control frames re-exchanged when the control channel becomes unavailable.

We further extend our experiment on performance evaluation and comparison by investigating the response of SUs when a PU claim is sensed on a control channel and thus the control channel becomes unavailable. Also, the CR node that first detects the PU claim on the control channel is unable to propagate the information about unavailability of control channel by any means. In this case, all other CR MAC protocols have to re-exchange the entire configuration dialogue and all frames need to be retransmitted. However, DDH-MAC is specially designed to handle this situation, and any node which first detects the PU occupancy on a control channel will launch a single frame which lets all CR nodes in the vicinity start using the backup control channel. Hence, there is no need to find the control channel and then re-dialogue the whole control information.

Clearly, DDH-MAC has to broadcast only one management frame to let other CR nodes know to switch onto the BCCH which has already been established and all CR nodes are aware of, while the protocol design of CREAM-MAC has to broadcast 4 control frames.

We also examine the performance of DDH-MAC in terms of queuing delay with another protocol and simulate an experiment when a PU claim has been sensed. By comparison, the re-exchange of the entire configuration dialogue forces the SUs deploying CREAM-MAC protocol to wait for longer. We capture this scenario in our simulation experiment and plot the results obtained in Figure 5.14. It can be clearly observed that more time spent re-exchanging the control information results in high values of queuing delay.

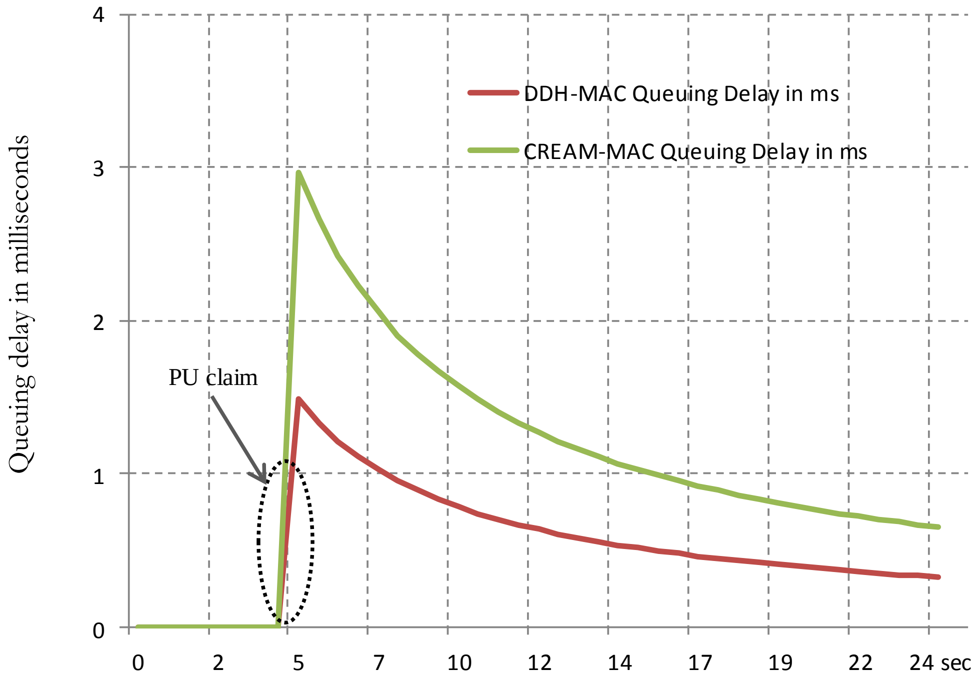


Figure 5.14. Performance comparison between DDH-MAC and CREAM-MAC on the queuing delay in milliseconds when a control channel becomes unavailable

5.6. Verifying Analytical and Simulation Results

The parameters used to analytically and experimentally evaluate the DDH-MAC protocol are summarized in Table 4.4 and Table 5.1. In this section we verify the consistency of our analytical model and simulation model.

5.6.1. The Aggregated Throughput Against PU Interference Probability

We first investigate the aggregated throughput for the saturation network case. Let the number of Tx with each SU be 2, and the channel utilization Ř be equal to 11Mbps. Using Equation 4.12, we plot the aggregated throughput against the PU interference probability δ in Figure 5.15. The experiment is run for two different numbers of SU, i.e., when SU is equal to 15 and 30 respectively.

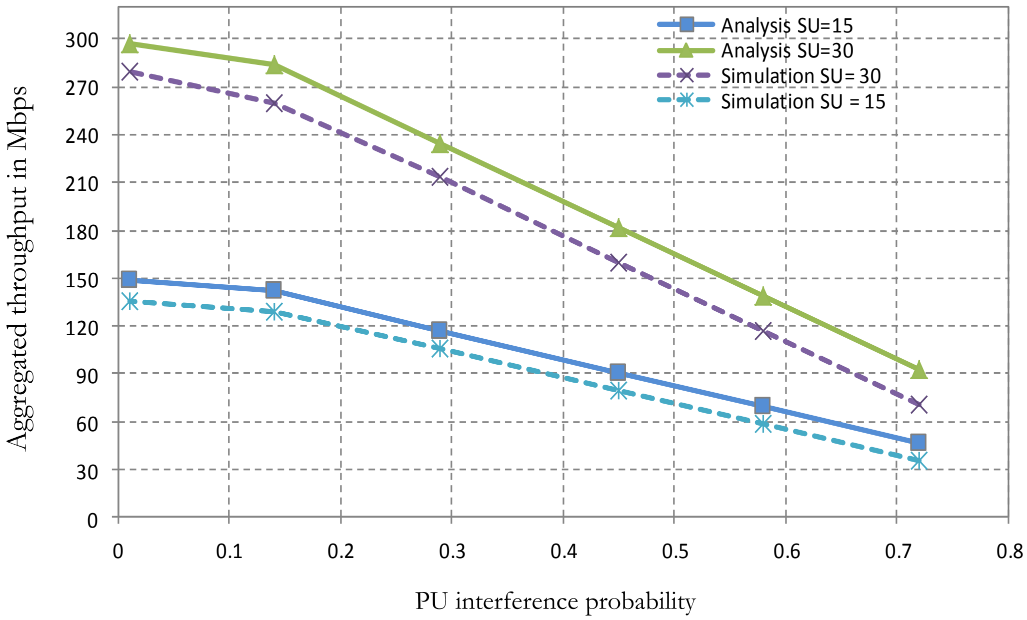


Figure 5.15. Aggregated throughput in analytical analysis and simulation experiment for two different numbers of SUs against the PU interference probability (δ), under the assumption that the number of transceivers is 2, that the channel data rate has been set to 11Mbps, and that the number of available data channels is 15.

The highest aggregated throughput of approximately 300Mbps is achieved when there is no PU interference and thus SUs can fully utilize all the available data channels. The aggregated throughput for the two numbers of SUs degrades linearly as the PU is more likely to claim the licensed data channels. This is expected because, given that there are sufficient licensed channels available, the aggregated throughput only depends on the δ. The same applies to the simulation experiment where we know the number of contending SUs in advance and thus we select the optimal value of CW_{min} which results in the highest throughput. For different numbers of SUs, the CW_{min} could be adjusted accordingly. This will help achieve the optimal performance.

5.6.2. The Aggregated Throughput against the Number of Available Data Channels

After setting the number of SUs equal to 15 and 30, we use Equation 4.12 to get the numerical results of the aggregated throughput against the number of available white spaces. From Figure 5.16, it can be observed that if fewer data channels are shared amongst more SUs, the aggregate throughput (Γ) linearly decreases, which implies that the SUs get less transmission opportunities to communicate with other CR nodes in the vicinity. Note that in this experiment we are considering the unavailability of the data channel due to their usage by other SUs. Another reason for DDH-MAC to achieve such a high throughput is the number of transceivers which continuously monitor any network changes through rapidly scanning the control channel while simultaneously taking opportunities for data transmission. The aggregated throughput for both the mathematical and simulation experiments reveals that DDH-MAC is resilient against any abrupt network changes due to a PU claim on either a control channel or a data channel.

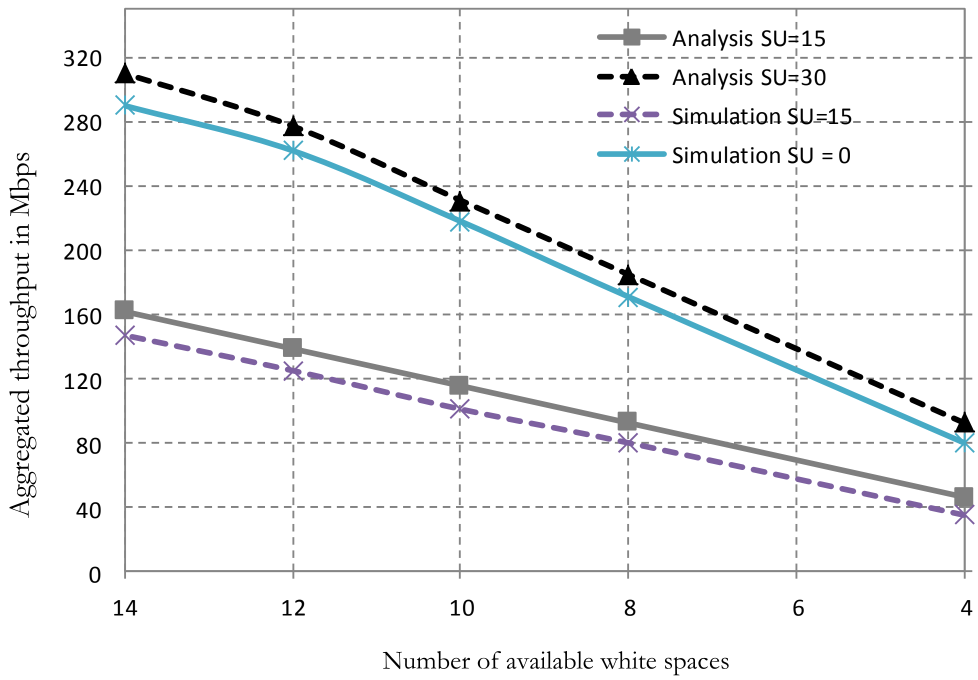


Figure 5.16. Aggregated throughput in analytical analysis and simulation experiment for two different numbers of SUs against the PU interference probability (δ), under the assumption that the number of transceivers is 2. That the channel data rate has been set to 11Mbps, and that the number of available data channels is 15.

5.6.3. Mathematical and Simulation Results of Aggregated Throughput with and without Noisy Channel Conditions

In our last experiment, we combine both the simulation and numerical results on the aggregated throughput against number of white spaces. We consider a non-saturated network case and obtain the aggregated throughput of 4 SUs with ideal channel conditions and without ideal channel conditions against the SU transmission probability ($\mathbb{P}_{CF}$) on the control channel. In this experiment, we investigate the SUs' data transmission after network convergence. The throughput performance is shown in Figure 5.17. Here, we assume that SUs have sufficient data channels and observe that aggregated throughput rapidly increases with the increase of SU transmission probability. This means that the network is fully converged and the SU pair are exchanging data on available and agreed upon white spaces. The aggregated throughput as reflected from both the mathematical result and the simulation result decreases as channel errors are introduced in the network. Unlike other CR MAC protocols, our scheme has low usage of the GCCC and thus improves the over-all network performance. Delivering the control information over the local control channel, which is less saturated, is a feasible solution to improve the aggregated throughput. Of course a lower number of SUs in the network is another reason for higher aggregated throughput values.

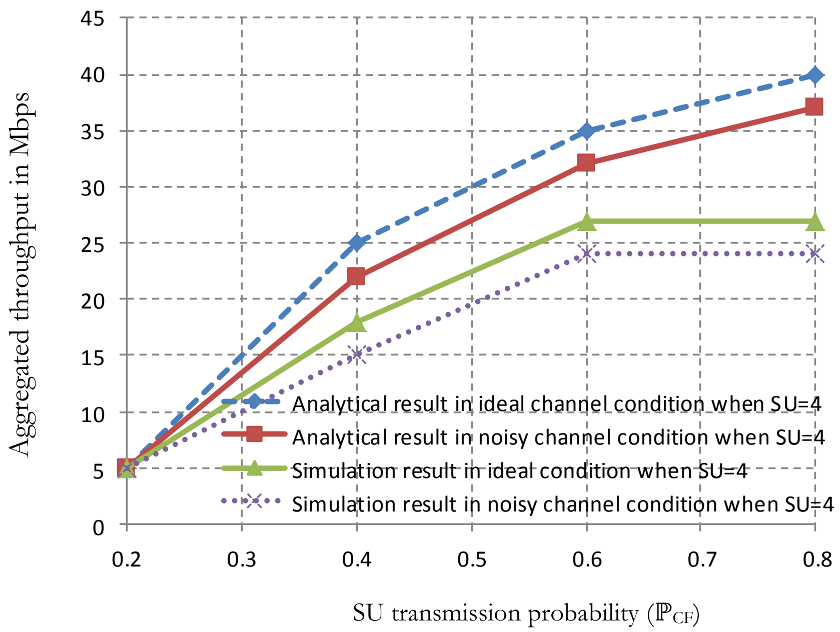


Figure 5.17. Aggregated throughput in analytical analysis and simulation experiment for 4-SUs against the SU transmission probability ($\mathbb{P}_{CF}$), under the assumption that the number of transceivers is 2, that the channel data rate has been set to 11Mbps, and that the number of available data channels is 6.

5.7. Summary

In this chapter, we developed simulation experiments to investigate the system throughput of a CR network, and a few other elements that impact the system performance. We have simulated different scenarios under both the saturated network case and non-saturated network case. We first examine the performance of DDH-MAC for parameters such as throughput, queuing delay, signal-to-noise ratio, and collisions on the control channel. We then compare the DDH-MAC protocol with the CREAM-MAC protocol for performance parameters such as throughput, the number of packets exchanged as control information, and the behaviour of each MAC protocol if a PU claim is sensed. We then extend our experiments by validating the simulation results with the mathematical results. We also examine the performance of DDH-MAC protocol under introduced errors on channels, and observe that the system throughput is directly proportional to the channel conditions.

We observe that in some cases, the compared protocols can achieve better throughput performance. This is because these protocols set an unrealistic assumption that a control channel is always available and reliable. However, this assumption of perfection does not reflect the real performance of a CR network. The simulation results have revealed that the performance of a CR MAC protocol is heavily dependent on the successful exchange of control information which can only be carried out on a control channel. Moreover, multiple control channels can significantly improve the network performance and the nodes deploying the DDH-MAC protocol can always have access to more than one control channel.

Chapter 6: Performance Enhancement of DDH-MAC Protocol

6.1. Introduction

DDH-MAC is a novel CR MAC protocol that efficiently and smartly makes use of the GCCC to initialize the operation of launching the BF. The CR nodes, after receiving the BF, switch to the PCCH and adjust their transmission parameters to use the BCCH if there is a PU claim. This unique feature of partially using the GCCC and then switching to the PCCH or further to the BCCH (if there is a PU occupancy) provides the DDH-MAC protocol with a few encouraging features in security, energy efficiency and QoS. CR nodes deploying the proposed MAC protocol always have access to one control channel. There are two most important functions of a CR MAC protocol: i) finding and agreeing upon a common control channel that is secure, reliable and always available; and ii) transmitting the control information over the control channel. Any subsequent data transmission amongst CR nodes is subject to a successful FCL transaction on a well-known, available and secure common control channel. DDH-MAC has been specially designed to perform the functionalities mentioned above. In this chapter, we further improve the performance of our proposed DDH-MAC protocol by incorporating new features which make DDH-MAC more efficient, more energy effective, and more secure and resilient against security threats and vulnerabilities. The performance optimization of DDH-MAC is discussed below.

6.2. Incorporating Security into DDH-MAC

The cognitive radio technology that consists of nodes, architecture and control strategies, appeared to be an efficient solution for heterogeneous networks. However, this leads to security issues because the same security standards could not be applied in all heterogeneous networks. The CR technology merges a core network with access networks in a heterogeneous environment. Wireless standards have different security strategies. For example, in a WLAN and a personal area network (PAN), the only mechanism to incorporate the security is identity authentication. In GSM [84], WiMAX [85], WCDMA [86] and WCDMA2000 [87], the legality of terminals and users is controlled by an authentication process from base station and SIM card authentication. The differences between technologies used for cognitive radio networks and for existing wireless networks make the security incorporation a difficult question. The adaptive nature of cognitive radio technology imposes additional complications and introduces new challenges. For example, an attacker may pretend to be a secondary user and intercept without authentication the FCL by a false claim of being an SU, or in another case, it can mimic the behaviour of a licensed user and then increase the probability of false alarm detection. This is a special type of denial-of-service (DoS) attack in CR networks and is commonly known as the primary user emulation (PUE) attack [215] [216] [217]. Another type of attack specific to CR networks is the jamming attack [218] that can push the nodes in the vicinity to select a specific spectrum band for control information exchange where another attacker seizes the control information.

Physical layer techniques have been intensively focused in recent studies to detect the anomalous usage of spectrum [216][217][219][220]. The detection of an unauthorized usage of the spectrum in zone-based networks has been investigated in [219]. Authorized users do not impose interference on each other because at most one authorized user, i.e., either none or one authorized user, can exist in each network zone. Received signal powers of unknown signals are measured to detect unauthorized spectrum usage. Chen *et al* [216] have proposed a mechanism to verify a transmitter which assumes that the Primary Signal Transmitter (PST) location is known in advance and that a PUE attacker cannot duplicate the energy of the legitimate signal. If the suspicious signal is being transmitted outside the range of PST, it is considered as a PUE attack. If the transmission of the suspicious signal is received in the PST vicinity, energy detection is used to authenticate the signal. A protocol for mitigating PUE attacks has been proposed in [221] where each SU uses a centralized spectrum decision to decrease the probability of false alarm. Goergen *et al* [222] present a method in which a watermark is added to the PU signal. The CR nodes retrieve the watermark to authenticate the transmitted signal. These tasks make use of the physical layer information only, and either PU signals are modified or prior information about the PU is required to detect the PUE and jamming attacks. Jamming attacks have also been studied in several recent studies[220][223][224]. A primary number sequence code has been used by the scheme proposed in [220], in which a jammer could not compute which channel to jam at a given time. A game theoretic approach is presented in [224] to model the jamming and its contravention in cognitive radio multichannel networks. One-stage and multi-stage games are obtained by a Nash equilibrium and a stochastic control strategy respectively. Xu *et al* [225] discuss signal measurement for jammer detection and argue that smart jamming attacks are a new trend in the CR networks and new artefacts need to be developed to efficiently address these issues.

To summarize, the work published so far mostly emphasizes the physical layer to address the security vulnerabilities in cognitive radio networks. MAC layer security for cognitive radio networks has been investigated only in [102]. It is believed that, apart from the security measurements at the physical layer, mechanisms must be derived to incorporate the security at MAC layer in the CR networks. This motivates us to incorporate security at multiple levels in the DDH-MAC protocol. The next section discusses the framework of the proposed security model for CR networks.

DDH-MAC has a novel design of MAC protocol for CRNs which not only benefits from the anytime license-free availability of the GCCC but also enjoys the secure communication by privately exchanging the FCL over one of the white spaces. The best features of the decentralized family of MAC protocols have been combined to make the proposed hybrid protocol efficient, dynamic, and decentralized. A detailed operation of the protocol, including a 2-level selection process, has already been presented in Section 3.4. The protocol takes into account different case scenarios in the cognitive radio environment and tunes its parameters efficiently and intelligently according to the current situation of the network, which makes the protocol adaptive, secure and energy efficient.

6.3. A Multi-Level Security Framework for DDH-MAC

The proposed protocol provides multiple levels of security. Each level provides an unique feature which, altogether with other features from other levels, makes the proposed protocol more secure and less vulnerable against threats.

6.3.1. Level 1-Encrypting the BF

As mentioned earlier, DDH-MAC makes a partial use of the GCCC which is in the ISM band and publicly available to all wireless applications. The free public availability of GCCC can make it more exposed to security vulnerabilities and threats. Since DDH-MAC also uses the GCCC, it is very important to secure the GCCC transactions. The first level of security is achieved by encrypting the BF before launching it in the GCCC. We have used bits transposition cryptography [226][227], which is a rather simple but efficient encryption scheme. The block cipher is encrypted by inverting the bits in the BF. The information about the PCCH and the BCCH is contained in the BF (1 byte is used to represent the channel ID of the PCCH and another 1 byte to represent the BCCH). Suppose that the PCCH is represented by a channel ID whose binary code is “10110011”. Using the bits transposition cryptography, the bits will be inverted and the encrypted cipher which will read as “01001100” will be launched. The receivers of the BF, which are the CR nodes deploying the DDH-MAC protocol, will use the relevant decryption scheme to read the information about the PCCH and the BCCH. The relevant decryption scheme is only known to the legitimate DDH-MAC nodes. Suppose, the BF has been sniffed and read by a malicious user who can easily access the GCCC. In this case, the malicious user will retrieve a channel ID for the PCCH and the BCCH which is different from the original one.

6.3.2. Level 2-Secure FCL Transaction

Most of the reported CR protocols [38][103][104][127][128] exchange the FCL through the GCCC which is publically available to everyone and more prone to security vulnerabilities and threats. DDH-MAC uses one of the white spaces as the PCCH and exchanges the FCL secretly on the chosen control channel which is only known to the legitimate CR nodes in the vicinity. Exchanging the FCL not in the GCCC but secretly through a white space which is known only to CR nodes after performing scanning and searching, adds another security level which is not available in other CR MAC protocols.

6.3.3. Level 3-Inclusion of Time Stamp in Data Transmission

The man-in-the-middle attack is not unusual in the cognitive radio environment and any type of information could be retrieved by the intruders. The DDH-MAC smartly and efficiently addresses the criticality of the situation by adding a time stamp in each data transmission. Data is expected to reach the destination in a specified time. An estimation about the data arrival time helps protect the data and ensures the integrity of data. If the data does not reach the intended recipient in a specified time, with an unusual amount of delay (considering any reasonable delays such as the propagation delay and processing delay), means that the integrity of the data could have been compromised and therefore the data is no longer trustworthy.

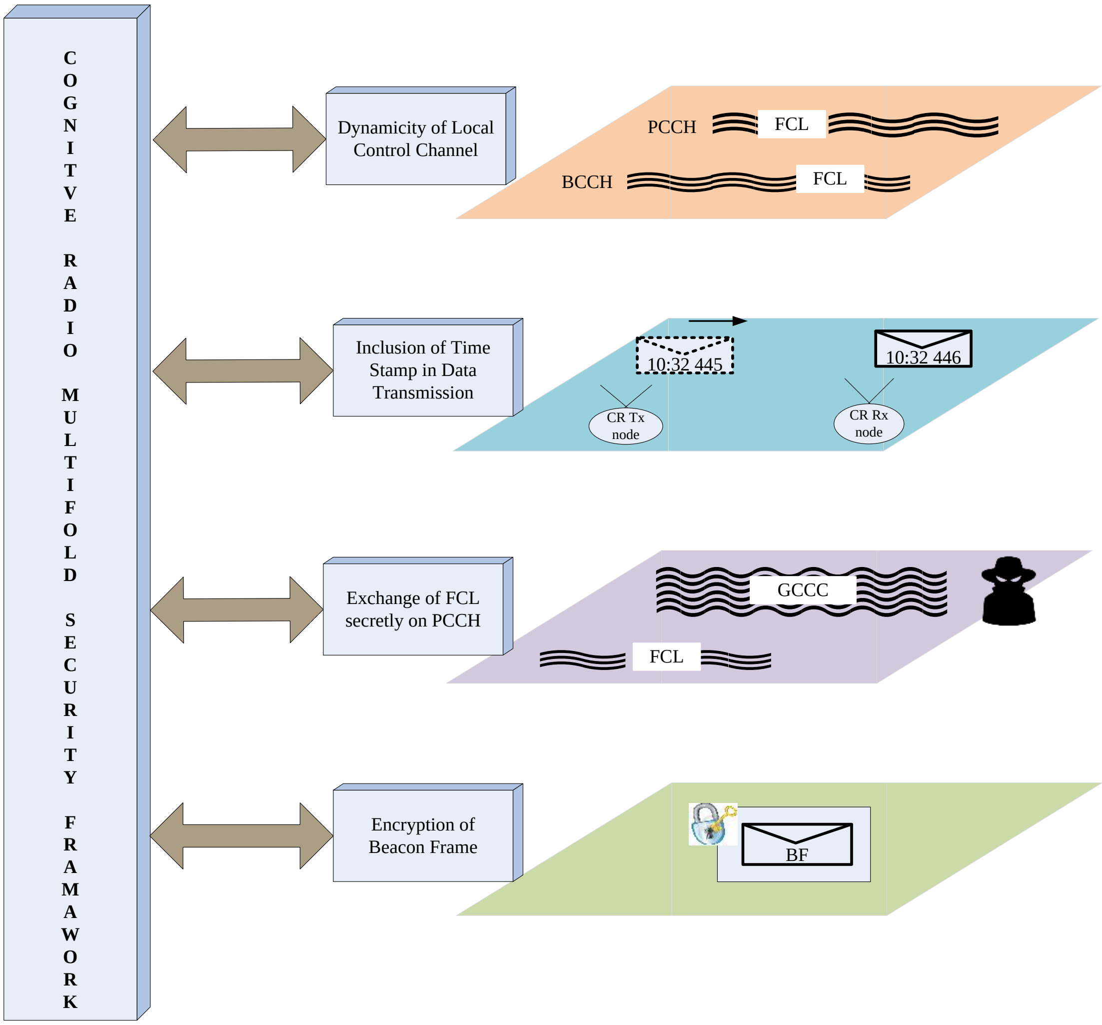


Figure 6.1: The DDH-MAC multi-fold security framework for CR networks.

6.3.4. Level 4-Dynamicity of the Control Channel

Since the DDH-MAC uses one of the white spaces as the PCCH and another as the BCCH, the PU claim on these local control channels could happen at any time. If the PCCH has been reclaimed by the PU, the CR nodes implementing the DDH-MAC will switch to the BCCH to continue exchanging control information. If, in the worst case, the BCCH has also been reclaimed by the PU, then nodes will have to switch to the GCCC to search for any BF. The PU claim on the PCCH and the BCCH is beneficial to DDH-MAC and it actually provides another level of security to the CR nodes. An attacker targeting the PCCH/BCCH through smart jamming and PUE attacks will have to re-compile the attack strategy from time to time. The dynamicity of control channels (PCCH/BCCH) offers the CR nodes the highest level of security.

6.4. Control Channel Efficiency in DDH-MAC

The CR technology aims to integrate the human intelligence in radio devices by making them aware, adaptive, smart, and decision making capable. In order to effectively perform the CR functionality, nodes must interact and cooperate with one another. This cooperation amongst CR nodes could only be established if they are adept at exchanging the knowledge learnt with other nodes on a well-known and centrally available common control channel. Robustness and security of the control channel are the two most challenging parameters of a CR MAC protocol. The existing design constraints for the common control channel are not smart enough to cope with the real time demands on cognitive radios. For example, there is no SUs' last resort in case of a PU occupancy on control channel. Also, if one control channel design category is used, the benefits of other categories could not be utilized. In other words, avoiding the drawbacks of one category creates certain limitations in the selected category.

To make cognitive radio fully functional and equipped to fulfil the real time demands of a cognitive radio network, we have proposed a novel MAC scheme which integrates the best features of all design strategies for control channel. The proposed scheme is robust against PU occupancy. The security of the proposed scheme has already been discussed in Section 5.2. We will briefly review some of the features of the control channel that make the proposed scheme more efficient.

6.4.1. Availability of More than One Control Channel

Equipping the CR with more than one control channel is a novel idea which has not been previously discussed. The existing literature either uses an assumed control channel, or spends more time on finding and converging on a local control channel. The CR network deploying our proposed scheme will have access to more than one control channel simultaneously. The access to any control channel by any CR node is without obligation and nodes can operate and cooperate independently. Also, the network initialization is not subject to any parent node or master node and the operation can be performed by any node instantly.

a) Control Channel GCCC

Due to the nature of the ISM band, the GCCC is primarily available to all CR nodes. In our scheme, we only access the GCCC for BF transmission. Apart from the BF, all the communication is established over the local channels (control/data). The GCCC is scanned and searched by other CR nodes in a few extreme cases. For example, when network initialization is required, GCCC will be used to launch a BF by a CR node, and when there is a worst case scenario where both PCCH and BCCH are occupied, GCCC would be used to launch a new BF containing the information about the newly established PCCH and BCCH.

b) Control Channel PCCH

The core part of DDH-MAC protocol is the PCCH. Once the network is initialized, the CR nodes can dialogue the control information over the control channel. Any communication which is carried out on the PCCH is overheard by all CR nodes. This keeps all the nodes well synchronized about network adaptions. Nodes must have access to the PCCH in order to become part of the DDH-MAC functionality.

c) Control Channel BCCH

To back up the core functionality of DDH-MAC, a BCCH is always there as a standby control channel. If there is a claim on the PCCH, nodes remain calm and consistent, and simply switch to the BCCH and resume the exchange of control information. We optimize the performance of DDH-MAC by discussing the following two extreme cases:

Case I: Both the PCCH and the BCCH are amongst the white spaces sensed by the CR nodes. It is not unusual for a PU to arrive at any time, and in this circumstance, a PU activity is always sensed prior to switching onto the PCCH or the BCCH. We have enhanced the functionality of DDH-MAC by adding the PU-activity-sensing feature. A sensor is added that continuously senses the control channel and reports any PU claims. Equipping this feature in DDH-MAC enhances the overall performance as nodes will spend less time in re-negotiations. This feature is depicted in Figure 6.2.

Case II: As previously discussed in Chapter 3 Section 3.4.2, nodes will switch to the BCCH if there is a PU claim on the PCCH. What if the BCCH is claimed by a PU before a PU claim is made on the PCCH? To address this issue, we modify the framework of the DDH-MAC protocol. The first node in DDH-MAC is responsible for launching the BF and then periodically broadcasting the BF in GCCC at regular intervals. This node is assigned with an additional operation, i.e., observing the PU activity on the BCCH when it is not transmitting the copy of the BF in the GCCC. If some PU activity is sensed on the BCCH, this node will quickly select another white space as a BCCH and broadcast an updated copy of the BF in the GCCC which will be received by all CR nodes in the vicinity. The receiving nodes will eventually update the information about the newly established BCCH and will resume the exchange of control information as usual.

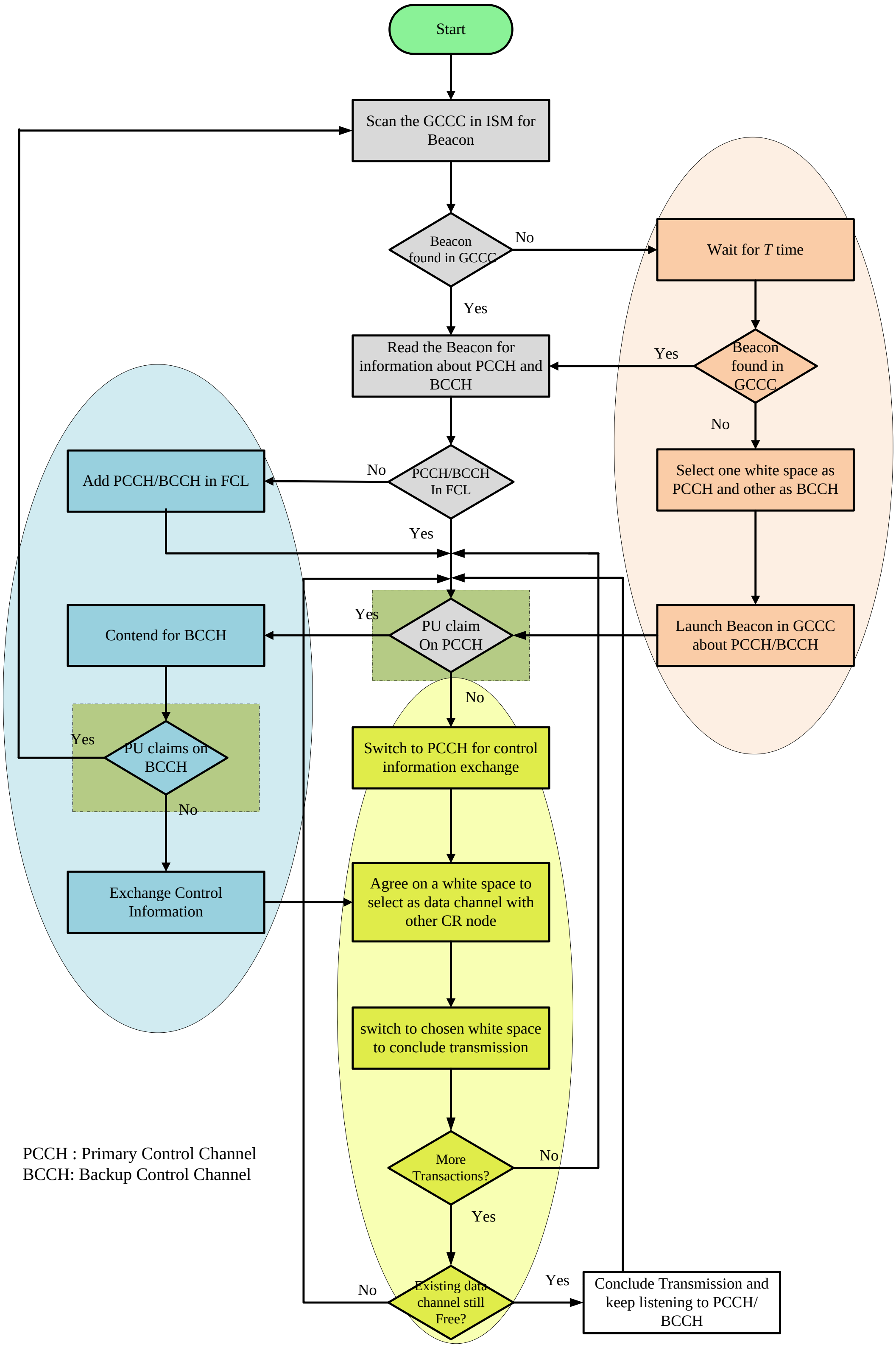


Figure 6.2. Optimized flow chart of DDH-MAC.

6.5. Energy Efficiency in DDH-MAC

The mobile nature of wireless devices always imposes new challenges for researchers and developers. One of the challenges that all wireless technologies face is energy efficiency. It is inconvenient for wireless devices to replace or recharge the battery. The development of a wider range of applications for wireless devices is making the issue of energy efficiency more challenging. Saving mobile energy has become more demanding in a cognitive radio network, which is a special type of wireless network, where nodes consume a lot of energy in scanning and searching the environment. In this section, we discuss the performance optimization of the DDH-MAC protocol by making our proposed scheme energy efficient.

6.5.1. A Multi-mode Energy Efficiency Model for DDH-MAC

Different techniques have been proposed to minimize energy consumption in wireless ad-hoc networks[228][229]. These schemes aim to save energy at the physical layer by using different techniques such as turning the transceivers into sleep mode if they are idle, or using the TDMA scheme to avoid collisions at the physical layer. A few CR protocols have been proposed that introduce energy saving at the MAC layer [230] [231][232]. DDH-MAC has been specially designed to save energy in the following ways.

a) Reducing the Number of Control Frames

Every data transaction in a CR network is constrained by successful exchange of control information. Most of the protocols exchange a minimum of 4 control frames to dialogue the control information [38][113][127]. The F^2-MAC protocol presented in [42], exchanges the highest number of frames as control information in a CR network. DDH-MAC saves a significant amount of energy by exchanging only three MAC frames as control information. The framework of DDH-MAC has been designed to achieve the same functionality without compromising the effectiveness of cognitive behaviours by exchanging three frames of DMCF, FCL and ACK prior to any data transaction.

b) Minimizing Size of Control Frames

We believe that energy efficiency could also be better achieved if the sizes of control frames are reduced. This could be achieved by avoiding unnecessary fields in the control frames. The CR MAC protocols [38][42][127], used for the comparison and performance evaluation, emphasize the data transmission and ignore the very important phase of the CR functionality, i.e. exchanging control information. These protocols therefore not only take a high amount of time for exchanging the control information but also make their antennas consume more power. For example, F^2-MAC [42] exchanges five types of control frames and the size of each control frame is 20 bytes, and CREAM–MAC [38] exchanges 4 control frames with each frame 20 bytes. So, a total of 100 bytes and 80 bytes respectively are exchanged as control information in these protocols. In contrast to this, DDH-MAC exchanges a total of 4 frames being sized 14 bytes, 20 bytes, 14 bytes and 20 bytes respectively. Also, one of the frames, i.e., BF, does not need to be exchanged for every control information transaction. Therefore, minimizing the size of control frames in DDH-MAC saves more energy.

c) Avoiding the Retransmission of Frames

The cognitive radio aims to use the spectrum band of a licensed user when it is not being used, provided the condition that there will be no interference to the licensed user. So, a reclaim of the licensed user on spectrum bands when cognitive radio has started using it is not unusual. A cognitive radio must be capable of finding other spectrum opportunities if there is a return of a licensed user. The CR MAC protocols must be designed to address this scenario efficiently. If a MAC protocol is not able to handle the PU claim, ultimately it would result in re-searching and scanning of other available spectrum bands and re-transmission of control information. This will not only be more time consuming but also the CR nodes holding the data will have to consume more energy.

As previously discussed, DDH-MAC deals with the return of a licensed user on the spectrum band effectively and it does not re-search and re-scan for other available spectrum bands. Instead, it simply switches to a backup control channel and resumes the control information exchange on the backup control channel. This gives an advantage to DDH-MAC protocol which other protocols lack. Transmitting no or minimal frames after a PU claim ultimately save mobile energy as nodes have to wait less for actual data transmission.

d) Avoiding Control Channel Re-negotiation

For CR nodes to converge and start to negotiate the transmission rules, a control channel is mandatory. In any CR MAC protocol, the design and selection criteria of a control channel are of significant importance. It is strongly believed that the

CR nodes cannot simply start data transmission until a common control channel is found and agreed upon. Unfortunately, this very important aspect of a CR MAC protocol has not been intensively researched, and the pre-existence of a common control channel and the CR nodes' awareness about the control channel have been assumed. It is strongly stated that any data transmission in a CR network is subject to successful exchange of control information on a well-known, available, and secure common control channel. A control channel must also be capable of handling any claims by licensed users (if it has been selected amongst one of the white spaces).

DDH-MAC has been optimally designed to be readily and rapidly available to the CR nodes, and, if there is any PU occupancy on the control channel, the backup control channel is always there to stand by the primary control. So the CR nodes deploying the DDH-MAC protocol do not need to re-negotiate and re-search the control channel.

6.6. A Numerical Example

In this section, we have first developed a numerical example to analyse the system energy consumption. We have simulated the example to investigate the energy efficiency. We have compared DDH-MAC with CREAM-MAC protocol [38].

In our mathematical analysis, we have derived numerical equations to calculate the energy consumption of DDH-MAC and compare it with other CR MAC protocols. We first calculate the time taken in exchanging the control information by following the standard parameters mentioned in IEEE802.11b [212]. The time spent in exchanging the control information for DDH-MAC and CREAM-MAC has been computed using Equations 6.1 to 6.2.

$$T_{DDH\text{-}MAC} = T_{DIFS} + T_{DMCF} + T_{FCL} + T_{ACK} + 2 \times SIFS \tag{6.1}$$

$$T_{CREAM\text{-}MAC} = T_{DIFS} + T_{RTS} + T_{CTS} + T_{CST} + T_{CSR} + 3 \times SIFS \tag{6.2}$$

We now calculate the energy (Ë) consumed for Equations 6.1 to 6.5 using the universal energy formula below:

$$\text{Ë} = \mathrm{P} \times T \tag{6.3}$$

where P represents the power used for transmission, and T is obtained from Equations 6.1 and Equation 6.2, and represents the time it takes to exchange the corresponding control frames. The DSSS PHY layer parameters used to calculate the energy consumption have been summarized in Table 6.1.

Table 6.1: Parameters Used to Calculate the Energy Efficiency of DDH-MAC

Parameter	Value
DIFS	2 × Slot_Time + *SIFS*
SIFS	10µs
T_x Power	1.5W
Data Rate	11Mbps
CW_{min}	32
CW_{max}	1024
Slot_Time	20µs

The numerical results obtained using the Equations 6.5 and parameters in Table 6.1 have been plotted in Figure 6.3. Clearly, the total energy consumed by DDH-MAC is less when compared with CREAM-MAC protocol. The obvious reason for less energy consumption in DDH-MAC is the difference in the number of control frames and the size of each control frame. The larger the size and the number of control frames, the higher will be the energy consumed by transmitting antenna of a CR node.

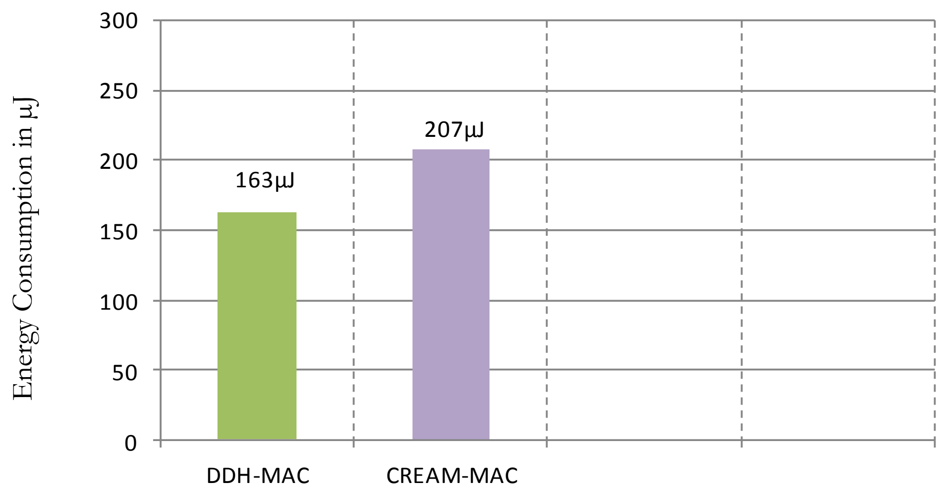


Figure 6.3: Energy consumption of DDH-MAC when compared with CREAM-MAC protocol.

In our simulation experiment, there are 4 control frames of size 20B each for the CREAM-MAC protocol. Settings of simulation parameters are shown in Table 6.2.

Table 6.2: Simulation Parameters for Calculating the Energy Efficiency of DDH-MAC.

Parameter	Value
DIFS	2 × Slot_Time + *SIFS*
SIFS	10μs
T_x Power	1.5W
R_x Power	1W
RTS, CTS, FCL, ACK_{other}	20Bytes
$BF_{DDH-MAC}$, $FCL_{DDH-MAC}$	14Bytes
$DMCF_{DDH-MAC}$, $ACK_{DDH-MAC}$	20Bytes
PHY Header	24 Bytes
Data Rate	11Mbps
CW_{min}	32
CW_{max}	1024
Slot_Time	20μs
Channel Bit rates	1.2Mbps

We now describe the result obtained from the simulation. The energy efficiency of the average control information exchange time of CR users has been presented in Figure 6.4. We observe that DDH-MAC consumes less energy. Clearly, the low energy consumption of DDH-MAC as compared with other two CR MAC protocols is the result of a few number of smaller sized control frames. It is further observed that the energy consumption has it highest values for all MAC protocols, including DDH-MAC, when the network is initialized. This is because when the network is initialized so many background operations are running. For example, all nodes contend for control to access a control channel which can cause collisions ultimately resulting in high energy consumption. The exchange of more control frames in other MAC protocols cause them to consume higher amounts of energy. It is worth mentioning that for this particular experiment, we did not delve into data transmissions. The statistics obtained through this simulation experiment only show the amount of energy consumed by different CR MAC protocols while exchanging the control information.

As we can see from Figure 6.4, DDH-MAC outperforms CREAM-MAC protocol in terms of energy efficiency. On average, DDH-MAC is about 40% more energy efficient when compared with CREAM-MAC protocol while exchanging the control information.

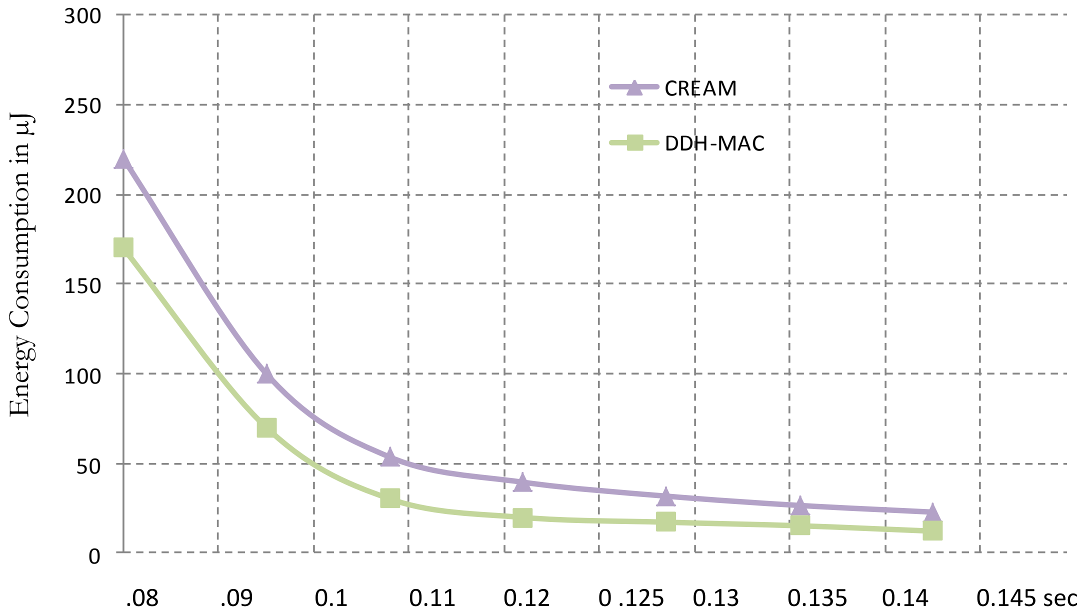


Figure 6.4. Simulation result of energy consumption of DDH-MAC when compared with CREAM-MAC protocol.

6.7. Summary

In this chapter, we optimized the performance of our proposed DDH-MAC protocol. The performance optimization is achieved in several different ways. We first incorporate a 4-fold security model to make our scheme resilient against security threats and vulnerabilities. To the best of our knowledge, this is the first security model in CR MAC protocols which provides 4-fold security at the MAC layer. We first encrypt the BF so that the information containing in the BF is only meaningful for legitimate CR nodes. The FCL is not broadcast on the GCCC which provides our protocol another level of security. The integrity of data is ensured by inclusion of a time stamp in each data transmission. The dynamicity of the control channel gives our protocol the fourth level of security.

We have further optimized the performance of our scheme by making 3 control channels always available to dialogue control information. In case, there is a PU reclaim on the control channel, the backup control channel standby is the core operation of DDH-MAC. We have further optimized the performance of DDH-MAC by considering the case where the BCCH becomes unavailable prior to PCCH. In this case, if a PU occupancy is detected on BCCH, an update copy of the BF will be launched which will have the information about the newly established BCCH.

DDH-MAC has been specially designed to address the energy efficiency issues in CR MAC protocols. The CR nodes consume a significant amount of energy on exchanging control information before any data transaction takes place. The CR nodes deploying our protocol can save energy by transmitting fewer control frames, by exchanging smaller sized control frames, and by avoiding researching and rescanning the control channel if it becomes unavailable. A reduced number of smaller sized control frames and the backup control channel are the keys to make the DDH-MAC protocol 40% more energy efficient.

Chapter 7: Conclusions and Future Work

Did we really make software radios more personal…..?

Yes, we did…..

By incorporating the features of opportunistic spectrum access and making software radios more context aware, the cognitive radio technology has emerged as a promising technology to address the spectrum scarcity issue. The objective of this thesis was to design, develop and analyse an opportunistic MAC protocol for decentralized, underlay, and cooperative cognitive radio networks. This chapter concludes the discussion and summarizes the achieved research goals and proposes some enhancements in the research for future work.

7.1. Summary

In Chapter 1, a detailed introduction of CR technology is presented and many definitions for CR are proposed. The industry standards and regularization of CR also form part of this chapter. We have explained how the unoccupied spectrum band could be utilized by cognitive radio and be applied in existing mobile networks, industry, disaster management, and public safety. We continue our discussion and highlight the issues and limitations of CR that are acting as a red flag in this technology. We explain why this technology, even after having been extensively researched, has not yet been widely accepted and implemented. In Chapter 2, we reviewed opportunistic MAC protocols for cognitive radio networks, which integrate the cooperation and scheduling amongst CR nodes.

Our findings in the literature motivated us to design a hybrid CR MAC protocol that accumulates the advantages of existing CR MAC protocols of both GCCC and non-GCCC families and is able to efficiently discover, recover and converge on a common control channel. In Chapter 3, we provide detailed architecture and description of our scheme, named as Dynamic, Decentralized and Hybrid MAC (DDH-MAC) protocol. Our protocol is dynamic because whenever there is a PU claim on a control channel, nodes adapt according to the environment and switch to another backup channel.

Defining cognitive radio, exploring its limitations and providing solutions to the faced challenges, have been our major achievement in this Chapter 1. Our contributions in Chapter 2 are the identification and the classification of existing CR MAC protocols. Our achievement in this chapter was providing a new feature to classify the existing CR MAC protocols and developing a model for classification of different MAC protocols for cognitive radio networks.

Using mathematical modelling, we analyse the performance of our proposed DDH-MAC protocol, we used the Markov chain model in Chapter 4 for two different approaches and determined the desirability of the CR network deploying our protocol. Each SU joins the network by receiving the BF and learning the network status through overhearing the control information over the control information. Our first approach evaluates the system performance with coalition amongst PUs and SUs. This means that both the PU and the SU can simultaneously access the spectrum subject to SUs' constraints. We extend our model in the second approach by considering a network scenario where SUs could not transmit until the PU vacated the occupied spectrum. Using these modelling techniques, we developed our protocol which enabled us to envision the performance of our MAC protocol.

Our main contributions in Chapter 5 are two-fold: first, implementation and simulation of our proposed DDH-MAC protocol; and second, combining two modelling techniques (analytical evaluation plus simulation) to observe and verify its correctness. We built our own simulation model for DDH-MAC. In this model, we enabled a SU to create a new CR network (if it was the first SU in the vicinity), and allowed other SUs to join an existing CR network after receiving the BF which is periodically broadcasted in the 2.4GHz spectrum band. Our protocol particularly addressed the unavailability or the saturation problem of the control channel. The suitability and correctness of our framework were further revealed after obtaining the global and local (object) statistics for parameters such as throughput, traffic sent, collision on control channel, queuing delay, signal-to-noise ratio, and network performance with and without ideal channel conditions etc. For our comparative performance evaluation with other CR MAC protocols, the aggregated throughput of DDH-MAC protocol was demonstrated to be better than CREAM-MAC protocol.

In Chapter 6, our main contribution was to enhance the performance of the DDH-MAC protocol. We optimized the DDH-MAC performance in two aspects: firstly, we incorporated a multi-fold security in DDH-MAC; and secondly, we made the DDH-MAC protocol energy efficient. We have presented a 4-tier security model and have incorporated security in DDH-MAC in all possible ways, which is the first part of our contributions in this chapter. At first level of security, we avoid using the GCCC and secretly transmit the FCL on a local control channel so that only the SUs deploying DDH-MAC can retrieve the FCL. At second level, we encrypt the BF and then launch it in the GCCC. The third level of security is achieved by inclusion of a time-stamp in outgoing data frames. The dynamicity of the control channel serves as the fourth level of security in DDH-MAC.

Our second contribution in Chapter 6 is making DDH-MAC protocol energy efficient. Note that the vital reason for a high amount of energy consumption is the frame re-transmission after any PU claim. DDH-MAC saves a significant amount of energy by avoiding frame re-transmission. Secondary users always have access to a backup channel, so SUs simply switch to the backup channel and avoid the transmission of those frames for rediscovering and recovering the control channel. Switching to a backup control channel not only saves time but also enables nodes with delay-sensitive data to quickly utilize the unoccupied spectrum band, which is another remedy for achieving a better energy efficiency in DDH-MAC.

7.2. Conclusions

To make cognitive radios technology more practical and widely acceptable we conclude our findings in literature by providing possible solutions to a few of the challenges faced by CR. We believe that FCC and IEEE standards for CR, switching to digital TV, using spectrum usage databases, and deploying multi-band antennas in CR are some of the key areas that will make the CR technology widely being used in daily life.

Our research on existing CR MAC protocols enables us to identify the problems and limitations in the literature. We conclude that the major classification of CR MAC protocols is based on whether they use the control channel in the ISM band (GCCC) or use a local control channel (non-GCCC). We find that both the GCCC and non-GCCC based CR MAC protocols have advantages specific to their own class but on the other hand, both suffer from certain disadvantages. For example, the CR MAC protocols which use the GCCC as a control channel enjoy the benefits of being always available and license-free, but contrary to this, the GCCC based CR MAC protocols are more prone to congestion and security threats. The non-GCCC CR MAC protocols are resilient to security threats, but it is difficult and time consuming for the CR nodes to discover non-GCCC.

Any CR MAC protocol that needs to be developed must be equipped with the design features provided in Table 7.1. For example, a MAC protocol could be either centralized or decentralized, contention-based or coordination-based (contention free), equipped with a single transceiver or multi-transceiver, etc. We conclude our findings through a table in which we list the characteristics of twenty CR MAC protocols reported in the literature.

Table 7.1 Design Features of a CR MAC Protocol

Common Control Channel	**Direct Access**	**Dynamic Spectrum Access**
• GCCC • Non-GCCC • Assumed • Hybrid (DDH-MAC)	• Contention based • Coordination based	• Genetic • Game Theoretic
Access Mechanism • Time slotted • Random • Hybrid Access	**Number of Radios** • Single transceiver • Multiple Transceivers	**Synchronous** **Asynchronous**
Overlay/Underlay	**Proactive/Reactive**	**Centralized/Decentralized**

We believe that in order to analyse the PU behaviour in a CR network accurately, a CR MAC protocol must be investigated in different possible network scenarios. We have proposed four network case-scenarios that deal with different possibilities of the PU claim on a control channel. Under an ideal network scenario, the secondary user scans the GCCC for a BF, and after reading the information, switches to the PCCH to dialogue the control information. In the worst network scenario, if a PU claim has been sensed, then, unlike other CR MAC protocols, secondary users do not have to re-negotiate the control information and can simply resume the conversation on a backup control channel. In this way, the pre-transmission time and other network overheads are significantly reduced. We compute the pre-transmission time for all network scenarios and discover that the average pre-transmission time of DDH-MAC is smaller when compared with other CR MAC protocols. We strongly argue that pre-transmission time plays a very important role in any CR MAC protocol. It is an overhead which each MAC protocol must aim to minimize in all possible ways.

Introducing the concept of more than one control channel, and enabling the nodes to exchange control information safely and efficiently, are novel ideas in developing the CR MAC protocols, which are our major contributions in this study. In this chapter, our other contributions are discussing and evaluating the pre-transmission time. We show that the pre-transmission time plays an important role and a smaller pre-transmission time helps to yield a higher throughput as nodes have to wait for less time before the actual transmission starts.

A system performance could not be validated until one or more of the following modelling techniques have been applied: i) analytical modelling; ii) implementation/simulation modelling; iii) combining both analytical and simulation modelling; and iv) testbeds. We have used first three techniques to observe the behaviour of our proposed MAC protocol. Different parameters such as throughput, PU interference probability, SUs' transmission opportunities to utilize available white spaces, and contention amongst CR nodes were evaluated. The framework achieved the desired results by ensuring that the network constitutes an exact CR network that has the potential to respond to external events and has the capability to adapt and reconfigure according to network scenario.

It is concluded that equipping each SU with two radios helps avoid the hidden terminal problem and also keeps nodes rapidly updated about any network change that occurs in the CR network. This task is accomplished by using both the radios simultaneously (one radio to scan and observe network activities on the control channel, and the other radio to transmit data). We have revealed main advantages of our scheme: i) more than one control channel is supplied; ii) two transceivers efficiently solve the hidden terminal problem in a multi-channel environment; iii) the control channel saturation problem is overcome. In particular, when a SU is exchanging the control information and the channel become unavailable, SUs simply switch to a backup control channel and thus avoid re-dialoguing the control information. We quantitatively identified the trade-off between the network aggregated throughput and the channel utilization, which provided us some useful guidelines to improve the QoS parameters in CR networks.

7.3. DDH-MAC Limitations

The DDH-MAC protocol has been specially designed to address the limitations of existing decentralized CR MAC protocols. Some of the promising features of DDH-MAC are reliability of control channel, energy efficiency and security at multiple levels. However, it is worth mentioning that DDH-MAC has certain limitations.

The CR nodes deploying the DDH-MAC protocol must have at least three available white spaces (Equation 3.1) or else DDH-MAC will not be operational. We believe that having at least three white spaces is not a serious issue as it is the nature of CR nodes to search and scan all possible white spaces in the vicinity. For example, if the CR network operates in 2.4 GHz, there are at least 14 channels available in this band which could be used for communication amongst CR nodes.

The optimal values of the pre-transmission time are subject to a design constraint, i.e., the initial waiting time (T_3) is required to launch the BF. This implies that the first CR node responsible for launching the BF must wait for T_3 . Also, it is not possible for two DDH-MAC nodes to attempt to launch the BF at the same time. Initially, this gives an impression that this wait time in DDH-MAC will degrade the network performance when compared with other CR MAC protocols. However, different analytical and simulation results have shown that the overall network performance significantly increases even if the first node waits for certain time to launch BF. And this is because the initial wait time helps with efficient network convergence and reliable exchange of control information.

Simulation modelling was the most complex and time consuming part of this research. From installing OPNET to obtaining its license, numerous difficulties were faced. It had been quite usual that some pieces of programme codes were running and producing output at one time but failed to run another time or produced strange outputs. The more complex the simulation model becomes, the more complex was it to troubleshoot. Also, simulating the complete functionality of DDH-MAC recorded approximately 5000 events, and not all the events could be used for output. It was even more complex to select the appropriate and relevant outputs.

7.4. Overall Research Contributions

The primary objective of this research is to develop a novel secure adaptive MAC protocol for cognitive radio networks. Achieving this goal requires the enhancement of existing CR MAC protocols and the development, analysis and simulation of a new protocol that satisfy the needs of a CR network.

The research contributions from this doctorate research are presented in each chapter of this thesis and are summarized in Table 7.2.

Table 7.2 Summary of research contributions

Chapter 1	Exploring Cognitive Radios in terms of definitions, regularization applications and challenges.
Chapter 2	A new model for classification of existing CR MAC protocols. Identifying new parameters to classify the existing CR MAC. Exploring all the features that existing CR MAC protocols are equipped with.
Chapter 3	Design of a CR MAC protocol with the following novel features • hybrid between GCCC and non-GCCC family of CR • emphasis on exchange of control information • use of more than one control channel • incorporating reliable channel access and rapid channel access • convergence analysis for the pre-transmission time
Chapter 4	Analytical modelling of our MAC protocol. Implementation of a Markov chain model for queuing and non-queuing network case scenarios. Analysing the network performance for different parameters. Performance evaluation for aggregated throughput in different scenarios. Performance comparison with other CR MAC protocols.

Chapter 5	Implementation and simulation of our scheme. Using analytical modelling, simulation modelling and combination of both modelling techniques. Performance evaluation for parameters such as throughput, queuing delay, SNR. Observing network behaviour in channel conditions. Performance comparison with other CR MAC protocols.
Chapter 6	Performance optimization of our scheme. Making the DDH-MAC protocol energy efficient. Novel 4-tier security model for DDH-MAC.

7.5. Future Work

Extensive research has been carried out each chapter area of this thesis, which gave birth to more research ideas. The following areas deserve further investigation and will form part of our future work.

7.5.1. Making the PCCH More Versatile and Dynamic

As another idea to enhance the existing framework for DDH-MAC, the CR nodes can select their own primary control channel that can remain valid for one FCL transaction. This means that once the control information has been exchanged on the PCCH by one SU pair, the next SU pair can elect a new PCCH using the same BF transmission in the GCCC. This will make the CR network more secure and dynamic. The validity of the PCCH will last for one FCL transaction.

7.5.2. A TDMA-based Variation of the DDH-MAC Protocol

Currently, the DDH-MAC protocol is contention-based. SUs have to contend for the control channel and data channel for transmission. We are considering the proposal of a TDMA-based version of the DDH-MAC protocol in which each SU will be given a time slot to access the control channel. This will avoid contention amongst SUs for the important resource, i.e., control channel in a CR network will be fairly allocated to each SU. The concept of a TDMA-based CR MAC protocol is not new, but converging on a control channel is a challenging task. We will combine the GCCC based BF launching concept and will merge with the TDMA concept in an existing CR MAC protocol to develop a much enhanced CR MAC protocol. We have briefly worked on this protocol and have obtained some preliminary simulation results which are provided in Figure 7. 1. However, when more SUs join the network, they have to wait for longer to access their allocated time slot. We believe this idea needs more sophisticated investigation and could be an exciting future work.

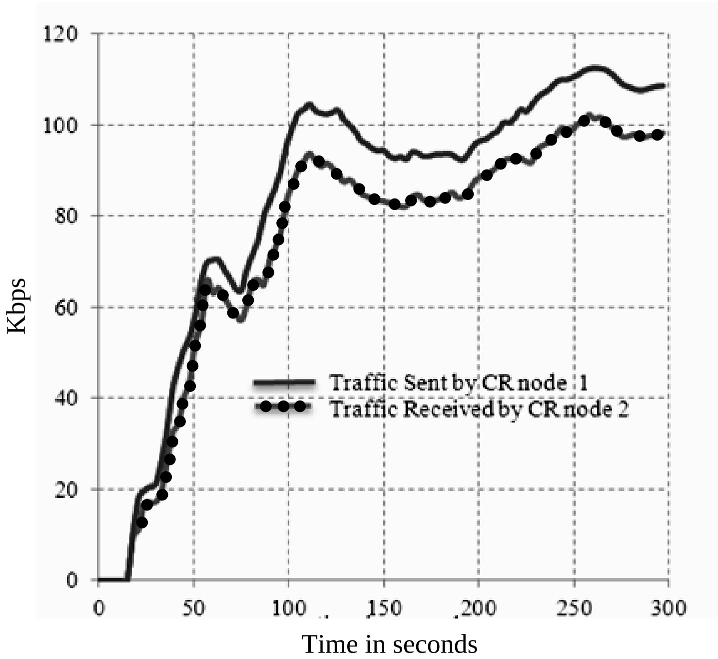


Figure 7.1. Traffic sent amongst SU pair in a TDMA-based DDH-MAC protocol.

7.5.3. Improving the Security with More Enhanced Security Features

More complex encryption schemes could be deployed to encrypt the BF and the FCL. This will make the CR network more secure against security threats. However, this will add more complexity and processing delays in the network. So far, no significant research has been carried out for authentication in decentralized CR networks. Incorporating the authentication mechanism in CR is of significant importance and could be another exciting research direction. Another level of security that could be added in the existing 4-tier security model is to add a self-destructive mechanism in data frames if the time stamp has expired. This idea is based on the TTL (time to live) value in a network packet which is discarded by a router if the TTL value has reached to zero. This means that if a data frame is sniffed during a transmission, it should be capable of destroying all its contents so that the information is not available to the sniffer. These areas need further investigation and exploration.

7.5.4. Adding a Back-up Data Channel and Simultaneous Parallel Data Transmission

The idea of the backup data channel and the simultaneous data transmission on more than one data channel in CR networks is not new as an effective way to achieve higher throughputs. However, this concept is constrained by certain design parameters such as availability of a minimum number of channels with each SU which can only be assumed in ideal scenario. Another constraint is the number of additional transceivers that would be required to send the data on more than one data channel. As a future work, simultaneous data transmission will be incorporated in DDH-MAC and the trade-offs for this feature will be investigated.

7.5.5. Introducing the Sleep Mode of SU in DDH-MAC to Save More Energy

The CR nodes in DDH-MAC have to set their NAV if the control channel is sensed busy or if a DMCF frame has been received. SUs in this case are not allowed to contend for any transmission and have to wait until the ACK frame has been received. Receiving the ACK frame means that the pair of SU has completed the exchange of the control information and the medium is now free for other SUs to contend for the control information dialogue. We can propose an idea that instead of setting their NAV, SUs should change their state from listening to sleep mode (putting the nodes into sleep mode is well-established in wireless ad-hoc networks research). This can save some energy at the mobile terminal. The amount of energy saved per transaction by an individual node may not be significant but the aggregated amount of energy saved by all CR nodes during all transactions will surely be significant. We aim to thoroughly investigate this in future as part of our future work.

References

[1] H. Hertz, “Electric Waves 2,” 1893.

[2] H. Hertz, *Electric waves: being researches on the propagation of electric action with finite velocity through space*. Dover Publications, 1893.

[3] F. C. Commission and others, “Spectrum policy task force report, FCC 02-155.” Nov, 2002.

[4] “The Radio Spectrum,” *Available Online at: http://transition.fcc.gov/Bureaus/OPP/working_papers/oppwp38chart.pdf*. [Online]. Available: http://transition.fcc.gov/Bureaus/OPP/working_papers/oppwp38chart.pdf.

[5] Ofcom, “UK frequcny Allocation Table,” 2010. [Online]. Available: http://stakeholders.ofcom.org.uk/binaries/spectrum/spectrum-policy-area/spectrum-management/ukfat2010.pdf. [Accessed: 09-Jan-2013].

[6] R. Tonjes, T. Paila, W. Hansmann, M. Frank, and M. Albrecht, “DRiVE-ing to the Internet: Dynamic Radio for IP services in Vehicular Environments,” in *Proceedings 25th Annual IEEE Conference on Local Computer Networks. LCN 2000*, pp. 281–289.

[7] “The UK Frequency Allocation Chart.” [Online]. Available: http://topdf.info/owners-manual/the-uk-frequency-allocations-pdf.pdf.

[8] D. Cabric, S. M. Mishra, and R. W. Brodersen, “Implementation issues in spectrum sensing for cognitive radios,” in *Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, 2004.*, vol. 1, pp. 772–776.

[9] P. J. Kolodzy, “Spectrum Policy Task Force Findings and Recommendations,” 2003. [Online]. Available: http://www.its.bldrdoc.gov/isart/art03/slides03/kol_p/kol_slides.pdf. [Accessed: 11-Jan-2013].

[10] B. M. Sadler, “A Survey of Dynamic Spectrum Access,” *IEEE Signal Processing Magazine*, vol. 24, no. 3, pp. 79–89, May 2007.

[11] S. Geirhofer, L. Tong, and B. Sadler, “Cognitive radios for dynamic spectrum access - dynamic spectrum access in the time domain: modeling and exploiting white space,” *IEEE Communications Magazine*, vol. 45, no. 5, pp. 66–72, May 2007.

[12] I. F. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty, “A survey on spectrum management in cognitive radio networks,” *Communications Magazine, IEEE*, vol. 46, no. 4, pp. 40–48, 2008.

[13] J. Mitola and G. Q. Maguire, “Cognitive radio: making software radios more personal,” *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.

[14] K. Araki, “Software Defined Radio,” *Institute Of Electronics Information And Communication Engineers*, vol. 83, no. 3, pp. 183–190, 2000.

[15] F. K. Jondral, “Software-defined radio: basics and evolution to cognitive radio,” *EURASIP J. Wirel. Commun. Netw.*, vol. 2005, no. 3, pp. 275–283, Aug. 2005.

[16] M. Dillinger, K. Madani, and N. Alonistioti, *Software defined radio: architectures, systems, and functions*. Wiley, 2003.

[17] B. A. Fette, "Software-defined radio." Google Patents, 2003.

[18] R. I.-R. ITU SM.2152, "Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS)," 2009.

[19] J. Mitola, "Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio," 2000.

[20] JTNC, "Joint Tactical Networking Center." [Online]. Available: http://jtnc.mil/Pages/AboutJTNC.aspx. [Accessed: 10-Jan-2013].

[21] PicoChip, "IEEE802.16m 'WiMAX' Software Reference Designs."[Online]. Available: http://www.picochip.com/page/30/WiMAX. [Accessed: 12-Jan-2012].

[22] IEEE, "802.21 Working Group Web Page." [Online]. Available: http://www.ieee802.org/21/.

[23] P. Marshall, "Current R&D Investments in Dynamic Spectrum Technology," in *DySPAN, Baltimore, MD*.

[24] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[25] U. S. F. C. Commission and others, "ET Docket No. 03-108," 2005.

[26] U. S. F. C. Commission and others, "Notice of proposed rule making and order: Facilitating opportunities for flexible, efficient, and reliable spectrum use employing cognitive radio technologies," 2005.

[27] IEEE USA, "Improving Spectrum Usage Through Cognitive Radio Technology," 2003. [Online]. Available: http://www.ieeeusa.org/policy/policy/2003/120903.html.

[28] "1900.1-2008 - IEEE Standard Definitions and Concepts for Dynamic Spectrum Access: Terminology Relating to Emerging Wireless Networks, System Functionality, and Spectrum Management," 2008.

[29] Virginia Tech Cognitive Radio Work Group, "Defining Cognitive Radio." [Online]. Available: http://support.mprg.org/dokuwiki/doku.php?id=cognitive_radio:definition. [Accessed: 14-Jan-2013].

[30] M. Shah, S. Zhang and C. Maple, "An Analysis on Decentralized Adaptive MAC Protocols for Cognitive Radio Networks," *International Journal of Automation and Computing*, vol. 10, no. 1, pp. 46–52, 2013.

[31] M. A. Shah, S. Zhang, and C. Maple, "An analysis on decentralized adaptive MAC protocols for Cognitive Radio networks," in *Automation and Computing (ICAC), 2012 18th International Conference on*, 2012, pp. 1–5.

[32] M. A. Shah, G. A. Safdar, and C. Maple, "DDH-MAC: A novel Dynamic De-Centralized Hybrid MAC protocol for Cognitive Radio Networks," in *2011 RoEduNet International Conference 10th Edition: Networking in Education and Research*, 2011, pp. 1–6.

[33] M. A. Shah, S. Zhang, and C. Maple, “A novel multi-fold security framework for cognitive radio wireless ad-hoc networks,” *18th International Conference on Automation & Computing*, pp. 1–6, 2012.

[34] J. O. Daniell, “Analysis and Design of Cognitive Radio Networks and Distributed Radio Resource Management Algorithms,” Virginia Polytechnic Institute and State University, 2006.

[35] J. Mitola, “The software radio architecture,” *IEEE Communications Magazine*, vol. 33, no. 5, pp. 26–38, May 1995.

[36] Federal Communications Commission, “Establishment of interference temperature metric to quantify and manage interference and to expand available unlicensed operation in certain xed mobile and satellite frequency bands.”

[37] J. Mitola, “Cognitive Radio for Flexible Mobile Multimedia Communications,” *Mobile Networks and Applications*, vol. 6, no. 5, pp. 435–441.

[38] X. Zhang and H. Su, “CREAM-MAC: Cognitive Radio-EnAbled Multi-Channel MAC Protocol Over Dynamic Spectrum Access Networks,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 5, no. 1, pp. 110–123, Feb. 2011.

[39] H. K. H. Kim and K. G. Shin, *Efficient Discovery of Spectrum Opportunities with MAC-Layer Sensing in Cognitive Radio Networks*, vol. 7, no. 5. IEEE, 2008, pp. 533–545.

[40] F. Wang, M. Krunz, and S. Cui, “Spectrum Sharing in Cognitive Radio Networks,” in *2008 IEEE INFOCOM - The 27th Conference on Computer Communications*, 2008, pp. 1885–1893.

[41] Wikipedia, “Frequency allocation,” 2006. [Online]. Available: http://en.wikipedia.org/wiki/Frequency_allocation. [Accessed: 15-Jan-2013].

[42] H. L. Chao, T. C. Lou, and S. Jiang, “F2-MAC: an efficient channel sensing and access mechanism for cognitive radio networks,” *Wireless Networks*, vol. 17, no. 5, pp. 1113–1126, 2011.

[43] T. Yucek and H. Arslan, “A survey of spectrum sensing algorithms for cognitive radio applications,” *IEEE Communications Surveys & Tutorials*, vol. 11, no. 1, pp. 116–130, 2009.

[44] Z. Challapali, K. and Mangold, S. and Zhong, “Spectrum agile radio: Detecting spectrum opportunities,” in *IEEE GlobeCOM*, 2004.

[45] Q. Zhao, L. Tong, A. Swami, and Y. Chen, “Decentralized cognitive MAC for opportunistic spectrum access in ad hoc networks: A POMDP framework,” *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 3, pp. 589–600, Apr. 2007.

[46] K. Ahmed, P. Dimitri and B. Magdy, "Opportunistic spectrum access challenges in distributed cognitive radio networks",Springer, pp. 33–39, Apr. 2013.

[47] Y. R. Kondareddy, P. Agrawal, and K. Sivalingam, “Cognitive Radio Network setup without a Common Control Channel,” in *MILCOM 2008 - 2008 IEEE Military Communications Conference*, 2008, pp. 1–6.

[48] A. Ghasemi and E. S. Sousa, "Spectrum sensing in cognitive radio networks: requirements, challenges and design trade-offs," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 32–39, Apr. 2008.

[49] C. Cormio and K. R. Chowdhury, "Common control channel design for cognitive radio wireless ad hoc networks using adaptive frequency hopping," *Ad Hoc Networks*, vol. 8, no. 4, pp. 430–438, Jun. 2010.

[50] S. Krishnamurthy, M. Thoppian, S. Venkatesan, and R. Prakash, "Control Channel Based MAC-Layer Configuration, Routing and Situation Awareness for Cognitive Radio Networks," in *MILCOM 2005 - 2005 IEEE Military Communications Conference*, pp. 1–6.

[51] M. A. Shah, S. Zhang, and C. Maple, "An Efficient and Robust Decentralized Control Channel Access Mechanism for Cognitive Radio Networks," in *Proceedings of 7th International Conference on Broadband Communications & Biomedical Applications (IB2COM'12)*, 2012, pp. 26–31.

[52] J. M. III, "Cognitive Radio An Integrated Agent Architecture for Software Defined Radio Dissertation," *Scientific American*, vol. 294, no. 3, pp. 66–73, 2000.

[53] C. J. Rieser, "Biologically inspired cognitive radio engine model utilizing distributed genetic algorithms for secure and robust wireless communications and networking," Virginia Polytechnic Institute and State University, 2004.

[54] B. Atakan and O. B. Akan, "BIOlogically-Inspired Spectrum Sharing in Cognitive Radio Networks," in *2007 IEEE Wireless Communications and Networking Conference*, 2007, pp. 43–48.

[55] Virginia Tech Cognitive Radio Work Group, "CoRTekS." [Online]. Available: ossie.wireless.vt.edu/trac/wiki/CORTEKS. [Accessed: 18-Jan-2013].

[56] adapt4, "The world's first, truely cognitive commercial radio." [Online]. Available: www.adapt4.com. [Accessed: 18-Jan-2013].

[57] L. Berlemann, S. Mangold, and B. H. Walke, "Policy-based reasoning for spectrum sharing in radio networks," in *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, pp. 1–10.

[58] P. Marshall, "Cognitive Radio Panel Session," *SDR Forum Technical Conference*. Nov 14-17,2005, Orange County CA., 2005.

[59] C. Cordeiro, K. Challapali, and D. Birru, "IEEE 802.22: the first worldwide wireless standard based on cognitive radios," in *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, pp. 328–337.

[60] R. W. Brodersen, A. Wolisz, D. Cabric, S. M. Mishra, and D. Willkomm, "Corvus: a cognitive radio approach for usage of virtual unlicensed spectrum," *Berkeley Wireless Research Center (BWRC) White paper*, 2004.

[61] A. O'hara, B. and Petrick, *IEEE 802.11 handbook: a designer's companion*. Standards Information Network, 2005.

[62] M. Sherman, A. N. Mody, R. Martinez, C. Rodriguez, and R. Reddy, "IEEE Standards Supporting Cognitive Radio and Networks, Dynamic Spectrum Access, and Coexistence," vol. 46, 2008.

[63] FBO, "Wireless Adaptable Network Node (WANN)," 2007. [Online]. Available: https://www.fbo.gov/index?s=opportunity&mode=form&id=b732c5d4c546f5dcb6fa35fd8858556a&tab=core&_cview=1. [Accessed: 19-Jan-2013].

[64] D. Mortensen, D. Bishop, and D. Chelmins, "STRS Radio Service Software for NASA's SCaN Testbed," 2013. [Online]. Available: http://www.nasa.gov/mission_pages/station/research/experiments/SCAN_Testbed.html.

[65] FCC, "FCC Memorandum Opinion And Order," 2006.

[66] S. Kamal, "SAIC," 2013. [Online]. Available: http://www.saic.com. [Accessed: 19-Jan-2013].

[67] IEEE, "URL for IEEE 1900." [Online]. Available: http://www.ieeep1900.org.

[68] IEEE, "URL for Approved IEEE Projects Authoriazation Requests (PARs)." [Online]. Available: http://standards.ieee.org/board/nes/approved.html.

[69] D. Setiawan, D. Gunawan, and D. Sirat, "Interference analysis of guard band and geographical separation between DVB-T and E-UTRA in Digital Dividend UHF band," in *International Conference on Instrumentation, Communication, Information Technology, and Biomedical Engineering 2009*, 2009, pp. 1–6.

[70] X. Zhao, Z. Guo, and Q. Guo, "A cognitive based spectrum sharing scheme for LTE advanced systems," in *International Congress on Ultra Modern Telecommunications and Control Systems*, 2010, pp. 965–969.

[71] S.-M. Cheng, S.-Y. Lien, F.-S. Chu, and K.-C. Chen, "On exploiting cognitive radio to mitigate interference in macro/femto heterogeneous networks," *IEEE Wireless Communications*, vol. 18, no. 3, pp. 40–47, Jun. 2011.

[72] J. Polson, "Cognitive radio applications in software defined radio," in *Prof. of the SDR 04 Technical Conference and Product Exposition*, 2004.

[73] N. Jesuale and B. C. Eydt, "A Policy Proposal to Enable Cognitive Radio for Public Safety and Industry in the Land Mobile Radio Bands," in *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2007, pp. 66–77.

[74] A. Saatsakis, K. Tsagkaris, D. von-Hugo, M. Siebert, M. Rosenberger, and P. Demestichas, "Cognitive Radio Resource Management for Improving the Efficiency of LTE Network Segments in the Wireless B3G World," in *2008 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2008, pp. 1–5.

[75] C. E. Palazzi, M. Roccetti, S. Ferretti, G. Pau, and M. Gerla, "Online games on wheels: Fast game event delivery in vehicular ad-hoc networks," *Proc. of V2VCOM*, 2007.

[76] S. M. Riera, O. Wellnitz, and L. Wolf, "A zone-based gaming architecture for ad-hoc networks," in *Proceedings of the 2nd workshop on Network and system support for games - NETGAMES '03*, 2003, pp. 72–76.

[77] A. Fehske, J. Gaeddert, and J. H. Reed, "A new approach to signal classification using spectral correlation and neural networks," in *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, pp. 144–150.

[78] T. X. Brown, "An analysis of unlicensed device operation in licensed broadcast service bands," in *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, pp. 11–29.

[79] L. Berlemann, S. Mangold, and B. H. Walke, "Policy-based reasoning for spectrum sharing in radio networks," in *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, pp. 1–10.

[80] K. Baclawski, D. Brady, and M. Kokar, "Achieving Dynamic Interoperability of Communication at the Data Link Layer through Ontology Based Reasoning," in *2005 SDR Forum Technical Conference, Nov*, 2005, pp. 14–17.

[81] S. Oh and J. Aberle, "Reconfigurable Antennas as an Enabling Technology for SDR," 2004.

[82] D. Domalapally, J. Wang, and Y. Zhang, "Reconfigurable Oscillator and Filter," 2004 SDR Forum Technical Conference, Phoenix AZ," 2004.

[83] B. Le, T. Rondeau, J. Reed, and C. Bostian, "Past, Present, and Future of ADCs," *IEEE Signal Processing Magazine*, 2005.

[84] M. A. Ozkan, B. Ors, and G. Saldamli, *Secure voice communication via GSM network*. IEEE, 2011, pp. II–288–II–292.

[85] T. Han, N. Zhang, K. Liu, B. Tang, and Y. Liu, "Analysis of mobile WiMAX security: Vulnerabilities and solutions," *2008 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, vol. 7, no. 11, pp. 828–833, 2008.

[86] Y. Khit, "Synchronization of WCDMA TDD node B using better security sequences," in *2005 Fifth International Conference on Information Communications and Signal Processing*, 2005, vol. 2005, pp. 989–993.

[87] J.-Y. Choung, T. Hameed, and I. Ji, "Catch-up in ICT standards: Policy, implementation and standards-setting in South Korea," *Technological Forecasting and Social Change*, vol. 79, no. 4, pp. 771–788, 2012.

[88] IEEE-SA Standards Board, "IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Policies and procedures for operation in the TV," 2011. [Online]. Available: http://www.ieee802.org/22/Technology/22-10-0073-03-0000-802-22-overview-and-core-technologies.pdf. [Accessed: 04-Mar-2013].

[89] J. L. Burbank, "Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security," in *2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*, 2008, pp. 1–7.

[90] D. Yu, W. L. Liu, and Z. H. Zhang, "Simple structure multiband patch antenna with three slots," in *2012 International Conference on Microwave and Millimeter Wave Technology (ICMMT)*, 2012, pp. 1–3.

[91] C. Kuo and S. Kan, "Multiband antenna." 21-May-2010.

[92] C. Stevenson, G. Chouinard, S. Shellhammer, and W. Caldwell, "IEEE 802.22: The first cognitive radio wireless regional area network standard," *IEEE Communications Magazine*, vol. 47, no. 1, pp. 130–138, Jan. 2009.

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

[94] N. Bolívar, J. L. Marzo, and E. Rodríguez-Colina, "Distributed Control Using Cognitive Pilot Channels in a Centralized Cognitive Radio Network," in *2010 Sixth Advanced International Conference on Telecommunications*, 2010, pp. 30–34.

[95] M. H. Islam, "Power Control and Channel Allocation in Cognitive Radio Networks with Primary Users' Cooperation," *IEEE Transactions on Mobile Computing*, vol. 9, no. 3, pp. 348–360, Mar. 2010.

[96] I. F. Akyildiz, W.-Y. Lee, and K. R. Chowdhury, "CRAHNs: Cognitive radio ad hoc networks," *Ad Hoc Networks*, vol. 7, no. 5, pp. 810–836, Jul. 2009.

[97] G.-M. Zhu, I. F. Akyildiz, and G.-S. Kuo, "STOD-RP: A Spectrum-Tree Based On-Demand Routing Protocol for Multi-Hop Cognitive Radio Networks," in *IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference*, 2008, pp. 1–5.

[98] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer Networks*, vol. 50, no. 13, pp. 2127–2159, 2006.

[99] J. So and N. H. Vaidya, "Multi-channel mac for ad hoc networks," in *Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing - MobiHoc '04*, 2004, p. 222.

[100] Y. R. Kondareddy and P. Agrawal, "Synchronized MAC Protocol For Multi-Hop Cognitive Radio Networks," in *2008 IEEE International Conference on Communications*, 2008, pp. 3198–3202.

[101] G. P. Joshi, S. W. Kim, and B.-S. Kim, "An Efficient MAC Protocol for Improving the Network Throughput for Cognitive Radio Networks," in *2009 Third International Conference on Next Generation Mobile Applications, Services and Technologies*, 2009, pp. 271–275.

[102] G. A. Safdar and M. O'Neill, "Common Control Channel Security Framework for Cognitive Radio Networks," in *VTC Spring 2009 - IEEE 69th Vehicular Technology Conference*, 2009, pp. 1–5.

[103] A. C.-C. Hsu, D. S. L. Wei, and C.-C. J. Kuo, "A Cognitive MAC Protocol Using Statistical Channel Allocation for Wireless Ad-Hoc Networks," in *2007 IEEE Wireless Communications and Networking Conference*, 2007, pp. 105–110.

[104] G. P. Joshi, S. W. Kim, and B.-S. Kim, "An Efficient MAC Protocol for Improving the Network Throughput for Cognitive Radio Networks," in *2009 Third International Conference on Next Generation Mobile Applications, Services and Technologies*, 2009, pp. 271–275.

[105] H. Jiang, L. Lai, R. Fan, and H. V. Poor, "Optimal selection of channel sensing order in cognitive radio," *IEEE Transactions on Wireless Communications*, vol. 8, no. 1, pp. 297–307, Jan. 2009.

[106] I. F. Akyildiz, "Optimal spectrum sensing framework for cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 10, pp. 3845–3857, Oct. 2008.

[107] D. Cabric, A. Tkachenko, and R. W. Brodersen, "Experimental study of spectrum sensing based on energy detection and network cooperation," in *Proceedings of the first international workshop on Technology and policy for accessing spectrum - TAPAS '06*, 2006, p. 12–es.

[108] H.-S. W. So and J. Walrand, "Comparison of Multichannel MAC Protocols," *IEEE Transactions on Mobile Computing*, vol. 7, no. 1, pp. 50–65, Jan. 2008.

[109] H. Su and X. Zhang, "Channel-hopping based single transceiver MAC for cognitive radio networks," in *2008 42nd Annual Conference on Information Sciences and Systems*, 2008, pp. 197–202.

[110] J. Jia and Q. Zhang, "Hardware-Constrained Multi-Channel Cognitive MAC," in *IEEE GLOBECOM 2007-2007 IEEE Global Telecommunications Conference*, 2007, pp. 4653–4658.

[111] L. A. DaSilva and I. Guerreiro, "Sequence-Based Rendezvous for Dynamic Spectrum Access," in *2008 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2008, pp. 1–7.

[112] M. Rashid, M. Hossain, E. Hossain, and V. Bhargava, "Opportunistic spectrum scheduling for multiuser cognitive radio: a queueing analysis," *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 5259–5269, Oct. 2009.

[113] M. Sha, G. Xing, G. Zhou, S. Liu, and X. Wang, "C-MAC: Model-Driven Concurrent Medium Access Control for Wireless Sensor Networks," in *IEEE INFOCOM 2009 - The 28th Conference on Computer Communications*, 2009, pp. 1845–1853.

[114] C. Cordeiro and K. Challapali, "C-MAC: A Cognitive MAC Protocol for Multi-Channel Wireless Networks," in *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2007, pp. 147–157.

[115] Y. Song-song and W. Wei, "A MAC Protocol for Congested Cognitive Radio Network," in *2009 Second International Conference on Intelligent Networks and Intelligent Systems*, 2009, pp. 228–232.

[116] L. Ma, X. Han, and C.-C. Shen, "Dynamic open spectrum sharing MAC protocol for wireless ad hoc networks," in *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, pp. 203–213.

[117] J. Jia, Q. Zhang, and X. Shen, "HC-MAC: A Hardware-Constrained Cognitive MAC for Efficient Spectrum Management," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 106–117, Jan. 2008.

[118] A. V Adamis, K. N. Maliatsos, and P. Constantinou, "A new MAC protocol with control channel auto-discovery for self-deployed cognitive radio networks," in *13th Program for European Wireless*, 2007.

[119] H. A. B. Salameh, M. M. Krunz, and O. Younis, "MAC Protocol for Opportunistic Cognitive Radio Networks with Soft Guarantees," *IEEE Transactions on Mobile Computing*, vol. 8, no. 10, pp. 1339–1352, Oct. 2009.

[120] S.-Y. Lien, C.-C. Tseng, and K.-C. Chen, "Carrier Sensing Based Multiple Access Protocols for Cognitive Radio Networks," in *2008 IEEE International Conference on Communications*, 2008, pp. 3208–3214.

[121] B. Hamdaoui and K. G. Shin, "OS-MAC: An Efficient MAC Protocol for Spectrum-Agile Wireless Networks," *IEEE Transactions on Mobile Computing*, vol. 7, no. 8, pp. 915–930, Aug. 2008.

[122] L. Pan and H. Wu, "Performance Evaluation of The SYN-MAC Protocol in Multihop Wireless Networks," in *2007 16th International Conference on Computer Communications and Networks*, 2007, pp. 265–271.

[123] L. A. DaSilva and I. Guerreiro, "Sequence-Based Rendezvous for Dynamic Spectrum Access," in *2008 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2008, pp. 1–7.

[124] D. Niyato and E. Hossain, "Cognitive radio for next-generation wireless networks: an approach to opportunistic channel selection in ieee 802.11-based wireless mesh," *IEEE Wireless Communications*, vol. 16, no. 1, pp. 46–54, Feb. 2009.

[125] H. Su and X. Zhang, "Channel-hopping based single transceiver MAC for cognitive radio networks," in *2008 42nd Annual Conference on Information Sciences and Systems*, 2008, pp. 197–202.

[126] H. Jiang, L. Lai, R. Fan, and H. V. Poor, "Optimal selection of channel sensing order in cognitive radio," *IEEE Transactions on Wireless Communications*, vol. 8, no. 1, pp. 297–307, Jan. 2009.

[127] S.-Y. Hung, Y.-C. Cheng, E. H.-K. Wu, and G.-H. Chen, "An Opportunistic Cognitive MAC Protocol for Coexistence with WLAN," in *2008 IEEE International Conference on Communications*, 2008, pp. 4059–4063.

[128] C. Cordeiro and K. Challapali, "C-MAC: A Cognitive MAC Protocol for Multi-Channel Wireless Networks," in *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2007, pp. 147–157.

[129] M.-R. Kim and S.-J. Yoo, "Distributed Coordination Protocol for Common Control Channel Selection in Multichannel Ad-Hoc Cognitive Radio Networks," in *2009 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 2009, pp. 227–232.

[130] H. S. H. Song and X. L. X. Lin, *A Leasing Oriented MAC Protocol for High Spectrum Usage in Cognitive Radio Networks*. Ieee, 2009, pp. 173–178.

[131] H. Song and X. Lin, "A Leasing Oriented MAC Protocol for High Spectrum Usage in Cognitive Radio Networks," in *2009 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 2009, pp. 173–178.

[132] C. Wang, B. Li, and L. Li, "A New Collision Resolution Mechanism to Enhance the Performance of IEEE 802.11 DCF," *IEEE Transactions on Vehicular Technology*, vol. 53, no. 4, pp. 1235–1246, Jul. 2004.

[133] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, pp. 535–547, Mar. 2000.

[134] A. Zuquete, "Improved CSMA/CA Protocol for IEEE 802.11," in *2008 Next Generation Internet Networks*, 2008, pp. 247–252.

[135] H. Kim and K. G. Shin, "In-band spectrum sensing in cognitive radio networks: energy detection or feature detection?," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, 2008, pp. 14–25.

[136] M. Y. El Nainay, D. H. Friend, and A. B. MacKenzie, "Channel Allocation & Power Control for Dynamic Spectrum Cognitive Networks using a Localized Island Genetic Algorithm," in *2008 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2008, pp. 1–5.

[137] D. Willkomm, M. Bohge, D. Hollos, J. Gross, and A. Wolisz, "Double Hopping: A new approach for Dynamic Frequency Hopping in Cognitive Radio networks," in *2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2008, pp. 1–6.

[138] H. Zheng and C. Peng, "Collaboration and fairness in opportunistic spectrum access," in *IEEE International Conference on Communications, 2005. ICC 2005. 2005*, vol. 5, pp. 3132–3136.

[139] C. Zou and C. Chigan, "A Game Theoretic DSA-Driven MAC Framework for Cognitive Radio Networks," in *2008 IEEE International Conference on Communications*, 2008, pp. 4165–4169.

[140] O. Younis and M. Krunz, "GMAC: A Game-theoretic MAC Protocol for Mobile Ad Hoc Networks," in *2006 4th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, pp. 1–9.

[141] A. Swami, "Decentralized cognitive mac for dynamic spectrum access," in *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, pp. 224–232.

[142] T. W. Rondeau, B. Le, C. J. Rieser, and C. W. Bostian, "Cognitive radios with genetic algorithms: Intelligent control of software defined radios," in *Software Defined Radio Forum Technical Conference*, 2004, pp. C3–C8.

[143] Q. Zhao, L. Tong, A. Swami, and Y. Chen, "Decentralized cognitive MAC for opportunistic spectrum access in ad hoc networks: A POMDP framework," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 3, pp. 589–600, Apr. 2007.

[144] Y. Yuan, P. Bahl, R. Chandra, P. A. Chou, J. I. Ferrell, T. Moscibroda, S. Narlanka, and Y. Wu, "KNOWS: Cognitive Radio Networks Over White Spaces," in *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2007, pp. 416–427.

[145] H. Su and X. Zhang, "Interference-Confined Adaptive Transmission Scheme for Cognitive Radio Networks," in *2010 IEEE International Conference on Communications*, 2010, pp. 1–5.

[146] L. Ma, X. Han, and C. Shen, "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.

[147] Y. Xing, C. Mathur, M. A. Haleem, R. Chandramouli, and K. P. Subbalakshmi, "Dynamic Spectrum Access with QoS and Interference Temperature Constraints," *IEEE Transactions on Mobile Computing*, vol. 6, no. 4, pp. 423–433, Apr. 2007.

[148] D. Niyato and E. Hossain, "A Game-Theoretic Approach to Competitive Spectrum Sharing in Cognitive Radio Networks," in *2007 IEEE Wireless Communications and Networking Conference*, 2007, pp. 16–20.

[149] C. Chou, S. N, H. Kim, and K. Shin, "What and how much to gain by spectrum agility?," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 3, pp. 576–588, Apr. 2007.

[150] S. Huang, X. Liu, and Z. Ding, "Opportunistic Spectrum Access in Cognitive Radio Networks," in *2008 IEEE INFOCOM - The 27th Conference on Computer Communications*, 2008, pp. 1427–1435.

[151] S. Huang, X. Liu, and Z. Ding, "Optimal Sensing-Transmission Structure for Dynamic Spectrum Access," in *IEEE INFOCOM 2009 - The 28th Conference on Computer Communications*, 2009, pp. 2295–2303.

[152] S. Huang, X. Liu, and Z. Ding, "Optimal Transmission Strategies for Dynamic Spectrum Access in Cognitive Radio Networks," *IEEE Transactions on Mobile Computing*, vol. 8, no. 12, pp. 1636–1648, Dec. 2009.

[153] S. Geirhofer, L. Tong, and B. Sadler, "Cognitive Medium Access: Constraining Interference Based on Experimental Models," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 95–105, Jan. 2008.

[154] E. Hossain, "Joint rate and power allocation for cognitive radios in dynamic spectrum access environment," *IEEE Transactions on Wireless Communications*, vol. 7, no. 12, pp. 5517–5527, Dec. 2008.

[155] A. Elezabi, M. Kashef, M. Abdallah, and M. M. Khairy, "Cognitive interference-minimizing code assignment for underlay CDMA networks in asynchronous multipath fading channels," in *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing Connecting the World Wirelessly - IWCMC '09*, 2009, p. 1279.

[156] B. Wang and D. Zhao, "Performance Analysis in CDMA-Based Cognitive Wireless Networks with Spectrum Underlay," in *IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference*, 2008, pp. 1–6.

[157] A. Hoang and Y. Liang, "A Two-Phase Channel and Power Allocation Scheme for Cognitive Radio Networks," in *2006 IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2006, pp. 1–5.

[158] L. Zhang, Y.-C. Liang, and Y. Xin, "Joint Beamforming and Power Allocation for Multiple Access Channels in Cognitive Radio Networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 38–51, Jan. 2008.

[159] H. A. B. Salameh, M. M. Krunz, and O. Younis, "MAC Protocol for Opportunistic Cognitive Radio Networks with Soft Guarantees," *IEEE Transactions on Mobile Computing*, vol. 8, no. 10, pp. 1339–1352, Oct. 2009.

[160] S. Srinivasa and S. Jafar, "COGNITIVE RADIOS FOR DYNAMIC SPECTRUM ACCESS - The Throughput Potential of Cognitive Radio: A Theoretical Perspective," *IEEE Communications Magazine*, vol. 45, no. 5, pp. 73–79, May 2007.

[161] L. Le and E. Hossain, "A MAC Protocol for Opportunistic Spectrum Access in Cognitive Radio Networks," in *2008 IEEE Wireless Communications and Networking Conference*, 2008, pp. 1426–1430.

[162] L.-C. Wang, A. Chen, and D. S. L. Wei, "A Cognitive MAC Protocol for QoS Provisioning in Overlaying Ad Hoc Networks," in *2007 4th IEEE Consumer Communications and Networking Conference*, 2007, pp. 1139–1143.

[163] L. Ma, C.-C. Shen, and B. Ryu, "Single-Radio Adaptive Channel Algorithm for Spectrum Agile Wireless Ad Hoc Networks," in *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2007, pp. 547–558.

[164] K. G. Shin, "Efficient Discovery of Spectrum Opportunities with MAC-Layer Sensing in Cognitive Radio Networks," *IEEE Transactions on Mobile Computing*, vol. 7, no. 5, pp. 533–545, May 2008.

[165] W. C. Hung, K. L. E. Law, and A. Leon-Garcia, "A dynamic multi-channel MAC for ad hoc LAN," in *Proc. 21st Biennial symposium on communications*, 2002, pp. 31–35.

[166] A. Nasipuri, J. Zhuang, and S. R. Das, "A multichannel CSMA MAC protocol for multihop wireless networks," in *WCNC. 1999 IEEE Wireless Communications and Networking Conference (Cat. No.99TH8466)*, pp. 1402–1406.

[167] A. Nasipuri and S. R. Das, "Multichannel CSMA with signal power-based channel selection for multihop wireless networks," in *Vehicular Technology Conference Fall 2000. IEEE VTS Fall VTC2000. 52nd Vehicular Technology Conference (Cat. No.00CH37152)*, vol. 1, pp. 211–218.

[168] N. Jain, S. R. Das, and A. Nasipuri, "A multichannel CSMA MAC protocol with receiver-based channel selection for multihop wireless networks," in *Proceedings Tenth International Conference on Computer Communications and Networks (Cat. No.01EX495)*, pp. 432–439.

[169] S.-L. Wu, C.-Y. Lin, Y.-C. Tseng, and J.-L. Sheu, "A new multi-channel MAC protocol with on-demand channel assignment for multi-hop mobile ad hoc networks," in *Proceedings International Symposium on Parallel Architectures, Algorithms and Networks. I-SPAN 2000*, pp. 232–237.

[170] J. Wang, Y. Fang, and D. Wu, "A Power-Saving Multi-Radio Multi-Channel MAC Protocol for Wireless Local Area Networks," in *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*, 2006, pp. 1–12.

[171] D. Raychaudhuri, "A spectrum etiquette protocol for efficient coordination of radio devices in unlicensed bands," in *14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003.*, vol. 1, pp. 172–176.

[172] E. Hossain, "Cognitive Wireless Communication Networks," Dec. 2009.

[173] L. Ma, X. Han, and C. Shen, "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, 2005.

[174] H. A. B. Salameh, M. M. Krunz, and O. Younis, *MAC Protocol for Opportunistic Cognitive Radio Networks with Soft Guarantees*, vol. 8, no. 10. IEEE, 2009, pp. 1339–1352.

[175] L. Le and E. Hossain, "A MAC Protocol for Opportunistic Spectrum Access in Cognitive Radio Networks," in *2008 IEEE Wireless Communications and Networking Conference*, 2008, pp. 1426–1430.

[176] T. Chen, H. Zhang, G. M. Maggio, and I. Chlamtac, "CogMesh: A Cluster-Based Cognitive Radio Network," in *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2007, pp. 168–178.

[177] Y. C. Y. Chen, Q. Z. Q. Zhao, and A. Swami, *Distributed Cognitive MAC for Energy-Constrained Opportunistic Spectrum Access*, no. POMDP. Ieee, 2006, pp. 1–7.

[178] H. Su and X. Zhang, "Cross-Layer Based Opportunistic MAC Protocols for QoS Provisionings Over Cognitive Radio Wireless Networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 118–129, Jan. 2008.

[179] D. Xue, E. Ekici, and X. Wang, "Opportunistic Periodic MAC Protocol for Cognitive Radio Networks," in *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, 2010, pp. 1–6.

[180] C.-F. Shih, T. Y. Wu, and W. Liao, "DH-MAC: A Dynamic Channel Hopping MAC Protocol for Cognitive Radio Networks," in *2010 IEEE International Conference on Communications*, 2010, pp. 1–5.

[181] W. S. Jeon, J. A. Han, and D. G. Jeong, "A Novel MAC Scheme for Multichannel Cognitive Radio Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 6, pp. 922–934, Jun. 2012.

[182] H.-L. Chao, T. Lou, and S. Jiang, "F2-MAC: an efficient channel sensing and access mechanism for cognitive radio networks," *Wireless Networks*, vol. 17, no. 5, pp. 1113–1126, Apr. 2011.

[183] A. De Domenico, E. Calvanese Strinati, and M.-G. Di Benedetto, "A Survey on MAC Strategies for Cognitive Radio Networks," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 1, pp. 21–44, 2012.

[184] J. Misic, "Cooperative Sensing at the MAC Level in Simple Cognitive Personal Area Networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 9, pp. 1711–1718, Oct. 2012.

[185] S. Agarwal, R. K. Shakya, Y. N. Singh, and A. Roy, "DSAT-MAC: Dynamic slot allocation based TDMA MAC protocol for Cognitive Radio Networks," in *2012 Ninth*

International Conference on Wireless and Optical Communications Networks (WOCN), 2012, pp. 1–6.

[186] Y. Li, Y. Qian, X. Wang, and M. Daneshmand, "A MAC protocol supporting Dynamic Control Channel for cognitive radio ad hoc networks," in *2011 International Conference on Electronics, Communications and Control (ICECC)*, 2011, pp. 37–40.

[187] X. Li and X. Zhang, "A cluster-based MAC protocol for cognitive radio ad hoc networks," in Springer *Wireless personal communications*, 2012, pp. 1–10.

[188] Q. Chen, Y.-C. Liang, M. Motani, and W.-C. Wong, "A Two-Level MAC Protocol Strategy for Opportunistic Spectrum Access in Cognitive Radio Networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 5, pp. 2164–2180, 2011.

[189] S. C. Jha, U. Phuyal, M. M. Rashid, and V. K. Bhargava, "Design of OMC-MAC: An Opportunistic Multi-Channel MAC with QoS Provisioning for Distributed Cognitive Radio Networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3414–3425, Oct. 2011.

[190] C. A. Patel and S. Kumar, "Enhancing Throughput Efficiency of Adhoc Wireless Networks Using Cognitive Radio Approach," in *2011 International Conference on Devices and Communications (ICDeCom)*, 2011, pp. 1–5.

[191] H.-L. Chao, T. Lou, and S. Jiang, "F2-MAC: an efficient channel sensing and access mechanism for cognitive radio networks," *Wireless Networks*, vol. 17, no. 5, pp. 1113–1126, Apr. 2011.

[192] M. Timmers, S. Pollin, A. Dejonghe, L. Van der Perre, and F. Catthoor, "A Distributed Multichannel MAC Protocol for Multihop Cognitive Radio Networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 1, pp. 446–459, Jan. 2010.

[193] N. Bolívar, J. L. Marzo, and E. Rodríguez-Colina, "Distributed Control Using Cognitive Pilot Channels in a Centralized Cognitive Radio Network," in *2010 Sixth Advanced International Conference on Telecommunications*, 2010, pp. 30–34.

[194] M. H. Islam, "Power Control and Channel Allocation in Cognitive Radio Networks with Primary Users' Cooperation," *IEEE Transactions on Mobile Computing*, vol. 9, no. 3, pp. 348–360, Mar. 2010.

[195] C. Cormio and K. R. Chowdhury, "A survey on MAC protocols for cognitive radio networks," *Ad Hoc Networks*, vol. 7, no. 7, pp. 1315–1329, 2009.

[196] Y. Ke and S.-J. Yoo, "MCR-MAC: Multi-channel cognitive radio MAC protocol for cooperative incumbent system protection in wireless ad-hoc network," in *2009 First International Conference on Ubiquitous and Future Networks*, 2009, pp. 6–11.

[197] H. Kim, and K. G. Shin, "Efficient Discovery of Spectrum Opportunities with MAC-Layer Sensing," *University of Michigan, Tech. Journal. Rep. CSE-TR-518-06*, 2006.

[198] J. Liu, W. Chen, Z. Cao, and Y. J. (Angela) Zhang, "Token-based opportunistic scheduling protocol for cognitive radios with distributed beamforming," *IET Communications*, vol. 6, no. 8, p. 945, 2012.

[199] M. Gast, *802.11 Wireless Networks: The Definitive Guide*. O'Reilly Media, Inc., 2005, p. 630.

[200] I.-S. S. Board, *Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, vol. 2012, no. March. 2012.

[201] H. L. Vu and T. Sakurai, “Collision probability in saturated IEEE 802.11 networks,” in *Australian Telecommunication Networks and Applications Conference, Australia*, 2006.

[202] B. Wang, Z. Ji, and K. J. R. Liu, “Primary-Prioritized Markov Approach for Dynamic Spectrum Access,” in *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2007, pp. 507–515.

[203] R. Chandramouli, S. Mangold, and S. S. N, “Dynamic spectrum access in open spectrum wireless networks,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 3, pp. 626–637, Mar. 2006.

[204] U. Mir, L. Merghem-Boulahia, M. Esseghir, and D. Gaiti, “A continuous time Markov model for unlicensed spectrum access,” in *2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2011, pp. 68–73.

[205] R. Chandramouli, S. Mangold, and S. S. N, “Dynamic spectrum access in open spectrum wireless networks,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 3, pp. 626–637, Mar. 2006.

[206] W. Wei, B. Wang, and D. Towsley, “Continuous-time hidden Markov models for network performance evaluation,” *Performance Evaluation*, vol. 49, no. 1–4, pp. 129–146, Sep. 2002.

[207] G. Latouche and V. Ramaswami, *Introduction to matrix analytic methods in stochastic modeling*, vol. 5. Society for Industrial Mathematics, 1987.

[208] R. Urgaonkar and M. J. Neely, “Opportunistic Scheduling with Reliability Guarantees in Cognitive Radio Networks,” *IEEE Transactions on Mobile Computing*, vol. 8, no. 6, pp. 766–777, Jun. 2009.

[209] H. B. Salameh, M. Krunz, and O. Younis, “Distance- and Traffic-Aware Channel Assignment in Cognitive Radio Networks,” in *2008 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, 2008, pp. 10–18.

[210] M. A. Shah, G. A. Safdar, C. Maple, and K. Sardar, “Network Performance Optimization: A Case Study of Enterprise Network Simulated in OPNET,” in *2011 Frontiers of Information Technology*, 2011, pp. 57–62.

[211] OPNET Technologies, “OPNET Application and Network Performance.” [Online]. Available: www.opnet.com.

[212] IEEE-SA Standards Board, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” 2007.

[213] “Network Simulator.” [Online]. Available: www.nsnam.org.

[214] “OMNeT++.” [Online]. Available: http://www.omnetpp.org/models.

[215] A. Sethi and T. X. Brown, “Hammer Model Threat Assessment of Cognitive Radio Denial of Service Attacks,” *2008 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, pp. 1–12, 2008.

[216] R. C. R. Chen, J.-M. P. J.-M. Park, and J. H. Reed, *Defense against Primary User Emulation Attacks in Cognitive Radio Networks*, vol. 26, no. 1. 2008, pp. 25–37.

[217] S. Anand, Z. Jin, and K. P. Subbalakshmi, "An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks," *2008 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, pp. 1–6, 2008.

[218] J. L. Burbank, A. R. Hammons, and S. D. Jones, "A common lexicon and design issues surrounding cognitive radio networks operating in the presence of jamming," in *Military Communications Conference, 2008. MILCOM 2008. IEEE*, 2008, pp. 1–7.

[219] S. Liu, Y. Chen, W. Trappe, and L. J. Greenstein, "ALDO: An Anomaly Detection Framework for Dynamic Spectrum Access Networks," *IEEE INFOCOM 2009 The 28th Conference on Computer Communications*, pp. 675–683, 2009.

[220] L. Ma and C.-C. Shen, "Security-enhanced Virtual Channel Rendezvous Algorithm for Dynamic Spectrum Access Wireless Networks," in *Third IEEE International Symposium on Dynamic Spectrum Access Networks 2008 DySPAN 2008*, 2008.

[221] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Robust Spectrum Decision Protocol against Primary User Emulation Attacks in Dynamic Spectrum Access Networks," *Communications Society*, pp. 6–10, 2010.

[222] N. Goergen, T. C. Clancy, and T. R. Newman, "Physical Layer Authentication Watermarks through Synthetic Channel Emulation," *2010 IEEE Symposium on New Frontiers in Dynamic Spectrum DySPAN*, pp. 1–7, 2010.

[223] H. Li and Z. Han, "Dogfight in Spectrum : Jamming and Anti-Jamming in Multichannel Cognitive Radio Systems," *IEEE Global Telecommunications Conference*, pp. 1–6, 2009.

[224] H. L. H. Li and Z. H. Z. Han, *Dogfight in Spectrum: Combating Primary User Emulation Attacks in Cognitive Radio Systems, Part I: Known Channel Statistics*, vol. 9, no. 11. 2010, pp. 3566–3577.

[225] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc ACM Mobihoc*, 2005, pp. 46–57.

[226] D. E. Robling Denning, *Cryptography and data security*. Addison-Wesley Longman Publishing Co., Inc., 1982.

[227] S. William and others, *Cryptography and Network Security, 4/e*. Pearson Education India, 2006.

[228] N. A. Pantazis, D. J. Vergados, D. D. Vergados, and C. Douligeris, "Energy efficiency in wireless sensor networks using sleep mode TDMA scheduling," *Ad Hoc Networks*, vol. 7, no. 2, pp. 322–343, Mar. 2009.

[229] S. A. R. Zaidi, M. Ghogho, D. C. McLernon, and A. Swami, "Energy Efficiency in Large Scale Interference Limited wireless ad hoc networks," in *2012 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, 2012, pp. 24–29.

[230] H. Su and X. Zhang, "Cognitive Radio Based Multi-Channel MAC Protocols for Wireless Ad Hoc Networks," in *IEEE GLOBECOM 2007-2007 IEEE Global Telecommunications Conference*, 2007, pp. 4857–4861.

[231] S. M. Kamruzzaman, E. Kim, and D. G. Jeong, "An energy efficient QoS routing protocol for cognitive radio ad hoc networks."

[232] F. F. Qureshi, "Energy efficient cognitive radio MAC protocol for adhoc networks," in *Wireless Telecommunications Symposium 2012*, 2012, pp. 1–5.