Design and development of MAC and routing protocols for cognitive radio based wireless mesh networks

How, Kiam Cheng

2014

How, K. C. (2014). Design and development of MAC and routing protocols for cognitive radio based wireless mesh networks. Doctoral thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/58909>

<https://doi.org/10.32657/10356/58909>

NANYANG TECHNOLOGICAL UNIVERSITY

**Design and Development of MAC and Routing
Protocols for Cognitive Radio Based Wireless Mesh
Networks**

How Kiam Cheng

**School of Electrical and Electronic Engineering
Nanyang Technological University**

*A thesis submitted to the Nanyang Technological University
in fulfilment of the requirements for the degree of
Doctor of Philosophy (EEE)*

Supervised by Assoc Prof. Ma Maode

2014

Statement of Originality

I hereby certify that content of this thesis is the result of work done by me and has not been submitted for a higher degree to any other University or Institution.

Date

How Kiam Cheng

Acknowledgement

First of all, I would like to thank my supervisor, Prof. Ma Maode for helping me so much in many ways. He has been an ideal supervisor from every aspect, both in terms of technical and instructive advice on my research and in terms of general advice on my career.

I would also like to thank Prof Qin Yang for her important advice and comments on my research. I would also like to express my gratitude to the anonymous reviewers for their valuable comments on my submitted papers and thesis.

Lastly, I would like to thank my wife Phyllis and my two children, Scarlett and Inge for their love and unconditional support over the years.

Table of Contents

Statement of Originality.....	ii
Acknowledgement	iii
Table of Contents.....	iv
Summary	vi
List of Figures	xi
List of Tables	xiii
List of Abbreviations	xiv
Chapter 1: Introduction.....	1
1.1 Motivation.....	4
1.1.1 Physical layer issues	4
1.1.2 MAC Layer Issues	6
1.1.3 Network Layer Issues	8
1.1.4 Cognitive Radio Security Issues	11
1.2 Research Objective	12
1.3 Summary of Contributions.....	13
1.4 Thesis Organisation	16
Chapter 2: Literature Survey	17
2.1 Legacy MAC-Layer Solutions	18
2.2 IEEE 802.11e-Based MAC Solutions	20
2.3 Legacy Routing Solutions	22
2.4 Cross Layer Solutions	25
2.4.1 Cross layer solutions supported by beam-forming/directional antennas	26
2.4.2 Cross layer solutions supported by multiple channels/radio interfaces/antennas	28
2.4.3 Cross layer solutions supported by power control and rate control	31
2.5 Cognitive Radio Solutions	33
2.5.1 Spectrum Sensing	33
2.5.2 Cognitive Radio Based MAC and Network Layer Solution	35
2.5.3 Cognitive Radio Based Resource Allocation Strategies	39
2.5.4 Cognitive Radio Security Solutions.....	42
2.6 Summary of Review Work	44
Chapter 3: MAC-Layer Solutions for QoS Provisioning.....	47
3.1 A MAC-Layer QoS Provisioning Protocol for Cognitive Radio Networks	48
3.1.1 System Model.....	48
3.1.2 Proposed Scheme.....	58
3.1.3 Mathematical Analysis of Throughput/Delay.....	65

3.1.4	Performance Evaluation.....	71
3.1.4	Conclusion.....	77
3.2	Elastic Bandwidth Allocation Scheme with Softened Peak Interference Power Constraint for the Dynamic Cognitive Radio Systems	77
3.2.1	System Model.....	79
3.2.2	Proposed Elastic Bandwidth Allocation Scheme.....	84
3.2.3	Numerical Results.....	89
3.2.4	Conclusion.....	93
Chapter 4:	Network Layer Solutions for QoS Provisioning.....	95
4.1	Dynamic Virtual Carrier Sensing and Interference Aware Routing Protocol	95
4.1.1	Route Discover and Maintenance in DVCSIR	96
4.1.2	Quietness Index (QI)	97
4.1.3	Dynamic Virtual Carrier Sensing	98
4.1.4	Interference Aware Routing	100
4.1.5	Simulation Model and Result	100
4.1.6	Conclusion.....	103
4.2	Opportunistic Service Differentiation Routing Protocol for the Dynamic CRNs	104
4.2.1	System Model.....	105
4.2.2	Proposed Scheme.....	110
4.2.3	Performance Evaluation.....	116
4.2.4	Conclusion.....	129
Chapter 5:	Trusted Routing	131
5.1	An Altruistic Differentiated Service Protocol in Dynamic Cognitive Radio Networks against Selfish Behaviours.....	132
5.1.1	System Model.....	133
5.1.2	Proposed Scheme.....	137
5.1.3	Numerical Results.....	146
5.1.4	Conclusion.....	151
Chapter 6:	Conclusion and Recommendation.....	152
6.1	Conclusion	152
6.2	Recommendations for Further Research	153
6.2.1	QoS Support for the IEEE 802.22-based Wireless Regional Area Network (WRAN)...	153
6.2.2	Research on Cognitive Radio Security	155
List of Publications		158
Journal Paper		158
Conference Paper.....		158
Papers in Submission.....		159
References		160

Summary

Wireless Mesh Networks (WMNs) are communications networks made up of radio nodes organized in a mesh topology. It is envisaged that WMNs can provide broadband wireless access and replace traditional wired based communications infrastructure in the near future. Correspondingly, WMNs are also expected to support delay sensitive and/or high bandwidth real-time streaming multimedia applications such as VoIP and video conferencing. However, Quality-of-Service (QoS) provisioning in WMNs is very challenging due to various factors. These include physical layer factors such as fading or attenuation of a transmitted signal over the wireless medium which results in a loss of signal power at the receiver. Other factors include the dynamical changing of topology, capacity limitations, link variability and multi-hop communications. On the network layer, many existing dynamic routing protocols select paths based on only one criteria (shortest hops, delay etc), which do not take into account topology, interference or traffic pattern. This causes the traffic to flow through nodes that experience high interference and thus increases the occurrences of dropped packets and retransmissions.

Despite on-going research efforts, one key limitation to the performance of the WMNs is the interfering nature of wireless transmissions which degrades the network capacity. This is made worse, especially for the case of devices operating in the unlicensed spectrum where it is becoming increasingly crowded due to the proliferation of diverse wireless communication systems. The overcrowding of the unlicensed spectrum aggravates the interference issues which further reduces the performances of wireless devices. The interference is further exacerbated in WMNs where traffic takes multiple hops to reach the destination.

Based on surveys that have shown that vast portions of the licensed spectrum remain underutilized across frequency, space and time, the use of cognitive radio (CR) based WMNs or cognitive radio networks (CRNs) is becoming increasingly popular due to their capability to exploit frequency bands currently unoccupied for use. Notwithstanding the great potential, there are also pitfalls in the adoption of CR technology.

In the course of our research, we have identified many gaps in the area of WMN and CRN research literature. There were inadequacy in terms of medium access control (MAC) and network layer solutions for QoS provisioning in both WMNs and CRNs. Furthermore, many schemes proposed for CRNs have introduced significant security loopholes and this has introduced significant challenges to the operation of the CRN across various network layers.

To address these gaps, we examined and proposed different strategies to tackle the challenging issue of QoS provisioning in CRNs across the three different networking layers, physical, MAC and network layer. In our work documented within this thesis, we have improved the capability of CRNs to meet the required QoS for broadband applications by designing and developing MAC and network layer protocols that provides superior performance compared to existing protocols. Our protocol design considers a combination of different metrics like network topology, traffic pattern, interference and transmission properties like transmission power, modulation, rate etc., instead of traditional shortest path approach.

Our first task was to design and implement the MAC-Layer QoS Provisioning Protocol (MQPP) for Cognitive Radio Networks which combines adaptive modulation and coding with dynamic spectrum access. The simulation results have indicated that the proposed MQPP scheme can provide a significant performance

improvement in terms of lower delay and higher throughput at the cost of only a slight increase of transmission power and protocol overheads. MQPP can also provide clear service differentiations for different traffic classes under all traffic loads.

Next, we examined resource allocation strategy by proposing an Elastic Bandwidth Allocation Scheme (EBAS) with a consideration for softened peak interference power constraint. Our proposed scheme is able to combine the strength of both overlay and underlay transmission mode and provide superior performance through the use of the softened peak interference power constraint. In a cognitive radio system with dynamic primary user activity, the EBAS scheme is able to provide a much higher capacity to cooperative nodes compared to an overlay or underlay only approach. EBAS is also able to provide differentiated service to secondary users with different priority and to sustain the service differentiation in the presence of primary user activity.

Although the physical and MAC layer solutions are able to improve the performance for the CRNs in terms of QoS provisioning, a judicious routing strategy is also equally important in ensuring a good performance in terms of the network delay and throughput. Thus, the second part of our research focuses on the design and implementation of dynamic routing protocols for CRNs.

In the first part of our work on dynamic routing protocols, we designed and implemented a dynamic virtual carrier sensing and interference aware routing protocol (DVCSIR). The basic idea is that an optimum path is not necessarily the shortest hop one, but is one that has the least cost according to several criteria like interference, path length, traffic condition etc. The proposed DVCSIR scheme selects the optimum path based on two criteria, shortest path and Quietness Index (QI). The QI is a novel metric which we have developed to quantify the potential interference

experienced by a node in the WMN. DVCSIR then makes use of the QI to find the least interference route from source to destination. We also introduced the dynamic virtual carrier sensing mechanism, where the virtual carrier sensing is performed on a node by node basis, depending on the node density. This allows the virtual carrier sensing mechanism to be applied only in parts of the network where collision is the likeliest to happen. The simulation results indicated that DVCSIR has superior performance due to its dynamic virtual carrier sensing mechanism, and interference aware path routing.

In the second part of our research on routing protocols, we extend on the idea of multi-metric routing by proposing and implementing the Opportunistic Service Differentiation Routing Protocol (OSDRP) for the dynamic CRNs. OSDRP discovers the minimum delay – maximum stability route in dynamic CRNs by considering the availability of spectrum opportunity in addition to switching delay and queuing delay across primary user networks. In addition, service differentiation can be achieved through a combination of transmit power control and opportunistic routing. Simulation results demonstrate that the OSDRP achieves much better performance in terms of lower delay and higher throughput compared to other existing routing protocols across various scenarios.

In the final part of our research, we consider the issue of security provisioning in CRNs. The designs of network protocols, especially those for spectrum sharing and management have introduced significant security loopholes. At the same time, most existing cognitive routing protocols assumed that each node honestly participates in packet forwarding. However, this assumption is no longer legitimate for CRNs due to the lack of a centralized trusted authority. QoS provisioning may also suffers as selfish nodes might incline towards self-centred behaviours in order to maximize their

interests. Examples of such acts include deliberately dropping others' packets, refusing to engage in forwarding of others' packets or mislabelling all packets from the current node as high priority. These selfish behaviours can lead to monopolization of the wireless channel by the selfish nodes, or in a more severe case, the failure of routing protocols. To address the QoS provisioning issue in CRNs with selfish nodes coexistence, we propose a cross-layer Altruistic Differentiated Service Protocol (ADSP) for the dynamic CRNs in the presence of selfish nodes. Simulation results demonstrate that the ADSP can achieve much better performance in terms of lower delay, higher throughput and better delivery ratio for the traffic originating from collaborative nodes compared to other cognitive routing protocols in the presence of selfish nodes.

We conclude our work and also provide a direction for future research at the end of the thesis.

List of Figures

Figure 1: Typical Wireless Mesh Network Architecture	1
Figure 2: Typical Cognitive Radio Network Architecture	3
Figure 3: Hidden Terminal Problem	7
Figure 4: Exposed Terminal Problem	8
Figure 5: Example of shortest hop route subjected to high interference.	10
Figure 6: Example of a topology-sensitive minimum interference route.	10
Figure 7: Spectrum Holes or Spectrum Opportunities.....	18
Figure 8: MQPP Control Frame Structure	51
Figure 9: Frequency interference region where $ F =1$	56
Figure 10: Frequency interference region where $ F =3$	57
Figure 11: Power Transmission Ratio vs. Normalized Forwarding Capacity	57
Figure 12: MQPP Handshaking	58
Figure 13: MQPP Flow Diagram.....	59
Figure 14: Example Snapshot of Channel Information Cache and VCL.....	60
Figure 15: Channel Switching Scenarios	62
Figure 16: Markov Chain model.....	66
Figure 17: Normalized Network Throughput	70
Figure 18: Normalized Delay.....	71
Figure 19: Delay vs. Offered Load	74
Figure 20: Throughput vs. Offered Load	74
Figure 21: Average Transmission Power vs. Offered Load	76
Figure 22: Total Protocol Overheads vs. Offered Load.....	76
Figure 23: Delivery Ratio vs. Offered Load	76
Figure 24: Channel Allocation.....	80
Figure 25: Overheads of Transmission Mode Switching	81
Figure 26: Power profile for priority c_I SUs with different Φ_j	86
Figure 27: Average capacity of the different schemes vs. Φ	91
Figure 28: Average capacity of SUs under EBAS with different priority vs. Φ	92
Figure 29: No. of PUs affected by noise vs. Φ	92
Figure 30: Average Capacity of EBAS scheme vs. Φ using different values of L	93

Figure 31: No. of PUs affected by noise vs. Φ	93
Figure 32: WLAN throughput comparison between DVCSIR and DSR	102
Figure 33: WLAN delay comparison between DVCSIR and DSR	102
Figure 34: WLAN throughput comparison under DVCSIR with different values of V	103
Figure 35: Two-State Semi-Markov Modelling of SOP.....	109
Figure 36: OSDRP Flow Diagram.....	111
Figure 37: Differentiated OR Candidate Selection Range.....	114
Figure 38: Simulated Topology	117
Figure 39: Average number of hops vs. p	119
Figure 40: Route Comparison between OSDRP, ccDSR, DORP and SAMER for $p =$ 0.1.....	119
Figure 41: Average End-to-end Delay vs. p	120
Figure 42: Total Throughput vs. p	121
Figure 43: Average End-to-end Delay vs. τ for $p = 0.5$ (Dynamic SOP Scenario) ...	122
Figure 44: Total Throughput vs. τ for $p = 0.5$ (Dynamic SOP Scenario)	123
Figure 45: Route Comparison among Different Traffic Priorities for OSDRP (Dynamic SOP Scenario).....	123
Figure 46: Average End-to-end Delay vs. τ for $p = 0.5$ (Node Mobility Scenario)...	124
Figure 47: Total Throughput vs. τ for $p = 0.5$ (Node Mobility Scenario)	125
Figure 48: Average End-to-End Delay vs. τ (ORTPC Unavailability Scenario).....	126
Figure 49: Total Throughput vs. τ (ORTPC Unavailability Scenario)	126
Figure 50: Total Routing Traffic vs. p (Baseline Scenario).....	127
Figure 51: Total Routing Traffic vs. Number of nodes per PRN (Baseline Scenario)	128
Figure 52: Total Routing Traffic vs. Number of nodes per PRN (Baseline Scenario with Node Mobility)	129
Figure 53: Two-State Alternating Renewal Process	135
Figure 54: ADSP Flow Diagram.....	139
Figure 55: Sequence of flow in ADSP.....	141
Figure 56: RTJ/CTJ Packet Format	141
Figure 57: Differentiated OR Candidate Selection Range.....	146
Figure 58: Simulated Topology	147
Figure 59: Average End-to-end Delay vs. s	149

Figure 60: Average End-to-end Delay vs. s	150
Figure 61: Average Throughput per Traffic Flow vs. s	150
Figure 62: Delivery Ratio vs. s	151

List of Tables

Table 1: Minimum SINR Required and Corresponding Data Rate for $\text{BER} \leq 10^{-5}$..	55
Table 2: Data Rate, Modulation, SINR threshold, Power and Supported Priority for BER $\leq 10^{-5}$	61
Table 3: QoS Requirements for SUs with different priorities	86
Table 4: Simulation Parameters	101
Table 5: Availability of SOPs in PRNs (Baseline)	117
Table 6: Traffic Flow Properties (Baseline)	118
Table 7: Availability of SOPs in PRNs.....	121
Table 8: Action Reward/Punishment	140
Table 9: SOP Availability Parameters	148
Table 10: Protocol Specific Traffic Flows Parameters	148

List of Abbreviations

ACK	Acknowledgement
AIFS	Arbitration Inter-Frame Spaces
AMC	Adaptive modulation and coding
AODV	Ad hoc On-Demand Distance Vector Routing
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
CR	Cognitive Radio
CR	Cognitive Radio Networks
CSMA	Carrier Sense Multiple Access
CSMA/CD	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear to Send
DECT	Digital Enhanced Cordless Telecommunications
DCF	Distributed Coordinated Function
DPC	Dirty Paper Coding
DSDV	Destination-Sequenced Distance-Vector Routing
DSM	Dynamic Spectrum Management
DSR	Dynamic Source Routing
EDCA	Enhanced Distributed Channel Access
ILP	Integer Linear Programming
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control or Medium Access Control
MANET	Mobile Ad Hoc networks
MIMO	Multiple-input multiple-output

MC	Mesh Clients
MR	Mesh Router
MR-LQSR	Multi-Radio Link Quality Source Routing
NAV	Network Allocation Vector
NIC	Network Interface Card
OLSR	Optimized Link State Routing Protocol
PDA	Personal Digital Assistant
QoS	Quality of Service
RF	Radio Frequency
RTS	Request to Send
SIC	Successive Interference Cancellation
SINR	Signal to Interference-plus-Noise Ratio
SNR	Signal-to-Noise ratio
TCP	Transmission Control Protocol
TPC	Transmit Power Control
UDP	User Datagram Protocol
VANETs	Vehicular Ad Hoc Networks
VCS	Virtual Carrier Sensing
VoIP	Voice over IP
WLAN	Wireless Local Area Network
WIFI	Wireless Fidelity or IEEE 802.11b
WMN	Wireless Mesh Networks
WRAN	Wireless Regional Area Network
WRP	Wireless Routing Protocol
ZF	Zero Forcing

Chapter 1: Introduction

In recent years, wireless networking technologies have gained popularity. Compared to traditional wired networking, wireless networking allows a user to access network resources without the need for a cable. Applications leveraging on wireless standards like IEEE 802.11 [1] or WIFI are now commonplace. One such example is the proliferation of wireless hotspots in shopping malls and cafeterias, which allow users to access the Internet using their laptops or PDAs. However in most deployments, the wireless client must always communicate via the access point. This severely limits the range of the service to only a couple of hundred of meters.

Picture credit <http://www.ece.ncsu.edu/wireless/WMN/index.html>

Figure 1: Typical Wireless Mesh Network Architecture

To provide extended coverage, wireless mesh network (WMN) has been proposed. Figure 1 shows a typical architecture of a WMN. In the WMN, many wireless nodes can self-organize into a network. There may also be gateway node(s) which connects this mesh network to a backbone, or to the Internet. The network traffic can then take multi-hop routes to the gateway node and then to the intended destination, therefore providing extended coverage.

Since WMNs offer an alternative to traditional wired broadband access, existing

applications like VoIP and video conferencing are expected to work well on the WMNs with few or no modifications. Specifically, WMNs need to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. However, existing WMNs suffer from many shortcomings such as low bandwidth, high error rate and high delay, which prevent them from fulfilling the QoS requirements that are required by these applications. Furthermore, QoS provisioning in WMNs is very challenging due to various factors such as dynamically changing topology, capacity limitations and link variability, multi-hop communications, etc. [2]. This can restrict the usefulness and performance of these applications on the WMN.

Currently, most of the radio spectrum is allocated statically by regulators such as the Federal Communications Commission (FCC) in the United States, the Office of Communications (Ofcom) in the United Kingdom and so on. Under such a policy, also known as static spectrum allocation policy [3], a license must be obtained in order for the spectrum user to gain exclusive access to a certain spectrum band. This spectrum band, also known as the licensed spectrum band allows the licensed user to operate over the spectrum on a long term basis for large geographical regions.

On the other hand, the unlicensed or license-free spectrum as it is sometimes called is a spectrum band that is available to anyone as long as they follow the rules pre-defined for both the hardware and deployment methods of the radio in such a manner that interference is mitigated by the technical rules defined for the bands. This has led to an explosive growth of diverse wireless communication systems and related applications that are deployed on the unlicensed spectrum [4].

However, surveys have shown that vast portions of the licensed spectrum remain underutilized across frequency, space and time. Cognitive radio (CR) [5] is a radically

new way to improve the effective use of existing radio spectrum by allowing secondary system to access the licensed spectrum as long as the licensee's or primary system's operation is not compromised. Building on spectrum sensing and other basic functions, the ultimate objective of a cognitive radio network is to provide highly reliable communication for all users in the networks, wherever and whenever needed and to facilitate efficient utilization of the radio spectrum in a fair-minded and cost-effective manner [6].

As a direct evolution of the WMNs, the Cognitive Radio Based WMNs or CRNs are similar to the WMNs in many ways. A typical architecture of a CRN is depicted in Figure 2. Some of the similarities between the WMNs and CRNs include physical layer constraints, layered protocol architecture, mesh network topology, support for multi-hop communications, and so on. Due to these similarities, many principles applicable to WMN design can also be applied to CRN design.

Picture credit <http://www.ece.gatech.edu/research/labs/bwn/CR/>

Figure 2: Typical Cognitive Radio Network Architecture

Despite their similarities, the design of CRN protocols is far more complicated compared to their WMN counterpart. There are two main reasons. Firstly, the nodes

in the CRN will most likely operate in distinct frequencies. This causes difficulties in MAC and network layer routing protocols where messages have to be exchanged between nodes in order for them to function correctly. Secondly, due to the requirement for the secondary user to vacate the spectrum when a licensed user returns, the frequency bands which the nodes operate in can no longer be viewed as a permanent resource indefinitely available during its activity. This may degrade the quality of service provided to secondary users, or even terminate on-going communications if there are no available frequency bands for secondary access.

Due to the similarities between the WMN and the CRN, we will review existing research literature on both WMN and CRN in order to have a better understanding of the constraints and limitations of these networks. With more knowledge and understanding of both WMN and CRN, we will propose MAC and network layer solutions to improve the general performance and capability of the CRN in the area of QoS provisioning.

1.1 Motivation

There are many factors that can affect the performance of a CRN. The main performance metrics are delay, error rate and throughput. In accordance to the layered network approach, we categorized them into physical layer, MAC layer and network layer issues.

1.1.1 Physical layer issues

Compared to most wired medium, the wireless medium is a shared, half-duplex medium and this reduces the network capacity. The wireless medium is also vulnerable to various electro-magnetic interferences. This can cause collisions to take

place at receivers and results in a corrupted packet which will further reduce the throughput. Furthermore, multi-hop wireless networks like WMNs worsen the interference problem as a multi-hop route requires more transmissions as compared to a single-hop connection [7]. It is also well-known that throughput capacity per node reduces significantly when the node density increases. This has been verified by research done in [8-10].

Another physical layer issue for wireless transmission is the effects of fading, or propagation loss. The wireless signal can suffer from signal degradation when it propagates through the medium. When that happens, the packet received at the receiver may be erroneous. This causes retransmissions to take place at the upper layers and results in higher delay. This can be mitigated to a certain extent by increasing the source transmission power, so that a stronger signal can be received at the destination, with less probability of error. However, increasing transmission power causes other problems, e.g. increase power consumption, increased noise leading to a higher chance of a corrupted packet at neighbouring nodes etc. However, since many of the existing allocated frequency bands/channels have not been utilized efficiently, it may be possible to make use of these vacant channels to carry existing traffic. In our work, we propose combining power control and rate control together with the use of multiple channels. The effects of the increased noise can then be mitigated by reducing the average node density per transmission channel.

Finally, the radio spectrum is a scarce and valuable resource. Due to the proliferation of diverse wireless communication systems and related applications, the unlicensed spectrum is becoming increasingly crowded. This is especially true for the unlicensed spectrum band which has to support a myriad of wireless systems such as WLAN, Bluetooth, DECT and so on. On the other hand, surveys [11] had shown that

vast portions of the licensed spectrum remain underutilized across frequency, space and time. This finding suggests that granting access to unlicensed users can lead to an improvement in spectrum utilization and alleviate the shortage problem [12]. The mismatch of demands on both over-utilized and under-utilized spectrum bands can be bridged by allowing unlicensed devices to access the licensed spectrum, as long as the primary system's operation is not compromised. This can be achieved through the use of CR, which is a radically new way to improve the effective use of existing radio spectrum.

1.1.2 MAC Layer Issues

The interference problem can be mitigated in networks through the use of Carrier Sense Multiple Access (CSMA) [13]. In CSMA, a station wishing to transmit has to first listen to the channel for a predetermined amount of time so as to check for any activity on the channel. If the channel is sensed "idle" then the station is permitted to transmit. If the channel is sensed as "busy" the station has to defer its transmission. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is a modification of pure CSMA and it is used to improve the performance of CSMA by attempting to be less "greedy" on the channel. If the channel is sensed busy before transmission then the transmission is deferred for a random interval. This reduces the probability of collisions on the channel.

CSMA/CA is used in IEEE 802.11 based wireless LANs. One of the problems of wireless LANs is that it is not possible to listen while sending; therefore collision detection is not possible. Another reason is the hidden terminal problem, whereby a node C, in range of the receiver B, is not in range of the sender A, and therefore cannot know that A is transmitting to B. When this happens, collisions will occur at

the receiver B. A simplistic scenario is shown in Figure 3, where there are three nodes, A, B, and C. Nodes A and C are transmitting to node B. Also, C is outside the range of A and vice versa. C will not be able to detect the on-going transmission of A to B by carrier sensing and, consequently, it can inadvertently interfere with B's reception of A's packet.

Figure 3: Hidden Terminal Problem

CSMA/CA can optionally be supplemented by the exchange of a Request to Send (RTS) packet sent by the sender, and a Clear to Send (CTS) packet sent by the intended receiver, alerting all nodes within range of the sender, the receiver, or both, to keep quiet for the duration of the main packet. This is known as the IEEE 802.11 RTS/CTS exchange or Virtual Carrier Sensing (VCS). Even though the VCS can reduce the impact of the hidden terminal problem, it actually aggravates the exposed terminal problem.

The exposed terminal problem occurs when a node is prevented from sending packets to other nodes due to a neighbouring transmitter. Figure 4 illustrates an example of 4 nodes labelled A, B, C, and D, where the two receivers are out of range from one another and the two transmitters in the middle are in range of each other. If a transmission between A and B is taking place, node C is prevented from transmitting to D as it concludes after carrier sense that it will interfere with the transmission by its neighbour A. However note that D could still receive the transmission of C without

interference because it is out of range from A.

Figure 4: Exposed Terminal Problem

In existing IEEE 802.11 networks, the VCS mechanism is turned on only when the transmitted packet size exceeds a certain threshold or not turned on at all. Thus, it is not able to react to any changes in the traffic level or the topology of the network. Turning on VCS indiscriminately in a network increases the communication overhead which further reduces throughput. However, turning off VCS increases the risk of the hidden terminal problem. In our research, we developed a dynamic VCS mechanism in our routing protocol to only turn on the VCS exchanges only at parts of the network where there is higher chance of hidden terminal problem happening. The VCS exchanges are disabled at all other nodes which help to reduce the impact of the exposed terminal problem.

1.1.3 Network Layer Issues

Numerous ad-hoc routing protocols were developed with the start of the Defense Advanced Research Projects Agency (DARPA) packet radio networks project in the 1970s. After which, the growth of the IEEE 802.11 standard and the popularity of mobile computing made mobile ad-hoc network (MANET) a popular research topic during the mid-1990s. This period oversaw the development of many more ad-hoc routing protocols, like Ad hoc On-Demand Distance Vector Routing (AODV) [14],

Destination-Sequenced Distance-Vector Routing (DSDV) [15], Dynamic Source Routing (DSR) [16], Wireless Routing Protocol (WRP) [17] and so on. The main concerns that drive the development of these ad-hoc protocols are due to several defining characteristics of MANET. These are dynamic topology, bandwidth constraints, energy constraints and limited physical security [18, 19].

Similar to MANETs, WMNs are dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves [20]. Because of this similarity, routing protocols developed for MANETs can also be used in WMNs. Since many of these MANET routing protocols are designed primarily to maintain network connectivity and to ensure reliable data delivery in a dynamically changing network topology, they perform poorly in the context of the WMN as the requirements on power efficiency and mobility are very different between WMNs and MANETs [20].

One of the main problems with these early routing protocols is that they utilised only one performance metric (shortest path, minimum delay etc.) and may select routes in a high density region due to their simplistic nature. This can result in increased required power to achieve an acceptable packet-error-rate on all active links of such a region due to increased interference, leading thus to inefficient power use. Multi-user Interference (MUI) should therefore be taken into account in route selection. This can be achieved by considering network topology, as shown in Figure 5 vs. Figure 6.

Figure 5 shows the shortest hop route, which is likely to cause high interference due to high network density. The highlighted route between nodes 1 and 8 is potentially subject to high interference, in particular at intermediate node 6.

Figure 5: Example of shortest hop route subjected to high interference.

Contrariwise, Figure 6 shows an alternative route that takes into account network topology and therefore avoids the high-density region. Compared to Figure 5, this route avoids highly interfered nodes such as node 6. In our research, we design cost criteria that take into consideration of factors like number of transmitting neighbours, traffic levels in addition to the number of hops. This enables the routing algorithm to have higher throughput and lower delay compared to existing legacy routing protocols.

Figure 6: Example of a topology-sensitive minimum interference route.

Subsequently, there were many new routing metrics specifically proposed to improve the routing performance in WMNs. For example, Expected Transmission Count (ETX) [21] selects route with the fewest expected number of transmissions in order to minimise the packet loss rate throughput along the path. Another proposed

routing metric is the Expected Transmission Time (ETT) [22] which considers the link loss and bandwidth as the criteria for routing. There are many more proposed protocols and they will be covered in greater detail in Chapter 2. These protocols are generally able to provide better performance compared to MANET routing protocols.

Despite the improvements over MANET routing protocols, most routing protocols proposed for WMNs assume that all nodes operate in the same frequency spectrum, which is no longer valid in the wake of recent developments like the cognitive radio network which utilizes multiple frequency bands. The issue of locating path is also more complex in CRNs due to the inconsistency in frequency bands along with their respective parameters such as centre frequency and bandwidth. Additionally, in a CRN, the available channels at the source node may not be the same as the available channels at the destination node. Thus, a single path may have to be formed across multiple channels operating in different frequency bands and with different bandwidth. Furthermore, when a path is formed, any deviation in neighbourhood interference or primary user access will require the path to be recalculated and possibly dropped. In this instance, it would be necessary for a new route to be discovered and communication re-established.

1.1.4 Cognitive Radio Security Issues

Initial research efforts on CR have largely focused on the issues of resource allocation, spectrum sensing and management, etc., but not on the security aspects of CRNs.

Similar to other types of wireless networks, security is important to the proper operation of CRNs. Although many of the security measures proposed against malicious attacks could be reused, the unique characteristic of CR also presents new

loopholes for security threats and attacks.

As the behaviour of a CR is adapted according to its perceived environment from its own sensing observation or interaction with other CRs, existing proposals for spectrum sharing and management may introduced significant security loopholes, causing severely disruptions to the proper functioning of the CRN.

For example, almost all existing cognitive routing protocols have assumed that each node honestly participates in packet forwarding. However, this assumption is no longer legitimate for CRNs due to the lack of a centralized trusted authority.

QoS provisioning may also suffers as selfish nodes might incline towards self-centred behaviours in order to maximize their interests. Examples of such acts include deliberately dropping others' packets, refusing to engage in forwarding of others' packets or mislabelling all packets from the current node as high priority. These selfish behaviours can lead to monopolization of the wireless channel by the selfish nodes, or in a more severe case, the failure of routing protocols.

We will discuss some of these security issues and relevant work in greater details in Chapter 2.

1.2 Research Objective

The overall objectives of this research are to develop suitable medium access schemes and routing protocols to meet the QoS requirements of broadband applications in CRNs. Our motivation comes from the belief that even though it may not be possible to eliminate interference totally, performance improvement can be achieved by minimizing the effects of interference through the use of appropriate MAC layer, network layer or cross-layer protocols. The techniques that we will utilize includes but are not limited to the following; power control, rate control, multiple communication channels, cognitive radio and routing/cross-layer protocols that

considers multiple network metrics like network topology, traffic level, noise level etc. This essentially becomes a multi-objective optimization problem given the different network parameters and constraints.

1.3 Summary of Contributions

The main contributions of the thesis are summarized as follows.

MAC Layer Solutions to support QoS Provisioning in WMNs and CRNs

We presented a hierarchical adaptive MAC-Layer QoS Provisioning Protocol (MQPP) for Cognitive Radio Networks [23] by which nodes can provide a differentiated service for different types of traffic via varying the transmission power to increase the signal to interference/noise ratio. The protocol also distributes traffic to a vacant frequency spectrum when desired data rate is unattainable via power control. Our proposed scheme has several advantages over current existing solutions. Firstly, costly switching delay is avoided by utilizing Transmit Power Control/Adaptive Modulation and Coding (TPC/AMC) as a primary option. Secondly, vacant channels are identified to support the data transmission rate required by high priority traffic when TPC/AMC is insufficient. To the best of our knowledge, the MQPP scheme is the first and the only scheme that can provide differentiated service for an IEEE 802.11-based CRN. Simulation results demonstrate that MQPP can achieve better performance in terms of lower delay and higher throughput compared to existing protocols.

We have proposed an elastic bandwidth allocation scheme (EBAS) with a softened peak interference power constraint for the dynamic cognitive radio systems. Our scheme is able to combine the strength of both overlay and underlay transmission

mode and provide superior performance through the use of the novel softened peak interference power (s-PIP) constraint. In a cognitive radio system with dynamic primary user activity, the EBAS scheme is able to provide a much higher capacity compared to an overlay or underlay only approach. EBAS is also able to provide a differentiated service to secondary users with different priority and to sustain the service differentiation in the presence of primary user activity. The performance of the EBAS scheme can also be improved by relaxing the s-PIP constraint especially when the probability of returning PU is low.

Network Layer Solutions to support QoS provisioning in WMNs and CRNs

Our contributions on the design of network layer solutions to support QoS provisioning in WMNs and CRNs are as follows:

We have presented the Dynamic Virtual Carrier Sensing and Interference Aware Routing Protocol (DVCSIR) routing protocol is to tackle the issue of QoS provisioning in WMNs. This is achieved by developing a new routing metric, Quietness Index (QI) to quantify the potential interference experienced by a node in the WMN. DVCSIR then makes use of the QI to find the least interference route from source to destination. We also developed the dynamic virtual carrier sensing mechanism in order to mitigate the weakness of the original IEEE 802.11 virtual carrier sensing mechanism. The virtual carrier sensing is performed on a node by node basis, depending on the node density and allows the virtual carrier sensing mechanism to be applied only in parts of the network where collision is likeliest to happen.

Subsequently, we propose a cross-layer cognitive routing protocol, the Opportunistic Service Differentiation Routing Protocol (OSDRP) for the dynamic CRNs [24]. As there is very limited work looking into routing related issues in

dynamic CRNs where the average available duration of the communication channel can be much shorter than the communication time, our proposed scheme addresses this weakness by considering the availability of spectrum opportunity in addition to switching delay and queuing delay across primary user networks. In addition, service differentiation can be achieved through a combination of transmit power control and opportunistic routing. Simulation results demonstrate that the OSDRP achieves much better performance in terms of lower delay and higher throughput compared to other existing routing protocols across various scenarios.

Cognitive Radio Security Solutions

Extending on the idea behind the design of the OSDRP, we proposed a cross-layer Altruistic Differentiated Service Protocol (ADSP) for the dynamic CRNs [25]. Different from the existing cognitive routing protocols, to the best of our knowledge, our proposal is the first routing solution with consideration of the reputation of the nodes, in addition to the availability of spectrum opportunities and delay in deciding the routing path. The idea behind this work is due to the fact that although there have been many proposed routing algorithm for CRNs, none of the proposed schemes address the problem of the presence of selfish nodes in the CRN. ADSP adopt an unique combination of transmit power control and opportunistic routing techniques, together with a reputation based scheme to negotiate paths with nodes that have better reputation which will further reduce the chance of a failed delivery. The simulation results have shown that ADSP can provide lower delay, higher throughput and better delivery ratio to the traffic flows originating from cooperative nodes compared to other existing cognitive routing protocols across various scenarios in the presence of selfish nodes. At the same time, traffic flows originating from selfish nodes have been

penalized, experiencing higher delay, lower throughput and lower delivery ratio.

1.4 Thesis Organisation

This rest of this thesis is organized as follow. Chapter 2 will review existing literature on issues affecting the performance of WMNs and CRNs, which in turn affects the ability of the CRNs to meet the QoS requirements of the broadband applications.

Chapter 3 of our thesis will focus on MAC layer solutions to the QoS provisioning issue in CRNs. First of all, the operation of the MAC-Layer QoS Provisioning Protocol for Cognitive Radio Networks is introduced. A simulation model is developed and results were presented in the same chapter. The second part of the same chapter introduces the Elastic Bandwidth Allocation Scheme with Softened Peak Interference Power Constraint for the Dynamic Cognitive Radio Systems. We also present the simulation model and results.

Chapter 4 will discuss about network layer issues in Cognitive Radio Networks. The first part of the chapter introduces the Dynamic Virtual Carrier Sensing and Interference Aware Routing Protocol. Subsequently, the later part of the chapter introduces the Opportunistic Service Differentiation Routing Protocol. The simulation model and results will also be presented at the end of the chapter.

Chapter 5 talks about the concept of trusted routing. We present our proposed Altruistic Differentiated Service Protocol (ADSP) in the same chapter, together with simulation model and results.

Finally, we present our conclusions and suggest possible future research directions in Chapter 6.

Chapter 2: Literature Survey

Wireless mesh networks (WMNs) has been envisioned as a cable-less alternative for broadband wireless Internet access. WMN is composed of radio nodes called mesh routers (MRs) and mesh clients (MCs). The MRs can dynamically self-configure into a mesh topology [26] and relay the traffic generated by their respective MCs. MRs called Gateway can also be provided with cabled connectivity to the Internet. When one MR fails, the rest of the MRs can still communicate with each other directly or through one or more intermediate MRs. Thus, WMNs provide numerous advantages like extended coverage, network robustness and low cost of deployment.

Although WMNs offer a convenient and economical alternative for providing broadband wireless Internet access, supporting the diverse quality of service (QoS) requirements of multimedia applications is one of the open issues in the research on WMNs. However, WMNs suffer from many shortcomings such as low bandwidth, high error rate and high delay, which prevent them from fulfilling the QoS requirements that are vital to these applications.

To overcome some of the above-mentioned shortcoming of the WMNs, there have been many research efforts by researchers over the world. These proposals are based on a wide variety of techniques to mitigate the impact of interference and to improve network capacity such as directional antennas, multiple-input-multiple-output (MIMO), etc. Increasingly, designs utilizing multiple-channels/interfaces have also gained popularity for improving the capacity of WMNs.

Particularly, cognitive radio based WMNs or cognitive radio networks (CRNs) [27, 28] have gained much attention due to their capability to exploit frequency bands currently unoccupied for use. As shown in Figure 7, the set of frequency bands are

also known as Spectrum Holes or Spectrum Opportunities (SOP).

Picture credit: [27]

Figure 7: Spectrum Holes or Spectrum Opportunities.

This development has presented new opportunities for improving the performance of WMNs as the SOP can either be used to carry existing traffic, thus alleviating the interference problem on existing communication channels, or can be used to admit new traffic flows to increase network capacity. The nodes in the CRNs communicate through dynamic channels and can be built upon physical or medium access techniques similar to those specified by existing standards such as IEEE 802.11, IEEE 802.15.4 and IEEE 802.16 [29].

In this chapter, we reviewed existing literature that aim to solve the problems affecting the performance of WMNs. With the objective of supporting better QoS support in CRNs in mind, these research proposals aim to improve the performance of the wireless mesh network; e.g., reducing delay and increasing throughput through developing novel MAC layer, network layer and cross-layer solutions.

2.1 Legacy MAC-Layer Solutions

As mentioned in Chapter 1, CSMA/CA is used as a basic mechanism by IEEE

802.11 MAC [1] to prevent concurrent transmission by multiple stations so as to reduce the chances of collisions on the channel. However, the IEEE 802.11 MAC suffers from some issues that affect its performance in WMNs. In [30], the authors presented an analysis of the MAC layer problems in an IEEE 802.11-based multi-hop network. Using a simulation model, they show that this can cause TCP instability and serious unfairness issues. The main reason for these issues was because the MAC protocol of IEEE 802.11 suffers from the hidden node problem and the exposed node problem. The authors concluded that the IEEE 802.11 MAC protocol does not work well in multi-hop wireless network and that resolving the hidden and exposed node problem are some of the ways in which the performance could be improved.

To alleviate the hidden terminal problem, [31] proposed a two-way handshake mechanism involving short packets whose exchange should precede the actual transmission. This mechanism is also known as virtual carrier sensing (VCS). The sender starts by transmitting a Request-To-Send (RTS) packet. After receiving RTS, the intended recipient sends a Clear-To-Send (CTS) packet to the sender. Both packets specify the length of time needed to transmit the actual data packet. Any nearby node receiving any of the two packets will know for how long it should refrain from transmission in order to avoid interfering with the exchange in progress.

In [32], the authors analysed the effectiveness of the VCS mechanism in eliminating the effect of interference. Contrary to the common assumption that transmission range is equivalent to the interference range, the authors show that this assumption does not hold when the transmitter-receiver distance exceeds a certain value. As a result, the VCS mechanism is ineffective for resolving large interference range that cause significant packet corruptions at the MAC layer. They also proposed a simple MAC layer scheme to mitigate this problem.

The drawback of the VCS mechanism is although the hidden terminal problem can be minimized, some non-interfering transmission that could be carried out in parallel could be prevented from taking place. This could potentially aggravate the exposed terminal problem [33]. Thus, the use of VCS inhibits the concurrent transmissions in the IEEE 802.11 MAC and is a key bottleneck in high performance packet forwarding in multi-hop wireless networks.

In [34], the authors designed the MACA-P scheme to increase the feasible set of concurrent transmissions by introducing a control gap between the RTS/CTS and DATA/ACK phases. This gap allows two neighbouring senders (recipients) to synchronize the start of DATA transmission and ACK reception. However, this requires the use of additional control packets and requires significant modification to the virtual carrier sensing mechanism.

Due to the lack of spatial reuse through the use of VCS, the authors of [35] proposed a scheme to utilising physical carrier sensing with tuneable sensing threshold to improve spatial reuse in IEEE 802.11 mesh networks. In physical carrier sensing, a station measures the received energy level starts packet transmission only if the measurement is below a carrier sensing threshold. This avoids concurrent transmissions that could result in interference. Results from the simulation model indicated an increase in aggregate throughput without the use of virtual carrier sensing.

2.2 IEEE 802.11e-Based MAC Solutions

There have been many efforts to improve QoS provisioning capabilities in IEEE 802.11 based networks. The most recently published IEEE 802.11-2007 or IEEE 802.11e [36] is an approved amendment to the IEEE 802.11 standard that defines a set

of Quality of Service enhancements for wireless LAN applications through modifications to the MAC layer. The standard is considered of critical importance for delay-sensitive applications, such as wireless VoIP and Streaming Multimedia. The amendment has been incorporated into the published IEEE 802.11-2007 standard.

With EDCA (Enhanced Distributed Channel Access) which is a QoS extension to legacy IEEE 802.11 distributed coordinated function (DCF), high priority traffic has a higher chance of being sent than low priority traffic. This is accomplished by using a shorter contention window (CW) and shorter arbitration inter-frame space (AIFS) for higher priority packets. Thus, a station with higher priority traffic will wait less time before it sends its packet, on average, than a station with low priority traffic. In [37], the authors improved the performance of IEEE 802.11 MAC by using wider contention windows for transmission retry, and through the use of express forwarding and retransmission. More recent works [38-41] also seek to improve performance through variations of algorithms by tuning different EDCA parameters.

The main deficiency of these schemes are that they do not grant greater protection to higher priority traffic from interference generated by legacy DCF-based and IEEE 802.11e stations as noise affects all traffic equally. Moreover, the implementation of these schemes implies that the stations have to monitor the channel conditions in order to dynamically tune up the actual values of the key system parameters, such as the threshold and window size [42].

Furthermore, studies have shown that the network performance and QoS provisioning of the above schemes can only be effectively achieved in collision limited scenarios [43]. The authors of [44] had also shown that the higher priority traffic is not effectively protected in the event of increasing traffic from the lower priority traffic.

2.3 Legacy Routing Solutions

The growth of the IEEE 802.11 standard coupled with the popularity of mobile computing has led to the development of numerous ad-hoc routing protocols. These ad-hoc routing protocols are generally classified as either table-driven or source initiated depending on how the routing information is updated. Table driven ad-hoc routing protocols attempt to maintain a route between every nodes and refresh these information periodically resulting in high overheads. The advantage of this approach is that a new data connection can send out the data packets quickly without the need of performing the route discovery process. Examples of table driven ad-hoc routing protocols include DSDV and WRP. On the other hand, the source initiated ad-hoc routing protocol has much lower overheads compared to the table driven approach, but if a node requires a route to a destination that is not inside its routing table, it will have to wait until such a route can be discovered. AODV and DSR are two well-known examples of source initiated ad-hoc routing protocols.

In [45], the authors compared the performance of DSR and AODV. The observation is that DSR performs better than AODV in scenarios when the load is lower, whereas AODV outperforms DSR when the load is higher. The authors also recommended that both routing protocols could benefit by using congestion-related metrics to evaluate routes rather than emphasizing the hop-wise shortest route. Also, they observed that the interplay between the routing and MAC layers could affect performance significantly, and thus emphasizes on the need to study the interactions between protocol layers when designing wireless network protocol.

In [46], the authors presented extensions to the AODV routing protocol with the aim to exploit the heterogeneity of hybrid wireless mesh networks, which are composed of both mesh routers and mesh clients. The assumption is that mesh routers

are more static and less resource constrained than the mobile mesh clients. In this work, it was proposed to replace the hop count metric with the metric Min (Hop Count – Mesh Router Count) where Mesh Router Count is the number of mesh router in the path. This seeks to select routes that minimises the number of mesh clients along the path. As the mesh clients are relatively more resource constrained compared to mesh routers, it gives a better overall performance. The authors also proposed that nodes forwarding the RREQ packets recommending a least loaded channel to be used for the reverse route second extension. This helps to minimise the co-channel interference. Through extensive simulations, the proposed extensions achieve a more than 100% improvement over the standard AODV in terms of key performance metrics such as packet delivery ratio, routing overhead and latency.

In another work, the authors proposed a new routing metric, Expected Transmission Count (ETX) [21] to select route with the fewest expected number of transmissions in order to minimise the packet loss rate throughput along the path. To do that, ETX estimates the probability of successful transmissions of a link by measuring the number of network probes received versus the number of probes expected. The authors compared the performance of using ETX as a routing metric, against both DSR and DSDV, both of which are using hop count as a metric. Measurements on a wireless test-bed show that ETX locate paths with significantly higher throughputs than a minimum hop-count metric, particularly for paths with two or more hops. One disadvantage of the ETX is that it does not consider the differences in transmission rates [47]. For example, a heavily utilised link may have very low loss rate, and two links with different data rates may have the same loss rate. In this case, ETX will favour fewer slow long distance links over a larger number of high speed links even though the later will provide better performance.

The Expected Transmission Time (ETT) metric [22] improves the ETX by including the bandwidth of the link in addition to the loss rate. The individual link weights are combined into a path metric called Weighted Cumulative ETT (WCETT). Through measurements performed on a testbed, it was found that WCETT can achieve a good trade-off between delay and throughput because it considers channels with good quality and channel diversity in the same routing protocol. One limitation of WCETT is that it does not explicitly consider the effects of inter-flow interference. Therefore, WCETT may route flows to dense areas where congestion is more likely and may even result in starvation of some nodes due to congestion [48].

As network traffic in WMNs is often aggregated and forwarded to the gateways, strategic placing and load balancing placement of gateway is important to the network performance. In [49], the authors proposed a proactive multi-path routing protocol which exploits the multiple routes between source and destination to balance traffic load. At each mesh router, the outgoing traffic can be sent over different links in a round robin manner, or according to the level of congestion of the downlink routers. This helps to redistribute the traffic among the different downlink routers and therefore alleviates congestions. The results show that the performance of multi-path routing is dramatically increased compared to single path routing due to lower packet loss.

In [50], the authors proposed a multi-path routing for ad-hoc wireless networks. The proposed QOLSR protocol is designed as an extension to the Optimized Link State Routing protocol (OLSR). The idea behind QOLSR is rather similar to the proposal in [49] where the protocol computes multiple node-disjoint paths in order to avoid interference. QOLSR also utilises bandwidth and delay as a routing metric and simulation results indicated that it is able to achieve better QoS guarantees to

applications and improve network resource utilization.

In [51], the authors proposed HEAT, a routing protocol based on field-based any-cast routing. The underlying routing concept is a field similar to a temperature field in thermal physics. In the beginning, new nodes are assigned a temperature of zero and gateway nodes are assigned the maximum value. The objective of the protocol is to route packets through nodes with the highest temperature, and subsequently towards the gateway. The temperatures of nodes can be recomputed based on a combination of factors. For example, their distances to the available gateways, the robustness of the paths toward these gateways and even the temperature of their neighbouring nodes. In extensive simulation experiments, the authors found that HEAT has excellent scalability properties due to a fully distributed implementation, and it provides much more robust routes than the unicast protocols, AODV and OLSR. The packet delivery ratio with HEAT is also more than two times higher.

2.4 Cross Layer Solutions

Traditionally, different protocol layers are required to be transparent from each other. This makes the protocol development and implementation easy and scalable. However, this methodology of layered protocol design does not necessarily lead to an optimum solution for wireless networks. For example, the physical channel in a wireless environment is variable in terms of capacity, bit error rate, power etc. Although different coding, modulation and error control schemes can be used to improve the performance of the physical channel, there is no way to guarantee fixed capacity, zero packet loss rate or reliable connectivity as expected by the higher layers. Therefore, higher layer protocols will be inevitably affected by the unreliable physical channel. To further improve the performance of a wireless network, MAC and network routing protocols have to work collaboratively together with the physical

later. Such interactions demand a cross-layer design among different protocols.

Recently, there are several research efforts to improve the capacity of wireless mesh networks by exploiting such alternative approaches as beam forming antennas, multiple channels/radio interfaces, multiple-input multiple-output (MIMO) techniques, power control, rate control, cognitive radio techniques or a combination of the mentioned approaches. We discuss some of these techniques below.

2.4.1 Cross layer solutions supported by beam-forming/directional antennas

Many systems use omni-directional antennas to avoid having to know the location of the receiver. An omni-directional antenna transmits a signal to all directions with the same power. Not only does this cause interference to the other nodes, but the power is also wasted in the directions away from the receiving node. The interference limits the number of users that a system can accommodate.

By using directional antennas, both transmitting and receiving nodes have the ability to generate beam patterns with high transmission gain and reception gain in the direction of each other and low gain elsewhere. The enhanced power efficiency enables the extension of the battery life of a node, which is crucial for wireless communication devices. Furthermore, the interference problem is significantly reduced, because only nodes with receiving antennas pointing at the main beam of a transmitting node are severely interfered by the transmitting node. This allows the system to have a larger number of users than with omni-directional antennas [52].

In [53], the authors measured data from a propagation study in an indoor environment. It shows that the effective directivity of directional antennas is heavily dependent upon the surrounding environment. The effect of antenna directivity upon system performance was evaluated for an indoor wireless system consisting of two

co-channel base stations. System performance was quantified in terms of average outage probability. With reference to the system using omni-directional antennas, both significant reductions and increases in average outage probability were observed in the same systems that employ different orientations of directional antennas. In the best case, the use of directional antennas decreased outage probability by 56%, while in the worst case the outage probability increased by 66%.

The work by [54] addressed several interference-aware routing problems in multi-hop wireless networks by using directional antennas. They presented new definitions for the link and path interference that are suitable for designing better routing algorithms. Based on these definitions, they have formulated several optimization problems related to routing in multi-hop wireless networks. These include the Power Constrained min-Max Interference single path (MIPCI) and Power Constrained min-Total Interference single path (TIPC) routing problems. From simulation results, the average path interference is reduced by approximately 40% or more at the cost of only a slight increase in average path power compared with the well-known minimum power path routing algorithm.

In [55], a location and mobility-aware (LMA) MAC protocol was developed for vehicular ad hoc networks (VANETs). The predictive location and mobility of the vehicles are adopted to provide robust communication links while using the directional beams. The deafness problem is also alleviated using the directional-listen mechanism in the proposed algorithm.

In [56], the authors proposed PMAC, a new MAC protocol to support the use of directional antennas in ad hoc networks. PMAC incorporates an efficient mechanism for neighbour discovery, and a scheduling based medium sharing that allows for exclusive directional transmissions and receptions. Results from analysis and

simulations show that each node can achieve a per node utilization of about 80% in static and about 45% in mobile scenarios. In terms of throughput, PMAC also outperform both the traditional IEEE 802.11 and previously proposed MAC protocols for use with directional antennas in ad hoc networks.

Even though the use of directional antennas provide several advantages, the hidden node problem can be worsen in WLAN setups with many nodes that use directional antennas, thus causing lower receiver throughput [57]. Furthermore, changing the antenna's direction requires either a mechanically or electronically steerable directional antenna system. It is likely that tuning the antenna to the desired direction will take a long time in comparison to the transmission time, thus limiting its effectiveness.

2.4.2 Cross layer solutions supported by multiple channels/radio interfaces/antennas

Multiple channels and/or radio interfaces could increase network capacity by exploiting the independent fading across different frequencies or the orthogonality of frequency bands. Similarly, systems employing multiple antennas for both transmitting and receiving (generally called MIMO systems) improve the capacity and reliability of wireless backbones by exploiting antenna diversity and spatial multiplexing. Diversity provides the receiver with several (ideally independent) replicas of the transmitted signal and is therefore a powerful technique to combat fading and interference [58].

In [59], the authors proposed a novel MIMO mesh network which can solve the problem of co-channel interference inherent in a conventional mesh network and improve network channel capacity via link multiplexing. As a MIMO transmission

scheme, linear (ZF) and nonlinear (SIC/DPC) algorithm were developed for proposed MIMO mesh network. Validity of the proposed schemes was confirmed by a numerical analysis of network channel capacity.

In [60], the authors designed and simulated the performance of a planned 2.4GHz wireless MIMO mesh network. The prototype consists of several different parts from normal mesh network: MIMO routers, special channel allocation, and balanced routing approach. A simulation of the prototype shows that this planned MIMO mesh network works well: compared with the normal multiple channels multiple interfaces mesh network, the average throughput is improved by more than 80% for 2-hop backbone transmission, and it is nearly doubled for 4-hop backbone transmission. The delay is reduced by approximately 50% and 70% for 2-hop and 4-hop scenarios, respectively.

One of the drawbacks of the MIMO system is the increased complexity and hardware cost due to the expensive radiofrequency chains required by each active antenna. On the other side, spatial multiplexing divides the channel into multiple “spatial channels” through which independent data streams or signals can be coded and transmitted simultaneously. As a consequence, diversity techniques make the channel less fading, which is of fundamental importance for wireless backbones, where deep fades can occur and the channel changes slowly, causing fades to persist over a long period of time. Nevertheless, when strong interference is also present, diversity processing alone cannot improve the signal.

Assigning orthogonal channels for neighbouring wireless transmissions can help to minimize the interference. However, for a single radio design, there is a need for dynamic channel switching in order to preserve the connectivity of the WMN. This requires tight time synchronization between the nodes. Thus, equipping each node

with multiple radios is a promising solution approach to improve the capacity of WMNs, and at the same time avoiding the pitfalls of channel switching. However, the assignment of channels to different nodes equipped with multiple network interface cards can be non-trivial.

In [61], the authors considered a static channel assignment in multi-radio multi-channel wireless mesh networks with the objective of maximizing overall end-to-end throughput. They presented an integer linear programming optimization model for this static channel assignment problem. Then, by taking into account the "bottleneck links" of multi-hop flows, they propose a flow-aware heuristic scheme, which decompose this ILP problem into a graph colouring sub-problem and a linear programming sub-problem. Simulation results on ring and grid topologies show that the scheme has significant gain in terms of network throughput.

In [62], the authors developed an exact binary linearization scheme to solve the channel and interface assignment problem. The simulation results showed that the proposed designs can lead to multi-channel WMNs which are more efficient and fair compared to their single channel counterparts. However, the scheme is computationally expensive, and a near-optimal design based on approximate dual decomposition techniques is proposed which is more practical for deployment.

In [63], the authors considered the problem of logical topology design, interface assignment, channel allocation and routing as a joint linear mixed-integer optimization problem. The model takes into account the number of available NICs in routers, the number of available orthogonal frequency channels, expected traffic load and capacity of the logical links. Their proposed scheme was able to provide higher aggregated network throughput and lower end-to-end delay for both TCP and UDP traffic.

In [64], the authors formulated and addressed the channel assignment problem in multi-radio multi-channel wireless mesh networks. They presented centralized and distributed algorithms that assign channels to communication links in the network with the objective of minimizing network interference. Through simulations and detailed experimental study on an 11-node test-bed, the proposed scheme was observed to be able to improve network throughput.

2.4.3 Cross layer solutions supported by power control and rate control

Improved performance of WMNs can also be achieved through combining power, modulation and rate control. Increasing transmission power (TPC), lowering the data rate and using a more robust modulation (AMC) improves signal quality at the receiver, reducing the probability of error and providing better throughput in the presence of noise. This principle is illustrated in the work by [65] where the authors proposed a user-aware rate adaptive control (UARAC) scheme for IEEE 802.11-based ad hoc networks. In the scheme, a receiver measures the SNR of a RTS frame, and then selectively returns the CTS frame with piggyback information showing the maximum feasible rate. One key feature of the scheme lies in that the probability that the receiver returns the CTS frame depends on the SNR of the RTS frame and the number of active stations in the network, so that the throughput can be further improved by multi-user diversity besides time-diversity.

Unlike the approaches taken in the IEEE 802.11e and its variant, schemes utilising power control and/or rate control provide differentiated QoS by varying the transmission power, data rate and modulation according to the traffic class. With AMC, the power of the transmitted signal is held constant over a frame interval, and the modulation and coding format is changed to match the current received signal

quality or channel conditions. This can improve signal quality at the receiver, reduce the probability of errors and provide better throughput in the presence of noise. TPC can also be performed in a communication system to achieve good performance. A higher transmit power translates into a higher signal power at the receiver, which in turn increases the signal-to-noise ratio (SNR) and reduces the bit error rate of a digital communication link. This can be used to provide protection to higher priority traffic by varying the transmission power according to traffic priority.

AMC can also be applied together with TPC for greater effectiveness. For example, in [66], the authors proposed a Power-Controlled Rate-Adaptive (PCRA) MAC protocol to provide differentiated service by tuning transmission power according to different types of traffic. Depending on the traffic priority and the corresponding desired data rate, the scheme dynamically determines the transmission power and modulation needed in order to achieve a minimum required SINR at the receiver. The authors of [67] developed a similar scheme where the error-control coding and modulation is adapted according to the channel conditions. The protocol also adjusts the transmission power when the most powerful combination of coding and modulation is inadequate. In another work [68], the authors proposed an algorithm for the joint-power-frequency-time intra-cluster resource allocation problem. Similarly, the proposed algorithm takes into consideration of power allocation, subcarrier allocation and packet scheduling in order to satisfy the QoS requirements of network traffic in WMNs.

Although schemes utilising AMC and/or TPC techniques are able to provide a satisfactory QoS provisioning capability for WMNs, they are ineffective when a wireless channel has been overwhelmed by noise. Furthermore, increasing transmission power worsens the interference problem by causing more interference at

nodes that are previously out of the transmission range when using a lower transmission power [69].

2.5 Cognitive Radio Solutions

Although multiple non-overlapped channels exist in the 2.4GHz and 5GHz spectrum, most IEEE 802.11-based multi-hop ad hoc networks today use only a single channel at any time. As a result, these networks cannot fully exploit the aggregate bandwidth available in the radio spectrum provisioned by the standards.

To mitigate the interference, network traffic can be distributed across multiple vacant channels to reduce the node density per transmission channel. Based on the software defined radio platform, CR is a promising technology that can be used to sense and to access vacant channels dynamically. CR was first proposed as a form of software radio [5]. The idea is to configure the radio hardware through the use of software that allows the hardware to sense and to react to changes in the environment. According to statistic [11] from the Federal Communication Commission (FCC), temporal and geographical variations in the utilization of the assigned spectrum range from 15% to 85%. The limited available radio spectrum and the inefficiency in spectrum usage necessitate a new communication paradigm to exploit the existing spectrum dynamically. Thus, CRN has been proposed to allow intelligent radios to provide unlicensed users with opportunistic access to the licensed bands without interfering with the existing users. In a CRN, a user can use spectrum sensing hardware/software to sense idle spectrum, select the best channel and coordinate access to this channel with other users.

2.5.1 Spectrum Sensing

Spectrum sensing is the key enabling function in order for the CR to detect

unoccupied channels for opportunistic spectrum access. To determine if a channel is occupied, direct sensing of the frequency band can be performed by using a matched filter (feature detection) or energy detector (energy detection) [70]. However, due to fading or shadowing, sometimes it may not be possible to detect the primary transmitter. To solve the problem, cooperative detection has been proposed as making use of sensing information from more nodes improves the accuracy of the transmitter detection.

In the work [71], the authors compared both feature detection and energy detection approaches for in-band spectrum sensing in CR networks. The proposed algorithm is based on cooperative sensing using a subset of sensors within a cluster. Although feature detection may perform better than energy detection with one-time sensing, the scheme is able to make use of energy detection by performing it more frequently as energy detection has a lower sensing time compared to feature sensing.

In [72], the authors develop a fixed and a variable relay sensing scheme to leverage on the spatial diversity on the detection capabilities of CR networks. By using the cognitive users to sense the environment and then feeding the data to a central base station, the scheme is able to reduce the primary user detection time. This scheme is particularly suitable to be implemented in WMNs as it employs cognitive users distributed at various locations as relays to sense data and to improve detection capabilities.

In [73], the authors devised a scheme to allow nodes equipped with a single tuneable transceiver to monitor the primary channels while continuing operation in the secondary band. The monitoring is done by measuring the aggregated received power on a node and then isolating the leakage power for each transmitter. However, it requires the mesh routers (MRs) to be aware of the location of other MRs which

might not be feasible in the real-life implementation.

In [74], the authors proposed a cross-layer based opportunistic multi-channel MAC protocol which allows the secondary user to identify unused frequency spectrum that can be used for opportunistic transmission while minimizing the level of interference caused to the primary users. Two channel sensing strategies, random sensing and negotiation-based sensing were proposed. The weakness of the random sensing policy is that the probability of all license channels is sensed is very low when the number of secondary users is smaller than or close to the number of licensed channels. The negotiation-based sensing policy was then proposed to address the weakness of the random sensing policy by allowing secondary users share information on the channels which they have already sensed, so that they can then select different channels to sense at the next time slot.

Regardless of the sensing methods used, once the vacant channels have been identified, new or existing traffic can be admitted to an available band according to the QoS requirements of the application. Dynamic spectrum management (DSM) is performed to reconfigure operating parameters like transmission power, modulation or data rate to access the new frequency spectrum [27]. This helps to reduce the node density per transmission channel and interference, thus improving the throughput and the delay. However, the time needed to access a new channel is non-trivial [75] and thus requires careful management.

2.5.2 Cognitive Radio Based MAC and Network Layer Solution

The benefits of CR technology can be further applied to existing IEEE 802.11 networks where there are multiple non-overlapping channels that can be used for communication. As the set of available channels may vary from one node to another,

channel rendezvous is an important function to allow cognitive nodes to coordinate with one another to choose a common communication channel. The channel rendezvous problem faces great difficulty in a cognitive radio setting as channel conditions may change suddenly due to the re-appearance of the primary user.

One of the works that attempted to address this issue is [76], where the authors developed a CSMA-based MAC protocol for CR-based multi-hop networks. In the proposal, nodes in the network can coordinate among themselves to negotiate and decide on a common control channel. Nodes that need to communicate with one another can then decide on a common data channel by exchanging messages on the common control channel. The criterion for choosing the data channel is based on a priority which is reduced on a failed communication attempt. Thus, over time, channels with record of more successful transmissions will be more likely to be chosen as the data channel since their priority will be higher.

In [77], the authors proposed a dynamic channel selection scheme for opportunistic spectrum access in IEEE 802.11-based multi-channel wireless mesh networks. The proposed scheme integrates fuzzy-logic based estimation with a learning algorithm used at a wireless node for dynamic channel selection based on traffic load condition so that the utility of the node can be maximized. The performance of the proposed scheme has been evaluated by simulations, and it has been observed that it performs significantly better than some of the traditional schemes.

There are also proposed schemes that consider channel management together with issues like routing or scheduling. In [78], the authors proposed a joint channel assignment and routing (JCAR) protocol in heterogeneous multi-radio multi-channel multi-hop wireless networks. A channel cost metric (CCM) was defined to capture the

interference cost. JCAR then jointly coordinates the channel selection on each wireless interface and the route selection among interfaces based on the CCM. The simulation results and experimental results through an experimental test bed demonstrated the efficacy and performance of the JCAR scheme.

In [79], the authors proposed a joint interaction between on-demand routing and spectrum scheduling. A delay-based metric was defined for evaluating the effectiveness of candidate routes. The path selection algorithm aims to minimize the sum of the switching delay, queuing delay and back-off delay for the considered route. Simulation results shows that the scheme can achieve a balance between assigning new frequency bands to allow simultaneous transmission and accommodating some nodes on one band to avoid expensive switching, thus achieves an overall optimal cumulative delay. However, the scheme requires that a common control channel be form between each node by using an additional dedicated wireless interface. This increases the cost, energy consumption and complexity of such a design. Furthermore, the common control channel can be overwhelmed by noise, thereby rendering it inoperable.

In [80], the authors proposed a capacity-based routing strategy for CRN. The scheme can improve performance by shifting traffic to the edge of the network, away from the higher density regions. However, the work did not consider issues like number of network interfaces needed, node synchronization issues and switching delay.

In [81], the authors proposed an on-demand protocol for routing and channel assignment in multi-hop single transceiver CRN. The scheme quantifies the additional delay caused by channel switching and the corresponding reduction in back-off delay. Using this algorithm, a node can then determine whether to assign an existing channel

to a flow, or if a new channel is needed. The simulation results show that the scheme is able to provide significant improvement in terms of network throughput compared to AODV in a network with high traffic load.

In [82], the authors devised a Multi-Channel Extremely Opportunistic Routing (MCExOR) for that makes use of multiple non overlapping RF channels in wireless multi-hop networks. The scheme improves the network performance by choosing the RF channel with the most promising candidate set for every transmission. However, the scheme requires nodes to discover neighbours through link probe packets. As MCExOR is a multi-channel protocol, link probes packets have to be broadcasted consecutively on different channels in a round robin manner. The combined switching delay can be non-trivial. To work around this, the authors assume a channel switching delay of $80\mu\text{s}$ which is several orders of magnitude lower than existing literature [83, 84]. However, even when a low channel switching delay is attainable, the total switching delay for multiple channels can be prohibitive, and therefore cannot be ignored.

In [85], the authors have designed a routing protocol that utilizes a link cost metric based on its spectrum usage history as opposed to its instantaneous state. Accordingly, a link's connectivity behaviour is tracked and assigned a persistent cost metric that gets updated periodically to reflect its overall state. In this way, a route can be found between a source and destination even if there is no continuous end-to-end connectivity.

In [86], the authors have proposed a spectrum-aware routing solution to opportunistically routes traffic across paths with higher spectrum availability and quality via a new routing metric, Path Spectrum Availability (PSA). The PSA is defined as the minimum aggregate throughput that can be supported by nodes along a

path. However, it assumes that nodes are able to communicate using several possibly disjoint channels at the same time. Furthermore, the routing algorithm works based on link state routing in which time is required to converge and to build a network topology map. As a result, this approach may not be suitable to the dynamic properties of the considered CRNs.

In [87], the proposed scheme aims to find the optimum path in CRNs using a novel metric that considers the maintenance cost of a route as channels or links that must be switched due to primary user activity. The authors have modelled the problem as an integer programming optimization model and have shown its polynomial time complexity in case of full knowledge of primary user activity.

2.5.3 Cognitive Radio Based Resource Allocation Strategies

There are three main cognitive radio network paradigms [88]. In spectrum overlay, it is assumed that the cognitive transmitter has prior knowledge of the non-cognitive users' codebooks as well as its messages. This information can be obtained from the non-cognitive users if they follow a uniform standard for communication based on a publicized codebook, or by listening to periodical broadcasting by non-cognitive users. The information can then be used to either mitigate or to cancel the interference seen at the receivers through techniques like dirty paper coding.

In spectrum interweave, there exist temporary space-time frequency voids in the licensed band (spectrum hole) which can be exploited by the secondary users (SU) for its own communication. The SU must be able to monitor the radio spectrum periodically in order to detect spectrum holes that can be used for opportunistic transmission as these spectrum holes can change with time and geographic location. Since the SUs are basically transmitting on a license spectrum, the primary user (PU)

may, at any time come back and take up the frequency bands currently available for secondary access. It simply implies that it is no longer valid to assume that the designated spectrum for secondary usage is fixed and always available. The lack of guaranteed resource availability is the primary reason for the difficulty in quality-of-service (QoS) provisioning in overlay CR systems.

The time-varying nature of the available resources in the spectrum interweave scenario can be mitigated through using spectrum underlay technique where simultaneous transmissions of primary and secondary systems are allowed. However, it means that the secondary transmitter must be very conservative in its output power so that the interferences introduced by the secondary system (SS) are below a certain threshold with regards to the primary system (PS). In this case, since the interference constraints in underlay systems are typically quite restrictive, SUs are limited to short range communications. While the underlay paradigm is most common in the license spectrum, it can also be used in unlicensed bands to provide different classes of service to different users [88]. For both overlay and underlay CR systems, orthogonal frequency division multiplexing (OFDM) is particularly suitable as a potential transmission technology for overlay CR systems with its flexibility in filling spectral gaps within the PS [89].

Notwithstanding the theoretical dissimilarities in modelling, design and analysis of the three CRN paradigms, there is a need to achieve a balance between optimizing the SUs' performance and maintaining adequate protection to the PUs. Therefore, efficient resource allocation methods should be investigated to balance this trade-off.

An optimal power loading algorithm for an OFDM-based CR system was proposed in [90]. The scheme works by assigning a higher power profile to subcarriers that have better channel quality and are relatively further away from the

PU's band. Doing this maximizes the downlink transmission capacity of the CR users while keeping the interference induced to the PUs below a specified threshold.

A resource allocation framework has been presented for spectrum underlay in cognitive wireless networks [91]. The authors consider both interference constraints for PUs and QoS constraints for SUs. Admission control algorithm were also designed for high network load conditions which are performed jointly with power control so that QoS requirements of all admitted SUs are satisfied while keeping the interference to PUs below the tolerable limit.

When fading channels are considered, another form of protection, known as the average interference power constraint can also be used. Compared to the normal form of the constraint that restricts the interference power at all times, also known as the peak interference power constraints, the average power constraint [92] only limits the average interference power over all fading states to be below the prescribed limit. Hence, in certain unfavourable states, the temporal interference power could possibly exceed this limit.

Although the above mentioned research proposals are able to provide optimized solutions for resource allocation in CR systems, they have not taken into consideration of the effects of PU activities. One of the potential weaknesses of these schemes is that there is no consideration for the delay from the time that a channel is reclaimed or released by the PU until the time that the SU is aware of this. This delay could be due to channel sensing, adjustment of transmission parameters etc required by the SU. As the availability of resources cannot be assumed in a dynamic environment which the CR systems operate, this means that the resource allocation performed by the above mentioned schemes could be based on already outdated information which is only valid in the past.

2.5.4 Cognitive Radio Security Solutions

There are many similarities in the security issues that both CR-based wireless networks and conventional wireless networks have to deal with. These issues include validating communication security requirements like Data Confidentiality and Privacy, Availability, Registration, Authentication and Authorization [93].

Due to the additional capabilities that differentiate the CR and its conventional counterpart in terms of spectrum sensing and dynamic spectrum access, CR-based wireless networks are at greater exposure to the myriad risks of network attacks [94].

One example of an attack specific to CR networks is the primary user emulation (PUE) attack [95]. By this attack, an adversary spoofs the primary users by transmitting signals whose characteristics emulate those of incumbent signals. This causes false alarms to the honest secondary users and can cause serious performance degradation of CRNs. Various schemes have also been proposed to combat the PUE threat using both proactive [95] and passive [96] approaches.

Another type of network attack can be carried out by untrusted secondary users that report false spectrum sensing information so that a primary user is reported to be present when it is not, or to report that a primary user is absent when it is actually present. This is also known as spectrum sensing data falsification attack [97]. An eigenvalues based spectrum sensing scheme to detect and counteract against the untrusted secondary users in a CR network has been proposed in [98].

The above mentioned are active attacks which are conducted to intentionally disrupt network activity. On the other hand, a passive attack, such as a selfish node behaviour or eavesdropping, drops packets with a selfish motivation to prioritize its traffic [99]. Even though such attacks do not cause any intentional damage to the networks, they can lead to the failure of most existing routing protocols. This is

because most existing routing protocols operate under the assumption that each node is willing to participate in packet forwarding, which is valid in a network managed by a single trusted authority.

Contrariwise, in a CRN, most of the secondary users are nomadic users which do not come under the jurisdiction of a centralized trusted authority (CTA). As a result, some of these secondary users may be unwilling in the collaboration that is not directly beneficial to them by dropping packets even if the channel is currently unoccupied by a primary user in order to preserve power, buffer and computing resources, thus invalidating the assumption. The selfish nodes may also flood the network with packets marked as high priority in an attempt to monopolize the wireless channel. These selfish acts can cause severe performance degradation in the CRN and rendered a well-designed routing protocol ineffective in such situations.

For instance, the authors of Delay motivated On-demand Routing Protocol (DORP)[79] have proposed a joint interaction between on-demand routing and spectrum scheduling. The routing algorithm aims to minimize the sum of the switching delay, queuing delay and back-off delay for the considered route. In another work, the authors of Spectrum Aware Mesh Routing Protocol (SAMER)[86] proposed a spectrum-aware routing solution to opportunistically routes traffic across paths by considering the minimum aggregate throughput that can be supported by nodes along a path. However, this algorithm assumes that nodes are able to communicate using several possibly disjoint channels at the same time. Furthermore, the routing algorithm works based on link state routing in which time is required to converge and to build a network topology map. As a result, this approach may not be suitable to the dynamic properties of the considered CRNs. The authors of [100] and [24] have proposed schemes that take into consideration of the dynamic properties of spectrum

availability, but did not consider the issue of selfish nodes presence.

As the spectrum resources needed for secondary access cannot be considered as infinitely available during its activities. The intermittent availability of spectrum bands can thus cause communication problems among secondary users. For instance, the sudden appearance of a primary user on a channel will require the secondary users to evacuate the channel, causing disruption to the on-going communications and causing packets to be dropped. Secondary users may also maintain radio silence due to nearby primary network activities. It can result in difficulties in determining the reason behind a dropped packet or a non-response of a CRN node, as it could be either due to the selfishness of the node, or due to the lack of available spectrum resources. Thus, most of the above proposed schemes will not perform well in the case of CRNs as they may penalize a CRN node unfairly even though the reason of packet dropping is not due to the selfishness of the CRN node.

2.6 Summary of Review Work

In this section, we provide a brief recap of the issues that are discussed in Chapter 1 and Chapter 2.

The performance of WMNs and the issue of QoS provisioning can be tackled from the viewpoint of various network layers, physical, MAC and network layer. Physical layer factors like interference [8-10], fading, propagation losses are one of the reasons why the performance of wireless networks are not as good as their wired counterpart. In recent years, the increased utilisation of the unlicensed wireless spectrum has also led to the aggravation of the interference issue in wireless networks. This has led to the development of opportunistic spectrum access through the use of Cognitive Radio.

The IEEE 802.11 MAC performance suffers from the hidden node problem and the exposed node problem. To alleviate the hidden terminal problem, a two-way

handshake mechanism involving short packets whose exchange should precede the actual transmission. This mechanism is also known as virtual carrier sensing (VCS). The drawback of the VCS mechanism is although the hidden terminal problem can be minimized, it inhibits the non-interfering concurrent transmissions in the IEEE 802.11 MAC. This aggravates the exposed terminal problem and is a key bottleneck in high performance packet forwarding in multi-hop wireless networks.

The MAC layer protocol with enhanced distributed channel access (EDCA) in the IEEE 802.11-2007 is able to provide differentiated QoS for different traffic types in wireless networks through varying the Arbitration Inter-Frame Spaces (AIFS) and contention window sizes. However, the performance of high priority traffic can be seriously degraded in the presence of strong noise over the wireless channels. Schemes utilizing adaptive modulation and coding (AMC) technique have also been proposed for the provisioning of QoS. They can provide limited protection in the presence of noise but are ineffective in a high noise scenario.

As mentioned earlier, many ad-hoc routing protocols are designed according to several defining characteristic of MANET. These protocols like the DSR and AODV are primarily designed for low-end MANETs and are therefore inefficient for the WMN scenario. They are designed to search for stable routes in order to be robust and resilient to mobility. However, in a WMN, nodes (mesh routers) in the backbone have minimal mobility and no constraint on power consumption, while mesh client usually desire the support of mobility and a power efficient routing protocol. Such differences imply that the routing protocols designed for ad hoc networks may not be appropriate for WMNs.

Most routing protocols proposed for WMNs also assume that all nodes operate in the same frequency spectrum, which is no longer valid in the CRN which utilizes

multiple frequency bands. The issue of locating path is also more complex in CRNs due to the inconsistency in frequency bands along with their respective parameters such as centre frequency and bandwidth.

Finally, most routing protocols are not designed specifically to handle the presence of selfish nodes. Since most routing protocols requires some kind of message exchanges or forwarding between participating nodes to work properly, the non-cooperation of nodes due to certain self-centred agenda will cause the routing protocol to fail. This is especially true in CRNs due to the lack of a centralized trusted authority. Another problem that could possibly happen is that some selfish nodes may flood the network with packets marked as high priority in an attempt to monopolize the wireless channel. These selfish acts can also cause severe performance degradation in the CRN and degrade the QoS provided to other nodes in the network.

Chapter 3: MAC-Layer Solutions for QoS Provisioning

As mentioned in Chapter 1, the proliferation of diverse network devices with multimedia capabilities has resulted in an increasing need for Quality of Service (QoS) provisioning in wireless networks. There were many proposed solutions utilising various techniques like varying the Arbitration Inter-Frame Spaces (AIFS) and contention window sizes [41] or through adaptive modulation and coding (AMC) technique where the transmission power, data rate and modulation are varied according to the traffic class [66] as mentioned in Chapter 2. However, these techniques were ineffective in protecting high priority traffic, especially in a high noise scenario. Furthermore, schemes utilising AMC technique may aggravate the noise problem through the use of increased transmission power.

The advent of cognitive radio technology has brought about a revolutionary way to solve the noise problem through dynamic spectrum management (DSM) techniques. The noise problem can be mitigated by identifying vacant channels and then distributing existing network traffic across these vacant channels to reduce the node density per transmission channel. A joint approach of using AMC and DSM can complement one another to provide better performance in a cognitive radio based network in a high noise scenario.

In this chapter, we present two MAC-layer routing solutions for QoS provisioning. We will first present the MAC-Layer QoS Provisioning Protocol (MQPP) for Cognitive Radio Networks in section 3.1. Then we will present the Elastic Bandwidth Allocation Scheme (EBAS) with Softened Peak Interference Power Constraint for the Dynamic Cognitive Radio Systems in section 3.2.

3.1 A MAC-Layer QoS Provisioning Protocol for Cognitive Radio Networks

First of all, we investigate the issue of the differentiated service provisioning by adopting a strategy of TPC/AMC and DSM in 802.11 cognitive radio based WMNs or CRNs. The major contributions produced from this work can be summarized as 1) hierarchical adaptive MQPP Protocol by which nodes can provide a differentiated service for different types of traffic via varying the transmission power to increase the signal to interference/noise ratio and 2) distributes traffic to a vacant frequency spectrum when desired data rate is unattainable via power control.

Our proposed scheme has several advantages over current existing solutions. Firstly, costly switching delay is avoided by utilizing TPC/AMC as a primary option. Secondly, vacant channels are identified to support the data transmission rate required by high priority traffic when TPC/AMC is insufficient. To the best of our knowledge, the MQPP scheme is the first and the only scheme that can provide differentiated service for an 802.11-based CRN.

The rest of the section is organized as follows. Section 3.1.1 describes the system model. Section 3.1.2 presents the detailed operations of the MQPP scheme. Section 3.1.3 evaluates the performance of the MQPP scheme. Section 3.1.4 concludes the section.

3.1.1 System Model

3.1.1.1 Physical Layer Modelling

We consider a physical layer similar to the 802.11a standard with a total of 12 non-overlapping wireless channels and the time needed for channel switching is in the order of milliseconds [75]. The modulation scheme used is orthogonal frequency-division multiplexing (OFDM) with data rates of 6, 9, 12, 18, 24, 36, 48, and 54

Mbps.

The system under the study is an 802.11a based multi-hop CRN consisting of N MRs. The CRN is based on an interweave model [88], i.e., the nodes in the CRN can only transmit when the primary users are not active. Thus, there is virtually no interference to the primary users and there is no restriction on the power level of the secondary users.

Each MR is equipped with one data radio transceiver and one control radio transceiver. The data radio transceiver works on the software defined radio platform and can be configured with different parameters such as transmission power, frequency, modulation and data rate. As MCs communicate using dynamic frequency channels in a CRN, it can lead to the “deafness problem” where two MCs are unable to communicate with each other if they are on different frequency channels. This results in difficulties when MCs in the CRN need to collect global information about the network, or to exchange control information about the spectrum status and routing specific data.

Two approaches have been advocated for CRNs [101]. The first is to use a synchronization window, while the second approach uses a specific common control channel for exchanging control information. Due to the difficulty in implementing centralized clocking among all the MCs by the first approach, the adoption of a common control channel is preferred in many MAC [102-104] and routing [79, 105] schemes.

The common control channel is usually a low-frequency reserved band selected from the unlicensed pool, which covers long distances but, on the other hand, supports low rates. This eliminates the synchronization problems that may arise from neighbours tuned to different channels. In our research work on cognitive MAC

protocols, we have debated about the pros and cons of using various approaches to exchange control messages among nodes which could possibly operate in several distinct channels.

A distributed solution, by which different control channels are used for different groups of nodes were considered first. However, this approach incurred additional overheads in order to establish and maintain those groups. There will also be overheads involved to share control information among different groups of nodes.

We have also considered an approach where we have not dedicated any channel for control and link establishment. Instead we allow all channels to be shared by control and data traffic. However, this approach requires the cognitive radio to scan all the available channels in some random or pre-established order until it is able to establish one or more links. It has the advantage of making the system more robust, but the handshakes are required for channel rendezvous. And channel allocation is even more complicated compared to the above approach.

Basically, we have found that there is a trade-off involved in the use of a control channel. And it is between the simplicity of design and the overheads incurred in channel rendezvous. Furthermore, a recent survey by [106] has indicated that most of the existing cognitive MAC protocols are using a common control channel.

Therefore, in our scheme, we adopt the use of a common control channel through the use of a dedicated control radio transceiver to ensure that routing messages can be received by nodes despite of the discrepancy between their frequency bands. We also assume that nodes are able to share and access spectrum related information through the common control channel like noise estimates, etc. through the implementation of the variable relay sensing scheme proposed in [72].

For ease of explanation and without loss of generality, we consider unidirectional

traffic, i.e., the traffic that only goes from the MRs to the gateway. We consider the case where applications with 3 different priorities (c_1 , c_2 and c_3) are deployed in the network.

3.1.1.2 MAC Layer Modelling

To support the operation of our proposed MQPP protocol, we extend the RTS/CTS exchange scheme based on the MAC layer protocol of the IEEE 802.11 standard. We modify the RTS/CTS frames to carry additional information used by MQPP as shown in Figure 8. The additional fields of the MQPP control frames are described as below.

Figure 8: MQPP Control Frame Structure

RTS: This frame is sent by a transmitter over the control channel before the start of a transmission. The “Vacant Channels List” (VCL) field contains a list of unused channels sensed by the transmitter that can be used for data transmission. Furthermore, the default channel (current operating channel of the transmitter), if it is

currently unused by any other nodes is always listed in front. The “Length” field indicates the length bytes of the data packet to be transmitted and the “Priority” field indicates the priority of the data packet.

CTS: This frame is sent by the receiver onto the control channel after receiving a RTS. The “Chosen Channel” field contains the ID of the channel that is to be used for the following data transmission. The “Power” field indicates the required transmitter power while the “Data Rate” field indicates the supported data rate.

FC: The Frequency Change (FC) frame is sent by the transmitter onto the control channel due to a frequency change after receiving a CTS. The “Chosen Channel” field contains the ID of the channel that is to be used for the following data transmission.

ACK: The ACK frame is sent by the receiver onto the data channel after successfully receiving the data frame from the sender.

The Network Allocation Vector (NAV) is virtual carrier sensing mechanism used with wireless network protocols such as IEEE 802.11 and IEEE 802.16 (WiMax). The virtual carrier sensing is a logical abstraction which limits the need for physical carrier sensing at the air interface in order to save power. The MAC layer frame headers contain a Duration field that specifies the transmission time required for the frame, in which time the medium will be busy. The stations listening on the wireless medium read the Duration field and set their NAV, which is an indicator for a station on how long it must defer from accessing the medium.

The NAV may be thought of as a counter, which counts down to zero at a uniform rate. When the counter is zero, the virtual CS indication is that the medium is idle; when nonzero, the indication is busy. The medium shall be determined to be busy when the station is transmitting.

Each station calculates how long it will take to transmit its frame (based on data

rate and frame length); this information is included in the Duration field of the frame header.

3.1.1.3 Capacity Analysis

There have been some significant research results on the capacity of wireless networks. In [8], the analytical lower and upper bounds of wireless ad-hoc networks can be determined for the stationary case. The throughput capacity per node reduces significantly when the node density increases, such that it is $O(1/\sqrt{n})$, where n is the number of nodes. This result, however, cannot be applied directly in the case of WMNs. This is because in ad-hoc networks, traffic flows between arbitrary pairs of nodes. In contrast, in WMNs, practically all the traffic is either to or from the gateway. This introduces hot spots in the network that act as bottlenecks. Due to the presence of these bottlenecks, the available capacity for each node is further reduced to $O(1/n)$ [10], where n is the number of users for one gateway.

In our analysis, we analysed the network forwarding capacity of the proposed MQPP scheme. The network forwarding capacity of a network is the sum of link capacity that can be utilized in a time period. To generalize, in a given topology, let F be the set of non-overlapping usable channels. Each node can operate in any one of $|F|$ frequency channels.

We define the frequency interference region by the interference range of each transmission at a frequency f , where $f \in F$, such that only one link in a given frequency interference region can be active at any time, and all other links have to be inactive. To determine the interference region, the Friis Transmission Equation [107] can be used.

$$\frac{P_r}{P_t} = G_t G_r \left(\frac{\lambda}{4\pi r} \right)^2 \quad (1)$$

in conjunction with the relationship between wavelength and frequency which is given by

$$\lambda = \frac{c}{f} \quad (2)$$

where P_t and P_r are the transmission power and received power of the transmitting and receiving antenna respectively, G_t and G_r are the antenna gain of the transmitting and receiving antennas respectively, λ is the wavelength, r is the distance between the transmitting and receiving antennas, c is the speed of light in km/s and f is the frequency in Hz.

Rearranging (1),

$$\text{we get } r = \frac{c}{4\pi f \sqrt{\frac{P_r}{P_t G_t G_r}}} \quad (3)$$

The considered topology is a rectangular area of M metres x N metres containing n nodes. We assume that the n nodes are randomly distributed within the area. We also assume that each link has forwarding capacity of R_t according to a minimum required SINR specified in Table 1.

Considering a random region of r metres x r metres within the area, we would expect to see $\frac{r^2 n}{MN}$ nodes in the region. When a source node transmits data to the gateway, it has to compete with its intermediate downstream node for transmission time by using the RTS/CTS.

Using a power-controlled rate adaptive scheme [66], P_t can be tuned to meet the minimum SINR requirements of different modulation schemes and corresponding data transmission rates R_b while keeping BER under acceptable level such as 10^{-5} .

$$SINR = (P_i G / (N_0 + Noise)) \geq \gamma \quad (4)$$

Table 1: Minimum SINR Required and Corresponding Data Rate for BER $\leq 10^{-5}$

Data Rate (Mbps)	SINR Threshold (dB)	Power Transmission Ratio P_{imin}/P_{0min}
6	6.02	1
9	7.78	1.5
12	9.03	2
18	10.79	3
24	17.04	12.65
36	18.8	18.97
48	24.05	63.53
54	24.56	71.45

where P_i denotes the transmission power of node i , G denotes the link gain from transmitting node to receiving node, N_0 denotes thermal noise of receiving node, $Noise$ denotes the measured noise due to other sources at receiving node and γ is the SINR threshold of the required data transmission rate.

From (4), we can derive the relationship between SINR and the transmission power. The ratios of transmission power P_{imin}/P_{0min} can be calculated with reference of the relationship between the SINR and data transmission rate specified in Table 1. P_{imin} is the minimum transmission power needed to reach a data transmission rate i , P_{0min} is the minimum transmission power needed by the lowest data transmission rate (6 Mbps).

For the case of a traditional WMN where all nodes are on the same frequency interference region, i.e., $|F|=1$, since the range of a transmitting node is r , only one node out of $\frac{r^2 n}{MN}$ nodes is able to transmit at one time due to them being in the same frequency interference region. An example is shown in Figure 9 where the interference region is shaded for the link $S4 \leftrightarrow S6$. The total forwarding capacity for this case is only R_t for one region and $\frac{MNR_t}{r^2}$ for the entire network.

Figure 9: Frequency interference region where $|F|=1$

For the same topology, MQPP allows nodes to communicate using vacant channels when current channel is occupied. If we assume that $|F|>1$ as shown in Figure 10, we can assign the nodes to non-overlapping channels. Even though the interference regions overlap in terms of coverage, they do not overlap in terms of frequency. For such a case, each node in an interference region is allowed to transmit.

Figure 10: Frequency interference region where $|F|=3$

The total forwarding capacity for the entire network is thus increased to $\frac{MNR_t|F|}{r^2}$.

Using $c = 3 \times 10^8$ m/s, $f = 2.4 \times 10^9$ Hz, $M = 2000$ m, $N = 2000$ m and assuming unity gain at both transmitting and receiving antennas, $G_t = 1$ and $G_r = 1$, we plot the theoretical forwarding capacity for both WMN and MQPP at different transmission power ratio.

Figure 11: Power Transmission Ratio vs. Normalized Forwarding Capacity

From Figure 11, we can see that as the power transmission ratio increases, the overall network capacity will actually decrease due to the increased interference which limits the number of possible concurrent transmissions in the entire network. Thus, even if AMC technique can be used to provide service differentiation for different traffic classes, it does so at an expense of the overall network forwarding capacity. From the graph, however, we can see that utilizing multiple channels for concurrent transmissions is a relatively cheap and easy way to mitigate the disadvantages of AMC, and this is the main motivation of our work.

3.1.2 Proposed Scheme

3.1.2.1 Overview

With the support of CR technique and the previous work on the power-controlled rate-adaptive MAC scheme [66], we have come up with the idea to design a hierarchical adaptive MAC protocol, the MQPP using a customized MQPP handshaking mechanism shown in Figure 12.

Figure 12: MQPP Handshaking

The differences between the MQPP handshaking mechanism and the usual IEEE 802.11 RTS/CTS handshaking mechanism are due to the addition of a FC frame. As mentioned in Section 3.1.1.2, the FC frame is sent by the transmitter onto the control channel due to a frequency change after receiving a CTS from the destination node. This allows all nearby nodes which overhear the FC frame to cancel the NAV generated by the initial RTS frame and to set a new NAV for the new allocated

channel. The cancelling of the initial NAV generated by the initial RTS frame allows other nodes to transmit using the previously reserved channel which would otherwise be wasted.

The MQPP provides two modes of transmission as shown in Figure 13. In the normal mode, the MAC layer adjusts the transmission power to reach the desired data transmission rates according to the requested priority and prevailing SINR. The MQPP handshaking process for this mode is similar to the 802.11 standard and is performed if AMC alone is sufficient to satisfy the minimum SINR threshold of the required data transmission rate.

In the extended mode, a vacant channel will be identified to support the required transmission when the current channel is not able to provide the required data rate requested at the prevailing SINR. The MQPP handshaking process involves the use of an additional FC frame to identify the vacant channel to support the required data transmission rate.

Figure 13: MQPP Flow Diagram

3.1.3.2 Detailed Operation

Before the start of a data transmission, the sender will inspect its Channel Information Cache and builds a vacant channels list or VCL. An example snapshot of the Channel information Cache and VCL consisting of channels with Network Allocation Vector (NAV) =0, and sorted in ascending order of noise is shown in

Figure 14. Additionally, if NAV of the current operating channel is 0, it is inserted into the front of the VCL. The transmitter then inserts the VCL into the RTS frame.

To determine the NAV field of the RTS frame, we use the minimum data rate according to traffic priority with reference to Table 2. The minimum data rate is 6 Mbps, 12 Mbps and 24 Mbps, respectively, for the priority c_3 , c_2 and c_1 traffic. The total length L of a data frame and priority c_k is also inserted into the RTS frame.

The RTS will be transmitted at the basic data rate K_0 and basic transmission power P_0 which is the minimum transmission power needed by the slowest data transmission rate (i.e. 6Mbps) onto the control channel. All nearby nodes that hear the RTS frame will store the channel and the associated NAV into the Channel Information Cache.

	Channel	Duration (NAV)	ID	Noise
	ID	μs		(dBm)
current operating channel ➔	2	3290	7	15.4
	3	0	0	5.3
	4	0	0	4.2
	5	970	6	6.9
	6	0	.0	10.7
	7	769	2	19.8
	8	1252	11	21.0
	9	0	0	8.5
	10	0	0	5.7
	11	352	12	9.7

Channel Information Cache

Channel ID
6
4
3
10
9

VCL

Figure 14: Example Snapshot of Channel Information Cache and VCL

Interference Estimation

Once the receiver receives the RTS frame successfully, it extracts the priority c_k of the data frame. Depending on the priority c_k , it seeks the SINR threshold γ_i^* of the maximum supported data transmission rate for c_k , K_i with reference to Table 2. (i = index of the table, where the first row is 0, second row is 1, and so on.)

The receiver also measures the received power of the RTS frame and determines

the link gain G from the transmitter to the receiver. This can be easily achieved since the transmission power of the RTS frame is known in advance (P_0).

Table 2: Data Rate, Modulation, SINR threshold, Power and Supported Priority for $\text{BER} \leq 10^{-5}$

Data Rate (Mbps) K_i	Modulation	SINR Threshold (dB) γ^*	Supported Priority c_k
6	BPSK	6.02	c_3
9	BPSK	7.78	c_3
12	QPSK	9.03	c_2, c_3
18	QPSK	10.79	c_2, c_3
24	16-QAM	17.04	c_1, c_2
36	16-QAM	18.8	c_1, c_2
48	64-QAM	24.05	c_1
54	64-QAM	24.56	c_1

Channel Decision

Due to the large delay arising from channel switching, it is desirable to provide the desired QoS through AMC over the existing operating channels. However, the data channels of both transmitter and receiver may not be tuned to the same channel since the nodes may communicate using dynamic channels. In order for both transmitter and receiver to agree on a common channel for data communication, we depict three scenarios here as in Figure 15.

In the first scenario, both transmitter and receiver are already on the same data channel, so there is no channel switching delay incurred if the current data channel is able to provide the desired QoS. In the second scenario, both transmitter and receiver have to be tuned to a new channel for data communication. In the third scenario, the transmitter and receiver are on different channels, and either one must switch to the channel that the other is already on.

For both scenarios two and three, channel switching delays are unavoidable. However, scenario two can provide a better performance since there is much greater

flexibility in the selection of channels. Scenario 3 is much more restrictive compared to scenario 2 as there are only two channels for selection, which is either the sender channel, or the receiver channel. This will severely impact the performance of the protocol as there may be better quality channels which could be used. Thus in our proposal, we will only consider scenario one and two.

Figure 15: Channel Switching Scenarios

Scenario 1

This is only possible when both transmitter and receiver's data channel are currently tuned to the same channel. To verify this, the receiver extracts the VCL field from the RTS frame and compares with its own VCL. If $VCL_s[0] = VCL_r[0]$, i.e. the current operating channel of both transmitter and receiver is the same, then set $Ch1 = VCL_r[0]$. In addition, choose a backup channel $Ch2 \in VCL_s \cap VCL_r$ with the least noise. If $Ch2 \equiv \emptyset$, there will be no backup channel.

Scenario 2

Choose a channel $Ch2 \in VCL_s \cap VCL_r$ with the least noise. If $Ch2 \equiv \emptyset$, terminate and do not sent CTS.

For both scenarios, the receiver calculates the current instantaneous SINR for the chosen channels using $SINR = (P_0 G / (N_0 + Noise)) \geq \gamma^*$ (5)

where P_0 denotes the transmission power of the transmitter, G denotes the link

gain from the transmitter to the receiver, N_0 denotes thermal noise of receiver and $Noise$ is the measured noise due to other sources at the receiver.

The receiver then calculates an average SINR value based on a window of previously measured SINR values. It is calculated as: $SINR_{ave} = (1 - w_q)SINR_{ave} + w_q SINR$ where $SINR$ is the current instantaneous SINR measured and w_q is the weight assigned to the current instantaneous SINR measured.

As shown in Table 2, by our scheme, the transmission of packets belonging to higher priority will use higher power. It results in better SINR at the receiver, thus achieving higher data rates compared to the lower priority traffic. Although power control can be used to increase data rate, the network interface card has a limit to the maximum transmission power P_{max} .

We model the power control scheme as follows. Let M_i represents the available modulation schemes with corresponding data transmission rate, K_i and SINR threshold γ_i^* at which $BER(M_i) = 10^{-5}$, $i = 0, 1, \dots, 7$. Packets with priority c_k can be transmitted at maximum transmission rate K_{9-2k} and minimum transmission rate K_{6-2k} .

Depending on traffic priority c_k and its maximum supported data rate, the required transmission power P can be calculated with the reference of the relationship among the SINR, priority and the data transmission rate specified in Table 2.

The required power P can be calculated as

$$P = \text{Max}(P_0 \times \gamma_i^* / \text{SINR}_{ave}, \text{rxsensitivity}(K_i) \times P_{RTS} / P_{rRTS}) \quad (6)$$

where $\text{rxsensitivity}(K_i)$ is the receiving sensitivity of rate K_i , P_{RTS} is the transmission power of RTS. P_{rRTS} is the received signal strength of RTS after attenuation.

For Scenario 1, if the calculated K_i and P for $Ch1$ satisfy the minimum supported data rate and the maximum power constraint, the receiver creates a CTS frame with

the selected channel, required power P , and supported data rate K_i . In addition, the NAV field can be updated according to the new data rate K_i and data frame length. The receiver then transmits the CTS frame. If the calculated K_i and P for $Ch1$ cannot satisfy the minimum supported data rate and the maximum power constraint, then it will be recalculated for the backup channel $Ch2$, after which Channel Switching will be performed.

For Scenario 2, K_i and P will only be calculated for $Ch2$. Channel Switching will be also performed.

Algorithm : Determine_Data_Rate_and_Power

Begin

For a packet with priority c_k where $k = 1, 2$ or 3

$i = 9-2k$;

while ($i >= 6-2k$)

$P = \text{Max}(P_0 \times \gamma_i^* / \text{SINR}_{\text{ave}}, \text{rxsensitivity}(K_i) \times P_{\text{RTS}} / P_{\text{rRTS}})$;

if ($P > P_{\text{max}}$)

$i = i-1$;

else

set supported data rate as K_i ;

set required power as P ;

exit procedure;

endif

end while

End

Channel Switching

Due to the overheads of channel switching, the receiver calculates the NAV field of the CTS field to include the channel switching delay. The receiver then creates a CTS frame with the selected channel, required power P , and the supported data rate K_i . The receiver transmits the RTS frame and also performs a channel switch to $Ch2$.

AMC

When the CTS frame is received by the transmitter, it inspects the “Chosen Channel” field to determine the data channel. If there is a need to perform channel switching, the transmitter will send out a FC frame onto the control channel that contains the indication of its new data channel. When the FC frame is received, the nodes will update the Channel Information Cache to cancel the NAV generated by the

initial RTS frame and to set a new NAV for the new allocated channel. After sending out the FC frame, the transmitter performs a channel switch and transmits the data frame onto the new data channel using the supported data rate K_i and power P .

3.1.3 Mathematical Analysis of Throughput/Delay

In this section, we evaluate the performance of the MQPP scheme in the assumption of ideal channel conditions and a finite number of nodes. This can be done by employing a two dimensional Markov chain analysis.

We first consider a fixed number n of contending nodes. In saturation conditions, each node always has a packet available for transmission, after the completion of each successful transmission. Each packet needs to wait for a random backoff time before transmitting according to the IEEE802.11 DCF binary exponential backoff scheme. The backoff time is uniformly selected in the range between 0 to $CW-1$, where the value of CW is dependent on the number of failed transmissions of a packet. At the first transmission attempt, $W = CW_{min}$, which is the minimum contention window. After each retransmission due to a collision, CW is doubled up to a maximum value, $CW_{max} = 2^m W$, where m is the maximum backoff stage.

Let $b(t)$ be the stochastic process representing the backoff time counter for a given node. A discrete and integer time scale is adopted: t and $t+1$ correspond to the beginning of two consecutive slot times. Furthermore, the backoff time counter of each node decrements at the beginning of each slot time. Let $s(t)$ be the stochastic process representing the backoff stage (0, ..., m) of the node at time t . We also assume that at each transmission attempt, and regardless of the number of retransmission attempts, each packet collides with constant and independent probability p . Once independence is assumed, it is possible to model the

bidimensional process $\{s(t), b(t)\}$ with the discrete-time Markov chain as shown in Figure 16. In this Markov chain, the only non-null one-step transition probabilities are:

Figure 16: Markov Chain model

$$\begin{cases} P\{i, k | i, k+1\} = 1 & k \in (0, W_i - 2) & i \in (0, m) \\ P\{0, k | i, 0\} = (1-p)/W_0 & k \in (0, W_0 - 1) & i \in (0, m) \\ P\{i, k | i-1, 0\} = p/W_i & k \in (0, W_i - 1) & i \in (1, m) \\ P\{m, k | m, 0\} = p/W_m & k \in (0, W_m - 1) \end{cases} \quad (1)$$

Let $b_{i,k} = \lim_{t \rightarrow \infty} P\{s(t) = i, b(t) = k\}$, $i \in (0, m)$, $k \in (0, W_i - 1)$ be the stationary

distribution of the Markov chain. We can obtain a closed-form solution for this Markov chain by noting that:

$$b_{i-1,0} \cdot p = b_{i,0} \rightarrow b_{i,0} = p^i b_{0,0} \quad 0 < i < m$$

$$b_{m-1,0} \cdot p = (1-p)b_{m,0} \rightarrow b_{m,0} = \frac{p^m}{1-p} b_{0,0} \quad (2)$$

Due to chain regularities, for each $k \in (0, W_i - 1)$,

$$b_{i,k} = \frac{W_i - k}{W_i} \begin{cases} (1-p) \sum_{j=0}^m b_{j,0} & i = 0 \\ p \cdot b_{i-1,0} & 0 < i < m \\ p \cdot (b_{m-1,0} + b_{m,0}) & i = m \end{cases} \quad (3)$$

Using (2) and the fact that $\sum_{i=0}^m b_{i,0} = \frac{b_{0,0}}{1-p}$, we can rewrite (3) as :

$$b_{i,k} = \frac{W_i - k}{W_i} \cdot b_{i,0} \quad i \in (0, m), \quad k \in (0, W_i - 1) \quad (4)$$

$b_{0,0}$ can be determined by imposing the normalization condition, that simplifies as follows:

$$\begin{aligned} 1 &= \sum_{i=0}^m \sum_{k=0}^{W_i-1} b_{i,k} = \sum_{i=0}^m b_{i,0} \sum_{k=0}^{W_i-1} \frac{W_i - k}{W_i} = \sum_{i=0}^m b_{i,0} \sum_{k=0}^{W_i-1} \frac{W_i + 1}{2} \\ &= \frac{b_{0,0}}{2} \left[W \left(\sum_{i=0}^{m-1} (2p)^i + \frac{(2p)^m}{1-p} \right) + \frac{1}{1-p} \right] \end{aligned} \quad (5)$$

from which

$$b_{0,0} = \frac{2(1-2p)(1-p)}{(1-2p)(W+1) + pW(1-(2p)^m)} \quad (6)$$

The probability τ that a node transmits a packet in a randomly chosen slot time can be expressed as

$$\tau = \sum_{i=0}^m b_{i,0} = \frac{b_{0,0}}{1-p} = \frac{2(1-2p)}{(1-2p)(W+1) + pW(1-(2p)^m)} \quad (7)$$

From (7), we can see that the transmission probability τ depends on the collision probability p . The probability p that a transmitted packet encounters a collision in the probability that at least one of the $(n-1)$ remaining nodes transmit in the same time slot. If all nodes transmit with probability τ , the collision probability p is :

$$p = 1 - (1 - \tau)^{n-1} \quad (8)$$

Therefore, (7) and (8) form a nonlinear system with two unknown parameters τ

and p , which can be solved by numerical method.

Note that $\tau \in (0,1)$ and $p \in (0,1)$.

Let P_{tr} be the probability that there is at least one transmission in the considered time slot. When n nodes contend on the same channel and each transmits with probability τ :

$$P_{tr} = 1 - (1 - \tau)^n \quad (9)$$

The probability P_s that an occurring packet transmission is successful is given by the probability that exactly one node transmits and the remaining $(n-1)$ nodes defer transmission, conditioned on the fact that at least one node transmits:

$$P_s = \frac{n\tau(1-\tau)^{n-1}}{P_{tr}} = \frac{n\tau(1-\tau)^{n-1}}{1 - (1-\tau)^n} \quad (10)$$

Let S be the normalised system throughput, defined as the fraction of time the channel is used to successfully transmit data bits.

$$\begin{aligned} S &= \frac{E[\text{data transmitted in a slot time}]}{E[\text{length of a slot time}]} \\ &= \frac{P_s P_{tr} T_{data}}{(1 - P_{tr})\sigma + P_{tr} P_s T_s + P_{tr} (1 - P_s) T_c} \end{aligned} \quad (11)$$

Where T_{data} represents the transmission time of the data, T_s is the average time that the channel is sensed busy due to a successful transmission, T_c is the average time that the channel is sensed busy by each node during a collision, and σ is the duration of an empty slot time.

We consider a system in which each packet is transmitted by means of the MQPP extended mode mechanism (Figure 12). In this case, a collision can only occur on RTS frames. Ignoring propagation and header delays,

$$T_s^{rts} = T_{DIFS} + T_{RTS} + T_{SIFS} + T_{CTS} + T_{FC} + T_{data} + T_{SIFS} + T_{ACK} \quad (12)$$

$$T_c^{rts} = T_{RTS} + T_{DIFS} \quad (13)$$

Considering that in the MQPP protocol, n nodes are distributed into $|F|$ possible communicating channels, there are $n/|F|$ nodes to compete at each channel, therefore,

$$P_{tr}(F) = 1 - (1 - \tau)^{(n/|F|)} \quad (14)$$

$$P_s(F) = \frac{(n/|F|)\tau(1 - \tau)^{(n/|F|)-1}}{P_{tr}(F)} \quad (15)$$

Therefore, the normalization throughput of each channel is:

$$S(F) = \frac{P_{tr}(F)P_s(F)T_{data}}{(1 - P_{tr}(F))\sigma + P_{tr}(F)P_s(F)T_s + P_{tr}(F)(1 - P_s(F))T_c} \quad (16)$$

The delay for each channel can then be easily derived since it is inversely proportional to the normalized throughput, $D(F) = \frac{1}{S(F)}$ (17)

According to (11) and (16), we compare the normalization network throughput achieved by MQPP with a single channel 802.11 protocol, through 1001 times MATLAB simulations.

Figure 17: Normalized Network Throughput

Figure 17 shows the normalized network throughput comparison between a single channel 802.11 based scheme versus the MQPP scheme with $|F|=3$ and $|F|=8$. The graph shows that when $|F|$ increases, MQPP will have a higher normalized network throughput due to the availability of more vacant channels for transmission. This agrees with the observation made in Section 3.1.1.3. From the graph, we can also see that as the number of nodes in the network increases, the network performance of all schemes deteriorates due to the increased probability of collision. However, the MQPP always significantly outperforms the single channel 802.11 or equivalent schemes.

Figure 18: Normalized Delay

Figure 18 shows the normalized network delay comparison between a single channel 802.11 based scheme versus the MQPP scheme with $|F|=3$ and $|F|=8$. The delay encountered by the 802.11 MAC increases at an exponential rate as the number of nodes grows. This is due to the numerous retransmissions occurring in the network due to frequent packet collisions. Nodes using MQPP encounter much less packet collisions and thus less overall delay due to the ability to utilise additional vacant channels for traffic transmission.

3.1.4 Performance Evaluation

Simulation experiments have been performed using OPNET to evaluate the performance of the proposed MQPP scheme.

3.1.4.1 Simulation Setup

A scenario with 64 MRs has been considered. The MRs form an 8×8 grid with a distance of 125m between any two neighbouring MRs. We performed 51 simulation

runs with different random number seed. For each run, a random MR is selected as the gateway and 16 other MRs are selected as traffic sources. Packets are forwarded in a multi-hop fashion to/from the gateway. The traffic generation is a Poisson process with packet inter-arrival time exponentially distributed with mean value of 25ms. The packet size is fixed at 512 bytes with three different priorities (c_1 , c_2 and c_3). Each priority of packets occupies 1/3 of entire traffic load. Receiver sensitivity is -95dBm, basic transmission power is 7dBm and maximum transmission power is 30dBm. Channel 1 is designated as the common control channel. Switching delay is set as 1ms.

We compare the performance of MQPP with that of other 3 schemes to show the benefit of MQPP. These schemes are (i) 802.11a based traditional WMN with Power Control (PCRA) [66], (ii) 802.11a based single interface CR-WMN [76] and (iii) 802.11e. For the PCRA and the 802.11e scheme, there is no channel switching when the requested data rate cannot be supported. Instead, the lowest data rate (6 Mbps) will be used. As the typical throughput at the unoccupied frequency band is 23 Mbps [109], if the current throughput is 24 Mbps, it is not necessary to initiate channel switching, due to the penalty of the switching overheads. However, if the data rate falls below 24 Mbps, e.g. 18 Mbps and below, then it is advantageous to switch to a less noisy channel. Thus, for CR-WMN, it is assumed that the channel switching is initiated when the supported data rate drops to 18 Mbps and below. The three major metrics for performance evaluation are single-hop average packet delay, network throughput, average transmission power and protocol overheads.

3.1.4.2 Simulation Results

The simulation results in Figure 19 show that packets experiences less delay by

the MQPP compared to other schemes under various traffic loads. CR-WMN performs poorly due to the need to switch back to the common control channel after every transmission. Due to lack of service differentiation features like EDCA or AMC, there is also no delay differentiation for different traffic classes.

MQPP also performs much better compared to PCRA because the MQPP can transmit across different frequency channels with higher data transmission rate when the existing channel is unable to provide the minimum required data rate due to noise. The performance of the higher priority traffic under 802.11e degrades when the offered load becomes larger. This is due to the scheme unable to provide protection to the higher priority traffic from the effect of noise and collisions under heavy load.

MQPP can also provide clear delay differentiation for different traffic classes with higher priority traffic experiencing lower delay compared to lower priority traffic. This is because higher priority packets are likely to be sent using a higher transmission power which makes them more resilient to noise compared to lower priority packets.

Figure 19: Delay vs. Offered Load

Figure 20 shows the throughput of all schemes under various traffic loads. When traffic load is at about 300 kbps all schemes have almost the same throughput. MQPP begins to outperform other schemes significantly when the offered load increases beyond 750 kbps. For the simulation scenario, a total of 16 traffic sources are transmitting at any one time. If we consider the total network load, it is about 12Mbps (16 x 750kbps). With retransmissions and protocol overheads, this figure will be closer to about 17-19Mbps. Since the typical throughput of an unoccupied frequency band is about 23Mbps [109], the total load is about 80% of the typical supported throughput. As MQPP is able to redistribute traffic to vacant channels using dynamic spectrum management techniques, its performance is much better compared to the other protocols under a heavy load situation.

At an offered load of 1.4Mbps, MQPP has 16%, 39% and 43% higher throughput compared to PCRA, CR-WMN and 802.11e respectively.

Figure 20: Throughput vs. Offered Load

Figure 21 shows the average transmitting power for all schemes under various traffic loads. When traffic load is 1.4Mbps, PCRA transmits at an average power of

14.8 dBm whereas MQPP's average transmitting power is 9.8 dBm. The reason for the higher power consumption for PCRA is that as transmission power increases, it interferes with the reception of packets at remote nodes, causing them to increase their transmitting power to compensate for the increased noise. It causes even more collisions and average transmitting power begins to spiral uncontrollably towards the maximum allowable power. MQPP suffers less from this shortcoming as it is able to spread the traffic load onto other channels. The transmission power for both 802.11e and CR-WMN are constant across all offered load as they do not have AMC features.

Figure 22 shows the total protocol overheads for all schemes under various traffic loads. It measures the overhead generated by the RTS/CTS and ACK packets to indicate the efficiency of the protocols. Under all traffic loads, the overheads for the MQPP scheme are higher than those of the other schemes. This is due to the additional control packets that are required for channel switching and updates. However, the volume of the control packets generally does not exceed 10% of the total traffic generated.

Figure 21: Average Transmission Power vs. Offered Load

Figure 22: Total Protocol Overheads vs. Offered Load

Figure 23 compares the delivery ratio of all schemes under various traffic loads. Due to the ability to redistribute traffic to vacant channels using dynamic spectrum management techniques, the delivery ratio of the MQPP scheme is much better compared to the other protocols under a heavy load situation since there is less retransmissions.

Figure 23: Delivery Ratio vs. Offered Load

3.1.4 Conclusion

In this section, we have proposed a MAC Layer QoS Provisioning Protocol for IEEE 802.11-based CRNs (MQPP) to support differentiated service in WMNs. Our scheme combines two approaches, AMC and DSM provided by cognitive radio technology. Mathematical analysis has shown that the MQPP is able to outperform existing schemes. This has also been validated by the simulation results which have shown that the proposed MQPP scheme can provide a significant performance improvement in terms of lower delay and higher throughput at the cost of only a slight increase of transmission power and protocol overheads. MQPP can also provide clear service differentiations for different traffic classes under all traffic loads. In the next chapter, we have described the extension of our work by implementing an interference-aware routing scheme to improve the end-to-end network performance with consideration of the overall network topology, traffic types and volume.

3.2 Elastic Bandwidth Allocation Scheme with Softened Peak Interference Power Constraint for the Dynamic Cognitive Radio Systems

In the previous section, we have proposed the MQPP scheme to support differentiated service for IEEE 802.11-based CRNs. The scheme allows vacant frequency channels to be made use by the secondary system (SS) (consisting of the mesh routers and mesh clients) when the Primary System (consisting of one or more Primary Users) is not occupying the channel.

In the above mentioned work, we assumed the spectrum interweave scenario, where the channel is always available. However, this may not be true in practical cognitive radio systems where the Primary Users (PUs) may suddenly re-appear. As mentioned in Section 2.6.3, the time-varying nature of the available resources in the

can be mitigated through using spectrum underlay technique where simultaneous transmissions of primary and secondary systems are allowed. The disadvantage of the spectrum underlay technique is that the secondary transmitter is severely restricted in its output power so as to keep interferences below a certain threshold.

In this section, we propose the design of an Elastic Bandwidth Allocation scheme to combine the strength and to mitigate the weaknesses of both spectrum overlay and underlay through a hybrid transmission strategy. In addition, the scheme adopts the use of a softened peak interference power (s-PIP) constraint to improve the performance of the secondary system while still granting superior protection to primary system transmissions. Specifically, we address the weaknesses of existing resource allocation schemes by considering the effect of PU activity in the design of QoS provisioning in OFDM-based dynamic CR systems.

The major contributions of our work are twofold. The first contribution is a proposal that uses a hybrid transmission strategy that consists of both spectrum overlay and spectrum underlay, with a unique elastic bandwidth allocation scheme.

In the literature, most of the existing proposed schemes consider a combination of both average interference power (AIP) and peak interference power (PIP) constraint. However, a key finding by [92] has shown that the AIP constraint is superior over the PIP constraint in terms of various forms of capacity limits achievable for the primary radio fading channel. Although the author [92] recommends that the AIP constraint should be used for the purpose of protecting the PS transmission as well as maximizing the SS throughput, it has also implied that the PIP is irrelevant for the purpose of protecting the PS transmissions.

This brings us to the other significant difference of our scheme compared to the existing schemes. Our second contribution is a scheme that performs resource

allocation subjected to a softened peak interference power (s-PIP) constraint, in addition to the AIP, whereas most existing schemes consider a combination of both AIP and PIP constraint. Adopting the s-PIP allows us to achieved a delicate balance between the recommendation by [92] and the need to consider the PIP in the resource allocation algorithm. To the best of our knowledge, the EBAS scheme is the first and only scheme that adopts a hybrid approach of combining both overlay and underlay transmission modes in dynamic OFDM-based CR systems with the consideration of s-PIP and AIP.

The remainder of this section is organized as follows. In Section 3.2.1, we describe the model of the CR system under study. In Section 3.2.2, we introduce our objective and constraints, and propose the elastic bandwidth allocation policy. In Section 3.2.3, we verify our elastic bandwidth allocation scheme through extensive simulations. Finally, we summarize the main observations from this work in Section 3.2.4.

3.2.1 System Model

We consider a PS of bandwidth B Hz supporting M PUs. The total bandwidth is divided into N subcarriers with each having the bandwidth of B/N Hz. Without loss of generality, we assume that each PU occupies a bandwidth that are integer multiples of B/N Hz. We consider the case that not all of the N subcarriers are assigned to the PUs, leaving spectrum gaps between bands that have been allocated to the PUs. The spectrum gaps can then be assigned to the SUs for opportunistic spectrum access. The SUs have different priorities c_1, c_2 and c_3 where c_1 ($c_1 > c_2 > c_3$) is the highest priority. We assume that the SUs have the requirement of a minimum transmission rate and maximum power constraints.

Due to the dynamic activities of the PUs, it is possible that the overlay subcarriers

are reoccupied by returning PUs. We denote the probability that the overlay subcarrier will be reoccupied by a returning PU in the current time frame by Φ . We further assume that when it happens, all overlay subcarriers that are previously occupied by a SU will be reoccupied by the PU that is occupying the left side of the frequency spectrum.

Figure 24: Channel Allocation

3.2.1.1 Hybrid Opportunistic Spectrum Access

In most existing schemes, SUs access the spectrum gaps through the use of OFDM subcarriers via the overlay mode in the vacant subcarriers. However, since the occupied subcarriers might have a very good channel quality for underlay access, SUs can also access the occupied subcarriers via spectrum underlay to improve their capacity. We make use of this hybrid opportunistic spectrum access strategy in our scheme. This is illustrated for SU_1 in the top channel allocation chart in Figure 24 where subcarrier 5 and 6 are accessed via the overlay method, and subcarrier 4 and 7 are accessed via the underlay method.

We denote the set of unallocated subcarriers, which are available for spectrum overlay, as K_0 and the set of subcarriers allocated to PU_j , which are available for spectrum underlay, as K_j . We suppose one subcarrier can only be allocated to one PU

and/or SU, i.e., $K_j \cap K_i = \phi, \forall i \neq j$ then $\bigcup_{j=0}^M K_j = \{1, 2, \dots, N\}$.

We denote the set of subcarriers allocated to SU_j as L_j . Thus, the SU_j is transmitting in the overlay mode when $(K_j \cup K_{j+1}) \cap L_j = \phi$ and transmitting in the hybrid mode when $(K_j \cup K_{j+1}) \cap L_j \neq \phi$.

3.2.1.2 Problems with Returning PUs

The dynamic nature of the spectrum usage due to PUs activities may result in the repossession of subcarriers that are previously available for secondary access via spectrum overlay. We assume that when this happens, all subcarriers that are previously occupied by a SU will be repossessed by the PU that is occupying the left side of the frequency spectrum.

There are two problems which can occur. Firstly, there will be a lack of vacant subcarriers available for overlay transmission and the SU has to change its transmission mode to the underlay paradigm. An example is shown in Figure 24 where PU_1 reoccupies subcarriers 4, 5 and 6, while PU_2 reoccupies subcarriers 10, 11 and 12. The total time d_{switch} required for channel sensing and adjusting the transmit power level, bandwidth, bit-rate, antenna beam etc is non-negligible. As such, it is entirely possible that the noise experienced by some PU subcarriers may temporarily exceeds its predefined threshold for a period of d_{switch} until the SU can react and adjust its transmission parameters accordingly. This is shown in Figure 25.

Figure 25: Overheads of Transmission Mode Switching

Secondly, when a PU appears and reclaims the vacant subcarriers, the SU can only transmit through these subcarriers through the underlay paradigm. This will mean that the QoS provided to the SU will inevitably suffer. By our scheme, we allow higher priority SUs to access additional subcarriers via the underlay transmission mode to mitigate the performance loss. This is performed depending on QoS requirements and is subjected to noise and power constraint. An example is illustrated for SU_1 in Figure 24 where subcarrier 5 and 6 are repossessed by PU_2 . The additional subcarriers that are used by SU_1 are subcarriers 4 and 7.

3.2.1.3 Transmit Power Constraint

In order to attain a higher system capacity, the secondary transmitter needs to allocate more power to stronger subcarriers and less or even no power to weaker ones. To ensure this condition, the MAC protocol may adjust the transmit power P up to a bound P_{max} , which is typically determined by the regulatory and/or hardware constraints. Regardless of whether it is overlay or underlay transmission mode, the transmit power constraint at the SU transmitter ensures the summation of power allocated over all subcarriers is within a power budget P_{max} of the SU transmitter.

$$P = \sum_{i \in L_j}^n P_i \leq P_{max} \quad (1)$$

where P_i denotes the power allocated to the subcarrier i of the SU transmitter.

3.2.1.4 Receive power constraint

The power density spectrum of the power signal transmitted by the SU transmitter on subcarrier i can be denoted by [89],

$$\Phi_i(f) = T_s P_i \left(\frac{\sin \pi f T_s}{\pi f T_s} \right)^2 \quad (2)$$

where P_i denotes the power allocated to the subcarrier i of the secondary transmitter and T_s is the symbol duration.

The interference power introduced by subcarrier i to the primary system subcarrier n can be found by integrating (Eq.2) across the primary system subcarrier [90].

$$I_i^n = |g^n|^2 \int_{(d-1/2)\frac{B}{N}}^{(d+1/2)\frac{B}{N}} \Phi_i(f) df \quad (3)$$

where g^n denotes the channel gain from the SU transmitter to the PU receiver on subcarrier n and $d = |i - n|$ represents the distance between the considered subcarrier i , the PS subcarrier n in multiples of B/N and Φ_i is the power density spectrum of the power signal.

According to [89], the interference caused by the SU to the PU increases as the subcarrier spacing between the SU and PU, i.e., d decreases. Thus, in the underlay mode where d is 0, the interference will be the greatest assuming all other parameters remain the same. Thus, reducing the SU transmitter power to less than a certain threshold can ensure that the received power constraint at the PU receiver can be met. For both overlay and underlay transmission mode, the interference-power constraints have been defined as the peak or the average interference power constraints.

$$\text{peak: } \sum_{i=1}^N I_i^n \leq I_{\max}^n, n \in K_j \quad (4)$$

$$\text{average: } \frac{1}{|K_j|} \sum_{i=1}^N \sum_{n \in K_j} I_i^n \leq I_{\max}$$

(5)

where $I_{\max}^n$ and $I_{\max}$ are the peak and the average interference power that the PU receiver can tolerate at each subcarrier n and over all subcarriers.

Constraint (4) and (5) ensures that the amount of the peak and average interference

received by the primary receiver at each subcarrier n is less than $I_{\max}^n$ and $I_{\max}$ respectively.

3.2.1.5 Capacity

According to Shannon-Hartley Theorem, the capacity of a communication channel can be calculated using:

$$C = B \log_2 \left(1 + \frac{S}{W} \right)$$

where C is the channel capacity in bits per second, B is the bandwidth in hertz, S is the total received signal power over the bandwidth in watts and W is the total interference power or noise received over the bandwidth in watts.

Thus, the capacity of SU_j can be calculated as:

$$C = \Delta f \sum_{i \in L_j} \log_2 \left(1 + \frac{|h^i|^2 P_i}{\sigma^2 + j(i)} \right) \quad (6)$$

where h^i is the channel gain between the CR transmitter and CR receiver on subcarrier i , σ denotes the additive white Gaussian noise (AWGN) variance, and $j(i)$ denotes the interference because of all PU bands into the SU_j on subcarrier i .

3.2.2 Proposed Elastic Bandwidth Allocation Scheme

From the viewpoint of the SUs (Eq.6), it is desirable to use a high transmission power in order to optimize the capacity of the SU. However, this strategy has a detrimental effect during the re-appearances of PUs where a higher noise is encountered due to the delay in the change of transmission mode from overlay to underlay mode. Thus it is desirable to keep the SU transmission power to as low as possible from the viewpoint of the PU (Eq.3). Since both of the above-mentioned goals are contradictory to each other, a trade-off must be achieved between the two.

Thus, the objective of our scheme is to minimize the number of PU subcarriers that will be affected by the increased interference during transmission mode switching and at the same time satisfying the required capacity of the SUs, subjected to noise constraints of the PU. It can be realized by considering the number of additional subcarriers used by each SU for underlay transmission and deciding on the appropriate transmission power for the SU considering the likelihood of the re-appearance of the PU.

3.2.2.1 Elastic Bandwidth Allocation Scheme (EBAS)

In this section, we present the low-complexity Elastic Bandwidth Allocation Scheme.

During opportunistic spectrum access, SUs access the spectrum gaps through the use of OFDM subcarriers via the overlay mode in the vacant subcarriers. Furthermore, SUs can access additional subcarriers on each side of their occupied bandwidth via spectrum underlay to improve their capacity. This is performed depending on QoS requirements and is subjected to noise and power constraint. An example of the system is illustrated in Figure 24 for SU_1 .

In our work, we assumed that the SUs are categorized into 3 priorities c_1 , c_2 and c_3 , where c_1 is the highest priority. According to the priority of the SUs, the EBAS scheme restricts the total number of additional subcarriers that these SUs can access via the hybrid or underlay transmission mode in order to provide a differentiated quality of service. This is illustrated in Table 3. Furthermore, SUs with a higher priority have a higher requirement of a minimum transmission rate compared to SUs with a lower priority.

Table 3: QoS Requirements for SUs with different priorities

Priority	Number of underlay subcarriers (s) accessible through hybrid mode	Required Capacity (Mbps)
c_1	4	18
c_2	2	12
c_3	0	6

The basic idea of the EBAS scheme is to allocate less power to overlay subcarriers that has a higher probability of returning PU in order to minimize the interference caused to the returning PU. At the same time, the scheme allocates a number of additional underlay subcarriers to the SUs according to their priority. We assume that an equally low power is assigned to all underlay subcarriers, and that the power allocated to the overlay subcarriers can never be less than that allocated to the underlay subcarriers. An example power profile is shown in Figure 26 for different probability of returning PU, Φ_j for SUs with different priority.

Figure 26: Power profile for priority c_1 SUs with different Φ_j

3.2.2.2 Softened Peak Interference Power Constraint

During the re-appearance of the PU, there will be a number of subcarriers that may experience temporary elevated levels of interference due to the high transmission power from the SU. In most existing proposed schemes, both the PIP and AIP constraint have to be met in order to protect the PS transmissions. However, an investigation in [92] has shown that the average interference power constraint is superior over the peak interference power constraint in terms of various forms of capacity limits achievable for the primary radio fading channel.

In our proposal, we make use of this result by relaxing the PIP constraint by

allowing a limited number of individual PU subcarriers to be temporarily affected by elevated of interference as long as the AIP across the PU subcarriers is still below a certain threshold. The result means that the PIP constraint can be somewhat relaxed in most cases to achieve better performance for the SS, without adversely affecting the transmissions from the PS. Thus, the primary goal of the scheme should be to satisfy the QoS requirement of the SUs, subjected to transmission power constraint and AIP constraint and lastly an acceptable limit in the number of PU subcarriers affected by the elevated levels of interference due to the high transmission power from the SU.

Despite the relaxation of the PIP constraint, there is still a need to make sure that most of the primary radio subcarriers are protected from the noise generated by the SU. Hence, we define the softened PIP constraint (s-PIP) as

$$\sum_{n \in K_j} s_j^n \leq L, \forall j \in M \quad (7)$$

where the auxiliary binary variables $\{s_j^n \in \{0,1\}\}_{j \in N}^{n \in K_j}$ are introduced, one per PU and subcarrier, and L denotes the acceptable number of PU subcarriers per PU that are affected by the temporary elevated levels of interference due to the high transmission power from the SU.

Each binary variable s_j^n represents the following question: Can the PIP constraint for subcarrier n of PU_j be met? We'll let $s_j^n = 1$ when the answer is “no” and $s_j^n = 0$ otherwise. Thus, L is a parameter that can be used to decide on the “tolerable limit” on the part of the PU.

3.2.2.3 Detailed Algorithm Description

The EBAS scheme heuristically allocates less power to the overlay carriers with a higher chance of returning PU, Φ_j . At the same time, the scheme also allocates a

number of additional underlay subcarriers to the SUs according to their priority. We assume that low power is equally assigned to all underlay subcarriers, and that the power allocated to the overlay subcarriers can never be less than that of the underlay subcarriers. We also only consider the effect only on the PU band where it causes the most amount of interference, i.e., the PU band to which it is closest.

The scheme first determines the total number of underlay subcarriers u_j for each SUs, depending on their priority, and also the total number of overlay subcarriers o_j . To work out the power profile for the subcarriers, we first consider two extreme cases.

For a Φ_j of 0, the scheme allocates all power to overlay subcarriers since it means that the PU will never reoccupy these subcarriers. Thus each individual overlay subcarrier will be allocated $\frac{1}{o_j}$ of the power budget.

For a Φ_j of 1, the scheme allocates power evenly across all underlay and overlay subcarriers since it means that the PU will definitely reoccupy the overlay subcarriers, and that the power allocated to overlay subcarriers can never be less than that of the underlay subcarriers. Thus each individual overlay subcarrier will be allocated $\frac{1}{o_j + u_j}$ of the power budget.

In general, for a Φ_j of between 0 and 1, the power profile for the overlay subcarriers can be expressed as

$$P_j^{overlay}(l) = \frac{P_{req}}{o_j} (1 - \Phi_j) + \frac{P_{req} \Phi_j}{o_j + u_j}, \forall l \in L_j \quad (8)$$

Correspondingly, the power profile for the underlay subcarriers can be expressed as $P_j^{underlay}(k) = \frac{P_{req} \Phi_j}{o_j + u_j}, \forall k \in (K_j \cup K_{j+1}) \cap L_j$ (9)

The value of P_{req} is determined in conjunction with the required capacity (Eq.6)

such that both total power budget (Eq.1) and interference constraint can be met at the same time (Eq.5 and 7).

Algorithm: EBAS Power Allocation

Begin

- 1) For each SU_j , determine priority c_j , number of currently vacant overlay subcarriers o_j , number of underlay subcarriers u_j allowed and corresponding required capacity from Table 3.
- 2) Calculate required transmission power P_j according to eq.6.
- 3) Determine the final transmission power P_{req} by choosing the lowest of the three power threshold calculated, required transmission power P_j , power budget P_{max} (eq. 1) and interference constraint according to AIP and s-PIP (eq. 5 and eq. 7)
- 4) Calculate the power profile for overlay subcarriers using e.q 8
- 5) Calculate the power profile for underlay subcarriers using e.q 9

End

3.2.3 Numerical Results

We evaluate the effectiveness of the proposed scheme by performing computer simulations using MATLAB. We compare the performance of our proposed EBAS scheme versus both the overlay only scheme and the underlay only scheme.

3.2.3.1 Simulation Setup

A total of 50,001 rounds of simulations have been performed to obtain the results presented in this section. In all simulations, the values of M , T_s and Δf are assumed to be 12, $4\mu s$ and 0.3125 MHz, respectively. The value of σ^2 is assumed to be 10^{-6} . Both the channel gain g^n and h^i are assumed to be Rayleigh fading with an average channel power gain of -9.5 dB. The total power budget is 0.001W. I_{max}^n and I_{max} are chosen to be 1.5×10^{-5} W and 1×10^{-5} W, respectively. L is chosen to be 1. We define the primary user activity in the network by Φ_j , which is the probability that PU_j will return in the current time frame.

For the overlay scheme, the SUs are allowed to make use of the vacant subcarriers for transmissions, but if the subcarriers are subsequently repossessed by the PUs, the

SUs affected will have to vacate the affected subcarriers. As a result, the available bandwidth available to the affected SUs will be reduced. In the event that there are no subcarriers available to any SUs, they will not be able to transmit at all.

For the underlay scheme, the SUs can transmit simultaneously in the same subcarriers that are in use by the PUs, with the condition that the peak and the average interference power experienced by the PUs are not exceeded. Furthermore, each SU is allowed to access a maximum of 6 subcarriers in the underlay scheme.

3.2.3.2 Simulation Results

In Figure 27, we plot the average capacity of the different schemes vs. Φ , where Φ varies from 0.0 to 1.0. We can see that as Φ increases, the capacity of the various schemes decreases. However, the capacity provided by the underlay paradigm is not affected by Φ since the basis for underlay transmission allows for simultaneous transmissions by both PUs and SUs. On the other hand, due to the conservative nature of the underlay transmission mode, the capacity provided is the lowest as it is unable to take advantage of the vacant subcarriers. EBAS is able to provide a much higher throughput using a hybrid approach of both overlay and underlay transmission mode together with an s-PIP constraint.

Figure 27: Average capacity of the different schemes vs. Φ

Figure 28 shows the average capacity for SUs with different priority under the EBAS scheme. As expected, SUs with a higher priority receives a much higher capacity due to the higher transmission power and larger number of underlay subcarriers. Even in the extreme case where $\Phi = 1$, EBAS is able to provide better service to higher priority SUs.

In Figure 29, we plot the number of PUs which experienced noise higher than the average interference power constraint vs. Φ , where Φ varies from 0.0 to 1.0. Since the transmission power in the underlay paradigm is the most conservative among the different schemes, the number of PUs affected by the increased noise is effectively zero regardless of Φ . The overlay transmission scheme has the highest number of PUs affected by the elevated noise. This is because the entire power budget was loaded into overlay subcarriers that provide the most capacity. However, this was done without considering the fact that PUs may return at any time. Our proposed scheme is able to restrict to a reasonably low number of PUs that are affected by noise by making use of the combined approach of overlay and underlay transmission mode and also by making use of additional subcarriers to spread out the transmission power.

Figure 28: Average capacity of SUs under EBAS with different priority vs. Φ

Figure 29: No. of PUs affected by noise vs. Φ

We also investigate the effect of increasing L , the acceptable number of PU subcarriers that are affected by the temporary elevated levels of interference due to the high transmission power from the SU, on the performance of the EBAS scheme. Figure 30 shows the average capacity of the EBAS scheme vs. Φ under the EBAS scheme where Φ varies from 0.0 to 1.0 and L from 1 to 3. It can be seen that increasing L improves the performance of the EBAS scheme due to the interference diversity phenomenon [92]. On average, increasing L by 1 improves the average capacity of the scheme by about 2.5%.

Figure 30: Average Capacity of EBAS scheme vs. Φ using different values of L

Figure 31 shows the number of PUs which experienced noise higher than the average interference power constraint vs. Φ , where Φ varies from 0.0 to 1.0, and for values of L from 1 to 3. As expected, increasing L causes the number of PUs to be affected by the increased noise to be increased as well, especially when Φ is above 0.3. Thus, there is a trade-off in terms of the total capacity, vs. levels of PU protection. However, when Φ is below 0.3, increasing L is a good way to improve capacity without introducing excessive interferences to the PUs.

Figure 31: No. of PUs affected by noise vs. Φ

3.2.4 Conclusion

In this section, we have proposed an elastic bandwidth allocation scheme with a softened peak interference power constraint for the dynamic cognitive radio systems.

Our scheme is able to combine the strength of both overlay and underlay transmission mode and provide superior performance through the use of the softened peak interference power constraint. In a cognitive radio system with dynamic PU activity, the EBAS scheme is able to provide a much higher capacity compared to an overlay or underlay only approach. EBAS is also able to provide a differentiated service to SUs with different priority and to sustain the service differentiation in the presence of primary user activity. The performance of the EBAS scheme can also be improved by relaxing the s-PIP constraint especially when the probability of returning PU is low.

Chapter 4: Network Layer Solutions for QoS Provisioning

In this chapter, we will present two network layer routing solutions for QoS provisioning. We will first present the Dynamic Virtual Carrier Sensing and Interference Aware Routing Protocol in section 4.1. Then we will present the Opportunistic Service Differentiation Routing Protocol for the dynamic CRNs in section 4.2.

4.1 Dynamic Virtual Carrier Sensing and Interference Aware Routing Protocol

As mentioned in Chapter 1 and 2, ad-hoc routing protocols are primarily designed for low-end MANETs and are inefficient for the WMN scenario. At the same time, the virtual carrier sensing mechanism which is commonly used to mitigate the hidden terminal problem in the IEEE 802.11 MAC further aggravates the exposed terminal problem.

Specifically, the design goals of the Dynamic Virtual Carrier Sensing and Interference Aware Routing Protocol (DVCSIR) routing protocol is to tackle the above two issues. Firstly, developing a new routing metric to provide better performance, in terms of higher throughput and lower delay compared to existing MANET protocol like the DSR protocol. Secondly, we developed the dynamic virtual carrier sensing in order to mitigate the weakness of the original IEEE 802.11 virtual carrier sensing mechanism.

We design a novel metric, Quietness Index (QI) to quantify the potential interference experienced by a node in the WMN. DVCSIR then makes use of the QI

to find the least interference route from source to destination. Although not as sophisticated as our next work as detailed in Section 4.2, the main purpose of the DVCSIR is to demonstrate that the lowest cost path from source to destination in a radio network is not necessarily a shortest hop one. Furthermore, DVCSIR underscores the importance of selecting a stable path in which communications between two end points can be reliably conducted without the problem of path breakages. This is especially important in cognitive radio networks where link breakages can occur suddenly due to a sudden appearance of a primary user. This design principle is also similarly applied to our next work in section 4.2. Secondly, we introduce the Dynamic Virtual Carrier Sensing mechanism, where the virtual carrier sensing is performed on a node by node basis, depending on the node density. This allows the virtual carrier sensing mechanism to be applied only in parts of the network where collision is the likeliest to happen.

The rest of this section is organised as follows. We first describe route discovery and maintenance mechanism of DVCSIR in section 4.1.1. We then introduce in section 4.1.2, the definition of Quietness Index (QI) and the formula to calculate the QI of the nodes in a wireless mesh network. Section 4.1.3 describes the dynamic virtual sensing algorithm. Section 4.1.4 will elaborate on how DVCSIR makes use of the QI to select routes that can provide better QoS support in WMNs. The simulation model and present the simulation results using OPNET Modeler in section 4.1.5. We conclude our work in section 4.1.6

4.1.1 Route Discover and Maintenance in DVCSIR

The DVCSIR is a source routing algorithm that is based on a well-known ad-hoc routing protocol, DSR. Like DSR, DVCSIR has two main functions, “Route

Discovery" and "Route Maintenance". These functions allow nodes to discover and maintain routes to arbitrary destinations in the wireless mesh network.

4.1.1.1 Route Discovery and Maintenance

The DVCSIR protocol implements the complete set of route discovery mechanisms which is similar to DSR. It comprises of broadcasting route requests to find a route and receiving route replies with a specific route to the destination. However, there are also some differences compared to DSR. The route discovery packet was modified to include an additional "cost" field. In the Route Request phase, this packet is flooded throughout the network. Each node, upon receiving a Route Request packet, rebroadcasts the packet to its neighbours if it has not forwarded already or if the node is not the destination node. When the destination node receives it, a Route Reply packet would be generated. The reply will be send to the source node through the reverse path the Route Request packet had traversed. Also, at each node, the cost field is updated to reflect the Path Quietness Index (PQI). When the Route Reply packet is received by the source node, the PQI information within will be used to update the route cache. The routes are stored in route caches on the nodes and they are checked for a valid route before initiating route discovery. The protocol allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets.

4.1.2 Quietness Index (QI)

The Quietness Index (QI) is an important metric used in the operation of DVCSIR. For any wireless mesh topology consisting of N nodes, each node counts the nodal degrees d_i or the number of neighbours which is 1 or 0 hops away (inclusive of itself). The system then takes the maximum of all the individual nodal degrees and assigned

it as D . This information is then disseminated to all the nodes. Also, for each time period, each node monitors and keeps a count of the number of transmitting neighbours, T_i . To calculate the QI for node i , we can use the formula below.

N = Number of nodes in the system

d_i = Nodal degree for node i

$$D = \text{Max}_{1 \leq i \leq N}(d_i)$$

T_i = Number of transmitting neighbours in the last time period

$$\text{Quietness Index (QI}_i) = \frac{D - T_i}{D + d_i}$$

In a dynamic mesh network where there can be node movement, nodal degree information is exchanged periodically between the nodes for calculating the QI. For a stationary mesh network, i.e., there is no node movement, D and d_i will remain constant and thus only need to be calculated once at the start of the simulation. That means that the QI can simply be calculated by monitoring the number of transmitting neighbours for each individual node. Based on the definition of the QI, when there are more transmitting neighbours, the QI for a node will decrease. Conversely, when the number of transmitting neighbours decreases, the QI will increase. Also, the QI for a node with more neighbours is lower than a node with fewer neighbours given the same number of transmitting neighbours. This property of QI allows it to represent the existing interference experienced by a node due to its transmitting neighbours, and also the possible interference generated by its non-transmitting neighbours.

4.1.3 Dynamic Virtual Carrier Sensing

In a wireless network with many hidden nodes, performing virtual carrier sensing via RTS/CTS handshaking can provide better overall network performance as the

effects of network collisions can be minimized [30]. However, in a wireless network where there are less hidden nodes and more exposed nodes, this benefit can be reduced or even reversed due to the reduction of channel spatial reuse efficiency. Normally, the virtual carrier sensing mechanism is performed based on a pre-set packet length threshold L . E.g., when a packet is about to be sent, if the size of the packet is greater than L bytes, then RTS/CTS handshaking is needed. This approach does not take into consideration of the node's location in the topology.

In our research, in addition to the packet size, we determine on a node by node basis, whether virtual carrier sensing will be performed based on a globally set QI Threshold, V . The operation of the dynamic virtual carrier sensing is as follow:

Let V denote the globally set parameter QI Threshold.

- 1) If $QI_i < V$, turn on RTS/CTS
- 2) If $QI_i \geq V$, turn off RTS/CTS

For the experiments that we have conducted, we vary V from 0.0 to 1.0. As network topologies and traffic conditions vary widely, the optimum value of V can be discovered via simulations. As a rule, the value for V indicates how high a collision level can be tolerated before virtual carrier sensing is enabled. Setting V to 0 has the same effect as turning off RTS/CTS handshaking for the whole network while setting V to 1 has the same effect as turning on RTS/CTS for the whole network. There are 2 advantages in using the QI as criteria to enable the virtual carrier sensing. Firstly, a low QI generally means that a node has more transmitting neighbours. In this case, it is desirable to turn on virtual carrier sensing so as not to cause interference to nearby nodes. Secondly, a low QI can also mean that a node has more neighbours but only a few is transmitting. However, having more neighbours can also means a higher likelihood of network transmission activity in the vicinity. In this case, by enabling

the virtual carrier sensing, network collision can be pre-empted.

4.1.4 Interference Aware Routing

In DVCSIR, the metric for consideration is the number of hops taken and the QI. Based on the definition of QI made in the earlier section, we define the Path Quietness Index as the multiplication of the QI of all the nodes along the path from source to destination.

Definition:

P = set of nodes on the path between source and destination.

QI_n = Quietness Index of node n on the path between source and destination.

$$\text{Path Quietness Index (PQI)} = \prod_{n \in P} QI_n$$

The PQI will be used as the path selection criteria in DVCSIR. For multiple paths to the same destination, the path with the highest PQI value will be selected. There are two advantages to doing this. Firstly, this ensures that the interference experienced by the path chosen is minimized. Secondly, a path with too many intermediate nodes will have a low PQI value, and thus will not be selected.

4.1.5 Simulation Model and Result

4.1.5.1 Simulation Model

The simulation was conducted using OPNET Modeler. We simulate a wireless mesh network using the parameters as indicated in Table 4. We compare the performance between DVCSIR and DSR since they are both source routing protocol. We also compare the performance of DVCSIR with different values of V .

Parameters	Values
Simulation Area	3000m x 3000m
Number of Nodes	100
Node Placement	Grid, inter node distance of 275m
Movement	Stationary
Transmitting Range	350m
Data Rate	11mbps
Traffic	Constant Bit Rate (CBR) 1 Packets/Sec for 30 minutes
Packet Size	1024 bytes

Table 4: Simulation Parameters

4.1.5.2 Simulation Results

From Figure 32, we can see that the throughput for the DVCSIR with V of 0.5 is the highest, followed by DSR without RTS/CTS and DSR with RTS/CTS. The reasons for the better performance for DVCSIR are twofold. Firstly, DVCSIR enables virtual carrier sensing at part of the wireless mesh network with higher chance of the hidden node problem, therefore reducing the impact of collision. Secondly, DVCSIR disables virtual carrier sensing at part of the wireless mesh network with higher chance of the exposed node problem. Finally, the route chosen by DVCSIR suffers from less interference as compared to DSR as it avoids nodes with more transmitting neighbours (E.g., higher chance of interference)

Figure 32: WLAN throughput comparison between DVCSIR and DSR

From Figure 33, we can see that DVCSIR has a slightly higher delay compared to DSR without RTS/CTS. This was due to some overheads incurred with the packet exchanges required for virtual carrier sensing in parts of the network for DVCSIR. However, this is just a small trade-off compared to the improvement in throughput as shown in Figure 32.

Figure 33: WLAN delay comparison between DVCSIR and DSR

In Figure 34, we compare the performance of DVCSIR with different settings of V . We can see that setting V to 0.5 provides the best performance in terms of

throughput.

Figure 34: WLAN throughput comparison under DVCSIR with different values of V

4.1.6 Conclusion

We design and evaluate the performance of DVCSIR. The simulation results indicated that DVCSIR has superior performance compared to DSR due to its dynamic virtual carrier sensing mechanism, and interference aware path routing. DVCSIR is able to provide a significant increase in terms of throughput at only a slight increase in delay. We also evaluated the performance of DVCSIR with different settings of V . We conclude that setting V to 0.5 is the optimum setting for CBR traffic for the grid topology. For other topologies and traffic load, we recommend that further simulations be conducted to find out the optimal value of V since it is likely to be different as compared to the case of a grid topology.

4.2 Opportunistic Service Differentiation Routing Protocol for the Dynamic CRNs

As mentioned in Chapter 2, many existing proposals for CRNs [79-81, 110-112] have assumed a static CRN that considers an available frequency band as a permanent resource indefinitely available during its activity. However, such assumptions are no longer valid in the context of the CRN. Some other proposed solutions [85-87, 113] also do not consider the issue of QoS provisioning in CRNs.

In this section, we propose a design and implementation of a cross-layer Opportunistic Service Differentiation Routing protocol (OSDRP) for the dynamic CRNs where the primary band can be exploited by a cognitive user while its intermittent availability can seriously affect the service offered for a CRN. The key idea of our scheme is that the availability of SOP across the different PRNs which made up the CRN must be considered in the route selection to achieve an efficient end-to-end performance.

In addition to the availability of SOP, we have also recognized that the broadcast nature of the wireless medium can have a detrimental effect on the performance of the CRNs. Our scheme turns this disadvantage into an advantage by leveraging on Opportunistic Routing (OR) [114] concept to improve the performance of CRNs. The idea behind OR takes the advantage of the broadcast nature of the wireless medium. When a node transmits, a number of nearby nodes can hear the transmission. A node can then be selected out of the several candidate forwarding nodes (CFNs) to transmit the received packet. This helps to cut down on unnecessary forwarding by intermediary nodes. The reduction in the number of transmissions needed to reach a destination helps to reduce energy consumption and improves the performance over the traditional unicast routing [82, 115].

Different from the existing cognitive routing protocols, OSDRP includes two significant new innovations, which are critical to ensure that it can perform well. They include

(1) A multi-metric route selection algorithm, which considers the availability of frequency band in addition to traditional metric like switching delay and queuing delay.

(2) A Combined Opportunistic Routing (OR) [114] with Transmit Power Control (TPC) schemes, which simplifies the selection of CFNs, improving the delivery ratios of CFNs and achieving service differentiation to traffic flows with different priorities.

We show that the proposed OSDRP scheme can significantly outperform other cognitive routing protocols through extensive simulations.

The rest of the section is organized as follows. The system model is described in Section 4.2.1. The detail operations of the OSDRP are presented in Section 4.2.2. We evaluate the performance of OSDRP by simulation experiments in Section 4.2.3. Finally, we conclude the section in Section 4.2.4.

4.2.1 System Model

4.2.1.1 Physical and MAC layer Modelling

In this work, we consider a dynamic multi-hop CRN consisting of N nodes with M end-to-end traffic flows. Each node has one CR transceiver. The CR transceiver allows each node to communicate with its neighbouring nodes by selecting an overlapping data channel in their respective SOPs. As nodes communicate using dynamic frequency channels in a CRN, it can lead to the “deafness problem” where two nodes are unable to communicate with each other if they are on different frequency channels. This causes difficulties when nodes in the CRN need to collect

global information about the network, or to exchange control information about the spectrum status and routing specific data.

To facilitate the exchange of control information, many protocols assume either a dedicated control channel with reserved frequencies within the licensed band, or the explicit use of the unlicensed band for the information exchange. These messages exchanges over the common control channel may be related to the (i) channel access and contention, (ii) neighbour discovery, and (iii) spectrum management [116].

One of the concerns for using the common control channel is that it might lead to a bottleneck situation for proposed protocols. In our research work on cognitive MAC protocols, we have debated about the pros and cons of using various approaches to exchange control messages among nodes which could possibly operate in several distinct channels. A distributed solution, by which different control channels are used for different groups of nodes were considered at first. However, this approach incurred additional overheads in order to establish and maintain those groups. There will also be overheads involved to share control information among different groups of nodes.

We have also considered an approach where we have not dedicated any channel for control and link establishment. Instead we allow all channels to be shared by control and data traffic. However, this approach requires the cognitive radio to scan all the available channels in some random or pre-established order until it is able to establish one or more links. It has the advantage to make the system more robust, but the handshakes are required for channel rendezvous. And channel allocation is even more complicated compared to the above approach..

Basically, we have found that there is a trade-off involved in the use of a control channel. And it is between the simplicity of design and the overheads incurred in

channel rendezvous. Furthermore, a recent survey [116] has indicated that most of the existing cognitive MAC protocols are using a common control channel. In addition, a recent development may be able to resolve the bottleneck issue of using a common control channel. The authors of [117] have designed a novel scheme to support an always-on common control channel that uses non-contiguous OFDM subcarriers placed within the guard bands separating the channels of the licensed spectrum. It has potential to greatly improve the bottleneck issue that plagues the use of the common control channel.

Therefore, in our scheme, we adopt the use of a common control channel to ensure that routing messages can be received by nodes despite of the discrepancy between their frequency bands. This is done by equipping each node with a conventional wireless interface to form a common control channel among the nodes.

Lastly, our scheme requires a MAC-Layer QoS Provisioning Protocol (MQPP) scheme [118] scheme or a similar one to be implemented at the MAC layer. It is necessary for the provisioning of differentiated QoS through the use of adaptive modulation and coding technique. For ease of simulation and explanation, we assume that there are 12 non-overlapping wireless channels specified by the physical layer of the IEEE 802.11a standard. Each of the channels has a bandwidth of 20 MHz with a maximum capacity of 54 Mbps. We also assume that channel 1 is utilized as the common control channel while the remaining 11 channels are available for data communication. The channel switching time is assumed to be t_d ms.

4.2.1.2 SOP Modelling

We assume an interweave model [88], i.e., the nodes in the CRN can only transmit when the primary users are not active. Thus, there is virtually no interference to the

primary users and there is no restriction on the power level of the secondary users. We also assume that the set of SOP is the same for every node in the same PRN. The availability of the primary band for transmissions by cognitive users is at the best intermittent.

In our work, we have not made any assumption on the underlying operation of the primary network, except that the occupation of channels can be described using two states, Busy and Idle. For ease of simulation and explanation, we have also assumed that the mean time spent in both the Idle and Busy states are same, and that it follows an exponential distribution. The assumption that both the Busy and Idle time periods follow the same distribution will not have much effect on our algorithm since we only consider idle channels as candidates for routing.

Thus, our SOP model must incorporate two separate components: 1) The states of the channel and their transition behaviour 2) The length of the period the system resides in each of the states. These prerequisites enable us to apply a two-state semi-Markov model (Figure 35) as a framework for a single channel. The two-state semi-Markov model combines the simplicity of a two-state model with flexibility to describe the state holding time in each state with arbitrary distribution. The two-state semi-Markov model has been popular in different areas of wireless communications research. It has been applied to describe the spectrum use in WLAN systems [3, 119] and it is also referred to as an alternating renewal process.

In order to fully describe a single channel, we have to determine realistic state holding time distributions. In the literature, the exponential [120] and geometric distribution [121] have been proposed. Using the two-state semi-Markov model, we model the availability of the intermittent channel by defining the probability p of the primary user transmitting in the next time period (channel unavailable for secondary

transmission). The probability of the primary user not transmitting in the next time period (channel available for secondary transmission) is thus $1-p$. We also define the mean duration of the channel spent in either status as the exponential distribution with mean τ .

Figure 35: Two-State Semi-Markov Modelling of SOP

Thus, the channel state will alternate between the periods of availability and unavailability according to p and τ as shown in Figure 35. We assume that the parameters p and τ are available for all nodes in their decision making. It is a reasonable assumption as there are existing schemes that allow nodes to monitor and utilize past channel histories to make predictions on future spectrum availability. For each available channel, we keep track of the elapsed time τ_{avail} that the channel has remained available. Each time when the channel state changes from unavailable to available; we set τ_{avail} to zero. Thus the expected available transmission time is defined as $EATT = (1-p)\tau/p - \tau_{avail}$.

For any two neighbouring nodes i, j to communicate, there must be at least one overlapping channel f among their respective SOPs. If there is more than one overlapping channel, the channel with the greatest $EATT$ will be selected. That is, choose $\text{Max} (EATT(i,j,f))$ where $f \in (SOP_i \cap SOP_j)$, $SOP_i \subseteq F$ and $SOP_j \subseteq F$, where F is the set of all channels in the primary band. SOP_i and SOP_j are the sets of Spectrum

Opportunities at node i and j , respectively. To evaluate the stability of a path, we also define the minimum expected available transmission time ($MEATT$) of a route as the minimum of the expected available transmission time for all nodes on the selected route. Thus $MEATT = \min_{1 \leq (i,j) \leq h} (EATT(i, j, f))$, where i and j are the nodes on the selected route and h is the number of hops.

4.2.2 Proposed Scheme

The challenging issue of QoS provisioning in dynamic CRNs has motivated us to design an on-demand source routing protocol for the dynamic CRNs, the OSDRP. The objectives of the OSDRP are to select the minimum delay - maximum stability route for an end-to-end traffic flow and to provide differentiated service to different traffic priorities. We define an end-to-end traffic flow by the following parameters, (1) flow duration τ_{flow} and (2) flow priority C_f .

In this section, we first present an overview of the Opportunistic Service Differentiation Routing Protocol (OSDRP) for the dynamic CRNs. We describe the modules in OSDRP and how they work with one another to achieve the objectives as above. Finally, we present the detailed algorithm for each of the functions within each module.

4.2.2.1 Overview

The OSDRP consists of 4 modules as shown in Figure 36. They are Route Discovery, Route Decision, Opportunistic Routing with Transmit Power Control (ORTPC) and Route Maintenance. Each of the modules is in turn consists of several functions.

The function of the Route Discovery module is to discover all possible paths

between a source node and a destination node. Once this is done, the list of paths is sorted according to delay and forms as an input to the next module, the Route Decision module. The Route Decision module will examine the list and choose the path that can satisfy the required flow duration of the considered end-to-end traffic flow. Next, the ORTPC module adjusts the transmission power and selects the CFNs according to the flow priority to achieve service differentiation with different traffic priorities. Finally, the Route Maintenance module is responsible for removing invalid or stale entries from the route cache. It is necessary so that the information in the route cache will be kept real-time and reduces the possibility of an undeliverable packet.

Figure 36: OSDRP Flow Diagram

4.2.2.2 Detailed Algorithm Description

Route Discovery

Before the start of the data transmission, the route cache will be examined to see if there is a valid route to the desired destination. If a valid route cannot be found in the

cache, route discovery will be triggered.

OSDRP performs path discovery by implementing the complete set of route discovery mechanisms similar to DSR. By sending out “Route Request” or RREQ packets, nodes can discover the routes with less delay to arbitrary destinations in the CRN. OSDRP allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets.

When the destination node receives the RREQ packet, a Route Reply or RREP packet would be generated with a copy of the accumulated route record from the RREQ packet. The RREP packet will be sent to the source node through the reverse path the RREQ packet had traversed. The route information, delay and *MEATT* information within the RREP packet will be used to update the route cache at the sender.

Algorithm 1: Initiate Route Discovery

```
Begin
  if (no valid route found on cache) then
    1. Create RREQ packet;
    2. Initialize route record in RREQ packet to empty, initialize delay to 0, initialize MEATT to 0;
    3. Broadcast RREQ packet on common control channel.
  else
    Perform Route Decision.
  endif
End
```

Route Decision

Once the routes with less delay have been discovered, OSDRP selects the minimum delay - maximum stability route to fulfil the required flow duration τ_{flow} of the traffic flow. Only the route with $MEATT \geq \tau_{flow}$ will be considered. This ensures that the SOP along the selected route is available during the transmission of the data in order to avoid costly route re-discovery. That is, for the entire duration τ_{flow} of the flow, the nodes along the selected path will not need to stop transmission due to the

sudden appearance of a primary user.

Algorithm 2: Propagate RREQ and Route Reply

```

Begin
  if (receive RREQ packet) then
    1. Determine if its address is on the list of route record;
    2. if (it is on the list of route record) then
      Discard RREQ packet.
    3. else
      1. Append own address and frequency channel to route record in RREQ packet;
      2. Set switching delay  $d_{switch} = t_d$  ms if the receiving frequency is fixed to the same channel as
         the previous hop node's transmitting frequency. Otherwise, the switching delay is set to
          $d_{switch} = 0$ ms;
      3. Add  $d_{switch}$  to the delay field;
      4. Add average queuing delay to the delay field where  $d_{queue} = \sum_n t_{nsend} - t_{nreceive} / n$ ,
         where  $t_{nsend}$  and  $t_{nreceive}$  are the send and receive time of the previous  $n$  packets;
      5. Update MEATT field.
      6. if (receiving node is destination) then
        1. Creates RREP packet;
        2. Send RREP packet.
      7. else
        Rebroadcasts the RREQ packet on the common control channel.
      endif
    endif
  endif
End

```

Algorithm 3: Route Decision

```

Begin
  1. Identify routes with  $MEATT > \tau_{flow}$ ;
  2. Sort route in ascending order of delay;
  3. Choose minimum delay route.
End

```

ORTPC

Once a route has been selected, ORTPC is performed during the transmission to provide a differentiated service according to traffic priority C_f . Different from existing OR techniques, OSDRP determines the CFNs from the remaining hops along the selected route according to traffic priority. Due to the implementation of the MAC-Layer QoS Provisioning Protocol (MQPP) scheme [118], higher priority packets will likely require a higher transmission power as compared to lower priority packets. Therefore, the high priority packet has a correspondingly higher chance of being

received at a further away node as compared to the lower priority packets. OSDRP utilizes this fact to vary the range of the CFNs selection. Thus, higher priority traffic will have a higher OR Candidate Selection Range compared to lower priority traffic. Figure 37 shows an example for node 1 where the OR Candidate Selection Range for priority c_1 , c_2 and c_3 traffic is 3, 2 and 1, respectively.

Figure 37: Differentiated OR Candidate Selection Range

When multiple nodes overhear a transmission, we want to ensure that only the node nearest to the destination will forward it. The best forwarding node should be selected in a cheap and distributed way. To achieve this, we implement the prioritized acknowledgement scheme proposed by [114]. Once the packets have been successfully received, candidate nodes acknowledge the successful reception of a packet in a prioritized manner according to the sequence indicated in the packet, i.e. a candidate node with higher priority sends its acknowledgement before any lower priority candidates. In Figure 37, node 4 will send its acknowledgement before node 3, and node 3 will send its acknowledgement before node 2. Among all nodes of a candidate set that successfully received a packet, the node with the highest priority will forward the packet. Once the forwarding node has been selected, it will send an Acknowledgement packet back to the sender. All other candidates that hear this Acknowledgement packet will forward it back to the sender. At the same time, they will also discard the received data packet from their queues.

Our CFN selection strategy has three benefits compared to the existing OR protocols. Firstly, the selection of CFNs is much simpler as only the nodes further along the selected path will be considered. Secondly, candidate nodes are range limited according to traffic priority resulting in the service differentiation provided. Finally, duplicate transmissions will be minimized as nodes will not be selected on possibly diverging paths.

Algorithm 4: Transmit Power Control and Opportunistic Routing

```

Begin
  switch (priority)
    case 'c1':
      1. minimum required data rate  $r_t = 24\text{Mbps}$ ;
      2. OR Candidate Selection Range = 3.
    case 'c2':
      1. minimum required data rate  $r_t = 12\text{Mbps}$ ;
      2. OR Candidate Selection Range = 2.
    case 'c3':
      1. minimum required data rate  $r_t = 6\text{Mbps}$ ;
      2. OR Candidate Selection Range = 1.
  endswitch
  1. Determine corresponding SINR threshold  $\gamma_t$  for  $\text{BER} \leq 10^{-5}$ ;
  2. Calculate required transmitter power  $P_i$  using  $\text{SINR}_{ij} = (P_i G_{ij} / (N_0 + \text{Noise})) \geq \gamma_t$  where  $G_{ij}$  denotes
     
$$i, j = 1, 2, \dots, N, i \neq j$$

     the link gain from node  $n_i$  to node  $n_j$ ,  $N_0$  denotes thermal noise of node  $n_j$ ;  $\text{Noise}$  is the measured
     noise due to other sources at the  $n_j$ 
  3. Based on OR Candidate Selection Range, examine remaining number of hops; insert CFNs into
     packet header;
  4. Transmit packet.
End

```

Route Maintenance

Route maintenance is performed periodically (once every second). By expiring stale entries from the route cache, route maintenance keeps the size of the route cache manageable and ensures that the route entries are current.

Algorithm 5: Route Maintenance

```

Begin
  for every 1 second
    if (route is valid) then
      1. Reduce  $MEATT$  by 1;
      2. If  $MEATT = 0$ , delete route entry from the cache.
    endif
  endfor
End

```

4.2.2.3 Complexity Analysis

The complexity analysis for OSDRP is similar to that on DSR in [122]. For a network consisting of N nodes and diameter d , the time complexity for route initialization is $O(2d)$. Since OSDRP maintains multiple routes to the same destination, the time complexity after a link failure is 0 for a cache hit and $O(2d)$ otherwise. The communication complexities for both initialization and after a link failure are both $O(2N)$.

4.2.3 Performance Evaluation

Simulation experiments have been performed using OPNET Modeler 14.5A with wireless extension to evaluate the performance of the proposed OSDRP scheme.

4.2.3.1 Simulation Setup

The primary design principles behind the OSDRP are to select the shortest delay path through the CRN, ensuring that the path selected are stable during the duration of the traffic flow and providing a distinct service differentiation to different traffic flows in terms of throughput and delay. To show the effectiveness of our scheme, we have compared the performance of our proposal with three other existing routing protocols, DSR protocol which uses traditional shortest-hop approach, the Delay motivated On-demand Routing Protocol (DORP) in [79] and the Spectrum Aware Mesh Routing Protocol (SAMER) in [86] proposed for CRNs with the issue of spectrum availability. We have modified the existing DSR protocol to exchange control information through a common control channel so that it can work in the CRN. The common control channel DSR (ccDSR) will randomly select an available channel for communication if the existing channel becomes unavailable. We have verified the effectiveness of our OSDRP scheme compared to ccDSR, DORP and

SAMER.

In our simulation, we have designed a baseline scenario and three other scenarios that are the variations of the baseline scenario. The network topology of the baseline scenario consists of 24 nodes spanning across 4 PRNs as shown in Figure 38. The nodes are grouped into 4 groups consisting of 6 nodes each. The nodes in each group are randomly scattered within a circular region of radius 500 metres. There are 4 circular regions and the position of the centre of each circle is 800 metres apart from each other. We assume that all nodes are stationary.

Figure 38: Simulated Topology

For ease of explanation without loss of generality, we assume that the probability p of the primary user coming online is the same for all the channels in each PRN. Table 5 lists the parameters indicating the availability of SOPs in each PRN. In our experiments, we vary the probability p between 0.1 – 0.9. For each value of p , we perform the simulation for 51 times, using a different random number seed for each run.

Table 5: Availability of SOPs in PRNs (Baseline)

Primary Networks	SOP Availability, $U(\tau - a, \tau + a)$
PRN1	$a = 5, \tau = 15$
PRN2	$a = 5, \tau = 45$
PRN3	$a = 5, \tau = 10$
PRN4	$a = 5, \tau = 30$

Nine sets of traffic flows with different priorities have been deployed. The traffic

generation is a Poisson process and the mean packet inter-arrival time is exponentially distributed between 10ms to 40ms. The packet size is fixed at 512 bytes. All traffic flows run for 30 seconds and the OR candidate selection range is 3, 2 and 1 for priorities c_1 , c_2 and c_3 , respectively. Other flow properties are defined in Table 6. Receiver sensitivity is -95dBm, basic transmission power is 7dBm and maximum transmission power is 30dBm. Channel switching delay is assumed to be 1ms.

Table 6: Traffic Flow Properties (Baseline)

Name	Priority	Originating PRN	Destination PRN
Flow1_1	c_1	1	4
Flow1_2	c_2	1	4
Flow1_3	c_3	1	4
Flow2_1	c_1	2	4
Flow2_2	c_2	2	4
Flow2_3	c_3	2	4
Flow3_1	c_1	3	4
Flow3_2	c_2	3	4
Flow3_3	c_3	3	4

4.2.3.2 Simulation Results

Baseline Scenario – Varying p

Figure 39 shows the average number of hops for the different traffic priorities for values of p between 0.1 – 0.9. The average number of hops taken by the priority c_1 traffic is lower than those of other flows. This is because the higher transmission power coupled with larger OR candidate selection range for priority c_1 traffic enables it to skip more nodes along the route. The higher transmission power also makes it more likely for the opportunistic routing to succeed.

The result also shows that the average number of hops is relatively constant under different values of p . It means that the “variability” of the SOP does not have any effect on the path length of the route taken by the traffic flows.

Figure 39: Average number of hops vs. p

Figure 40 compares the route taken by Flow1_1 between OSDRP, ccDSR, DORP and SAMER when $p = 0.1$. The number of hops taken by ccDSR, DORP and SAMER is 7 while the number of hops taken by OSDRP is 3. The ORTPC feature of the OSDRP allows the high priority traffic to skip a number of intermediate nodes from source to destination while this is not possible in ccDSR, DORP and SAMER.

Figure 40: Route Comparison between OSDRP, ccDSR, DORP and SAMER for $p = 0.1$

Figure 41 shows the average end-to-end delay for different traffic flows with values of p between 0.1 – 0.9. For the case of OSDRP, the higher priority traffic experiences less delay compared to the lower priority traffic. This is due to the less number of intermediate nodes that the higher priority traffic has to go through in order to reach the destination.

The result also shows that as the values of p increases, the end-to-end delay also increases. This is due to the increased likelihood of the primary user appearing that causes breakage in the end-to-end path. As a result, there is an increased channel switching and route rediscovery overhead. However, the delay for both priority c_1 and c_2 traffic remains below 120ms which is acceptable for most multimedia broadband applications.

Figure 41: Average End-to-end Delay vs. p

Figure 42 shows the total throughput for different schemes with values of p between 0.1 – 0.9. In the graph, we can see that OSDRP and SAMER provide the highest throughput. SAMER is able to perform better than OSDRP for p between 0.1 – 0.6 due to its ability to utilize multiple channels for concurrent transmissions.

However, as p increases beyond 0.65, OSDRP starts to outperform SAMER as OSDRP is able to route traffic through nodes with greater spectrum stability.

Figure 42: Total Throughput vs. p

Dynamic SOP Scenario – Varying τ

To verify the effectiveness of the OSDRP notwithstanding the dynamic nature of the SOP, we have designed a scenario where the route taken by OSDRP, DORP, ccDSR and SAMER initially goes through PRN2. It can be achieved by manipulating the positions of the nodes in PRN2 to be physically closer to the intended destination. We set the average τ for PRN1, PRN3 and PRN4 to 60s and progressively reduced the τ for PRN2 from 45s to 10s in steps of 5s (Table 7). All other parameters remain unchanged.

Table 7: Availability of SOPs in PRNs

Primary Networks	SOP Availability, $U(\tau - a, \tau + a)$
PRN1	$a = 5, \tau = 60$
PRN2	$a = 5, \tau = 10 \text{ to } 45$
PRN3	$a = 5, \tau = 60$
PRN4	$a = 5, \tau = 60$

Figure 43 shows the average end-to-end delay for different traffic flows when p is set to 0.5. As τ decreases, the delays by DORP and ccDSR begin to increase due to

the frequent changes in SOP in PRN2 because both DORP and ccDSR are unable to react to the changes of SOP. Even though SAMER is designed primarily for CRNs, it also performs poorly because SAMER chooses its path via nodes with higher spectrum availability. For example, a node with N vacant channels will be favoured over another node with M vacant channels ($N > M$). However, it has not taken into full consideration of the statistical behaviour of the spectrum usage. As a result, it is unable to react to the changes of τ . The delay experienced by OSDRP is quite constant despite the variation of τ , due to the selection of alternative routes through PRN3 when τ drops below certain level in PRN2.

Figure 43: Average End-to-end Delay vs. τ for $p = 0.5$ (Dynamic SOP Scenario)

Figure 44 shows the total throughput for different schemes when p is set to 0.5. As τ decreases, the throughputs by DORP, ccDSR and SAMER begin to decrease due to the frequent changes of SOP in PRN2. SAMER performs poorly when τ starts to drop below 30s, as it is unable to route traffic through nodes that can support the required traffic flow period of 30s. It further confirms that the duration of the availability of the communication channel needs to be taken into consideration when selecting a path. The throughput of OSDRP is quite constant despite the variation of τ , due to the

selection of alternative routes through PRN3 when τ drops below certain level in PRN2.

Figure 44: Total Throughput vs. τ for $p = 0.5$ (Dynamic SOP Scenario)

Figure 45 shows the routes taken by Flow1_1, Flow1_2 and Flow1_3 by OSDRP when τ is 10. It can be seen that all three traffic flows are routed through PRN3. OSDRP prefers paths through PRN3 where the spectrum is available for a longer period as compared to in PRN2. Even it is not shown here, the paths taken by DSR, DORP and SAMER are still routed through PRN2 which is similar to Figure 40.

Figure 45: Route Comparison among Different Traffic Priorities for OSDRP (Dynamic SOP Scenario)

Node Mobility Scenario

To investigate the effect of node mobility on the performance of the different protocols, we implement the random waypoint model in the simulation. At every instant, a node randomly chooses a destination and moves towards it with a velocity selected randomly from a uniform distribution $[0, 50]$ metres/sec. After reaching the destination, the node stops for a duration of 30 seconds during which it chooses another random destination and repeats the whole process until the simulation ends. The movement of the nodes is confined within the boundary of their respective PRNs. All other parameters remain unchanged as those in the dynamic SOP scenario.

Figure 46 and Figure 47 shows the average end-to-end delay and total throughput for the different schemes when p is set to 0.5. We can observe that all schemes experience deteriorations in performance for the node mobility scenario. However, the performance in terms of delay and throughput by OSDRP remains relatively constant despite of the node movements.

Figure 46: Average End-to-end Delay vs. τ for $p = 0.5$ (Node Mobility Scenario)

Figure 47: Total Throughput vs. τ for $p = 0.5$ (Node Mobility Scenario)

ORTPC Unavailability Scenario

We also verify the effectiveness of the OSDRP in the event that the ORTPC features are unavailable. All other parameters remain the same as those in the Dynamic SOP scenario. As expected, Figure 48 shows that there are minimal differentiations for all traffic flows with different priorities under the OSDRP. However, the OSDRP still performs better compared to DORP, ccDSR and SAMER with its ability to select a minimum delay – maximum stability route by considering spectrum availability information on its routing. From the graph, we can see that as the values of τ decreases, the channel behaviour becomes more dynamic. This result in a larger performance differences between OSDRP and other protocols as protocols other than OSDRP tend to suffer a drop in their performance since they do not consider the dynamic behaviour of channels in their selection of paths. This does not affect OSDRP as much since OSDRP take into consideration of channel dynamics in the path selection.

Figure 48: Average End-to-End Delay vs. τ (ORTPC Unavailability Scenario)

Figure 49 shows the total throughput for OSDRP when ORTPC features are unavailable compared to the other schemes. The throughput for OSDRP remains relatively constant for the various values of τ . Even without ORTPC features, OSDRP performs better compared to other schemes when τ is between 10s and 25s. Once again, this shows the effectiveness of OSDRP compared to the other protocols with its ability in scenarios where channel availability is more dynamic.

Figure 49: Total Throughput vs. τ (ORTPC Unavailability Scenario)

Routing Overheads

Figure 50 shows the total routing traffic sent and received by the respective protocols for values of p between 0.1 – 0.9 under the baseline scenario. From the graph, we can see that SAMER requires the largest amount of control traffic since it is a link state protocol, which requires periodical exchange of control messages among nodes. However, the amount of control traffic generated is relatively constant in spite of the variations of p . The amount of control traffic by OSDRP exceeds those by DORP and ccDSR when p is between 0.1 - 0.3 due to the larger control packet size required by OSDRP to perform route discovery and ORTPC. However, when p exceeds 0.3, the amount of control traffic generated by DORP or ccDSR begins to increase at a faster rate compared to OSDRP due to the larger amount of control traffic generated by DORP and ccDSR for route re-discovery when route failures occur.

Figure 50: Total Routing Traffic vs. p (Baseline Scenario)

To evaluate the impact of node density on the effect of routing traffic overhead, we fix p to 0.5 and vary the number of nodes for each PRN from 4 to 8. All other parameters remain the same as those in the baseline scenario. Figure 51 shows the

total routing traffic sent and received by the respective protocols with the number of nodes per PRN changing from 4 to 8. When the number of nodes per PRN increases, the overhead incurred by OSDRP begins to increase faster compared to the other protocols. OSDRP has a larger overhead compared to the other protocols in a denser network because OSDRP discovers and maintains multiple routes to the same destination, and this is more likely in a denser network. This means that OSDRP may not perform as well as the other protocols in terms of overheads in a dense network. One of the possible ways to reduce the overheads in this case is to limit the number of routes to the same destination to a smaller number.

Figure 51: Total Routing Traffic vs. Number of nodes per PRN (Baseline Scenario)

We also evaluate the impact of node mobility on the effect of routing traffic overhead by implementing the random waypoint model as in the Node Mobility Scenario. The movement of the nodes is also confined within the boundary of their respective PRNs. In addition, we fix p to 0.5 and vary the number of nodes for each PRN from 4 to 8. All other parameters are the same as those in the Baseline Scenario.

Figure 52 shows the total routing traffic sent and received by the respective protocols with number of nodes per PRN changing from 4 to 8. The overheads

incurred by all the protocols increases about 10% due to node movements and route re-discovery. Interestingly, the routing overheads are slightly higher when the number of nodes per PRN is 4 compared to 5. The reason of this fact is that node movements can cause more link breakages and route re-discovery because of fewer relaying nodes in a sparser network.

Figure 52: Total Routing Traffic vs. Number of nodes per PRN (Baseline Scenario with Node Mobility)

4.2.4 Conclusion

In this section, we have proposed an Opportunistic Service Differentiation Routing Protocol for Cognitive Radio Networks (OSDRP). Our scheme utilizes multi-metric routing with the consideration of SOP availability to discover the minimum delay – maximum stability path. In addition, TPC and OR have been performed to provide differentiated service for different traffic priorities. Simulation results have indicated that the proposed OSDRP scheme can provide a lower end-to-end delay and a higher throughput for the traffic flows at different levels of spectrum availability across different PRNs in various scenarios. The simulation results have also shown that the OSDRP can provide clear service differentiations for different traffic classes in

various scenarios.

Chapter 5: Trusted Routing

There has been much research for CRs in the area of spectrum sensing, resource allocation, fairness, routing for CR-based wireless networks and so on. However, the security aspects of CR-based wireless networks or cognitive radio networks (CRN) is often neglected in the endeavour to design more powerful or faster ways to move data across the network.

As mentioned in Chapter 2, although there were many proposed routing algorithm for CRNs, most of these schemes do not or only partially considers the dynamic behavior of PUs and its effect on secondary traffic. Furthermore, none of the proposed schemes specifically address the problem of the presence of selfish nodes in the CRN, which can further complicate the routing problem when considered together with the spectrum availability issue.

On the other hand, the selfishness issue has been well studied in the area of non-cognitive radio wireless networks. An excellent review of the selfishness issues in multi-operator WMN is provided in [99]. There are also various proposed schemes to tackle the selfishness issue in delay tolerant networks (DTN) [123, 124]. However, these schemes are not directly applicable in the case of the CRNs due to their dynamic nature.

Clearly, there is a need to design effective cognitive routing protocols for dynamic CRNs in the presence of selfish nodes. The proposed solution must be able to detect selfish behaviours and discard the non-conforming packets before the performance of other nodes are affected, in addition to the considerations of delay, bandwidth, availability of spectrum opportunities (SOP), and so on. Mechanisms should also be available for cooperative nodes to route packets through other cooperative nodes

instead of selfish nodes to achieve better packet delivery performance.

5.1 An Altruistic Differentiated Service Protocol in Dynamic Cognitive Radio Networks against Selfish Behaviours

In this work, our goal is to address the QoS provisioning issue in CRNs with selfish nodes coexistence. One of the problems with existing schemes is the assumption that the spectrum resources needed for secondary access is considered infinitely available during its activities. However, this cannot be the case in real life situation as the intermittent availability of spectrum bands can cause communication problems among SUs. For instance, the sudden appearance of a PU on a channel will require the SUs to evacuate the channel, causing disruption to the on-going communications and causing packets to be dropped. SUs may also maintain radio silence due to nearby primary network activities. It can result in difficulties in determining the reason behind a dropped packet or a non-response of a CRN node, as it could be either due to the selfishness of the node, or due to the lack of available spectrum resources. Thus, most of the proposed schemes in Chapter 2 will not perform well in the case of CRNs as they may penalize a CRN node unfairly even though the reason of packet dropping is not due to the selfishness of the CRN node.

To summarize what we have learnt so far, there are three unique challenges of QoS provisioning in cognitive radio networks in the presence of selfish nodes versus a conventional wireless network. The first challenge is to ensure good general routing performance in face of the dynamic behavior of PUs and its detrimental effect on secondary traffic. The second challenge is to provide better service (lower delay and higher delivery ratio) for packets originating from collaborative nodes in the presence of selfish nodes in the network. The final challenge is to differentiate collaborative nodes that are situated in a disadvantaged area from purely selfish nodes and not to

penalize the collaborative nodes unfairly.

With this goal in mind, we propose to design a cross-layer Altruistic Differentiated Service Protocol (ADSP) for the dynamic CRNs. Different from the existing cognitive routing protocols, to the best of our knowledge, our proposal is the first routing solution with consideration of the reputation of the nodes, in addition to the availability of SOP and delay in deciding the routing path in dynamic CRNs. To provide better service to collaborative nodes, the proposed ADSP scheme also adopts a unique combination of TPC and OR [114] techniques to negotiate paths through nodes with better reputation which will further reduce the chance of a failed delivery.

The remainder of this chapter is organized as follows. In Section 5.1.1, we describe the system model. In Section 5.1.2, we present our proposed scheme. In Section 5.1.3, we verify the effectiveness of our scheme through extensive simulations. Finally, we conclude our work in Section 5.1.4.

5.1.1 System Model

5.1.1.1 Physical Layer Model

In this paper, a dynamic multi-hop CRN consisting of N nodes with M end-to-end traffic flows is under the study. Each node has one CR transceiver. The CR transceiver allows each node to communicate with its neighboring nodes by selecting an overlapping data channel in their respective SOPs. As nodes can encounter the “deafness problem” while communicating using dynamic frequency channels in a CRN, we adopt the use of an always on common control channel proposed in [125] with the same rationale provided in our previous work [24]. Our scheme also requires a MAC-Layer QoS Provisioning Protocol (MQPP) scheme [118] to be implemented on the MAC layer.

We assume that there are 12 non-overlapping wireless channels specified by the physical layer of the IEEE 802.11a standard. Each of the channels has a bandwidth of 20 MHz with a maximum capacity of 54 Mbps. The channel switching time is assumed to be t_d ms.

5.1.1.2 MAC Layer Model

An interweave model [24] is assumed, i.e., the nodes in the CRN can only transmit when the primary users are not active. Thus, there is virtually no interference to the primary users and there is no restriction on the power level of the secondary users.

We model the intermittent availability of the primary radio band for transmissions by cognitive users using a two-state alternating renewal process model, where the two states are Busy and Idle. The availability of the intermittent channel can be described by using three parameters: (1) The probability p of the primary user transmitting in the next time period (channel unavailable for secondary transmission), (2) Mean duration τ_i spent in the Idle state and (3) Mean duration τ_b spent in the Busy states. Thus, the channel state will alternate between the periods of availability and unavailability according to p , τ_i and τ_b as shown in Figure 53.

We assumed that both τ_i and τ_b follows an exponential distribution. We further assume that the parameters p , τ_i and τ_b are available for all nodes in their decision making. It is a reasonable assumption as there are existing schemes that allow nodes to monitor and utilize past channel histories to make predictions on future spectrum availability.

5.1.1.3 Node Behaviour

In this work, we assume that the nodes in the CRNs are not actively malicious, which means that they will not seek to sabotage the operation of the CRNs or other

nodes by transmitting fake information, or by interfering with others' transmissions. However, the nodes may be selfish in their behaviour by dropping others' packets when it has its own data to transmit or by remaining silent when a requestor node requests for its help in forwarding a packet. In both cases, the packet from the requesting node will not be forwarded to its destination. In our work, we model the probability of selfish behaviour by defining a selfishness factor sf . A node with sf of s will forward packets from other nodes with probability $1-s$. Thus, a node with $sf = 0$ will always forward packets from other nodes, while a node with $sf = 1$ will never forward packets from other nodes.

Figure 53: Two-State Alternating Renewal Process

5.1.1.4 Decentralized Trust Model

In order to enforce the reliability of the forwarding operations and also to discourage selfish behaviours within the CRNs, it is necessary to establish the identity of each node in the CRN. To do so, we make use of the well-known RSA algorithm[126] for this purpose.

The commercial implementation of RSA requires the presence of a CTA. This is needed as a valid subscriber can join from anywhere, and thus the keys are needed to correlate to the real identity of the subscriber, no matter where it joins. In our usage

of the RSA algorithm, nodes make use of the key generation and encryption/decryption capabilities to initiate a secure join request or a localized identity authentication. These operations are performed locally by requestor nodes, or nodes adjacent to the requester nodes. Therefore this do not requires the implementation of a system wide CTA since the keys are only maintained locally or on nodes adjacent to the requestor node.

RSA involves a public and a private key pair. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated in the following way:

At the end of the key generation process, every node will have two keys, a public key (n, e) and a private key d .

To measure the trust placed upon a node by the node's neighbours, we define a collaboration index (CI), which reflects the confidence that the neighbours have on the ability of the node to forward information. The CI is a value between 0 and 1, and is set to 0.5 initially. The CI of each node is stored on their neighbouring nodes instead of a CTA. The CI values will be updated by individual nodes as they overhear control or data traffic from their neighbours. There are two advantages in adopting this approach compared to using a CTA. Firstly, updates on the nodes' reputation are localized thus preventing unnecessary flooding of information to other portions of the

network. Secondly, the use of a CTA can lead to a system wide failure which can be avoided if the information is stored on individual nodes instead.

5.1.1.5 Complexity Analysis

The complexity analysis for ADSP is similar to that on DSR in [122]. For a network consisting of N nodes and diameter d , the time complexity for route initialization is $O(2d)$. Since ADSP maintains multiple routes to the same destination, the time complexity after a link failure is 0 for a cache hit and $O(2d)$, otherwise. The communication complexities for both initialization and after a link failure are both $O(2N)$.

5.1.2 Proposed Scheme

The challenges of security provisioning in dynamic CRNs have motivated us to design the ADSP. The objective of the ADSP is to select the best path taking into consideration of nodes' reputation, SOPs and delay. In our proposed scheme, we adopt a cross-layer approach to solve the routing problem through CRN which may contain selfish nodes. The techniques are implemented across two layers of the protocol stack:

- (1) MAC Layer – Key Generation, Secure Join Request, Secure RTS/CTS, Identity Authentication and Transmit Power Control.
- (2) Network Layer – Route Discovery, Route Selection and Opportunistic Routing (OR)

At the MAC layer, a database is created that is being used to store the information that is being shared between the MAC layer and the network layer. This allows the different layers to share information by each layer that is performing different function. The information includes node identity, node reputation, SOP information,

delay information and key information. An interface has been created to enable a back and forth flow mechanism for sharing information.

Using the above approaches, the proposed scheme can provide radically different capabilities from the existing cognitive routing protocols. They are: (1) Trust framework does not require the presence of a CTA, (2) Service Differentiation based on the level of cooperation of the node, (3) Opportunistic route selection and (4) Selfishness-aware routing.

5.1.2.1 Overview

The main difficulty in ensuring a good routing performance in dynamic CRNs is due to the fact that the average available duration of the communication channel may be much shorter than the communication time required. Coupled with the presence of selfish nodes, it is imperative that the proposed solution can determine the main reason behind a failed communication session and react appropriately. To do so, several functionalities are required which include the ability to authenticate nodes identity, measuring nodes' level of cooperation, multi-metric routing and so on.

In this section, we first present an overview of the ADSP for the dynamic CRNs. We describe each of the modules and the cooperation among them to achieve the objectives as above. Finally, we present the detailed algorithm for each of the module.

The ADSP consists of 2 modules as shown in Figure 54. They are Secure MAC and Selfishness Aware Routing. Each of the modules in turn consists of several functions. The main functionalities of the Secure MAC module are to provide a mechanism for authenticating nodes' identity and to facilitate the exchange of control and data frames in a secure manner. The purpose of the Selfishness Aware Routing module is to discover the best route from a source to a destination through the

exchange of Route Request and Route Reply packets. Opportunistic Routing (OR) is also performed during actual routing to further reduce the chance of a failed delivery.

Figure 54: ADSP Flow Diagram

5.1.2.2 Management of the Trust Model

For all nodes, the CI is set to 0.5 upon joining the CRN. However, as nodes cooperate, their CI will be updated over time. The amount in which the CI increases depends on the type of service that the node has provided. Conversely, if a node is not cooperative, then its CI will be decreased. The list of actions and their corresponding reward/punishment are listed in Table 8.

The CI of a node can vary from 0.0 to indicate bad reputation to 1.0 to indicate good reputation. The CI is stored in the local cache at each node. To further encourage cooperative behaviours, the reward of forwarding packets is tied to the CI value of the originating packet. To differentiate the case where the node is cooperative, but is unable to forward the packet due to it being situated in a disadvantaged area, i.e., frequent appearance of the primary user, we make use of the parameters p and τ_b . For example, the reward for forwarding others' packet is proportionately related to p , which implies that a node will be rewarded more if it forwards others' packet if it is situated in a CRN with high possibility of primary user

re-appearances.

Our scheme also penalizes nodes that do not response to the forwarding requests from their neighbours, but subsequently lifted radio silence to transmit their own packets. Recognizing that some nodes may be temporarily unable to respond due to the presence of the primary user, the penalty is reduced in cases when the packets are transmitted outside τ_b sec of maintaining radio silence.

Table 8: Action Reward/Punishment

Action	Reward
Sponsoring node join to CRN	+ 0.10
Forwarding others' packets	+ 0.05* $CT*p$
Responding to RTS with CTS Packet	+ 0.01
Maintaining radio silence	- 0.1*($1-p$)
Forwarding own packet within τ_b sec of maintaining radio silence	- 0.05
Forwarding own packet outside τ_b sec of maintaining radio silence	- 0.02

5.1.2.3 Detail Algorithm Description

In this section, we will describe the details of the ADSP algorithm. Figure 55 shows the sequence of flow for messages used in the various modules of ADSP.

1) Secure Join Request

A join request is facilitated via an exchange of Request-to-Join (RTJ) and Clear-To-Join (CTJ) packets. The formats of both packets are shown in Figure 56. A node wishing to join a CRN has to broadcast a RTJ packet on the control channel. The RTJ packet is a 336 bits packet containing the MAC address of the node, its public key and a signed digest of its MAC address generated using the cryptographic Secure Hash Algorithm (SHA-1). The RTJ serves two purposes. Firstly, the signed MAC digest can be used to authenticate the identity of the requesting node. Secondly, the public key allows the requesting node to receive encrypted packets from other nodes.

Figure 55: Sequence of flow in ADSP

Figure 56: RTJ/CTJ Packet Format

The requesting node m can produce a digest of its MAC address using the cryptographic Secure Hash Algorithm (SHA-1) and signed it by performing $S = M^d \bmod n$ where M is the digest of its MAC address, while S the corresponding signed digest. The Requestor MAC Address, public key (n, e) and Signed Requestor MAC Digest S are stored in the RTJ packet and sent through the common control channel.

Secure Join Request

Begin

if (not member of CRN) then

1. Compute $M = \text{SHA1}(\text{MAC Address})$.
2. Compute $S = M^d \bmod n$.
3. Create *RTJ* packet with the values (MAC Address, (n,e), S);
4. Broadcast *RTJ* packet on common control channel.

endif

End

2) Identity Authentication

A node which accepts the requesting node to join the CRN is called a sponsor node. When a sponsor node receives the *RTJ*, it uses the SHA-1 in conjunction with the requesting node's MAC address to calculate M . It performs the operation $M' = S^e \bmod n$ and compares the resulting digest M' with the message's actual digest M . If $M' = M$, then the sender of the message is in possession of requesting node m's private key, and that the message has not been tampered with. After authenticating the identity of the requesting node, the sponsor node admits the requesting node into the CRN by replying with a 384 bits Clear-to-Join (*CTJ*) packet. The information of the requesting node is stored in the local cache, and also propagated to the rest of the network via the control channel.

After the *CTJ* packet is received by the requestor node, the requestor node verifies the identity of sponsor node contained in the packet and adds the sponsor information to its local cache.

```

Identity Authentication
Begin
  if (received RTJ packet) then
    1. Compute  $M = \text{SHA1}(\text{Requestor MAC Address})$ .
    2. Compute  $M' = S^e \bmod n$ , where S is the Signed Requestor MAC Digest.
    3. If  $M' = M$  then
      1. Compute  $M_s = \text{SHA1}(\text{Sponsor MAC Address})$ .
      2. Compute  $S_s = M_s^d \bmod n$ .
      3. Create CTJ packet with the values (Sponsor MAC Address,
        Requestor MAC Address, (n,e),  $S_s$ );
      4. Transmit CTJ; If CI is null, set CI for requestor node to 0.5;
    else
      discard RTJ packet;
    endif
  else
    if (received CTJ packet) then
      1. Compute  $M = \text{SHA1}(\text{Sponsor MAC Address})$ .
      2. Compute  $M' = S^e \bmod n$ , where S is the Signed Sponsor MAC Digest.
      3. If  $M' = M$  then
        Store sponsor node information on local cache;
        Update CI for sponsor node;
      else
        discard CTJ packet;
      endif
    endif
  endif
End

```

3) Route Discovery

Before the start of the data transmission, the route cache will be examined to see if there is a valid route to the desired destination. If a valid route cannot be found in the cache, route discovery will be triggered. The ADSP performs path discovery by implementing a complete set of route discovery mechanisms similar to the DSR. By sending out the “Route Request” or RREQ packets, nodes can discover routes to arbitrary destinations in the CRN. When the destination node receives the RREQ packet, a Route Reply or RREP packet will be generated with a copy of the accumulated route record from the RREQ packet. The RREP packet will be sent to the source node through the reverse path the RREQ packet had traversed. The route information, delay, *Average_CI* and *Minimum_CI* information within the RREP packet will be used to update the route cache at the transmitter.

Initiate Route Discovery

Begin

if (no valid route found on cache) **then**

1. Create RREQ packet;
2. Initialize route record in RREQ packet to empty, initialize *delay* to 0, initialize *Average_CI* to 0; *Minimum_CI* to 0;
3. Broadcast RREQ packet on common control channel.

else

Perform Route Selection.

endif

End

Propagate RREQ and Route Reply

Begin

if (receive RREQ packet) **then**

1. Determine if its address is on the list of route record;
2. **if** (it is on the list of route record) **then**
Discard RREQ packet.
3. **else**
 1. Append own address and frequency channel to route record in RREQ packet;
 2. Set switching delay $d_{switch} = t_d$ ms if the receiving frequency is fixed to the same channel as the previous hop node's transmitting frequency. Otherwise, the switching delay is set to $d_{switch} = 0$ ms;
 3. Add d_{switch} to the delay field;

4. Add average queuing delay to the delay field where $d_{queue} = \sum_n t_{nsend} - t_{nreceive} / n$,

t_{nsend} and $t_{nreceive}$ are the send and receive time of the previous n packets;

5. Lookup *CI* for the previous node;
6. Update *Average_CI*;
7. If *CI* is less than *Minimum_CI*, set *Minimum_CI* = *CI*;
6. **if** (receiving node is destination) **then**
 1. Creates RREP packet;
 2. Send RREP packet.

7. **else**

Rebroadcasts the RREQ packet on the common control channel.

endif

endif

endif

End

4) Route Selection

Once the routes have been discovered, the ADSP selects all the routes that fulfil the requirement where $Minimum_CI > CI_{min}$ and $Average_CI > CI_{ave}$ where CI_{min} and CI_{ave} are the minimum and average *CI*, respectively that are acceptable for a particular traffic flow. The selected routes are then further sorted according to delay in ascending order.

Route Selection

Begin

1. Identify routes with $Minimum_CI > CI_{min}$ and $Average_CI > CI_{ave}$
2. Sort route in ascending order of delay;
3. Choose minimum delay route.

End

5) Secure Request of RTS/CTS and Opportunistic Routing with Transmit Power Control

The Secure RTS/CTS is an enhancement of the modified RTS/CTS handshaking mechanism from [66]. The CTS packet contains an additional *CI* field which is embedded in the data packet of the transmitter. The *CI* of the packet is used to decide the order of transmission of the local queue. This mechanism can be used to punish misbehaving nodes in heavy traffic situations by dropping packets originating from the nodes with lower *CI* when the local transmission queue is full. At the physical layer, the transmission power is also tied to the *CI*. Packets with *CI* between 0.0 – 0.33, 0.34 – 0.66 and 0.67 – 1.0 will be mapped to priority c_3 , c_2 and c_1 , respectively, regardless of their original priority. At the network layer, using OR technique, the ADSP determines the candidate forwarding nodes (CFNs) from the remaining hops along the selected route according to *CI*. According to the differentiated transmission power at the MAC layer, higher *CI* packets have correspondingly higher chances to be received at a farther away node compared to the lower *CI* packets. The ADSP utilizes this fact to vary the range of the CFNs selection. Thus, higher *CI* packets will have a higher OR Candidate Selection Range compared to lower *CI* packets. Figure 57 shows an example for node *I* where the OR Candidate Selection Range for packets with *CI* of 0.3, 0.6 and 0.9 is 3, 2 and 1, respectively. This selection strategy has three benefits over the existing OR protocols. Firstly, it has a simpler selection of CFNs. Secondly, candidate nodes are range limited according to packet priority to provide service differentiation. Finally, duplicate transmissions are minimized as nodes will not be selected on possibly diverging paths.

To ensure that only the node closest to the destination performs the forwarding, we have implemented the prioritized acknowledgement scheme [114] where candidate nodes acknowledge the successful reception of a packet in a prioritized manner according to the sequence indicated in the packet, i.e. a candidate node with

higher priority will send its acknowledgement before any lower priority candidates. For the example in Figure 57, node 4 will send its acknowledgement before node 3, and node 3 will send its acknowledgement before node 2. This strategy takes advantage of the broadcast nature of the wireless medium to further reduce the likelihood of a dropped packet due to the selfish behaviours of intermediate nodes. When a node transmits, a number of nearby nodes can hear the transmission. A node can then be selected out of the several candidate forwarding nodes (CFNs) to transmit the received packet. It can help to cut down on the cases where intermediary nodes do not respond to the forwarding request.

Figure 57: Differentiated OR Candidate Selection Range

5.1.3 Numerical Results

Simulation experiments have been performed using OPNET Modeler 14.5A with wireless extension to evaluate the performance of the proposed ADSP scheme.

5.1.3.1 Simulation Setup

In our simulation, the network topology consists of 54 nodes spanning across 3 PRNs as seen in Figure 58. The nodes are not energy-constrained and are grouped into 3 groups consisting of 18 nodes each. For each PRN, out of the 18 nodes, 1/3 of them are always altruistic ($sf = 0$), 1/3 of them are always selfish ($sf = 1$) and the remaining are selfish with a probability of s , and altruistic for a probability of $1-s$. ($sf = s$)

Figure 58: Simulated Topology

The nodes in each group are randomly scattered within a circular region of radius 800 metres. There are 3 circular regions and the position of the centre of each region is 1200 metres apart from each other. All the nodes are mobile and follow the random waypoint model in the simulation. At each instant, a node randomly chooses a destination and moves towards it with a velocity selected randomly from a uniform distribution $[0, 50]$ metres/sec. After reaching the destination, the node stops for a duration of 30 seconds during which it chooses another random destination and repeats the whole process until the simulation ends. The movements of the nodes are confined within the boundary of their respective PRNs.

Three nodes where $sf = 0$, $sf = 1$ and $sf = s$ are randomly selected from each PRN.

Each node then selects a random destination for three sets of traffic flows with priority c_1 , c_2 and c_3 . ($c_1 > c_2 > c_3$) The traffic generation is a Poisson process and the mean packet inter-arrival time is exponentially distributed from 5ms to 25ms.

Additional SOP availability parameters and protocol specific flow properties are specified in Table 9 and Table 10. All traffic flows are pre-run for 30 seconds, and the simulation results are then collected for another 90 seconds.

Table 9: SOP Availability Parameters

Primary Networks	SOP Availability $p, U(\tau_i - a, \tau_i + a), U(\tau_b - a, \tau_b + a)$
PRN1	$p = 0.2, a = 5, \tau_i = 90, \tau_b = 45$
PRN2	$p = 0.1, a = 5, \tau_i = 90, \tau_b = 30$
PRN3	$p = 0.4, a = 5, \tau_i = 90, \tau_b = 60$

Table 10: Protocol Specific Traffic Flows Parameters

Priority	ADSP	OSDRP	DORP
c_1	$CI_{min} = 0.75$ $CI_{ave} = 0.75$	min data rate = 24Mbps OR Candidate Selection Range = 3	N/A
c_2	$CI_{min} = 0.5$ $CI_{ave} = 0.5$	min data rate = 12Mbps OR Candidate Selection Range = 2	N/A
c_3	$CI_{min} = 0.25$ $CI_{ave} = 0.25$	min data rate = 6Mbps OR Candidate Selection Range = 1	N/A

5.1.3.2 Simulation Results

To show the effectiveness of our scheme, we compare the performance of our proposal with three other routing protocols proposed for CRNs, the Delay motivated On-demand Routing Protocol (DORP) [79], Spectrum Aware Mesh Routing Protocol (SAMER) [86] and the Opportunistic Service Differentiated Routing Protocol (OSDRP) [24]. We vary s from 0.0 to 1.0 with step of 0.1. For each value of s , we run the simulation for 51 times with a different random number seed in each run.

Figure 59 shows the overall average end-to-end delay vs. s for priority c_1 traffic flows for values of s from 0.0 to 1.0. For ADSP, there is a clear service differentiation for traffic originating from the nodes with different sf. The service differentiation comes from the multi-layer service differentiation according to the nodes' CI. As

DORP, OSDRP and SAMER cannot differentiate traffic by their originating nodes' CI, it is not shown in the figure. The result also shows that as s increases, the end-to-end delay also increases for all traffic due to the increased likelihood of packet drops by selfish nodes in the network. The delay of traffic flows of other priorities show similar conclusion but we omit it here for brevity sake.

Figure 59: Average End-to-end Delay vs. s

Figure 60 shows the average end-to-end delay vs. s for traffic flows originating from nodes with $sf = 1$ for values of s from 0.0 to 1.0. The performance is very similar despite the differences in packet priority as ADSP does not rely on priority labelling to provide differentiated service. In fact, the selfish node is unable to “cheat” by labelling all its packets as high priority.

Figure 61 shows the average throughput per traffic flow vs. s for values of s from 0.0 to 1.0. From the graph, we can see that the throughput by ADSP, where $sf = 0$, is generally the highest among those by different schemes. This is especially true for the values of $s > 0.3$, which shows its effectiveness in networks with more selfish nodes. ADSP's throughput is slightly less compared to OSDRP for values of $s < 0.3$. This is due to ADSP's higher overheads and the fact that OSDRP places more emphasis in spectrum availability and network delay in its route selection, whereas ADSP places

more emphasis on CI which may not provide the best path in networks with relatively less selfish nodes.

Figure 60: Average End-to-end Delay vs. s

Figure 61: Average Throughput per Traffic Flow vs. s

Figure 62 shows the delivery ratio by different schemes vs. s for values of s from 0.0 to 1.0. For all schemes, the delivery ratio decreases as the number of selfish nodes increases. However, ADSP is able to provide the best delivery ratio to the packets originating from nodes where $sf = 0$. Even in the case where $s = 1.0$, the number of packets delivered is about 50%.

Figure 62: Delivery Ratio vs. s

5.1.4 Conclusion

In this section, we have proposed the ADSP scheme for CRNs. The major contribution of our proposal is the design and implementation of a routing scheme that considers the reputation of the nodes, in addition to the availability of SOP and delay in deciding the routing path. ADSP also adopts a unique combination of TPC and OR techniques to negotiate paths with nodes that have better reputation which will further reduce the chance of a failed delivery.

The simulation results have shown that ADSP can provide lower delay, higher throughput and better delivery ratio to the traffic flows originating from cooperative nodes compared to other existing cognitive routing protocols across various scenarios in the presence of selfish nodes. At the same time, traffic flows originating from selfish nodes have been penalized, experiencing higher delay, lower throughput and lower delivery ratio.

Chapter 6: Conclusion and Recommendation

We conclude this thesis by summarizing our contributions, and recommending some directions for further research.

6.1 Conclusion

Based on the literature survey and the research done in the area of WMNs/CRNs, we have gained valuable insights to the problems affecting the performance of WMNs/CRNs and their proposed solutions from the research community. We have designed two MAC protocols, MQPP and EBAS, and three network routing protocol DVCSIR, OSDRP and ADSP to improve QoS provisioning capabilities in WMNs and CRNs.

Addressing the weakness of the IEEE802.11 MAC, the MQPP scheme considers the transmission power, rate, modulation and interference in providing a differentiated QoS to different traffic classes. Interference is mitigated through the use of multiple vacant channels identified through spectrum sensing.

We propose a strategy to combine the strength and to mitigate the weaknesses of both spectrum overlay and underlay through a hybrid transmission strategy in the EBAS scheme. The scheme also adopts a softened peak interference power constraint to improve the performance of the secondary system while still granting superior protection to primary system transmissions.

In DVCSIR, the design considers the network topology and traffic pattern to provide a minimum interference route from source to destination. A novel dynamic

virtual carrier sensing mechanism was also proposed to address the weakness of the IEEE 802.11 MAC.

Subsequently, we further develop the multi-metric routing idea and came up with the OSDRP. The OSDRP discovers the minimum delay – maximum stability route in dynamic CRNs by considering the availability of spectrum opportunity in addition to switching delay and queuing delay across primary user networks. In addition, service differentiation can be achieved through a combination of transmit power control and opportunistic routing.

Although there have been many proposed routing algorithm for CRNs, none of the proposed schemes address the problem of the presence of selfish nodes in the CRN. Furthermore, most of the schemes assume assumed a static CRN that considers an available frequency band as a permanent resource indefinitely available during its activity. Clearly, such assumptions do not differ from those considered in multi-channel mesh networking. Through the ADSP scheme, we design a cross-layer routing protocol for the dynamic CRNs. Different from the existing cognitive routing protocols, ADSP considers the reputation of the nodes, in addition to the availability of spectrum opportunities (SOP) and delay in deciding the routing path. A unique combination of transmit power control and opportunistic routing techniques can also allow the ADSP to negotiate paths with nodes that have better reputation which further reduces the chance of a failed delivery.

6.2 Recommendations for Further Research

6.2.1 QoS Support for the IEEE 802.22-based Wireless Regional Area Network (WRAN)

The IEEE 802.22-based wireless regional area network (WRAN) is the first

world-wide standard for cognitive radio networks. It uses the same radio spectrum currently allocated for TV service. The standard uses the concept of cognitive radio based on dynamic spectrum access to provide wireless access services in a large coverage area. Similar to existing networking standards like the 802.16, a variety of traffic types with different QoS requirements will need to be supported in a WRAN.

As the 802.22 MAC operates in a point-to-multipoint networking model, it is comparatively simpler than the decentralized networking scenarios. Although the 802.22 MAC provides a few mechanisms to support QoS in infrastructure-based networks, they are unsuitable for peer-to-peer or decentralized networks. Thus, there is a need to design and to implement additional enhancements, possibly at several network layers to further the support of QoS provisioning in 802.22-based networks. Some of these works currently undergoing development are:

- 1) Developing MAC protocols to support dynamic spectrum sensing and resource allocation among WRANs. The 802.22 system needs to sense the channels and detect radio signals to protect the incumbent users. The channel sensing is done by both BS and CPEs during the quiet periods which are carefully scheduled by BS. Because of this, no transmission can be scheduled during the quiet periods so that any signal which is detected in quiet periods can be determined as incumbent signals. Furthermore, the quiet periods need to be scheduled quite regularly and considerably long in order to have a more accurate and reliable sensing result. This can significantly affects the throughput of network since no transmissions are allowed during the quiet period. Therefore, optimizing the trade-off between throughput and reliable channel sensing will be a chief issue for 802.22-based system.

- 2) Developing routing protocols to avoid congestion in the relay stations and/or mesh routers. Network congestion can occur when relay stations and/or mesh routers

are overwhelmed with traffic sent by the CPEs. This is particularly important for 802.22-based systems as they need to cover a large geographical area, typically 17-30 km in radius. The routing protocol must be intelligent enough to gauge the amount of backlogged traffic packets in participating nodes when routing decisions are made in order to establish the optimal path between source and destination. This may require a careful consideration of the trade-off between the shortest path route, spectrum availability history, traffic load and so on. Otherwise, a wrong decision may lead to excessive delays or retransmissions that can cause the quality of service to deteriorate.

3) Developing traffic scheduling scheme to allocate available TV bands according to flow priority. Real time traffic such as voice and video have strict requirements on the acceptable end-to-end packet delay. When there are different types of traffic with different requirements on tolerable latency, a properly designed 802.22-based packet scheduling schemes will be able to provide an adequate QoS for real time services.

4) Developing admission control scheme to support QoS provisioning.

6.2.2 Research on Cognitive Radio Security

Currently, there has not been much work on the security aspect of cognitive radios. One of the main security issues is due to the programmable capability of cognitive radios. This introduces an entirely new vulnerability compared to using traditional wireless device as it is relatively easy to launch a low-cost denial-of-service attack by creating a wide range of authorized and unauthorized waveforms using low-cost consumer devices. Thus, protecting mission critical networks would be of the utmost importance. Future research will be required to develop a trusted security framework which can be easily implemented across different platforms and hardware architectures. There is also an urgent need to develop solutions across the

different layers. Some of the issues currently being worked on in this area are:

- 1) Identify the implications of software-based radio implementations.
- 2) Identify the different types of denial-of-service and other security attacks that are made possible by emerging cognitive radio technology.
- 3) Identify authentication mechanisms needed to support cooperative cognitive networks.
- 4) Developing trusted cognitive radio architecture.
- 5) Developing schemes (reputation-based etc.) to complement/upgrade existing conventional PKI authentication protocols

Compared to traditional wireless radios, cognitive radios offer significant new capabilities to defend against intrusions or denial of service attacks. The configurability of the software radio with its spectrum sensing capability allows it to leverage on recent developments in wireless security in which physical layer properties like RF signatures are used for authentication or secure communication. Furthermore, spectrum scanning and frequency agility associated with cognitive radios networks allow them to migrate away from frequency channels that are experiencing denial-of service attacks. Utilizing location/geographic information via global positioning system (GPS) can also allow the cognitive radio system to defend itself against certain kinds of attacks.

The current developments on this area include:

- 1) Identify physical layer security enhancements for wireless networks and evaluation of performance in real life environments.
- 2) Evaluate different denial-of-service attack scenarios and methods for defence.
- 3) Leveraging on geo-location for improved wireless network security.
- 4) Designing cooperative methods for detecting and isolating intruders.

While the early results show some promise, we must take note that most of the evaluations were limited to lab environments. Thus, it is unclear if these techniques will be effective in real world deployments. What is really required is larger scale testing in CRNs. Because CRNs are still in their infancy, there is a chance to make security part of the architecture of CRN from day one, instead of implementing security solutions as an afterthought. Doing this will require the effort and coordination of the research community.

List of Publications

Journal Paper

- K.C. How, "Supporting Differentiated Service in Cognitive Radio Wireless Mesh Networks," *CCSE Computer and Information Science*, Vol. 3, No.3, 2010, pp. 3-13
- K.C. How, M. Ma, and Y. Qin, "Routing and QoS provisioning in cognitive radio networks," *Computer Networks*, Vol. 55, No.1, 2011, pp. 330-342.
- K. C. How, M. Ma, and Y. Qin, "A MAC-Layer QoS Provisioning Protocol for Cognitive Radio Networks," *Wireless Personal Communications*, vol. 65, pp. 203-222, 2012.
- K. C. How, M. Ma, and Y. Qin, "Differentiated service provisioning in the MAC layer of cognitive radio mesh networks," *Int. J. Communication Networks and Distributed Systems*, vol. 8, Nos. 3/4, pp. 213-229, 2012.
- K. C. How, M. Ma, and Y. Qin, "An altruistic differentiated service protocol in dynamic cognitive radio networks against selfish behaviors," *Computer Networks*, vol. 56, pp. 2068-2079, 2012.

Conference Paper

- K.C. How and Y. Qin, "Dynamic Virtual Carrier Sensing and Interference Aware Routing Protocol in Wireless Mesh Networks," in Proc. *11th IEEE Singapore International Conference on Communication Systems*, Guangzhou, China, 19-21 Nov. 2008, pp. 1155-1159.
- K.C. How, M. Ma, and Y. Qin, "A Cognitive Power-Controlled Rate-Adaptive MAC Protocol to Support Differentiated Service in Wireless Mesh Networks," in Proc. *7th International Conference on Information, Communications and Signal Processing*, 2009, pp. 1-5.
- K.C. How, M. Ma, and Y. Qin, "An Opportunistic Service Differentiation Routing Protocol for Cognitive Radio Networks," in Proc. *GLOBECOM 2010, IEEE Global Telecommunications Conference*, 2010, pp. 1-5.
- K.C. How, M. Ma, and Y. Qin, "A cross-layer selfishness Avoidance Routing Protocol for the dynamic Cognitive Radio Networks," in *IEEE GLOBECOM Workshops (GC Wkshps)*, 2011, pp. 942-946.

Papers in Submission

- K.C. How, M. Ma, and Y. Qin, "An Elastic Bandwidth Allocation Scheme with Flexible Peak Interference Power Constraint for the Dynamic Cognitive Radio Systems," submitted to *IEEE CCIS 2012*.
- K.C. How, M. Ma, and Y. Qin, "Elastic Bandwidth Allocation Scheme with Softened Peak Interference Power Constraint for the Dynamic Cognitive Radio Systems," submitted to *IEEE Transactions of Parallel and Distributed Systems*.

References

- [1] "IEEE Std. 802.11, "IEEE Standard for Local and Metropolitan Area Networks"," 1999.
- [2] S. Marwaha, J. Indulska, and M. Portmann, "Challenges and Recent Advances in QoS Provisioning in Wireless Mesh Networks," in *8th IEEE International Conference on Computer and Information Technology*, 2008., 8-11 July 2008, pp. 618-623.
- [3] S. Geirhofer, L. Tong, and B. M. Sadler, "COGNITIVE RADIOS FOR DYNAMIC SPECTRUM ACCESS - Dynamic Spectrum Access in the Time Domain: Modeling and Exploiting White Space," *IEEE Communications Magazine*, vol. 45, pp. 66-72, 2007.
- [4] M. J. Marcus, "Unlicensed cognitive sharing of TV spectrum: the controversy at the Federal Communications Commission," *Communications Magazine, IEEE*, vol. 43, pp. 24-25, 2005.
- [5] J. Mitola, III and G. Q. Maguire, Jr., "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, pp. 13-18, Aug. 1999.
- [6] S. Haykin, D. J. Thomson, and J. H. Reed, "Spectrum Sensing for Cognitive Radio," *Proceedings of the IEEE*, vol. 97, pp. 849-877, 2009.
- [7] N. Nandiraju, D. Nandiraju, L. Santhanam, B. He, J. Wang, and D. P. Agrawal, "Wireless Mesh Networks: Current Challenges and Future Directions of Web-In-The-Sky," *IEEE Wireless Communications*, vol. 14, pp. 79-89, Aug. 2007.
- [8] P. Gupta and P. R. Kumar, "The Capacity of Wireless Networks," *IEEE Transactions on Information Theory*, vol. 46, pp. 388-404, Mar. 2000.
- [9] S. Toumpis, A. J. Goldsmith, and J. Sayir, "Capacity Results for Asymmetric Wireless Networks," in *International Zurich Seminar on Communications*, 2004, pp. 180-183.

- [10] J. Jun and M. L. Sichitiu, "The Nominal Capacity of Wireless Mesh Networks," *IEEE Wireless Communications*, vol. 10, pp. 8-14, Oct. 2003.
- [11] "FCC Spectrum Policy Task Force, FCC Report of the Spectrum Efficiency Working Group," Nov. 2002.
- [12] M. Nekovee, T. Irnich, and J. Karlsson, "Worldwide trends in regulation of secondary access to white spaces using cognitive radio," *Wireless Communications, IEEE*, vol. 19, pp. 32-40, 2012.
- [13] L. Kleinrock and F. Tobagi, "Packet Switching in Radio Channels: Part I--Carrier Sense Multiple-Access Modes and Their Throughput-Delay Characteristics," *Communications, IEEE Transactions on*, vol. 23, pp. 1400-1416, 1975.
- [14] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on*, 1999, pp. 90-100.
- [15] C. E. Perkins and P. Bhagwat, "Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers," presented at the Proceedings of the conference on Communications architectures, protocols and applications, London, United Kingdom, 1994.
- [16] D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," in *Mobile Computing*, 1996, pp. 153-181.
- [17] S. Murthy and J. J. Garcia-Luna-Aceves, "An efficient routing protocol for wireless networks," *Mob. Netw. Appl.*, vol. 1, pp. 183-197, 1996.
- [18] J. M. S. Corson, "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," www.ietf.org/rfc/rfc2501.txt, Jan. 1999.
- [19] M. S. Corson, J. P. Macker, and G. H. Cirincione, "Internet-based mobile ad hoc networking," *Internet Computing, IEEE*, vol. 3, pp. 63-70, 1999.

- [20] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Computer Networks*, vol. 47, pp. 445-487, 2005.
- [21] D. S. J. D. Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," *Wirel. Netw.*, vol. 11, pp. 419-434, 2005.
- [22] R. Draves, J. Padhye, and B. Zill, "Routing in multi-radio, multi-hop wireless mesh networks," presented at the Proceedings of the 10th annual international conference on Mobile computing and networking, Philadelphia, PA, USA, 2004.
- [23] K. C. How, M. Ma, and Y. Qin, "A MAC-Layer QoS Provisioning Protocol for Cognitive Radio Networks," *Wireless Personal Communications*, vol. 65, pp. 203-222, 2012.
- [24] K. C. How, M. Ma, and Y. Qin, "Routing and QoS provisioning in cognitive radio networks," *Computer Networks*, vol. 55, pp. 330-342, 2011.
- [25] K. C. How, M. Ma, and Y. Qin, "An altruistic differentiated service protocol in dynamic cognitive radio networks against selfish behaviors," *Computer Networks*, vol. 56, pp. 2068-2079, 2012.
- [26] I. F. Akyildiz and X. Wang, "A Survey on Wireless Mesh Networks," *IEEE Communications Magazine*, vol. 43, pp. S23-S30, Sep. 2005.
- [27] S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, pp. 201-220, 2005.
- [28] 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, pp. 2127-2159, 2006.
- [29] M. Sherman, A. N. Mody, R. Martinez, C. Rodriguez, and R. Reddy, "IEEE Standards Supporting Cognitive Radio and Networks, Dynamic Spectrum

- Access, and Coexistence," *IEEE Communications Magazine*, vol. 46, pp. 72-79, 2008.
- [30] S. Xu and T. Saadawi, "Does the IEEE 802.11 MAC Protocol Work Well in Multihop Wireless Ad Hoc Networks?," *IEEE Communications Magazine*, vol. 39, pp. 130-137, 2001.
 - [31] P. Karn, "MACA, "A New Channel Access Method for Packet Radio", in *9th Computer Networking Conference on ARRL/CRRL Amateur Radio*, September 1990, pp. 134-140.
 - [32] K. Xu, M. Gerla, and S. Bae, "How Effective is the IEEE 802.11 RTS/CTS Handshake in Ad Hoc Networks," in *IEEE Global Telecommunications Conference*, 2002, pp. 72-76 vol.1.
 - [33] A. Rahman and P. Gburzynski, "Hidden Problems with the Hidden Node Problem," in *23rd Biennial Symposium on Communications*, 2006, pp. 270-273.
 - [34] A. Acharya, A. Misra, and S. Bansal, "MACA-P: A MAC for Concurrent Transmissions in Multi-hop Wireless Networks," in *First IEEE International Conference on Pervasive Computing and Communications*, 2003, pp. 505-508.
 - [35] J. Zhu, X. Guo, L. L. Yang, and W. S. Conner, "Leveraging Spatial Reuse in 802.11 Mesh Networks with Enhanced Physical Carrier Sensing," in *IEEE International Conference on Communications*, 2004, pp. 4004-4011 Vol.7.
 - [36] "<http://standards.ieee.org/getieee802/802.11.html>."
 - [37] M. Benveniste, "A Distributed QoS MAC Protocol for Wireless Mesh," in *Second International Conference on Sensor Technologies and Applications*, 2008, pp. 788-795.
 - [38] L. Zhao, J. Y. Wu, H. Zhang, and J. Zhang, "Integrated Quality-of-Service Differentiation over IEEE 802.11 Wireless LANs," *IET Communications*, vol. 2, pp. 329-335, 2008.

- [39] J. Lee, W. Liao, J.-M. Chen, and H.-H. Lee, "A Practical QoS Solution to Voice Over IP in IEEE 802.11 WLANs," *IEEE Communications Magazine*, vol. 47, pp. 111-117, 2009.
- [40] Y. He, J. Sun, R. Yuan, and W. Gong, "A reservation based backoff method for video streaming in 802.11 home networks," *IEEE Journal on Selected Areas in Communications*, vol. 28, pp. 332-343, 2010.
- [41] P. Serrano, A. Banchs, P. Patras, and A. Azcorra, "Optimal Configuration of 802.11e EDCA for Real-Time and Data Traffic," *IEEE Transactions on Vehicular Technology*, vol. 59, pp. 2511-2528, 2010.
- [42] A. Nafaa, "Provisioning of Multimedia Services in 802.11-Based Networks: Facts and Challenges," *IEEE Wireless Communications*, vol. 14, pp. 106-112, 2007.
- [43] J. Villalón, P. Cuenca, and L. Orozco-Barbosa, "On the capabilities of IEEE 802.11e for multimedia communications over heterogeneous 802.11/802.11e WLANs," *Telecommunication Systems*, vol. 36, pp. 27-38, 2007.
- [44] A. Torres, C. T. Calafate, J. C. Cano, and P. Manzoni, "Deploying a real IEEE 802.11e testbed to validate simulation results," in *IEEE 34th Conference on Local Computer Networks, 2009. LCN 2009.*, 2009, pp. 109-115.
- [45] C. E. Perkins, E. M. Royer, S. R. Das, and M. K. Marina, "Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks," *IEEE Personal Communications*, vol. 8, pp. 16-28, 2001.
- [46] A. A. Pirzada and M. Portmann, "High Performance AODV Routing Protocol for Hybrid Wireless Mesh Networks," in *Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*, 2007, pp. 1-5.
- [47] S. Waharte, B. Ishibashi, R. Boutaba, and D. Meddour, "Interference-Aware Routing Metric for Improved Load Balancing in Wireless Mesh Networks," in *Communications, 2008. ICC '08. IEEE International Conference on*, 2008, pp. 2979-2983.

- [48] Y. Yang, J. Wang, and R. Kravets, "Designing routing metrics for mesh networks," *Proceedings of the IEEE Workshop on Wireless Mesh Networks (WiMesh)*. IEEE Press, 2005.
- [49] S. N. Nagesh, S. N. Deepti, and P. A. Dharma, "Multipath Routing in Wireless Mesh Networks," in *IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS)*, 2006, 2006, pp. 741-746.
- [50] H. Badis and K. Al Agha, "QOLSR multi-path routing for mobile ad hoc networks based on multiple metrics: bandwidth and delay," in *IEEE 59th Vehicular Technology Conference, 2004. VTC 2004-Spring*. 2004, 2004, pp. 2181-2184 Vol.4.
- [51] R. Baumann, S. Heimlicher, and B. Plattner, "Routing in Large-Scale Wireless Mesh Networks Using Temperature Fields," *IEEE Network*, vol. 22, pp. 25-31, 2008.
- [52] P.-C. Yeh, W. E. Stark, and S. A. Zummo, "Performance Analysis of Wireless Networks With Directional Antennas," *IEEE Transactions on Vehicular Technology*, vol. 57, pp. 3187-3199, 2008.
- [53] A. H. Wong, M. J. Neve, and K. W. Sowerby, "Performance Analysis for Indoor Wireless Systems Employing Directional Antennas," *IEE Proceedings-Communications*, vol. 152, pp. 890-896, 2005.
- [54] J. Tang, G. Xue, C. Chandler, and W. Zhang, "Interference-aware Routing in Multihop Wireless Networks Using Directional Antennas," in *IEEE INFOCOM 2005, 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, 2005, pp. 751-760 vol. 1.
- [55] K.-T. Feng, "LMA: Location- and Mobility-Aware Medium-Access Control Protocols for Vehicular Ad Hoc Networks Using Directional Antennas," *IEEE Transactions on Vehicular Technology*, vol. 56, pp. 3324-3336, 2007.
- [56] G. Jakllari, W. Luo, and S. V. Krishnamurthy, "An Integrated Neighbor Discovery and MAC Protocol for Ad Hoc Networks Using Directional

- Antennas," *IEEE Transactions on Wireless Communications*, vol. 6, pp. 1114-1024, 2007.
- [57] G. Li and J. Zhu, "Performance Analysis on Utilizing Directional Antenna in High-Density WLAN," in *Sixth International Conference on Networking*, 2007, pp. 90-90.
 - [58] H. Bolcskel, A. J. Paulraj, K. V. S. Hari, R. U. Nabar, and W. W. Lu, "Fixed Broadband Wireless Access: State of the Art, Challenges, and Future Directions," *IEEE Communications Magazine*, vol. 39, pp. 100-108, 2001.
 - [59] F. Ono and K. Sakaguchi, "Multiple Access Interference Cancellation and Link Multiplexing for MIMO Mesh Network," in *IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007.*, 2007, pp. 1-5.
 - [60] D. Wang, S. Yang, Y. Hu, and D. Teng, "9Square: A New Architecture for MIMO WMN," in *International Conference on Wireless Communications, Networking and Mobile Computing*, 2006, pp. 1-4.
 - [61] F. Ye, Q. Chen, and Z. Niu, "End-to-End Throughput-Aware Channel Assignment in Multi-Radio Wireless Mesh Networks," in *IEEE Global Telecommunications Conference*, 2007, pp. 1375-1379.
 - [62] A. H. M. Rad and V. W. S. Wong, "Cross-Layer Fair Bandwidth Sharing for Multi-Channel Wireless Mesh Networks," *IEEE Transactions on Wireless Communications*, vol. 7, pp. 3436-3445, Sep. 2008.
 - [63] A. H. Mohsenian-Rad and V. W. S. Wong, "Joint logical topology design, interface assignment, channel allocation, and routing for multi-channel wireless mesh networks," *IEEE Transactions on Wireless Communications*, vol. 6, pp. 4432-4440, Dec. 2007.
 - [64] A. P. Subramanian, H. Gupta, S. R. Das, and J. Cao, "Minimum Interference Channel Assignment in Multiradio Wireless Mesh Networks," *IEEE Transactions on Mobile Computing*, vol. 7, pp. 1459-1473, 2008.

- [65] Y. Zhu and Z. Niu, "User-aware Rate Adaptive Control for IEEE 802.11-based Ad Hoc Networks," in *IEEE Global Telecommunications Conference*, 2005, pp. 5 pp.-2609.
- [66] M. Ma, J. Zheng, Y. Zhang, Z. Shao, and M. Fujise, "A Power-Controlled Rate-Adaptive MAC Protocol to Support Differentiated Service in Wireless Ad Hoc Networks," in *IEEE GLOBECOM 2006*, 2006, pp. 1-5.
- [67] M. B. Pursley and T. C. Royster, "Low-Complexity Adaptive Transmission for Cognitive Radios in Dynamic Spectrum Access Networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, pp. 83-94, Jan. 2008.
- [68] H. T. Cheng and W. Zhuang, "Joint Power-Frequency-Time Resource Allocation in Clustered Wireless Mesh Networks," *IEEE Network*, vol. 22, pp. 45-51, Jan.-Feb. 2008.
- [69] K. Shih, Y. Chen, and C. Chang, "A Physical/Virtual Carrier-sense-based Power Control MAC Protocol for Collision Avoidance in Wireless Ad Hoc Networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. PP, pp. 1-1.
- [70] A. Ghasemi and E. S. Sousa, "Spectrum Sensing in Cognitive Radio Networks: Requirements, Challenges and Design Trade-offs," *IEEE Communications Magazine*, vol. 46, pp. 32-39, Apr. 2008.
- [71] H. Kim and K. G. Shin, "In-band spectrum sensing in cognitive radio networks: energy detection or feature detection?," presented at the Proceedings of the 14th ACM international conference on Mobile computing and networking, San Francisco, California, USA, 2008.
- [72] G. Ganesan, Y. Li, B. Bing, and S. Li, "Spatiotemporal Sensing in Cognitive Radio Networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, pp. 5-12, Jan. 2008.
- [73] K. R. Chowdhury and I. F. Akyildiz, "Cognitive Wireless Mesh Networks with Dynamic Spectrum Access," *IEEE Journal on Selected Areas in Communications*, vol. 26, pp. 168-181, Jan. 2008.

- [74] H. Su and X. Zhang, "Cross-Layer Based Opportunistic MAC Protocols for QoS Provisionings Over Cognitive Radio Wireless Networks," *Selected Areas in Communications, IEEE Journal on*, vol. 26, pp. 118-129, 2008.
- [75] H. Skalli, S. Ghosh, S. K. Das, L. Lenzini, and M. Conti, "Channel Assignment Strategies for Multiradio Wireless Mesh Networks: Issues and Solutions," *IEEE Communications Magazine*, vol. 45, pp. 86-95, Nov. 2007.
- [76] M. Thoppian, S. Venkatesan, and R. Prakash, "CSMA-Based MAC Protocol For Cognitive Radio Networks," in *IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks*, 18-21 June 2007, pp. 1-8.
- [77] 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, pp. 46-54, 2009.
- [78] H. Wu, F. Yang, K. Tan, J. Chen, Q. Zhang, and Z. Zhang, "Distributed Channel Assignment and Routing in Multiradio Multichannel Multihop Wireless Networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 1972-1983, 2006.
- [79] G. Cheng, W. Liu, Y. Li, and W. Cheng, "Joint On-Demand Routing and Spectrum Assignment in Cognitive Radio Networks," in *IEEE ICC 2007*, 2007, pp. 6499-6503.
- [80] Y. Liu and D. Grace, "Improving Capacity for Wireless Ad Hoc Communications Using Cognitive Routing," in *CrownCom 2008*, 2008, pp. 1-6.
- [81] H. Ma, L. Zheng, X. Ma, and Y. Luo, "Spectrum Aware Routing for Multi-Hop Cognitive Radio Networks with a Single Transceiver," in *3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, 2008, pp. 1-6.
- [82] A. Zubow, M. Kurth, and J. P. Redlich, "An Opportunistic Cross-Layer Protocol for Multi-Channel Wireless Networks," in *IEEE PIMRC 2007*, 2007, pp. 1-5.

- [83] D. Murray, M. Dixon, and T. Koziniec, "Scanning Delays in 802.11 Networks," in *The 2007 International Conference on Next Generation Mobile Applications, Services and Technologies, 2007. NGMAST '07.*, 2007, pp. 255-260.
- [84] R. Chandra and P. Bahl, "MultiNet: Connecting to Multiple IEEE 802.11 Networks Using a Single Wireless Card," in *INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies*, 2004, pp. 882-893 vol.2.
- [85] A. C. Talay and D. T. Altılar, "ROPCORN: Routing Protocol for Cognitive Radio Ad Hoc Networks," in *International Conference on Ultra Modern Telecommunications & Workshops*, 2009, pp. 1-6.
- [86] I. Pefkianakis, S. H. Y. Wong, and S. Lu, "SAMER: Spectrum Aware Mesh Routing in Cognitive Radio Networks," in *IEEE DySPAN 2008.*, 2008, pp. 1-5.
- [87] I. Filippini, E. Ekici, and M. Cesana, "Minimum Maintenance Cost Routing in Cognitive Radio Networks," in *IEEE MASS 2009*, 2009, pp. 284-293.
- [88] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking Spectrum Gridlock With Cognitive Radios: An Information Theoretic Perspective," *Proceedings of the IEEE*, vol. 97, pp. 894-914, 2009.
- [89] T. Weiss, J. Hillenbrand, A. Krohn, and F. K. Jondral, "Mutual interference in OFDM-based spectrum pooling systems," in *IEEE 59th Vehicular Technology Conference, 2004. VTC 2004-Spring. 2004* 2004, pp. 1873-1877 Vol.4.
- [90] G. Bansal, M. J. Hossain, and V. K. Bhargava, "Optimal and Suboptimal Power Allocation Schemes for OFDM-based Cognitive Radio Systems," *IEEE Transactions on Wireless Communications*, vol. 7, pp. 4710-4718, 2008.
- [91] L. B. Le and E. Hossain, "Resource Allocation for Spectrum Underlay in Cognitive Radio Networks," *IEEE Transactions on Wireless Communications*, vol. 7, pp. 5306-5315, 2008.

- [92] R. Zhang, "On peak versus average interference power constraints for protecting primary users in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 8, pp. 2112-2120, 2009.
- [93] G. Baldini, T. Sturman, A. Biswas, R. Leschhorn, G. Godor, and M. Street, "Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead," *Communications Surveys & Tutorials, IEEE*, vol. PP, pp. 1-25.
- [94] J. L. Burbank, "Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security," in *3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008.*, 2008, pp. 1-7.
- [95] R. Chen, J.-M. Park, and J. H. Reed, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, pp. 25-37, 2008.
- [96] H. Li and Z. Han, "Dogfight in Spectrum: Combating Primary User Emulation Attacks in Cognitive Radio Systems, Part I: Known Channel Statistics," *IEEE Transactions on Wireless Communications*, vol. 9, pp. 3566-3577, 2010.
- [97] F. R. Yu, H. Tang, H. Minyi, L. Zhiqiang, and P. C. Mason, "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," in *Military Communications Conference, 2009. MILCOM 2009. IEEE*, 2009, pp. 1-7.
- [98] S. Xu, Y. Shang, and H. Wang, "Eigenvalues based spectrum sensing against untrusted users in cognitive radio networks," in *4th International Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2009. CROWNCOM '09.*, 2009, pp. 1-6.
- [99] L. Santhanam, X. Bin, and D. Agrawal, "Selfishness in mesh networks: wired multihop MANETs," *Wireless Communications, IEEE*, vol. 15, pp. 16-23, 2008.

- [100] Q. Guan, F. R. Yu, S. Jiang, and G. Wei, "Prediction-Based Topology Control and Routing in Cognitive Radio Mobile Ad Hoc Networks," *IEEE Transactions on Vehicular Technology*, vol. 59, pp. 4443-4452, 2010.
- [101] H. Khalife, N. Malouch, and S. Fdida, "Multihop Cognitive Radio Networks: To Route or Not to Route," *IEEE Network*, vol. 23, pp. 20-25, 2009.
- [102] 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, pp. 106-117, 2008.
- [103] K. Ghaboosi, M. Latva-aho, and Y. Xiao, "A Distributed Multi-channel Cognitive MAC Protocol for IEEE 802.11s Wireless Mesh Networks," in *3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, 2008, pp. 1-8.
- [104] 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, pp. 1339-1352, 2009.
- [105] H. Khalife, S. Ahuja, N. Malouch, and M. Krunz, "Probabilistic Path Selection in Opportunistic Cognitive Radio Networks," in *IEEE GLOBECOM 2008*, 2008, pp. 1-5.
- [106] C. Cormio and K. R. Chowdhury, "A survey on MAC protocols for cognitive radio networks," *Ad Hoc Networks*, vol. 7, pp. 1315-1329, 2009.
- [107] H. T. Friis, "A Note on a Simple Transmission Formula," *Proceedings of the IRE*, vol. 34, pp. 254-256, 1946.
- [108] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE Journal on Selected Areas in Communications*, vol. 18, pp. 535-547, 2000.
- [109] P. Mahasukhon, M. Hempel, C. Song, and H. Sharif, "Comparison of Throughput Performance for the IEEE 802.11a and 802.11g Networks," in

21st International Conference on Advanced Information Networking and Applications, 21-23 May 2007, pp. 792-799.

- [110] S. Ju and J. B. Evans, "Spectrum-Aware Routing Protocol for Cognitive Ad-Hoc Networks," in *IEEE Global Telecommunications Conference*, 2009, pp. 1-6.
- [111] S. Deng, J. Chen, H. He, and W. Tang, "Collaborative Strategy for Route and Spectrum Selection in Cognitive Radio Networks," in *Future Generation Communication and Networking (FGCN 2007)*, 2007, pp. 168-172.
- [112] Z. Yang, G. Cheng, W. Liu, W. Yuan, and W. Cheng, "Local Coordination Based Routing and Spectrum Assignment in Multi-Hop Cognitive Radio Networks," *Mob. Netw. Appl.*, vol. 13, pp. 67-81, 2008.
- [113] 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 Global Telecommunications Conference*, 2008, pp. 1-5.
- [114] S. Biswas and R. Morris, "ExOR: Opportunistic Multi-Hop Routing for Wireless Networks," *SIGCOMM Comput. Commun. Rev.*, vol. 35, pp. 133-144, 2005.
- [115] E. Rozner, J. Seshadri, Y. Mehta, and L. Qiu, "SOAR: Simple Opportunistic Adaptive Routing Protocol for Wireless Mesh Networks," *IEEE Transactions on Mobile Computing*, vol. 8, pp. 1622-1635, 2009.
- [116] 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, pp. 430-438.
- [117] K. Chowdhury and I. Akyildiz, "OFDM based Common Control Channel Design for Cognitive Radio Ad Hoc Networks," *To appear in the IEEE Transactions on Mobile Computing*.

- [118] K. C. How, M. Ma, and Y. Qin, "A MAC-Layer QoS Provisioning Protocol for Cognitive Radio Networks," *Wireless Personal Communications*, pp. 1-20, 2011.
- [119] S. Geirhofer, L. Tong, and B. M. Sadler, "A Measurement-Based Model for Dynamic Spectrum Access in WLAN Channels," in *IEEE Military Communications Conference, 2006. MILCOM 2006.*, 2006, pp. 1-7.
- [120] D. Datla, R. Rajbanshi, A. M. Wyglinski, and G. J. Minden, "Parametric Adaptive Spectrum Sensing Framework for Dynamic Spectrum Access Networks," in *2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007.* , 2007, pp. 482-485.
- [121] Q. Zhao, L. Tong, S. Ananthram, 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, pp. 589-600, 2007.
- [122] E. M. Royer and C.-K. Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," *IEEE Personal Communications*, vol. 6, pp. 46-55, 1999.
- [123] M. Karaliopoulos, "Assessing the vulnerability of DTN data relaying schemes to node selfishness," *IEEE Communications Letters*, vol. 13, pp. 923-925, 2009.
- [124] Y. Li, P. Hui, D. Jin, L. Su, and L. Zeng, "Evaluating the Impact of Social Selfishness on the Epidemic Routing in Delay Tolerant Networks," *IEEE Communications Letters*, vol. 14, pp. 1026-1028, 2010.
- [125] K. R. Chowdhury and I. F. Akyldiz, "OFDM-Based Common Control Channel Design for Cognitive Radio Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 10, pp. 228-238, 2011.

- [126] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, pp. 120-126, 1978.