Intelligent Spectrum Management Techniques for Wireless Cognitive Radio Networks

Yasir Ahmed Abdullah Al-Mathehaji

Newcastle University

Newcastle upon Tyne, UK

A thesis submitted for the degree of

Doctor of Philosophy

April 2017

To my beloved parents and siblings.

Acknowledgements

All praise is due to Allah (God), I thank him and seek his help, guidance, and forgiveness. Working on the PhD has been a wonderful and often overwhelming experience. I am indebted to many people for making the time working on my PhD an unforgettable experience.

I would like to express my greatest and deepest gratitude to my supervisor Professor Said Boussakta for his motivational discussions, consistent support, and encouragement throughout my academic journey. His valuable comments and feedbacks have helped in enriching my research. I would also like to thank Dr. Martin Johnston for serving as a co-supervisor and for his productive discussions, constructive comments and suggestions.

My gratitude and appreciation to my colleagues and friends at Communications, Sensors, Signal and Information Processing (ComS2IP) group. The electrical and electronic engineering school administration and staff definitely deserve many thanks for helping out in numerous issues over the past years.

I would also like to thank the Higher Committee For Education Development in Iraq (HCED-Iraq) for providing me with an opportunity and all the funding to pursue my PhD degree.

Last but not the least, I would like to thank all my family members and friends. No words can express my gratitude for their unlimited love, support and encouragement in my journey to reach the highest level of education.

Abstract

This thesis addresses many of the unique spectrum management challenges in CR networks for the first time. These challenges have a vital effect on the network performance and are particularly difficult to solve due to the unique characteristics of CR networks. Specifically, this thesis proposes and investigates three intelligent spectrum management techniques for CR networks. The issues investigated in this thesis have a fundamental impact on the establishment, functionality and security of CR networks.

First, an intelligent primary receiver-aware message exchange protocol for CR ad hoc networks is proposed. It considers the problem of alleviating the interference collision risk to primary user communication, explicitly to protect primary receivers that are not detected during spectrum sensing. The proposed protocol achieves a higher measure of safeguarding. A practical scenario is considered where no global network topology is known and no common control channel is assumed to exist.

Second, a novel CR broadcast protocol (CRBP) to reliably disseminate the broadcast messages to all or most of the possible CR nodes in the network is proposed. The CRBP formulates the broadcast problem as a bipartite-graph problem. Thus, CRBP achieves a significant successful delivery ratio by connecting different local topologies, which is a unique feature in CR ad hoc networks.

Finally, a new defence strategy to defend against spectrum sensing data falsification attacks in CR networks is proposed. In order to identify malicious users, the proposed scheme performs multiple verifications of sensory data with the assistance of trusted nodes.

Contents

List of Figures

List of Tables

Nomenclature

Symbols

$\mathbf{\Phi_{idle}}$	Available channel set
$\mathbf{\Psi}$	Euclidean distance
$\mathbf{e(i,j)}$	Link that connects CR_i and CR_j
$\mathbf{E_k}$	Encryption function
$\mathbf{G(X,Y,E)}$	Bipartite graph
$\mathbf{H}(.)$	Hash function
$\mathbf{Q_F}$	Probability of a false alarm
$\mathbf{Q_{MD}}$	Probability of missed detection
$\mathbf{Q_{SSDF}}$	Probability of SSDF attack
$\mathbf{S_{pack}}$	Group of s signatures
$\mathbf{Z(PU)}$	Primary user protected zone

Acronyms/Abbreviations

ACK	Acknowledgement
AOD	Average Overlapping Degree
BAIS	Byzantine Attacks Identification Scheme
BCS	Broadcast Channels Set
BS	Base Station
CAF	Cyclic Autocorrelation Function

CCC	Common Control Channel
CLT	Central Limit Theorem
CogNeA	Cognitive Networking Alliances
COOPON	Cooperative Cognitive Neighbouring Nodes
CR	Cognitive Radio
CRBP	Cognitive Radio Broadcast Protocol
CRC	Cognitive Radio Connectivity
CRCN	Cognitive Radio Cognitive Network
CRN	Cognitive Radio Network
CSD	Cyclic Spectrum Density
CSS	Channel Set Size
CSS	Collaborative Spectrum Sensing
DBP	Distributed Broadcasting Protocol
DCR	Decision Convergence Ratio
DSA	Dynamic Spectrum Access
ETRI	Electronics and Telecommunications Research Institute
FC	Fusion Centre
FCC	Federal Communications Commission
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers
ISM	Industrial, Scientific and Medical
LEDS	Location-aware end-to-end Data Security
MAC	Medium Access Control
MAC	Message Authenticated Code

MANET	Mobile Ad-Hoc Network
MCRC	Maximize Cognitive Radio Connectivity
MPUP	Maximize Primary User Protection
NCR	Network Connectivity Ratio
NS	Network Simulator
Ofcom	Office of Communications
PDR	Packet Delivery Ratio
PHY	Physical Layer
PIR	Potential Interference Ratio
PU	Primary User
PUBS	Primary User Base Station
PUE	Primary User Emulator
QoS	Quality of Service
RCSSS	Reliable Collaborative Spectrum Sensing Scheme
RF	Radio-Frequency
RS	Random Strategy
SB	Selective Broadcasting
SCC	Standards Coordinating Committee
SDR	Software Defined Radio
SNR	Signal-to-Noise Ratio
SSDF	Spectrum Sensing Data Falsification
SURF	Select Unoccupied Radio Frequency
TC	Tuning Channel
TVWS	TV white space

UWB	Ultra-Wideband
VANET	Vehicular Ad-Hoc Network
WMN	Wireless Mesh Network
WRAN	wireless region area network
WSN	Wireless Sensor Network

Chapter 1

Introduction

The demand for wireless traffic has been substantially increased in the last decade due to the proliferation of wireless technology and the globalisation of smart phones, Internet-based applications and services [1]. However, according to the Federal Communications Commission (FCC), the limited natural spectrum resources do not satisfy the dramatic spectrum demand, as most of the radio spectrum for wireless communications has already been allocated. Recent spectrum measurements reveal that the allocated spectrum is underutilized by up to 85% [2]. Hence, the FCC highlights that the current spectrum scarcity problem is explained by inefficient and inflexible regulations rather than the physical spectrum shortage. In order to overcome the incompatibility between the spectrum underutilization and the increase in the wireless spectrum demand, the FCC has suggested a new paradigm for dynamically accessing the assigned spectrum bands, known as cognitive radio technology.

Cognitive Radio (CR) has emerged as a revolutionary technology to deal with the disparity between the continuously increasing demand for wireless radio spectrum and the spectrum underutilization by licensed users based on Dynamic Spectrum Access (DSA) [3]. There are two types of users in the CR networks: 1) licensed user (usually referred to as primary user (PU)) who can operate in a certain range of frequencies at any time within a geographical area and 2) unlicensed user (usually referred to as cognitive radio user (CR)) who can opportunistically use the vacant licensed spectrum bands assigned to licensed users. Unlike conventional spectrum policy in which designated parts of the spectrum are allocated specifically for exclusive use to licensed users, CR technology permits unlicensed users to opportunistically and dynamically take advantage of the licensed spectrum resources that might

be available at a certain time and location [4]. These resources can potentially be deployed in several bands of different bandwidth. Furthermore, the availability of this spectrum might dynamically change over time, as the primary users occupy or free up a given band. However, the operations of any CR user should not affect the communications of primary users.

1.1 CR Fundamental Functionalities

The idea of CR technology is to enable CR users to opportunistically use the vacant licensed spectrum. Therefore, new and essential functionalities are needed to support this adaptivity in CR networks [5]. The fundamental functionalities for CR networks can be summarized as follows:

(i) Spectrum sensing: Spectrum sensing technology is considered a fundamental functionality of Cognitive Radio Networks (CRNs). CR nodes sense primary user activity and determine channel availability in order to allow CR users access to vacant licensed bands in an opportunistic manner [6]. Hence, the accuracy of this sensory information is very important for cognitive radio network communications. Otherwise, CR traffic may cause interference to the licensed users.

(ii) Spectrum management: CR users select the best available spectrum band which meets their communication requirements. The captured spectrum should not cause negative interference to PUs. Amongst all available spectrum bands, CR users choose the best spectrum channel to meet the different Quality-of-Service (QoS) requirements. The spectrum management functions are so important for the CR network operation [7]. These management functions may be labelled as: 1) spectrum analysis and 2) spectrum decision.

(iii) Spectrum mobility: CR technology allows CR users to access the licensed spectrum in a dynamic and opportunistic manner. Therefore, based on the radio spectrum environment, CR users can change the frequency channel to operate in the most suitable available channel. The transition to a better spectrum band should respect the outlined requirements in order to achieve seamless communication. In addition, CR users should vacate the spectrum

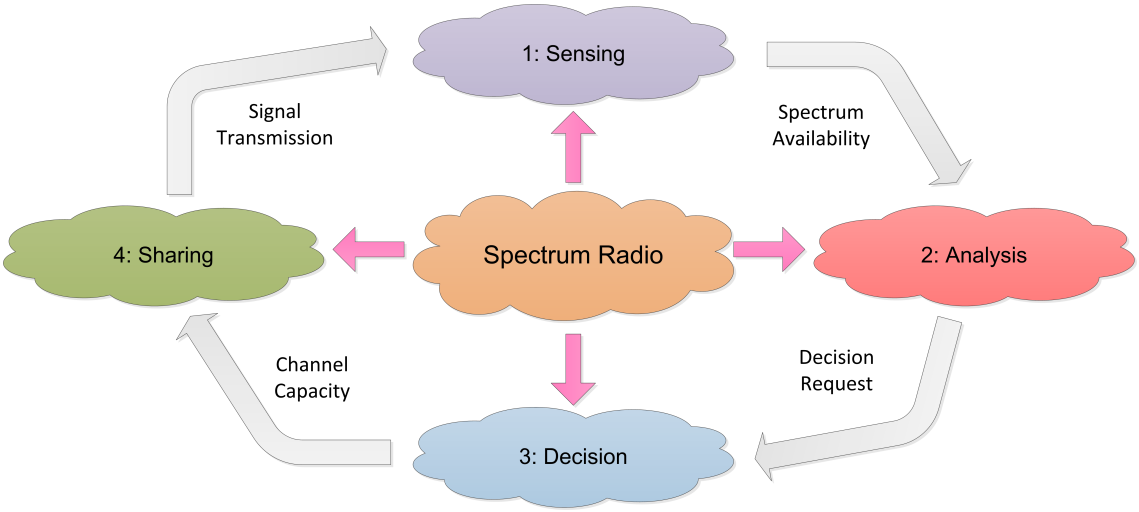


Figure 1.1: A typical cognitive radio cycle

when a licensed user is detected to be active on the same channel. This is a new and unique feature in CR networks, where CR users determine, identify and hop to new available spectrum bands in order to continue their transmissions when the current spectrum band is not available.

(iv) Spectrum sharing: CR nodes need to coordinate access to available channels in order to fairly share the spectrum through scheduling methods. The main objective of the spectrum sharing is to improve spectrum efficiency by jointly allocates the available resources among different CR users.

A typical cognitive cycle that states the major functionalities of CR and is relevant to reconfigurability and capability is illustrated in Figure 1.1.

1.2 Overview of the Proposed Intelligent Spectrum Techniques

In the last decade, several important studies have been carried out in the field of CR Networks. These works have mainly focused on spectrum sensing and spectrum sharing [5]. However, spectrum management of CR technology remains underdeveloped due to a lack of sufficient research efforts. In this research, the design of intelligent spectrum management techniques for wireless CR networks is investigated. In order to form an operative framework for CR networks, it is essential to interconnect most of the fundamental CR functionalities (i.e., spectrum sensing, spectrum sharing, and spectrum decision). Figure 1.2 illustrates the overview of the

proposed intelligent techniques for spectrum management. The issues investigated in this research have crucial impact on the establishment, functionality, performance and security of CR networks. They are fundamental for laying the foundations of CR networks and operating networking protocols for reliable communications in CR networks.

First of all, we propose a fully-distributed control information exchange protocol for CR ad hoc networks that makes the following contributions: i) alleviates risk of collision in PU communications; ii) guarantees protection for PU-receivers and iii) provides a highly successful broadcast ratio. We consider several practical scenarios in our design: 1) limited knowledge of the network environment; 2) no common control channel is assumed to exist and 3) the sets of available channels of neighbouring CR nodes are not assumed to be the same. To the best of our knowledge, this is the first work that investigates the design of broadcasting protocol under a PU-receiver protection scenario for CR ad hoc networks. The main performance metrics for our proposed protocol are: PU-receivers protection from harmful interference (i.e., the interference collision risk of CR broadcast packets with PU communications) and the successful packet delivery ratio (i.e., the average number of packets successfully delivered in the network).

Furthermore, a distributed reliable Cognitive Radio Broadcast Protocol (CRBP) for cognitive radio ad hoc networks is proposed that addresses the problems of network connectivity and reliable data dissemination. The proposed protocol focuses on multi-hop CR ad hoc networks without specific network topology assumptions, where each user is equipped with a single transceiver and has limited knowledge of the network environment. A key novelty of the proposed CRBP is the formulation of the broadcast problem from the viewpoint of connecting different local topologies, which is a unique feature in cognitive radio networks. We map the network topologies and the spectrum observations as a bipartite graph, which allows the channel selection undertaken at each node to capture the spectrum information and the environmental topologies of all the neighbouring nodes. In addition, we believe that the consideration of different topologies in the same neighbourhood, transmitter-receiver synchronization and the coordination of the broadcast process without a common channel uniquely distinguishes CRBP from the other works in the literature.

Finally, a novel security scheme is proposed to fight against Spectrum Sensing

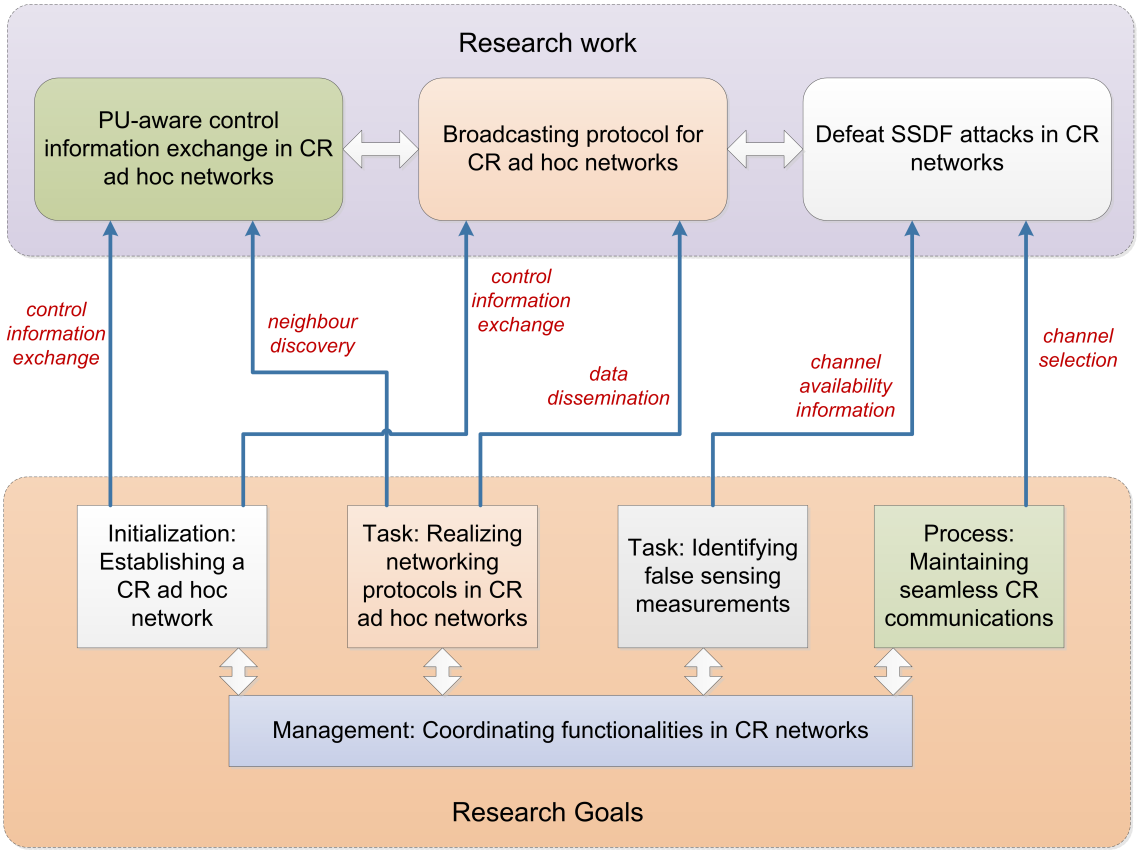


Figure 1.2: Illustration of the proposed intelligent techniques for spectrum management.

Data Falsification (SSDF) attacks and identify malicious CR users whom report fraudulent sensing data in CR networks. Multi-levels of defence are used to maintain an adequate level of protection. First, we employ a secure authentication protocol between the Fusion Centre (FC) and the collaborative nodes. Second, three tiers of verification, the unique signature of the node, the cell-mates signatures and the seal of the trusted nodes have to be checked by the FC to validate the received sensory data. Finally, an efficient reputation-based fusion scheme is used as a third level of defence, which enables the FC to select trusted nodes with the objective of ensuring the reliability of the received sensory information.

1.3 Thesis Outline

This thesis is organized as follows: Chapter 2 presents the technical background, broadcasting challenges, spectrum sensing and security threats in CR networks. This chapter also reviews the related work on broadcasting protocols and security schemes in CR networks. In Chapters 3, 4 and 5, we propose, analyse and evaluate three spec-

trum management techniques for CR networks. In particular, Chapter 3 presents a distributed control information exchange protocol for CR ad hoc networks. Two broadcasting schemes, *maximize PU protection* (MPUP) and *maximize CR connectivity* (MCRC) are proposed in this chapter. Chapter 4 elaborates the novel design of a distributed reliable *cognitive radio broadcast protocol* (CRBP) for cognitive radio ad hoc networks. The proposed CRBP formulates the broadcast problem from the viewpoint of connecting different local topologies, which is a unique feature in cognitive radio networks. Chapter 5 describes a novel defeating scheme based on multi-layer security and reputation evaluation that can defeat and identify SSDF attackers trying to inject false sensory information into the central learning engine. In Chapter 6, we conclude the thesis contributions and discuss future research.

1.4 Research Publications

The outcome of this thesis has resulted in the following publications:

- Y. Al-Mathehaji, S. Boussakta, M. Johnston and H. Fakhrey, "CRBP: A broadcast protocol for cognitive radio ad hoc networks", in *IEEE International Conference on Communications (ICC)*, pp. 7540-7545, June 2015.

- Y. Al-Mathehaji, S. Boussakta, M. Johnston and J. Hussein, "Primary receiver-aware opportunistic broadcasting in cognitive radio ad hoc networks", in *IEEE Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 30-35, July 2016.

- Y. Al-Mathehaji, S. Boussakta and M. Johnston, "Reliable broadcast over cognitive radio networks: a bipartite graph-based algorithm", Cognitive Radio, Dr. Tonu Trump (Ed.), InTech, DOI: 10.5772/intechopen.69216, 2017. Available from: https://www.intechopen.com/books/cognitive-radio/reliable-broadcast-over-cognitive-radio-networks-a-bipartite-graph-based-algorithm

- Y. Al-Mathehaji, S. Boussakta, M. Johnston and H. Fakhrey, "Defeating SSDF attacks with trusted nodes assistance in cognitive radio networks", in *IEEE Sensors Letters*, 2017 (Accepted).

- Y. Al-Mathehaji, S. Boussakta, M. Johnston and H. Fakhrey, "Reliable collaborative spectrum sensing for cognitive radio networks in malicious environ-

ments", submitted for *IEEE Transactions on Cognitive Communications and Networking*, 2017.

Chapter 2

Background and Related Work

This chapter discusses the operation of broadcasting in CR ad hoc networks and the security issues in CR networks. It reviews existing research related to broadcasting protocols and defending schemes against SSDF attacks.

This chapter is organized as follows. The background on CR networks are first introduced in Section 2.1. CR Network standards are listed in Section 2.2. The broadcasting problems in CR ad hoc networks are presented in Section 2.3. The unique challenges of broadcasting in CR ad hoc networks are reviewed in Section 2.4. The state-of-the-art technologies used in broadcasting are discussed in 2.5. Local and cooperative spectrum sensing in CR networks are covered in Section 2.6. The security threats in CR networks are presented in Section 2.7. Current defending schemes against SSDF attacks are reviewed in Section 2.8. We conclude this chapter with a summary in Section 2.9.

2.1 Background on CR Networks

In 1999, J. Mitola and G. Maguire invented the term cognitive radio [8]. However, depending on the focus of research and the applications, people have different understanding and expectations of CR. Therefore, there is no definition of CR commonly accepted [9], [10], [11]. For example, the FCC views CR as a radio that can change its transmitter parameters based on interactions with the environment in which it operates. The majority of cognitive radios will probably be SDRs (Software Defined Radios), but possessing software and being field programmable are not requirements of a cognitive radio [12]. Other definitions stress the importance of learning capability, while some may emphasise the importance of radio flexibility. CR is significantly

important for addressing the spectrum scarcity problem and spectrum conservation. Since it is able to share the licensed spectrum with the primary users and guarantee that interference is kept to a minimum, CR may be considered as an environmentally friendly radio solution [13].

According to the deployment scenario, CR networks can be classified into two basic types of networks, one is the *infrastructure-based CR networks* and the second is the *infrastructure-less CR networks*. In the infrastructure-based CR networks, all CR nodes directly communicate with the central network entity, which is responsible for managing the network operations, for instance, spectrum sensing and spectrum assignment. On the other hand, in the infrastructure-less CR networks, also known as CR ad hoc network, no central entity is present. Hence, CR nodes have to rely on themselves for spectrum sensing, assignment and management. CR networks can be useful if applied in demanding environments, such as public safety, civil emergencies, natural disasters and military operations.

2.2 CR Network Standards

The rapid growth of research in the field of CR technology has motivated standardisation institutes, such as FCC, Institute of Electrical and Electronics Engineers (IEEE), and Office of Communications (Ofcom) to develop standards for CR networks.

- ***IEEE 802.22:*** The first complete CR-base standards that support opportunistical communication in the TV bands is the IEEE 802.22 wireless region area network (WRAN) [14]. This technology is developed as an infrastructure-based CR network and initially presumed to work in rural areas or areas suffering from limited communications infrastructure. It is expected to operate in the TV bands 54-862 MHz with up to 47 channels. These spectrum bands permit a typical transmission range from 17-30 km with a maximum communication range of 100 km.

- ***SCC41:*** Standards Coordinating Committee 41 (SCC41) (formerly known as P1900) addresses techniques of dynamic spectrum access [15]. This technology considers software defined radio as the key enabler for DSA among 3G/4G, WiFi, and WiMax networks [16].

- ***IEEE 802.11af:*** IEEE 802.11af [17] is a technology developed for opportunistic utilization of the TV white space (TVWS) portion of the spectrum. This standard is developed for ad hoc configuration. It is expected to utilize the TV bands 54-790 MHz with a total of 39 channels. In addition, this standard permits bond/aggregate up to 4 channels and allows a maximum transmission communication of 5 km.

- ***CogNeA:*** CogNeA(Cognitive Networking Alliances) standard is an open industry alliance that proposes a new wireless communication paradigm for low power personal/portable application on the TVWS [18]. Philips, HP, Samsung Electro-Mechanics and ETRI (Electronics and Telecommunications Research Institute) form the board of directors of CogNeA. CogNeA's promising applications include: in-home high definition multi-media networking, tele-health, Internet access for communities, campuses using ad hoc mesh networking, and home automation and control.

2.3 Broadcasting in CR ad hoc Networks

When a wireless ad hoc network is deployed and before exchanging any control information, each user initially only acquires its own local network information and is unaware of other users network information. However, the realization of most network protocols in the ad hoc network depends on exchanging control information among neighbouring nodes. This fundamental information is usually sent out as a network-wide broadcast messages (i.e. messages that are sent out to all users in a network). Broadcasting is one of the most classical operations in wireless networks, as well as in distributed CR networks [19]. In CR networks, several specific functionalities such as spectrum sensing, channel assignment and routing information are achieved through local or global broadcast messages. In addition, some important data such as alarm signals and emergency messages are also delivered via network wide broadcasts [20]. In traditional single-channel or multi-channel ad hoc networks, all nodes follow the rules of a precise wireless standard. Due to uniform channel availability, broadcast is easily implemented as all nodes can be tuned to a single common channel. Thus, the source node only needs to transmit over one channel to let all its neighbouring nodes receive the broadcast message. However, broad-

casting in cognitive radio ad hoc networks is a much more challenging task. The complexity emerges from the fact that harmful interference with the transmissions of primary users must be avoided. Furthermore, different CR users might acquire different channels at different times depending on their locations and the activity of primary users. Therefore, the CR source node may have to broadcast the message using different channels in order to deliver the broadcast message to all neighbours. Indeed, the successful delivery of the broadcast message to neighbouring nodes in CR ad hoc networks relies on connecting different local topologies. The broadcast channel(s) should be carefully selected and dynamically allocated to guarantee the network operation.

In the literature, numerous works have extensively studied the broadcasting issue in traditional ad hoc networks, Mobile Ad-Hoc Networks (MANETs), Wireless Mesh Networks (WMNs), Vehicular Ad-Hoc Networks (VANETs) and Wireless Sensor Networks (WSNs) [21], [22], [23], [24], [25], [26], [27], [28], [29], [30]. All these schemes assume that the channel availability is uniform for all nodes, hence only single channel is used for broadcasting. Therefore, extending traditional broadcast protocols to CR ad hoc networks is not feasible as they cannot guarantee optimal performance.

2.4 Challenges of Broadcasting in CR ad hoc Networks

Designing a reliable broadcast protocol for wireless CR ad hoc networks is a very challenging task in practical scenarios, where avoiding collisions with primary communications and achieving a high successful broadcast delivery ratio are essential. In traditional ad hoc networks, all nodes can tune to the same channel due to the uniformity of channel availability. However, in CR ad hoc networks, the opportunity of a common channel available for all CR nodes may not exist. In addition, different CR users might acquire different channels at different times. This difference in channel availability leads to unique challenges when considering the performance of broadcasting protocols under practical scenarios in CR ad hoc networks.

- Most importantly, different from traditional ad hoc networks, single-hop broadcasting in CR ad hoc networks is not always successful in an error-free envi-

ronment. This is because in traditional ad hoc networks, when the source node transmits the broadcast message, all its single-hop neighbouring nodes receive the broadcast message when they tune to the same channel. However, the availability of a common channel for all neighbouring nodes in CR ad hoc networks may not exist [31], [32], [33], [34], [35]. Correspondingly, the broadcast operation may fail. Furthermore, even if a common channel is available, the source CR node and its neighbours may not be able to tune to the common channel at the same time, which will also result in an unsuccessful broadcast.

- Secondly, in traditional ad hoc networks, the respective locations of a pair of nodes do not have an effect on the successful delivery of the broadcast message as long as they are within the communication range of each other. However, in CR ad hoc networks, the successful delivery of a broadcast message is influenced by the sender and the receiver's corresponding locations. This is because the channels availability of a CR node is acquired based on the sensing measurements in its vicinity. Accordingly, CR nodes that are in the same proximity have a similar set of available channels and they may have better delivery ratio, compared to CR nodes that are far away from each other as their available channels are usually less similar.

- Furthermore, in the case of CR ad hoc networks, where no centralized entity is presented, broadcasting is much complicated, due to CR nodes have to locally analyse the collected information to select the best available channel for data dissemination. Intelligent channel selection may lead to higher data dissemination reachability. In addition, considering PU activity during channel selection can reduce the successful delivery ratio of the broadcast messages.

- Finally, in traditional ad hoc networks, the single-hop broadcast delay is often one time slot in an error-free environment. As the source node only requires one time slot to deliver the broadcast message to all its neighbouring nodes. On the other hand, in CR ad hoc networks, it is always more than one time slot. This is due to the variance in the channel availability at different times and different locations. Therefore, the source node may have to broadcast over multiple channels, hence it may need more than one time slot to finish the broadcasting. The number of neighbouring nodes and the channel availability

are considered as the main factors that influence the single-hop broadcast delay in CR ad hoc networks.

2.5 Existing Broadcast Protocols in CR ad hoc Networks

In the last decade, several important studies have been carried out in the field of CR networks. These works have mainly focused on infrastructure-based networks that rely on the existence of a centralized coordinator [36]. In these single-hop architectures, each CR node directly communicates with the central entity as the end destination. Furthermore, this entity is responsible for managing the network operations for all CR users within its coverage, like spectrum sensing, channel assignment, etc. Recently, CR ad hoc networks have attracted considerable research attention due to several open challenges [5]. However, the application of CR technology in distributed scenarios is still in its infancy. In the literature, there are certain papers that address the issue of broadcasting in CR ad hoc networks that operate in multichannel environments [37], [38], [39], [40], [41], [42], [43] [27], [28], [33], [44]. These works are designed to achieve different performance goals, for instance, optimization of throughput, data delivery, delay, etc. However, most of these papers adopt impractical assumptions which make them unrealistic for use in practical scenarios.

Related work on broadcasting in CR ad hoc networks currently falls into two categories: (i) works that have been undertaken for general CR ad hoc networks and (ii) works that have been undertaken for CR ad hoc networks with specific assumptions, as follows:

2.5.1 General CR ad hoc Networks

Recently, many solutions have been proposed for exchanging the control messages in CR networks. One of these solutions is to use unlicensed bands such as ISM (Industrial, Scientific and Medical) or UWB (Ultra-Wideband) for carrying these messages [45]. The reliability cannot be guaranteed in this case due to the fact that these unlicensed bands are already shared among various wireless devices that can operate in the same radio frequency, which may lead to harmful interference and result in significant performance degradation. One of the simplest solutions

to enable broadcasting in multichannel networks is the use of a dedicated control channel [46, 47] usually called *Common Control Channel (CCC)*. In this case, all the CR users must switch to the *CCC* in order to transmit or receive broadcast messages. However, due to the lack of availability of a constant idle channel, this approach is not feasible in CR networks. A collaborative message dissemination is proposed in [44]. Instead of the source node transmitting the message to every channel, neighbours will collaborate in the message dissemination. Upon receiving the broadcast message, each node will transmit the received message randomly on one of the available channels. Due to the random nature of channel selection, the performance of this mechanism cannot be guaranteed.

Different schemes have been proposed for local establishing a *CCC* [48], [49], [50], [41]. Since these channels can be used to exchange control information messages in CR ad hoc networks, the proposed schemes could also be considered as broadcasting protocols. However, these proposals need prior information about the channel availability of all the CR nodes. Moreover, there are some proposals on channel hopping that can be used to find a *CCC* between CR nodes [42], [51], [52]. However, these schemes suffer from various limitations and cannot guarantee reliable broadcasting. For instance, the CR nodes need to obey robust channel hopping sequences in order to guarantee both CR sender and receiver hopping within a finite time on the same channel. In [42], CR users hop across the channels according to a random channel-hopping sequence for packet broadcasting. However, this approach cannot guarantee successful broadcasting even if they have common available channels. Furthermore, it works only when two CR nodes have the same number of available channels. Therefore, these channel hopping schemes [42], [51] are of limited value for practical broadcast scenarios where the channel availability of CR nodes in CR ad hoc networks is usually non-uniform. The channel hopping algorithm proposed in [53] requests tight time synchronization. This scheme is also not feasible without exchanging the control information. A Quality-of-Service (QoS)-based broadcast scheme under blind information is proposed in [54]. The proposed approaches in [43] assume that the CRs should have time-synchronization and symmetric spectrum to operate. Two data dissemination protocols are proposed in [55] for multi-channel wireless networks. The first protocol aims to reduce the amount of time to propagate large data across the network. While the second protocol designed to locally disseminate information in the cluster. In [56], the authors studied

the issue of broadcasting on multiple access channels using deterministic distributed protocols. A packet latency comparison of deterministic protocols and back-off randomized protocols is provided in this work. The authors in [57] proposed a strategy to broadcast in the presence of adversaries for multi-channel wireless networks. They derived the ideal number of channels that have to be accessed by nodes in order to minimize the reception delay. In addition, they used network coding to reduce the impact of attackers on the performance of data dissemination. A power-saving data dissemination model for mobile units is proposed in [58]. The proposed technique is suitable for any dissemination-based architectural model in multi-channel environments. The proposed scheduling algorithm in [59] calculates the average expected delay of multiple channels while considering access frequency, variable length and bandwidth of each channel. The strategy proposed in [37] classifies the channels on the basis of PR unoccupancy and CR occupancy, then selects the best channel for transmission. The non-uniform channel availability makes it hard to use a single channel for CRNs to broadcast. Broadcasting using multiple transceivers has been proposed as an alternative solution [38], where each CR node should have a number of transceivers equal to the number of channels. The utilization of multiple transceivers increases the complexity and the operational cost of the CR device which makes this choice undesirable. In [60], the authors investigated latency, speed and limits of the data dissemination in mobile CR networks. In [61], the performance limits of data dissemination in multi-channels single radio is analysed under random packet loss. The authors proved that, for any arbitrary topology, the problem of minimizing the expected delay of data dissemination can be formulated as a stochastic shortest path problem. However, it is likely that the number of available channels is not fixed, which leads to variable communication links.

2.5.2 CR ad hoc Networks with Specific Assumptions

Several existing works assume knowledge of the global network topology and the spectrum availability information at each node [62, 63]. Based on this information, the authors in [62] propose a time-efficient broadcast algorithm that selects a set of nodes and channels to transmit a message from the source node to all other nodes in a multi-hop CR network. A simple heuristic solution to broadcast the messages in multi-hop cognitive radio networks is proposed in [63], where CR nodes need

to be either equipped with multiple radios or use a single transceiver to transmit over multiple channels. In the second case, neighbours require a synchronization mechanism in order to successfully exchange control information. Additionally, a dedicated control channel for the whole network is employed in [39], which is not feasible in CR networks. In [64], the authors propose a unified channel allocation to handle both unicast and broadcast traffic. The channels are weighted according to their relative interference and connectivity parameters depending on the proportions of broadcast and unicast traffic in the network. Chraiti et al. [65], propose a secondary broadcast network composed of one multi-antenna secondary transmitter (ST) and a set of single-antenna secondary receivers (SRs). The ST is responsible for broadcasting the data to all the SRs in the presence of primary communication. By using orthogonal beamforming techniques, the secondary network is allowed to access the spectrum without affecting the primary transmission.

Most of the aforementioned studies consider impractical scenarios in their design where global network topology is known, predefined *CCC* is assumed to be in existence, information about available channels of all CR nodes are assumed to be known and multiple transceivers are used. In addition, in all the aforementioned papers, the CR users select the channel with the least PU activity for its communication. However, this approach only guarantees protection to the PU-transmitters. The probable harmful interference that may affect the PU-receivers within the transmission range of the CR devices is not accounted for in these approaches. This can seriously undermine the performance of PU communication. To the best of our knowledge, there is no existing broadcast protocol for CR ad hoc networks that considers these limitations.

In this research, we therefore propose two broadcasting protocols for CR ad hoc networks by considering the assumptions and limitations of works in the related literature. They are:

1) a primary receiver-aware opportunistic broadcasting protocol that makes the following contributions: i) alleviates the interference collision risk to PU communications; ii) guarantees protection to the PU-receivers and iii) provides a high successful broadcast ratio. To the best of our knowledge, this is the first work that considers the broadcasting challenges specifically in CR ad hoc networks under a PU-receiver protection scenario.

2) a distributed reliable broadcast protocol (CRBP) for cognitive radio ad hoc networks that addresses the problems of network connectivity, reliable data dissemination over multi-hops and the issue of securing PR communications. A key novelty of the proposed CRBP is the formulation of the broadcast problem from the viewpoint of connecting different local topologies, which is a unique feature in cognitive radio networks.

Unlike the limitations of related work in the literature, we consider practical scenarios in our design where limited knowledge of the network environment is assumed to be known, no *CCC* is assumed to exist and the sets of the available channels of neighbouring CR nodes are not assumed to be the same.

2.6 Spectrum Sensing

Spectrum sensing technology is considered as a fundamental functionality of CR networks. CR nodes sense primary user activity and determine the channel availability in order to access the vacant licensed bands in an opportunistic manner [6]. Hence, the accuracy of this sensory information is very important for CR communications. Otherwise, CR traffic may cause interference to the licensed users. Spectrum sensing techniques can be classified into two types: local spectrum sensing and collaborative spectrum sensing (CSS). Next, an overview of both sensing techniques is provided.

2.6.1 Local Spectrum Sensing

The existing local spectrum sensing techniques include energy detection, cyclostationary feature detection and matched filter detection.

- **Energy Detection:** The energy detection is considered as the simplest technique for local spectrum sensing. In this sensing technique, an energy detector is used to infer the existence of a PU on a specific channel based on the measured energy level. In order to measure the energy level accurately, first a bandpass filter processes the received signal, then the processed signal is passed to the integrator which squares and integrates the measured signal over the observation time interval. Finally, a predefined threshold is compared with the output signal to decide whether a PU is being active or not on the corresponding band. Based on the channel conditions, the threshold value is

set to be fixed or variable [66]. The energy detector technique is optimal when a CR receiver does not have enough information about PU's signal, such as the the power of the Gaussian noise and the characteristics of the PU' signal [67]. Furthermore, the energy detection is the most popular spectrum sensing technique because it requires no priori information about the PU signal [68], [69].

- **Matched Filter Detection:** The matched filter technique requires prior information about the PU signals to reliably detect spectrum holes. The required PU information includes modulation type, preambles, pulse shape, synchronization codes, etc. The matched filter is a linear filter designed to maximize the received signal-to-noise ratio (SNR) in stationary Gaussian noise. Hence, it is considered as the best detector in this case [13], [70]. There are some advantages of the matched filter over the energy detector. For instance, fewer samples are required compared to the energy detector, consequently it needs less detection time. In addition, different signal types in the spectrum band can be distinguished in this technique. In contrast, the performance of the match filter technique mainly depends on the accuracy of the prior knowledge about the PU signal, which is considered a disadvantage of this technique [70].

- **Cyclostationary Feature Detection:** The cyclostationary feature technique detects PU signals by utilizing the cyclic feature of these signals. For instance, both the cyclic spectrum density (CSD) and the cyclic autocorrelation function (CAF) can be used to detect the features of PU signals [71], [66]. The main advantages of the cyclostationary feature technique are its capability to identify different types of signals in the spectrum band and its ability to detect PU signals in the case of a stationary noise with unknown variance [72]. On the other hand, the complex computation and the required long observation interval are considered the main disadvantages of this detection technique [71].

2.6.2 Collaborative Spectrum Sensing

Spectrum sensing that is individually performed by a single CR user based on local sensing information might lead to poor sensing measurements due to several reasons (e.g., potential signal degradation, hidden terminal problems, energy level

constraints, etc.) [73] [74]. Collaborative Spectrum sensing (CSS) overcomes these destructive effects by exploiting multiple CR nodes spatial diversity which results in enhancing the performance of the sensing operation. Consequently, most of the existing standards and proposals (i.e., IEEE 802.22, IEEE 802.11af and CogNeA) have adopted collaborative spectrum sensing [75], [76], [18]. In CSS, each CR user is represented as a sensing workstation that conveys local sensing. The local measurements are collected by the fusion centre (or data collector), which determines the final decisions regarding spectrum band availability [77]. CSS can be classified into two main categories: centralized coordinated technique and decentralized coordinated technique.

- **Centralized Coordinated Technique:** In an infrastructure-based CR network, CSS can be carried out in a straightforward way: the CR users serve as sensing stations while the base station acts as the data collector. In this technique, once a sensing terminal detects the presence of a PU on the spectrum band, it informs the central entity which can be a single-hop or multi-hop distance. Then, using a broadcast control message, the Fusion Centre (FC) notifies all the CR users about the unavailability of the corresponding band.

- **Decentralized Coordinated Technique:** In CR ad hoc networks, due to the absence of a central administrator, CR nodes cooperate to organize the network's functionalities. In such network deployment, each CR node is equipped with a CR engine, which enables the CR node to serve simultaneously as a fusion centre and a sensing terminal. Neighbouring CR nodes usually exchange their local sensing results in this type of collaborative sensing. Based on the local sensing measurements received from other neighbours, each CR user determines the final spectrum sensing measurements [78]. Different algorithms have been used to improve the decentralized sensing technique. For example, clustering protocols [79] and gossiping schemes [80] are proposed for CR ad hoc networks to enable CR users to gather clusters and auto coordinate themselves.

Although collaborative sensing alleviates channel fading problems and consumes less resources at individual CR nodes, its application faces several challenges. The presence of attackers may considerably degrade its performance, leading to harmful

interference with the PU communications and/or a significant loss of the free spectrum. Therefore, robust and reliable collaborative sensing is critical in cognitive radio networks and justifies its place in current empirical research.

2.7 Security Threats in CR Networks

Recent literature identifies several CR approaches, for example, spectrum sensing, channel negotiation, spectrum hand-off, optimization and spectrum management. Unfortunately, most of these works underestimate the security issue. In CR networks, the technical area of wireless security generally and spectrum sensing in particular have received little attention. Like all other wireless networks, CR networks also inherit various security vulnerabilities. However, due to their unique characteristics, CR networks face new security challenges and threats. The collaborative spectrum sensing process is not an exception. Two major attacks that target the sensing process, as defined in [81] are: 1) Primary User Emulator (PUE) attacks and 2) Spectrum Sensing Data Falsification (SSDF) attacks. In PUE attacks, a malicious CR node emulates the characteristics of PU transmission signals in order to prevent other users from accessing the free band for selfish or malicious purposes. The presence of PUE malicious CR nodes makes the FC believe that the spectrum band is under PU activity; this gives PUE attackers unrivalled access to the spectrum gaps. On the other hand, under SSDF attacks a malicious CR node injects false sensory information into the central data collector during the fusion process. This may cause the FC to make wrong spectrum sensing decisions, as illustrated in Figure 2.1. Furthermore, an intermediate malicious CR node could manipulate the received message before forwarding it to the FC. Recent research shows that SSDF attacks are so severe that they might seriously exacerbate the spectrum access probability. The Fusion centre needs to use a robust data fusion technique to maintain an adequate level of accuracy in the presence of malicious users that fraud local spectrum measurements.

In this research, we consider only SSDF attacks that target the sensing learning cycle. In a CR network, the realization of most networking protocols relies on the channel availability information (e.g., routing protocols [82] and channel rendezvous protocols [83], [84], [85]). When a malicious node shares false channel information with the central entity or with its neighbouring nodes, an incorrect decision may

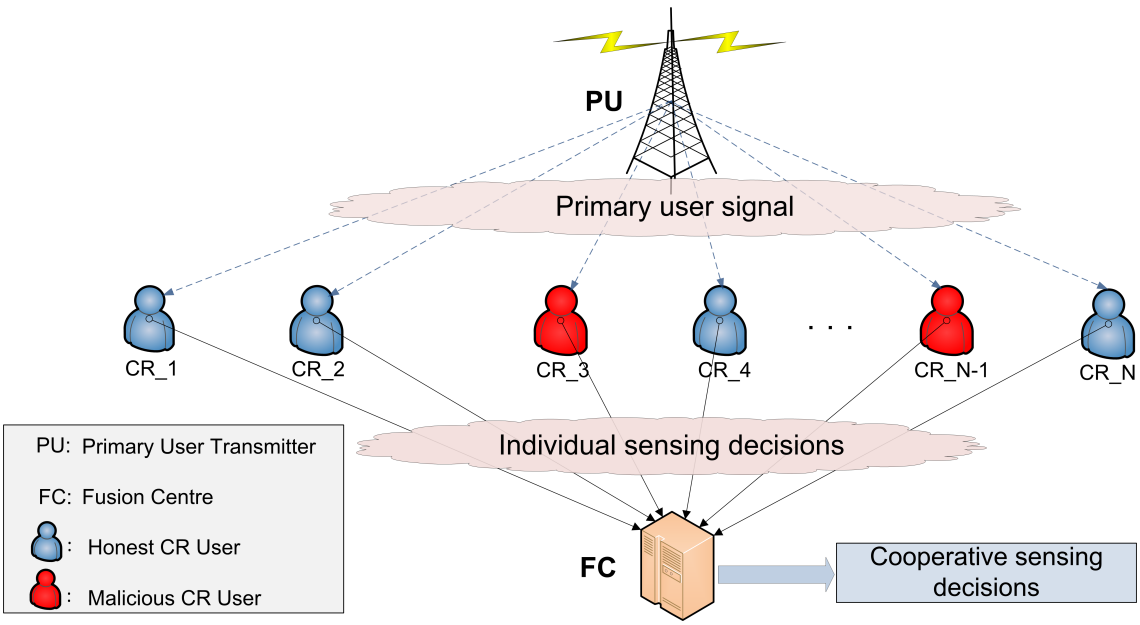


Figure 2.1: Illustration of malicious SSDF attackers who try to inject tampered data and degrade the performance of cognitive radio networks.

be made about the channel availability of other nodes and this will affect the operation of the networking protocols. For example, if a channel is free to use but a malicious CR node claimed it is occupied by PU, this channel cannot be used by the victim CR nodes for their communications. Consequently, the performance of CR networks may experience significant degradation. In contrast, if a channel is occupied by PU but a malicious CR node claimed it is free to use, transmitting on this channel may lead to harmful interference to the PU communications. The SSDF attacks will not only significantly degrade the performance of CR networks, but also cause remarkable difficulties to defend against them. As mentioned above, although failed data transmissions may indicate that there is an interference with PU communications, it is really difficult to realize the waste in the available channels. Recently, a more dangerous SSDF attack has been revealed, in which the malicious node anticipates which spectrum band will be used by CR users and attacks those specific bands [86]. Hence, a reliable scheme is needed to fight this type of attack and identify the malicious CR users.

2.8 Existing Security Schemes to Defend SSDF Attacks in CR Networks

Within the literature, certain studies have tried to analyse and justify SSDF attacks. Wei et al. [87] propose a distributed spectrum sensing algorithm to thwart SSDF attacks. In their system they characterize the distributed sensing algorithm as an M-ary hypotheses problem instead of a binary one. They assume the detection made by the CR nodes is mutually exclusive. Relay nodes are assumed to act as a bridge between CR nodes and the FC which makes the final decision. In [88], the authors document reported histories of secondary users and analyse the Hamming distance between them to calculate the accumulated suspicion level and distinguish between honest users and attackers. Sodagari et al. [89] use a utility based mechanism to tackle SSDF attacks through minimizing the surplus utility of misreporting nodes, leaving minimal motivation for malicious nodes. Rawat et al. [86] present a reputation-based method to identify SSDF attackers based on how their transmissions compare with those expected from honest nodes. Based on their results, this approach is not reliable in the presence of a large number of attackers. In the presence of 50% independent malicious CR nodes, the FC becomes blind and unable to differentiate between honest users and malicious users. However, for a collaborative attack, this ratio decreases to 35%.

A reputation-based collaborative scheme suggested by Zeng et al. [90] is employed to identify misbehaving nodes. The sensing information from other CR nodes is incorporated into the collaborative decision only when their reputation is verified. In contrast, adversary nodes do not always misreport, thus, the authors adopt a different approach. Therefore, a new defence scheme that considers this limitation should to be developed. The authors in [91] propose a dynamic threshold-based strategy to defend against the SSDF attacks. The proposed scheme updates the dynamic threshold according to the upper and lower bounds of the fusion value. Recently, an adaptive reputation based clustering scheme has been proposed to defend SSDF attacks [92]. In their study, a bi-level voting algorithm including of intra-cluster and inter-cluster is used to make the final decision. In [93], the authors present a detection technique called cooperative neighbouring cognitive radio nodes (COOPON), whereby legitimate CR neighbours cooperate to detect malicious users. However, this technique becomes ineffective when the number of malicious

nodes is significantly high. Some other models apply the multi-armed bandits to CR network problems. A distributed protocol based on a competitive multi-armed bandit is applied by Lai et al. [94]. Furthermore, a defence strategy based on non-stochastic bandits model is present by Wang et al. [95]. In this strategy, transmitter and receiver adaptively switch their arms without exchanging control information. Nevertheless, none of the above mentioned papers are able to combat SSDF attacks. In addition, they assume a distributed policy used individually by each CR node.

A decentralised detection scheme is proposed by [96] to detect malicious SSDF users. The scheme utilizes a robust outlier-detection technique for the spatial correlation of the received measurements from CR users in close proximity. Neighbours majority voting strategy is used for CR users to decide whether a specific CR user is malicious. This scheme requires prior knowledge of the maximum number of malicious CR users. Our scheme does not require prior knowledge of the reliability status of CR nodes. In [97], the authors suggest a defeating clustering scheme based on an adaptive reputation algorithm to detect both independent and collaborative SSDF attackers. However, several issues were not specified by the authors, for example, how to set the initial threshold for reputation and how the cluster is updated. In order to secure data authenticity, two localization-based defence schemes are proposed in [98] and [99]. It is assumed that any sensing report that is not endorsed by at least a threshold number of CR nodes should be dropped by the FC. However, compromising the threshold number of endorsing nodes will compromise the entire cell, which is the main drawback of these schemes. In addition, fake sensing reports can be easily generated by that cell and will be accepted by the FC as a legitimate report.

However, to the best of our knowledge, there is no specific protocol that considers both SSDF attack and end-to-end secure sensing in CR networks. With this motivation and to overcome drawbacks found in the aforementioned works, we propose a new robust security mechanism to protect sensory information in an adversarial CR network environment.

- In our proposed scheme, an efficient reputation-based algorithm has been employed to analyse the behaviour of each CR node. According to its historical and recent behaviour, the reputation of each CR user is updated. This enables the FC to select trusted nodes with the objective of eliminating the effects of

adversaries on the reliability of spectrum sensing data.

- Location information for generating security credentials has been used in many works. However, unlike other works, our proposed scheme adopts a three-tier verification process as additional security to decrease the probability of forging fake sensory data. Hence, to compromise a particular cell, the adversary needs to control the threshold number of nodes in the cell alongside the trusted nodes to successfully legitimise the sensory reports.

- The proposed defence scheme considers end-to-end security instead of hop-to-hop security. The proposed scheme encrypts the sensory data of each node using a unique secret key in order to protect the confidentiality and the integrity of sensory messages. Furthermore, we employ a secure authentication protocol between the FC and the collaborative nodes. Therefore, controlling intermediate nodes would not result in multiple gain and does not allow the adversary to break the confidentiality or the integrity of other cells.

- In our proposed algorithm, malicious nodes can be detected very quickly. Thus, the adversaries and their negative effects can be removed from sensing decisions in a few iterations. This can significantly improve the reliability of the spectrum sensing decisions.

- Due to its elegant framework, the proposed scheme is flexible for simplification and modification. For instance, the proposed scheme can be easily expanded to detect several kinds of attacks beyond the SSDF attack.

2.9 Conclusion

Although broadcasting protocols and defending schemes are active areas of research, relevant challenges have yet to be studied. The realization of the networking protocols and the security aspects of CR networks need to be addressed before the advantages of CR technology can be fully harvested. In this chapter, an overview of the technical background and a review of the literature underpinning this research has been provided. We started by discussing the broadcast issue and the challenges associated with it in cognitive radio ad hoc networks. Additionally, we highlighted the security threats in CR networks, specifically the SSDF attacks and its effect on

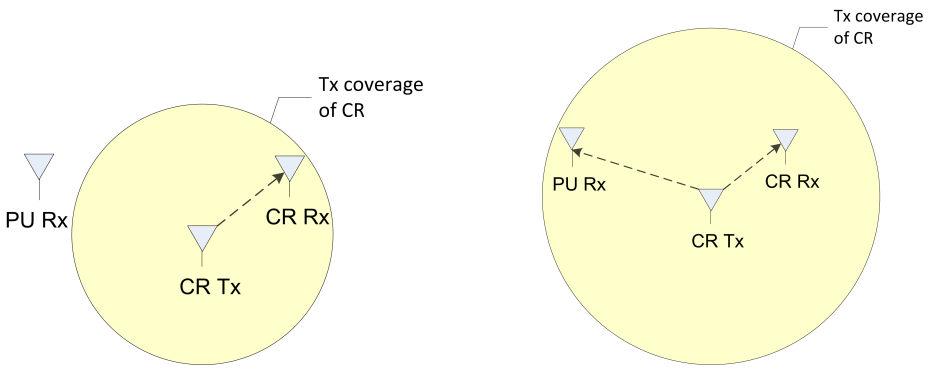
the performance of the CR network. Furthermore, a survey of existing research related to the broadcasting protocols and the defending schemes against SSDF attacks is provided.

In the next chapters, we will present our contributions in the field of spectrum management techniques for wireless CR networks.

Chapter 3

Primary Receiver-Aware Opportunistic Broadcasting in Cognitive Radio Ad Hoc Networks

In the previous chapter, we have comprehensively studied the state-of-the-art on broadcasting protocol for CR ad hoc networks. However, very less effort has been done so far. The main challenge of broadcasting in CR ad hoc networks is how to prevent CR transmission signals from causing harmful interference to PU communications. The most common known technique that can be used to address the above challenge is spectrum sensing, under which a CR user can access the spectrum band of interest only if the PU activity is measured to be off on the corresponding band. With the assistant of spectrum sensing, CR users opportunistically exploit unused frequency bands within radio spectrum. Various spectrum detection approaches have been proposed, such as primary transmitter detection through energy detection, matched filter detection, and cyclostationary feature detection [68], [69], [71]. In this chapter, our goal is to investigate the challenge from a different angle. Due to the complex implementation of spectrum sensing and non-zero probability of false detection leads us to ask the question: is there an alternative method to spectrum sensing that enhances the broadcasting goal of CR networks? Our investigation concludes an alternative technique of achieving the above mentioned objective of alleviating harmful interference by CR transmission signals to PU communications, specially PU receivers within the transmission range of CR devices. To achieve this goal, we examine a location-aware spectrum sharing scenario, where CR users pro-



(a) Considering PU receiver

(b) Without considering PU receiver

Figure 3.1: A spectrum sharing scenario of considering PU receiver in CR ad hoc networks

pose to operate over the same frequency band which is dedicated to the licensed PU users. The goal is to maximise the CR users transmission region, while at the same time minimising interference to PU communications. Selecting CR broadcasting channels is very important in order to guarantee the quality of CR and PU communications. To achieve this goal, we examine a location-aware spectrum sharing scenario, where CR users propose to operate over the same frequency band which is dedicated to the licenses PU users. Figure 3.1 illustrates a spectrum sharing scenario of considering PU receivers and the scenario of not considering PU communications when broadcasting in ad hoc CR networks. Figure 3.1(a) demonstrates that with the consideration of PU receivers, when a PU receiver is within the transmission range of a CR, simultaneous transmissions become possible by selecting the proper frequency band ensuring non-interference to the PU receivers for the CR broadcasting. However, without considering protection to PU communications, concurrent transmissions are not feasible when a PU receiver is within the interference range of a CR transmitter as shown in Figure 3.1(b). In this chapter, we define the concurrent transmission region as the transmission circle of CR user within which the CR broadcasting can be carried out without interfering PU receivers.

The main contributions of this chapter are: 1) The broadcasting channel selection and its impact on PU receivers is mathematically modelled for the first time. 2) The trade-off between CR successful broadcasting as well as average CR collision risk with PU receivers is investigated for the first time which takes into consideration the PU protected zone and the impact of PU activity on the broadcasting process. 3) Two optimal broadcasting protocols based on the modelled trade-off are proposed for

CR ad hoc networks. 4) The Network Simulator NS-2 is developed to include the PU activity model. To the best of our knowledge, this is the first work that investigates the optimal design of broadcasting protocol under a PU-receiver protection scenario for CR ad hoc networks.

The rest of this chapter is organized as follows. We discuss the network model and assumptions in Section 3.1. We review the broadcast design for CR networks in Section 3.2. We give detailed description of the proposed broadcast protocol for CR ad hoc networks in Section 3.3. Performance evaluation is conducted in Section 3.4. Finally, Section 3.5 summarizes the chapter.

3.1 Network Model

The probable harmful interference that may affect the PU receivers within the transmission range of the CR devices is considered in this work. Thus, as shown in Figure 3.2, PU receivers might be affected by neighbouring CR users' transmissions and this can seriously undermine the performance of PU communication. In this work, we consider a spectrum sharing scenario in which a CR ad hoc network co-exist with a licensed network. We consider a CR ad hoc network with no centralized coordinator. In this type of network setting, we assume that the network environment tasks like spectrum sensing, neighbour discovery, channel selection decision, etc., are accomplished by the CR nodes individually. N CR users and M PU transmitters co-exist in an $L\ x\ L$ area, where CR nodes opportunistically access K licensed channels. The transmission range of a CR_i on the k^{th} channel is represented by a circle with a radius of $R(CR_i^k)$. Any CR node within the transmission range of the source CR node is considered as a neighbouring node of the corresponding CR. A CR receiver within the transmission range of a CR transmitter is considered as a neighbour only when the signal-to-noise ratio (SNR) at the CR receiver is considered to be convenient for reliable communications. Furthermore, the CR node is able to detect any PU who is currently active on the spectrum and within the sensing range of the corresponding CR. Since different CRs have different local sensing ranges, which include different PUs, their acquired available channels may be different.

In addition, in this chapter, the PU channel activity is modelled as an ON/OFF process, where the length of the ON period is the length of a PU occupying a channel and the length of the OFF period is the length of a channel free from PU activity.

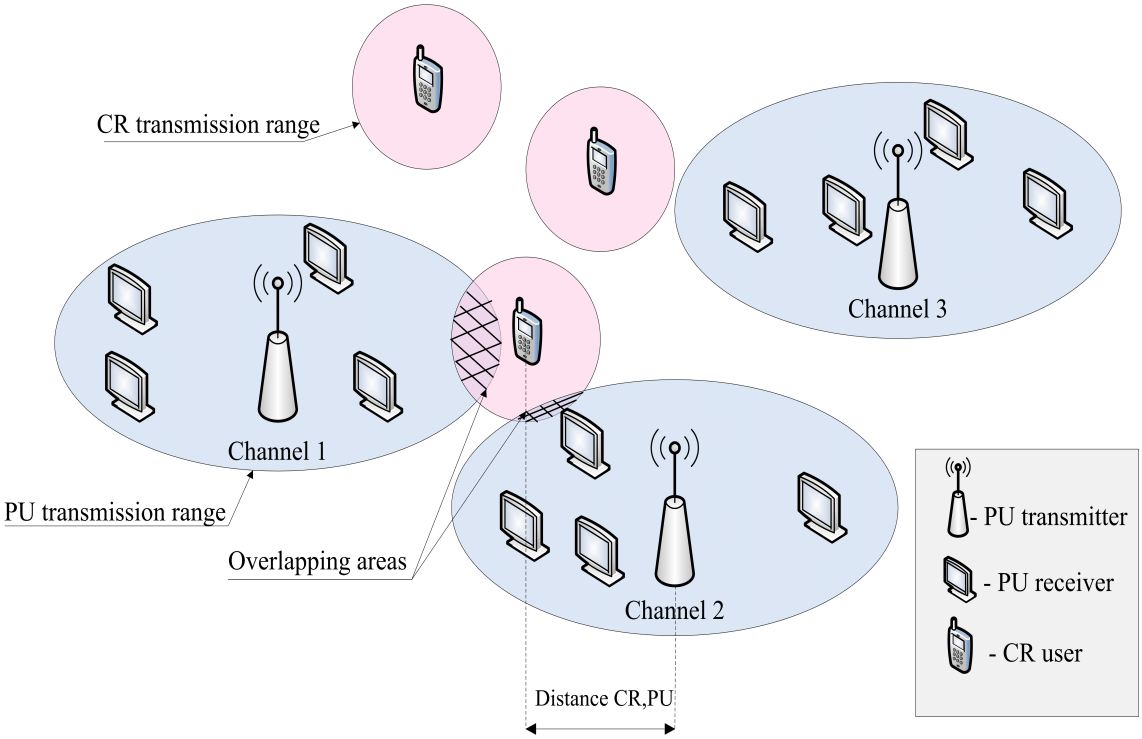


Figure 3.2: PU receiver protection in CR ad hoc networks.

We assume that PU can randomly select any channel from the spectrum band for its communications. Furthermore, in this work, the PU transmitters and receivers are geographically fixed.

If a PU is currently active within the transmitting range of a corresponding CR, then the CR user is able to detect its presence. Different CR users sense different PU signals at different locations, hence their acquired available channels may be different [23][87]. In addition, as the channel availability of each CR is obtained based on the sensing measurements within its sensing range, a CR user is not allowed to communicate with CR users outside its sensing range because it may mistakenly use an active channel and cause an interference toward on-going PU-communications. Our work focuses on CR ad hoc networks without specific network topology assumptions, where each user is equipped with a single transceiver and has limited knowledge of the network environment. Furthermore, we consider practical scenarios in our design where no global network topology is known and no common control channel is assumed to exist. The main notations used in the chapter are summarized in Table 3.1 for easy reference.

Table 3.1: Symbols used for describing the proposed protocols

Symbols	Descriptions
N	Set of CR nodes
M	Set of PU nodes
K	Set of licensed channels
N_i	Set of single-hop neighbours of CR_i
T_s	Spectrum sensing time for CR users
T_t	Transmission time for CR users
Φ_{idle}	The available channel set
$Z(PU)$	The PU protected zone
$R(CR)$	Transmission range of CR user
Ψ	The Euclidean distance

3.1.1 Spectrum Sensing

Spectrum sensing aim to identify the available spectrum and prevent any harmful interference to the primary users. We assume the cognitive radio nodes undertake spectrum sensing periodically in order to detect any PU activity and ensure up-to-date information regarding the spectrum occupancy. Furthermore, we assume all CR users are synchronized to the same sensing cycles. During the sensing duration, all CR users must be silent and no transmission is allowed. Consequently, the time needed to disseminate a message in the network will be affected when the CR users are unable to transmit owing to the enforcement of the silent zone. The spectrum sensing and the transmission times for any CR user are T_s and T_t respectively. Where T_t is the effective duration of time for which transmission is allowed for any CR node on any choice of free spectrum, while T_s is the duration of time that all CR nodes must be silent for the purpose of sensing. $T_s + T_t$ gives the frame time for each user when considered together.

3.1.2 Neighbour Discovery

In order to successfully deliver the broadcast messages to all the CR nodes in each neighbourhood, CRs must discover the network topology and the common idle channels that can be used to communicate among neighbours, these tasks typically accomplished during the neighbour discovery. In the absence of a common control channel, discovering neighbours in CR ad hoc networks is undoubtedly a challenging task, we propose a neighbour discovery mechanism to address this issue. Initially, we assume that individual nodes are tuned to different channels and have no prior

knowledge of their neighbours and the network topology. Furthermore, each CR node maintains the local idle channel list based on the information received from the spectrum sensing. At the beginning of constructing the network, every CR node has to broadcast its information (node's id and its available channels) on all the locally available channels, one-by-one. As a result, all single hop neighbours that are tuned to any idle channel could receive a copy of this message. Each CR node receives this beacon message and records the transmitter's CR node information in its single-hop neighbours list N_i. After forming and configuring the network, the CR nodes do not have to beacon messages unless there is a change in their channel availability.

3.2 Reviewing Broadcast Design in CR ad hoc Networks

In order to investigate the broadcast design in CR ad hoc networks without a common control channel, two straightforward schemes of broadcasting in CR ad hoc networks, *random broadcasting strategy* and *full broadcasting strategy* are explored. Understanding their mechanism and identifying their limitations will serve as an important first step toward proposing a new broadcasting protocol for CR ad hoc networks. It has been noticed that both broadcasting strategies have some drawbacks which make them infeasible to be used in multi-hop CR ad hoc networks. In the rest of this chapter, the term sender is used to indicate a CR source node that broadcasts messages. In addition, the term receiver is used to indicate a CR who has just received the broadcast packet and will rebroadcast it to its neighbouring CR nodes.

3.2.1 Random Broadcasting Strategy

The first broadcasting scheme we investigate is called the random broadcasting strategy. Due to the absence of other CR nodes' channel availability information before issuing the broadcast process, a CR sender takes a straightforward action by randomly selecting a channel from the set of available channels as the broadcasting channel. Correspondingly, because CR receivers are unaware of senders channel availability information, it is difficult to constantly stay on a single channel through-

out the broadcast process. This channel may not be available for the receiver, which can lead to failures in the broadcast procedure. Therefore, the only reasonable action for the CR receiver is to randomly pick up an available channel for message reception in each time slot. If by somehow the receiver selects the same channel as the sender, the broadcast messages can be successfully delivered. Under blind information CR ad hoc networks, this broadcast strategy can be easily implemented. Nevertheless, this scheme cannot promise protection to PU communications or channel rendezvous (i.e., the receiver and the sender tune onto the same channel at the same time and set up a communication link). In other words, the sender tries its best to deliver the broadcast message to its neighbouring CR nodes in each time slot. When the number of available channels is large, the probability of matching channel selection between the sender and receiver is low, thus the probability of successful broadcast using the random broadcasting strategy is fairly low. In Figure 3.3, we show the simulation results of the random broadcasting strategy using different numbers of available channels and PU activity. We define the packet delivery ratio as the probability that all CR nodes in the network receive the broadcast message successfully. It is clear from Figure 3.3 that when the number of channels is large, the random broadcasting strategy leads to a very low successful delivery rate. In addition, we define the interference risk for PU as the total number of times CR messages collide with PU messages. It is shown in Figure 3.4 that the random broadcasting scheme causes harmful interference to PU communications specially when the PU activity on the channels is high, which is not well suited to be used in multi-hop CR ad hoc networks when the number of available channels is large.

3.2.2 Full Broadcasting Strategy

The second broadcasting scheme we investigate is called the full broadcasting strategy under which each CR node broadcasts to all the available channels in the spectrum. Different from the random broadcasting strategy where the channel is randomly selected by a CR in each time slot, in the full broadcasting strategy, a CR sender transmits to all the available channels by broadcasting the message sequentially to all its available set of channels. Indistinguishably, a CR receiver listens sequentially to its available channels. Furthermore, we use two different channel hopping schemes for the full broadcast strategy: i) the random channel hopping se-

quence in which each CR node randomly visits all the available channels (denoted as Full Broadcasting I); and ii) the sequential channel hopping sequence in which each CR node sequentially visits all the available channels (denoted as Full Broadcasting II).

In Figure 3.3, we show the simulation results of the full broadcasting strategy using different channel hopping schemes under different numbers of available channels. Similar to the random broadcasting strategy, the full broadcasting strategy also suffers a low packet delivery ratio when the number of channels is large for both channel hopping sequence schemes. This is because these channel hopping schemes in the full broadcasting strategy can not guarantee reliable channel rendezvous. In addition, compared to the Full broadcasting I strategy, the Full broadcasting II strategy leads to a significant low packet delivery ratio when the number of available channels is large. On the other hand, it is shown in Figure 3.4 that the full broadcasting strategies lead to very high interference collision rate when the channels are under high PU activities. Furthermore, the Full broadcasting II strategy leads to an extremely high collision rate when the probability of finding an idle channel is low, compared to the Full broadcasting I strategy. Hence, it is not suitable for broadcast in CR ad hoc networks where successful broadcast messages is often required.

3.2.3 Observations

It is clear from the aforementioned discussion that these straightforward broadcasting strategies cannot be used in multi-hop CR ad hoc networks due to the discussed limitations. We obtain two important insights for designing an efficient broadcasting protocol for CR ad hoc networks based on the outcomes of investigating these broadcasting strategies. Firstly, it is obvious that the three strategies (random broadcasting, full broadcasting I and full broadcasting II) cannot achieve high delivery rates when the number of available channels is large. This is because these strategies cannot assure channel rendezvous as shown in Figure 3.3. Therefore, the channel availability information of other CR nodes is required for channel hopping sequences in order to guarantee channel rendezvous which results in very successful delivery rates. Secondly, all these broadcasting strategies are quite costly when the number of channels is large in terms of the negative interference collision risk on the PU communications generally and on PU receivers specifically, which is not advan-

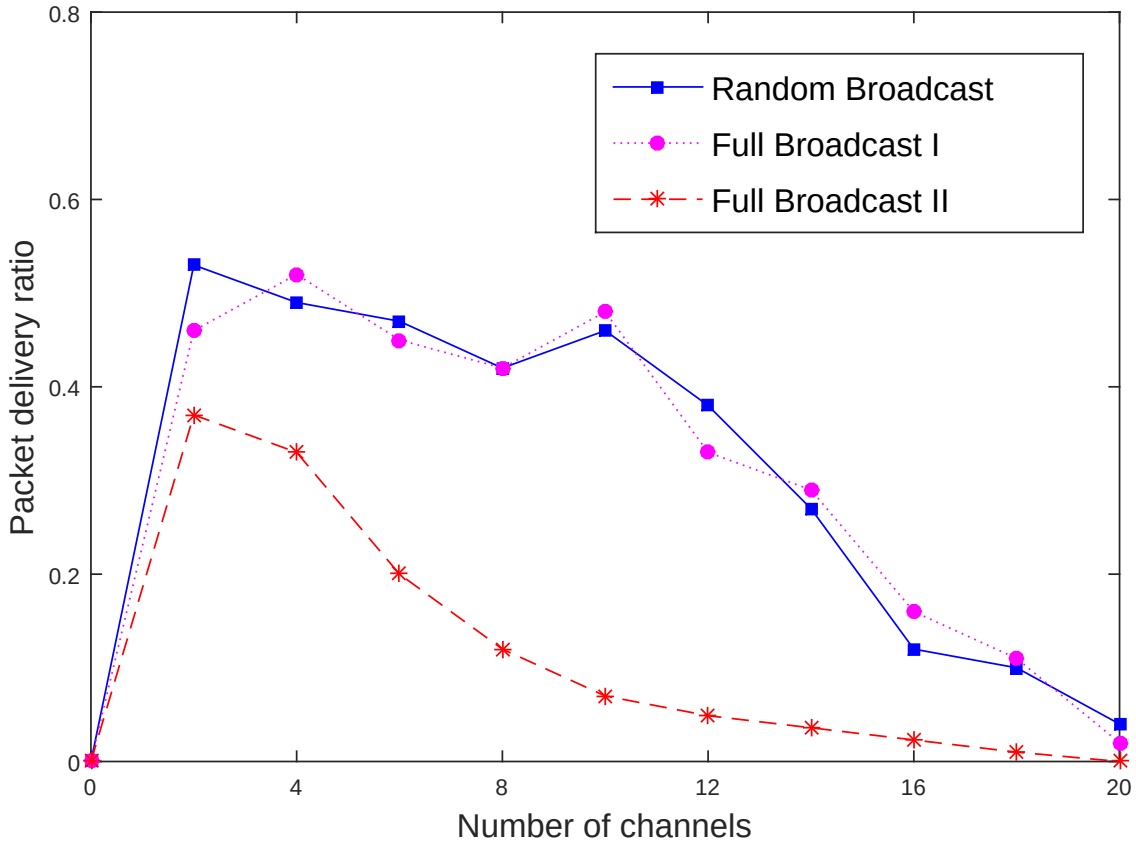


Figure 3.3: Packet delivery ratio of the random and full broadcast strategies using different numbers of channels.

tageous for efficient broadcast. This is because CR nodes need to broadcast blindly on all the available channels in the spectrum. In the case of using only a subset from the available channels for broadcasting, the successful delivery rate may decreased considerably. Furthermore, as fewer channels are used for broadcasting, the harmful interference with PU communications may reduced accordingly. Moreover, if CR nodes select the tuning channels randomly, there are very less chances that the neighbouring CR transmitters also use the same channel for broadcasting. Thus, an intelligent channel selection scheme is essential for broadcasting protocol that reduces the interference to PU receivers and maximizes the message dissemination reachability.

Considering the aforementioned observations, hereafter we list the key characteristics required for a robust control channel selection scheme in CR ad hoc networks:

1) Primary Users restrictions: The broadcasting scheme should guarantee that CR users transmissions do not cause negative interference to PUs.

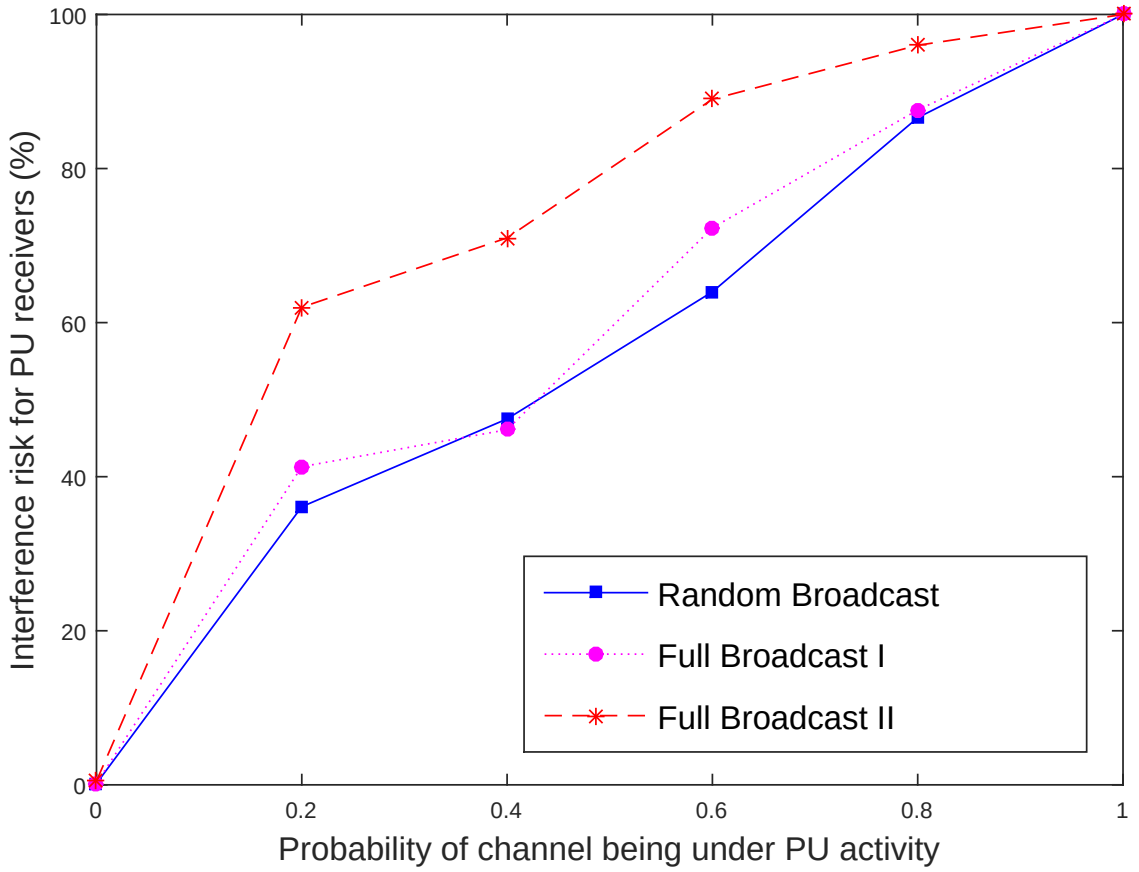


Figure 3.4: Probability of PU interference collision risk of the random and full broadcast strategies using different channel activity.

2) CR neighbour connectivity: A good channel selection protocol should increase the probability of successful message delivery to single-hop CR neighbouring nodes.

3) Distributed decision: In decentralized CR ad hoc networks, CR nodes have to make decisions autonomously. Hence, channel selection decision should be made based on locally inferred information and without the help of any centralized authority.

4) CR sender and receiver rendezvous: The broadcasting scheme must ensure that both transmitter and receiver tune with high probability on the same channel.

3.3 The Proposed Broadcast Protocol

In this section, we introduce our intelligent distributed broadcasting protocol for efficient broadcast in ad hoc CR networks. The straightforward broadcasting strategies are not adequate for CR ad hoc networks, as mentioned in Section 3.2. Accordingly, based on the realizations that we obtained from these broadcasting schemes, a broadcasting protocol should be able to intelligently select the broadcast channel according to the current network characteristics which guarantees successful broadcast operation without causing interference to the PU communications. In addition, it should support a channel hopping scheme for both the CR sender and the CR receiver in order to guarantee channel rendezvous.

We propose an intelligent and distributed protocol for efficient broadcasting in ad hoc cognitive radio networks. The problem is formulated by investigating the trade-off between maximizing successful CR broadcast and maximizing PU receiver protection. The proposed protocol picks the broadcast channel carefully and adapts itself according to the current network characteristics in order to guarantee successful broadcast operation without interfering with the PU communications. To guarantee the protection of PU receivers, it is also important to ensure that a CR transmission signal does not affect the PU transmissions area. Indeed, selecting a channel that overlaps with PU receivers may undermine the performance of PU nodes. The key for achieving an efficient broadcast that enables the coexistence of both PU and CR transmissions within a specified vicinity is to apply strict control over the channel selection. With the proposed protocol, every CR node individually classifies the available channels based on local observations of the primary activities over the primary channels and the channels connectivity. This classification is then refined by deciding which channel will be used for broadcasting as it has the minimum overlap with the PU protected zones. In addition, a CR node with no data to transmit uses the same criteria to select the tuning channel that offers best connectivity for data reception. Moreover, it is likely that CR users in the transmitter's vicinity share the same channel availability, hence, adopting the same classification by all CR nodes in the network allows the nodes within a close geographic area to choose with high probability the same channel. Once a CR receives a packet, it undergoes the same procedure again to convey the data to its CR neighbours. The proposed protocol ensures perfect protection for the PU communication and guarantees a high packet

broadcast ratio.

We next describe the detailed operation of the proposed protocol and different metrics that influence the choice of broadcasting and channel selection. The CR-specific metrics considered during channel selection are (i) propagation characteristics of the wireless spectrum, (ii) primary users protected zone, (iii) average degree of overlap, (iv) probability of spectrum availability and (v) CR users' connectivity.

3.3.1 Propagation Characteristics of Wireless Spectrum

Since not all wireless spectra have the same propagation characteristics, frequency has a significant effect on radio communication. At the low-band spectrum, radio waves tend to have better propagation and penetration characteristics than the high-band spectrum. Using the same level of transmission power, a lower frequency signal goes further than higher frequency. Thus, the lower frequencies of the radio spectrum are often considered quite valuable. Comparatively speaking, lower frequency spectrum requires fewer transmitters to cover an equivalent area than a higher frequency. The spectrum propagation characteristics of low frequencies help in enhancing the end-to-end latency and improving the per-hop coverage distance. Hence, allowing the network to be covered by fewer intermediate transmitters. In addition, lower bands can result in lower energy consumption compared to higher bands. This is a particularly useful advantage for CR users of battery-powered devices such as laptops, sensors, smart-phones, etc.

The CR node's transmission coverage depends on the propagation characteristics of the selected channel. As radio signals propagate out from the i^{th} CR node's antenna, its intensity decreases with distance, d. Assuming the simple path loss propagation model, we obtain the maximum propagation distance $R(CR_i^k)$ of the CR node at which the received power is above the system-dependant threshold, given as:

$$R(CR_i^k) = \left[\frac{CR_{power}^{tx}}{CR_{power}^{\delta}} \left(\frac{c}{4\pi f_k} \right)^2 \right]^{\frac{1}{\alpha}}, \tag{3.1}$$

where f_k is the frequency of the k^{th} channel, CR_{power}^{tx} is the CR user transmission power, CR_{Power}^{δ} is the CR receiver threshold, c is the speed of light and α is an attenuation factor. The CR node's transmission coverage is proportional to the square

of the operational frequency, therefore a lower frequency will have a better propagation distance. CR networks should prefer spectrum band with better propagation characteristics when considering coverage, power consumption or latency.

3.3.2 Primary Users Protected Zone

Based on the concept of coverage range, the performance of a PU receiver can be modelled as a function of its distance from the PU transmitter. Therefore, the coverage area of the PU transmitter must be protected from any CR transmissions to prevent any interference from the unlicensed users affecting the licensed users. The coverage range of a Primary User Base Station (PUBS) transmitter can be defined in many ways. For instance, once a target signal-to-noise ratio (SNR) is fixed, the maximum distance from the PU transmitter which guarantees that a PU receiver is able to decode the signal and achieve the targeted SNR is known as the coverage area. Assuming flat Rayleigh fading for the PUs and the maximum transmission power of the PUBS transmitter is fixed and equal to PU^{tx}_{power}, the SNR at distance d from the PU transmitter is given by,

$$SNR(d) = \frac{PU^{tx}_{power}\ \sigma}{N_0}\ d^{-\beta}\ |h|^2, \tag{3.2}$$

where N_0 is the noise power, β is the path loss exponent, σ is the attenuation factor considered as constant due to shadowing effects and h is the channel fading gain distributed as a complex Gaussian random variable with zero mean and unit variance. The PU's protected zone (the radius of the protected contour) of a primary user j using channel k is defined as the distance at which the average SNR at the PU receiver is equal to a given value γ. Therefore,

$$Z(PU^k_j) = \Big(\frac{PR^{tx}_{power}\sigma}{\gamma\ N_0}\Big)^{\frac{1}{\beta}}. \tag{3.3}$$

The CR broadcast protocol must provide protection to the PU receivers by reducing the possibility of interference within the PU protected area.

3.3.3 Average Overlapping Degree

The potential interference to the existing PU receivers can be mapped as the size of the intersection region between the coverage areas of a PU and the CR transmit-

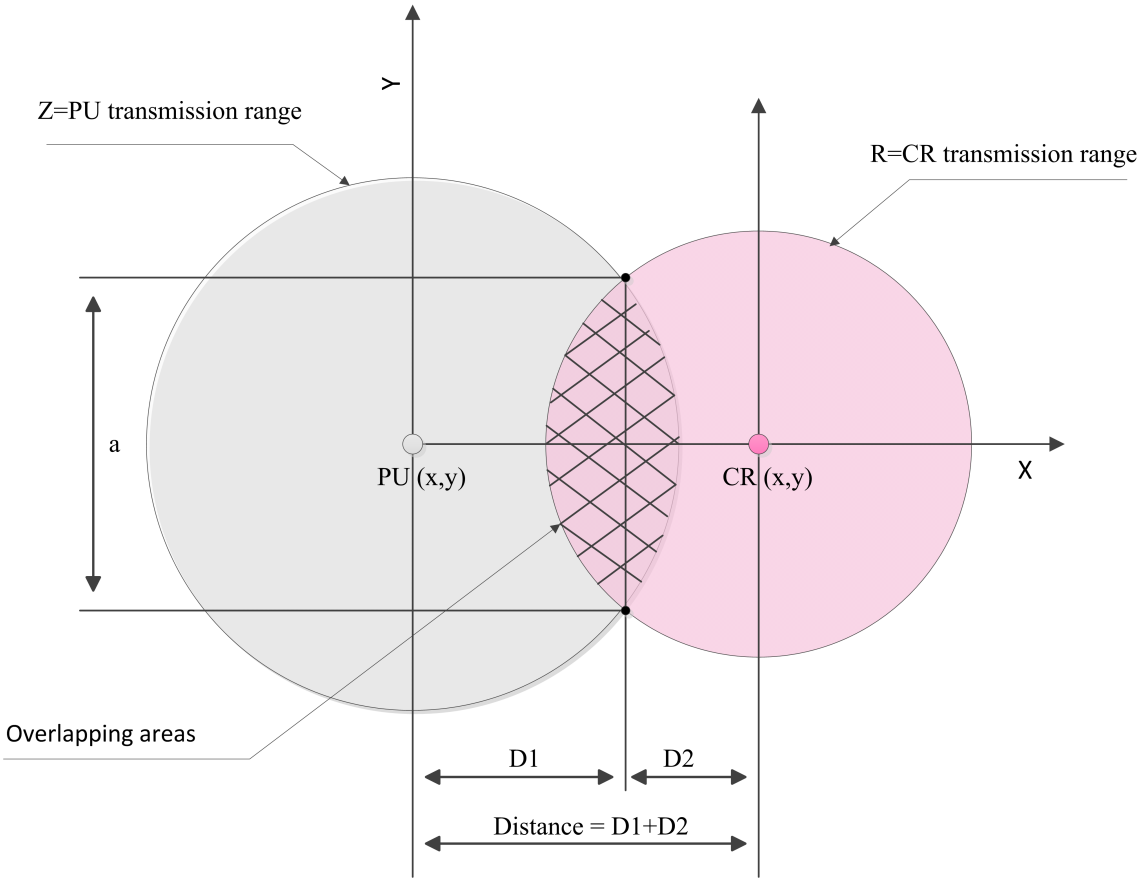


Figure 3.5: General overlap case between PU transmitter and a CR node.

ters. Reducing this vulnerable region will minimize interference to primary radio communications. Figure 3.5 shows two nodes PU_j and CR_i represented by two circles of radii equal to the PU_j and the CR_i transmission ranges $Z(PU_j)$ and $R(CR_i)$, respectively. We start by calculating the expected area of intersection between the two nodes. Practically, the CR user can use the radio resources if no PU receivers exist within its transmission area.

Let Ψ be the Euclidean distance between CR_i and PU_j.

$$\Psi_{i,j} = \sqrt{(x_{cr} - x_{pu})^2 + (y_{cr} - y_{pu})^2}. \tag{3.4}$$

CR_i and PU_j completely overlap if $\Psi = 0$, and there is no overlapping if $\Psi \geq R(CR_i) + Z(PU_j)$. To obtain the average intersection area between CR_i and PU_j, assume that the two circles intersect in some area $I(CR_i, PU_j)$. Then the in-

tersection area $I(CR_i, PU_j)$ can be obtained based on geometrical calculations [36],

$$I(CR_i, PU_j) = R(CR_i^k)^2 \cos^{-1}\left[\frac{R(CR_i^k)^2 - Z(PU_j^k)^2 + \Psi^2}{2\Psi R(CR_i^k)}\right] + Z(PU_j^k)^2 \cos^{-1}\left[\frac{Z(PU_j^k)^2 - R(CR_i^k)^2 + \Psi^2}{2\Psi Z(PU_j^k)}\right] - \frac{1}{2}\sqrt{W(W - 2R(CR_i^k))(W - Z(PU_j^k))(W - 2\Psi)}, \quad (3.5)$$

$R(CR_i^k)$ is obtained from equation (3.1), $Z(PU_j^k)$ is the radius of the protected contour of the primary user transmitting on the k^{th} channel obtained from equation (3.3), Ψ is the distance between the CR and PU nodes as shown in Figure 2 and $W = (\Psi + R(CR_i^k) + Z(PU_j^k))$. If both PU and CR users have the same transmission range (R), the average intersection area can be simplified to,

$$I(CR_i, PU_j) = 2R^2 \cos^{-1}\left[\frac{\Psi}{2R}\right] - \frac{1}{2}\Psi\sqrt{4R^2 - \Psi^2}\ . \quad (3.6)$$

Using these results, the average overlapping degree (AOD) can be calculated as:

$$AOD_{i,j}^k = \frac{I(CR_i^k, PU_j^k)}{\pi Z(PU_j^k)^2}\ . \quad (3.7)$$

In a scenario where multiple PU transmitters occupy the k^{th} channel, the CR user's transmission might affect a set of PU protected zones according to their positions in the plane. In order to exploit the spectrum efficiently and guarantee the performance of the PU communication, we need to calculate the total average overlapping degree of the channel before using it.

$$AOD_{i,j}^k = \sum_{j=1}^{N} AOD_{i,j}\ . \quad (3.8)$$

The overlapping region represents the area where PU receivers may be presented. In order to protect these PU receivers, each CR node must choose the channel that has the minimum overlap with the PU's protected zone for its transmission. The average overlapping degree is a valuable input metric which must be considered when developing a protocol for cognitive radio networks.

3.3.4 Probability of Spectrum Availability

The performance of CR networks is closely related to the activities of the primary users over licensed channels. Therefore, the estimation of these activities plays an essential role in the performance of any cognitive radio protocol. The PU activity model has been used very widely in the literature [36], [100], [101], [102], [103], [104], [105]. The primary user traffic can be modelled as an alternating renewal process consisting of *ON* (busy) and *OFF* (idle) periods. In this model, both *ON* and *OFF* periods of the primary users are assumed to be independent and identically distributed (i.i.d.), where the alternating renewal process is modelled as a two state birth-death process with death rate λ_{off} and birth rate λ_{on} [65], [103], [104],.

Let $\frac{1}{\lambda_{on}}$ and $\frac{1}{\lambda_{off}}$ be the average *ON* and *OFF* times of the k^{th} channel. The probability of the k^{th} channel being busy is given by:

$$P_{busy}^{k} = \frac{\lambda_{off}}{\lambda_{on} + \lambda_{off}} \ , \tag{3.9}$$

where $1 \leq k \leq K$ (the total number of channels). Therefore, the probability of utilizing the k^{th} channel (i.e., the channel being idle) without causing harmful interference to the primary users is:

$$P_{idle}^{k} = 1 - P_{busy}^{k} = \frac{\lambda_{on}}{\lambda_{on} + \lambda_{off}} \ . \tag{3.10}$$

Let Φ represent the set of channels that meet the user requirements, i.e. channels that have a probability of availability equal to or greater than the threshold probability P_{th}. From equation (3.10), for each CR node the set of channels Φ is chosen such that:

$$\Phi_{idle}^{k} \geq P_{th}, \forall k \in \Phi : 1 \leq k \leq K. \tag{3.11}$$

3.3.5 CR User Connectivity

Successful packet delivery in CR networks depends on a good channel selection algorithm. In fact, selecting a channel that connects a larger number of CR neighbours as a broadcast channel will result in a high level of network connectivity and consequently increase the packet delivery of the broadcast packets [106], [100]. The CR connectivity (CRC) reflects the ratio of CR neighbours having the same channel used by the transmitter in their unoccupied channel list. For a particular CR

user i broadcasting on channel k, the CR users' connectivity of the k^{th} channel is calculated as follows:

$$CRC_i^k = \frac{\varphi}{\Omega} \ , \tag{3.12}$$

where φ is the total number of neighbours who share the same channel k in their free channel list Φ, and Ω is the total number of single-hop neighbours of CR user i.

As connecting most of the CR users is important, each CR node must choose the channel that has maximum connectivity with its single-hop CR neighbours for its transmission. The CR users' connectivity is an important input metric when developing a broadcast protocol for cognitive radio networks.

In order to calculate the CR user connectivity, each CR user needs to acquire information regarding neighbouring nodes and their channel availability. This information can be obtained through the neighbour discovery mechanism as in [106]. In addition, our proposed protocol can jointly work with any neighbour discovery mechanism.

3.3.6 Broadcast Channel Selection Optimization

The CR node autonomously identifies the best channel locally available for broadcasting based on combining the above described metrics for the preferred objective. In order to better investigate the trade-off between maximizing the successful broadcast ratio as well as maximizing the protection to PU communications. We formulate two optimization functions, maximize PU protection (MPUP) and maximize CR connectivity (MCRC). They achieve two different broadcast goals, along with the constraints as given below:

$$\text{To find: } Channel\ k \in K, \tag{3.13}$$

$$MPUP : \text{To Minimize: } = AOD_{i,j}^k \ R(CR_i^k), \tag{3.14}$$

$$(or)$$

$$MCRC : \text{To Maximize: } = CRC_i^k \; R(CR_j^i), \tag{3.15}$$

Subject to:

$$P_{idle}^k \geq P_{th}, \tag{3.16}$$

$$CRC_i^k \geq \frac{1}{\Omega}, \tag{3.17}$$

$$AOD_{i,j}^k < \xi. \tag{3.18}$$

1) *MPUP broadcast:* The major objective of this function is the protection of the primary users, particularly the undetected PU receivers. The interference between the i^{th} CR transmitter and the primary receivers in the j^{th} PU protected zone is mapped as a function of average overlap, $AOD_{i,j}^k$. Since the primary users communication protection is considered more important than CR connectivity in this type of broadcast, our optimization function tries to minimize the product term of the CR propagation distance, $R(CR_i)$, and the average overlap between cognitive-primary transmission coverages. Minimizing the value of the metric $AOD_{i,j}^k$, will result in improving the PU receivers' protection. Moreover, smaller distances for CR propagation cause a smaller probability of interference to PU users. The optimization function chooses the best channel k which has the minimum overlap with the PU protected zone. Algorithm 3.1 represents the details of our proposed distributed channel selection for this objective.

2) *MCRC broadcast:* For this broadcast class, the priority is to increase the packet delivery reliability by increasing the CR network connectivity. The propagation distance for a given transmission power and the CR connectivity are composed in one product term *MCRC*. Hence, *MCRC* is maximized to enhance the transmission coverage of CR users so that the highest number of CR nodes can receive the transmitted packets over the largest possible transmission distance. The optimization function selects the most efficient channel that maximizes the CR network connectivity. Algorithm 3.2 represents

the details of our proposed distributed channel selection for this objective.

The choice of the channel must meet the user-specified constraints (equations 3.16, 3.17 and 3.18):

(i) The channel availability at each CR node must meet the user-assigned constraint in equation (3.16). In this work, we assume that Φ is the set of channels that probabilistically meets the constraint of channel availability, P_{th}.

(ii) The φ^k in the CR users' connectivity formula (CRC_i^k) reflects the number of CR neighbours who might be using the k^{th} channel for communication. If none of the neighbours share this channel with the sender (i.e., $\varphi^k = 0$), then broadcasting over this channel will result in a disconnected CR network.

(iii) Finally, the average overlapping degree AOD_i^k must not exceed the maximum threshold of interference, ξ, which is specified by the user in equation (3.18).

The pseudo-codes for selecting the broadcasting channels are shown in Algorithm 3.1 and 3.2.

3.3.7 Protocol Flow Chart

This section summarizes the procedure of the proposed broadcasting schemes. In Figure 3.6, we illustrate the flow chart of the proposed broadcast protocol. As shown in the flow chart, before the starting of the broadcast process, every CR node first classifies its locally available set of channels and discovers its single-hop neighbouring nodes using the neighbour discovery scheme proposed in [106]. If the main goal of broadcasting is to protect primary receivers, each CR node calculates the overlapping degree of all the available channels with the PU protected zones and selects the broadcasting channel based on Algorithm 3.1. On the other hand, if the priority is to maximize data dissemination, CR node uses the best channel that offers best connectivity with its single-hop neighbouring nodes and broadcasts message based on Algorithm 3.2. Every CR node uses either Algorithm 3.1 or Algorithm 3.2 according to the broadcast goal, whether it is the source or the receiver node. Since all nodes in the close vicinity are more likely to share the same channel availability, and as all nodes use the same metrics to select the broadcasting channel, there is high probability to guarantee channel rendezvous.

Algorithm 3.1 *Selecting the broadcast channel BC_i for a CR node i, priority to PU receivers protection*

1: INPUT: $\Phi_{idle}, \Omega_i, R(CR)_i, AOD_i$

2: OUTPUT: BC_i

3: $BC_i \leftarrow \emptyset$

4: $u \leftarrow 1$

5: $min \leftarrow R(CR)^1.AOD^1$

6: **for** $u = 1$ to K **do**

7: **if** $R(CR)^u.AOD^u < min$ **then**

8: $min \leftarrow R(CR)^u.AOD^u$

9: $BC_i \leftarrow u$

10: **end if**

11: **end for**

12: **return** BC_i

Algorithm 3.2 *Selecting the broadcast channel BC_i for a CR node i, priority to CR connectivity*

1: INPUT: $\Phi_{idle}, \Omega_i, R(CR)_i, AOD_i$

2: OUTPUT: BC_i

3: $BC_i \leftarrow \emptyset$

4: $u \leftarrow 1$

5: $max \leftarrow R(CR)^1.CRC^1$

6: **for** $u = 1$ to K **do**

7: **if** $R(CR)^u.CRC^u > max$ **then**

8: $max \leftarrow R(CR)^u.CRC^u$

9: $BC_i \leftarrow u$

10: **end if**

11: **end for**

12: **return** BC_i

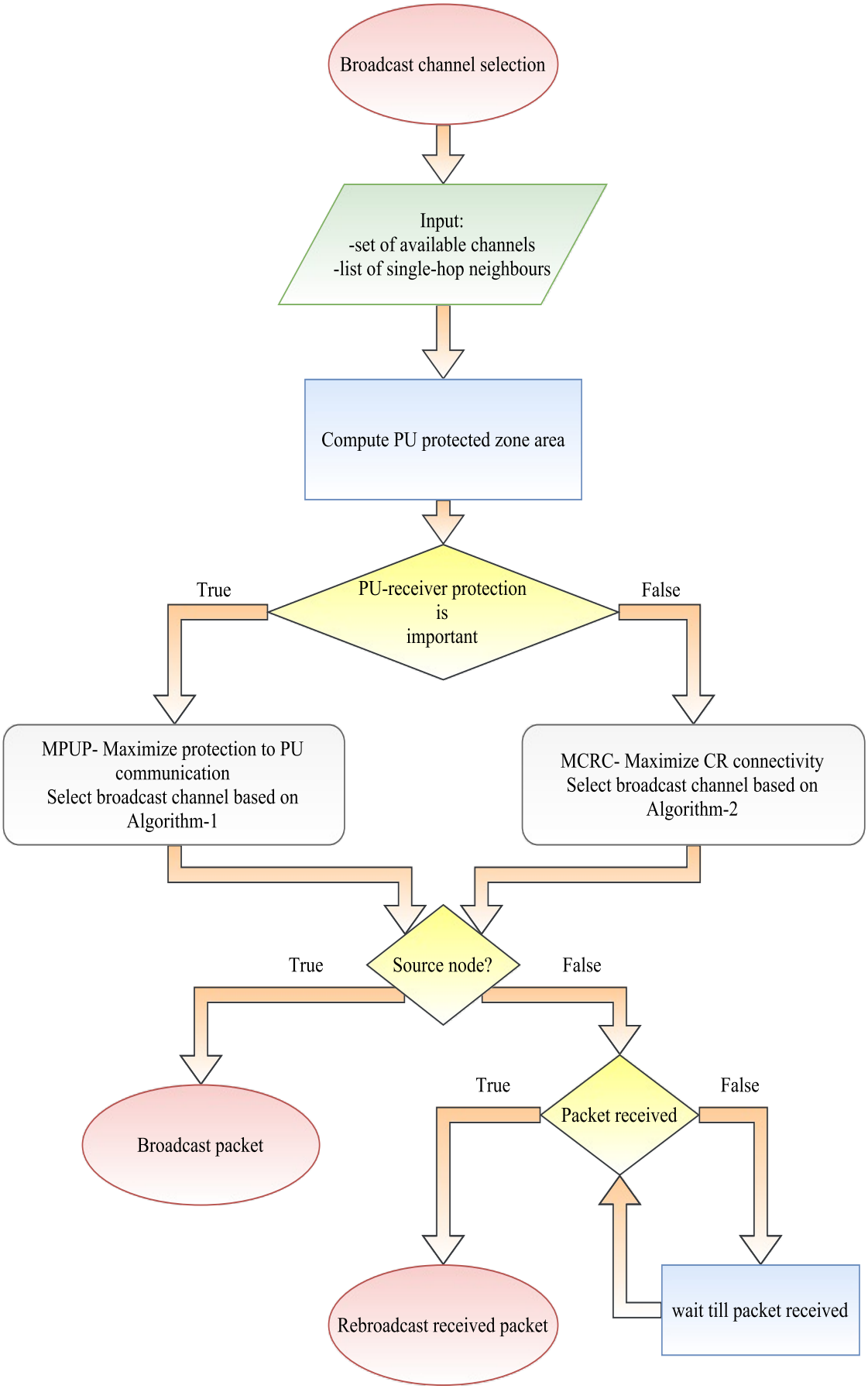


Figure 3.6: Proposed broadcast protocol flow chart

3.4 Performance Evaluation

In this section, we analyse the performance of our proposed broadcasting protocols, *MPUP* and *MCRC* through extensive simulations.

3.4.1 Implementation Setup

We have implemented the proposed protocols using the Cognitive Radio Cognitive Network (CRCN) patch of the NS-2 simulator [107]. As shown in Figure 3.7, there are three building blocks that support the functionalities of CR networks in the Cognitive Radio Cognitive Network (CRCN) patch of the Network Simulator (NS-2). These blocks are the cognitive radio physical layer, the cognitive radio MAC layer and the cognitive radio network layer. The physical layer supports several functions, like propagation model, controlling the transmission power, SNR, etc. The MAC layer is responsible for spectrum sharing and mobility, keeping track of PU traffic activity, etc. The network layer maintains the neighbour list and the routing information. In addition, It is responsible for making the channel selection based on the information shared between all the layers. The cross layer coordinator collects and shares the information with multiple layers in order to achieve the highest possible adaptivity of the CR network. The activity of PU nodes is not modelled in the basic design of the CRCN patch. Therefore, we have developed the CRCN patch by modelling the PU activity block (dotted box) as shown in Figure 3.7.

The main responsibilities of the PU activity block are to generate and keep track of PU activities over all the spectrum bands. i.e., keep tracking the spectrum utilization over the simulation time (sequence of OFF and ON periods by PU nodes). Accordingly, channel availability follows these parameters.

3.4.2 Performance Parameters

We assume the primary users are the TV broadcast towers, where its locations are fixed and known by the CR users. We consider a network topology of a square region with sides 1000 m that is further divided into four square cells as shown in Figure 3.8. Four PUs were located at the centre point of the cells and a total of 100 CR nodes are randomly distributed in the whole area. We consider the free space

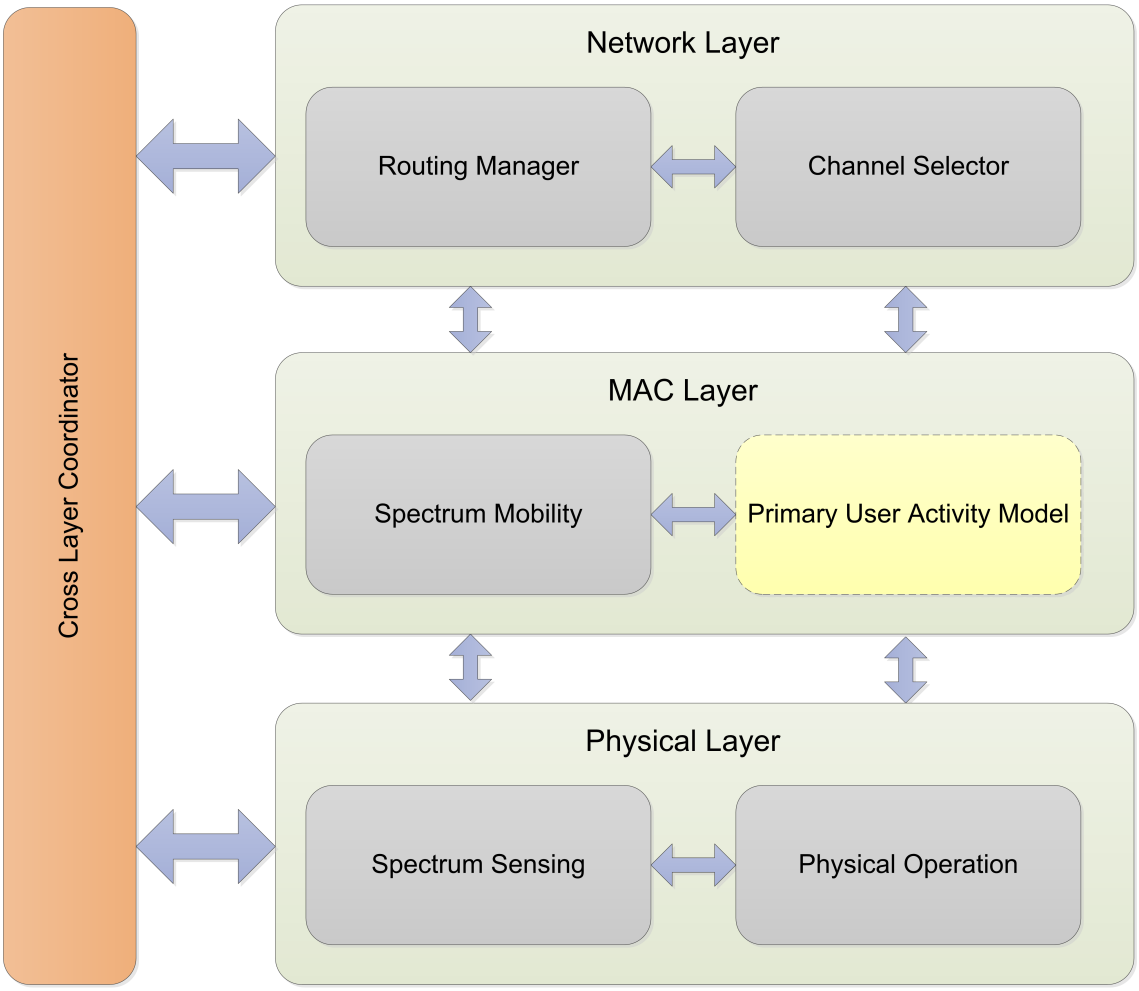


Figure 3.7: The CRCN patch of NS-2 including the PU activity model.

path loss model for CR users and Rayleigh fading channels for PU users. The PU transmitters have a transmission range of 250 m, while the transmission range of each CR node is 100 m. In addition, each CR also has a circular sensing range with a radius of 150 m. Hence, if a PU is currently active within the sensing range of a CR node, the corresponding CR is able to detect its activity. In order to get stable performance results, we repeat the experiments for 1000 times and the results are averaged, where each packet is sent by a randomly selected CR node. Since our goal is to efficiently disseminate the broadcasting data, protect the PU receivers from harmful interference and rendezvousing both CR transmitter and receiver nodes. In this chapter, we define the following performance metrics:

(i) Interference risk for PU-receiver: the interference probability of the total number of times CR packets collide with the PU receivers over the total number of broadcasting packets

(ii) Interference-time product received: the sum of the product of both the received

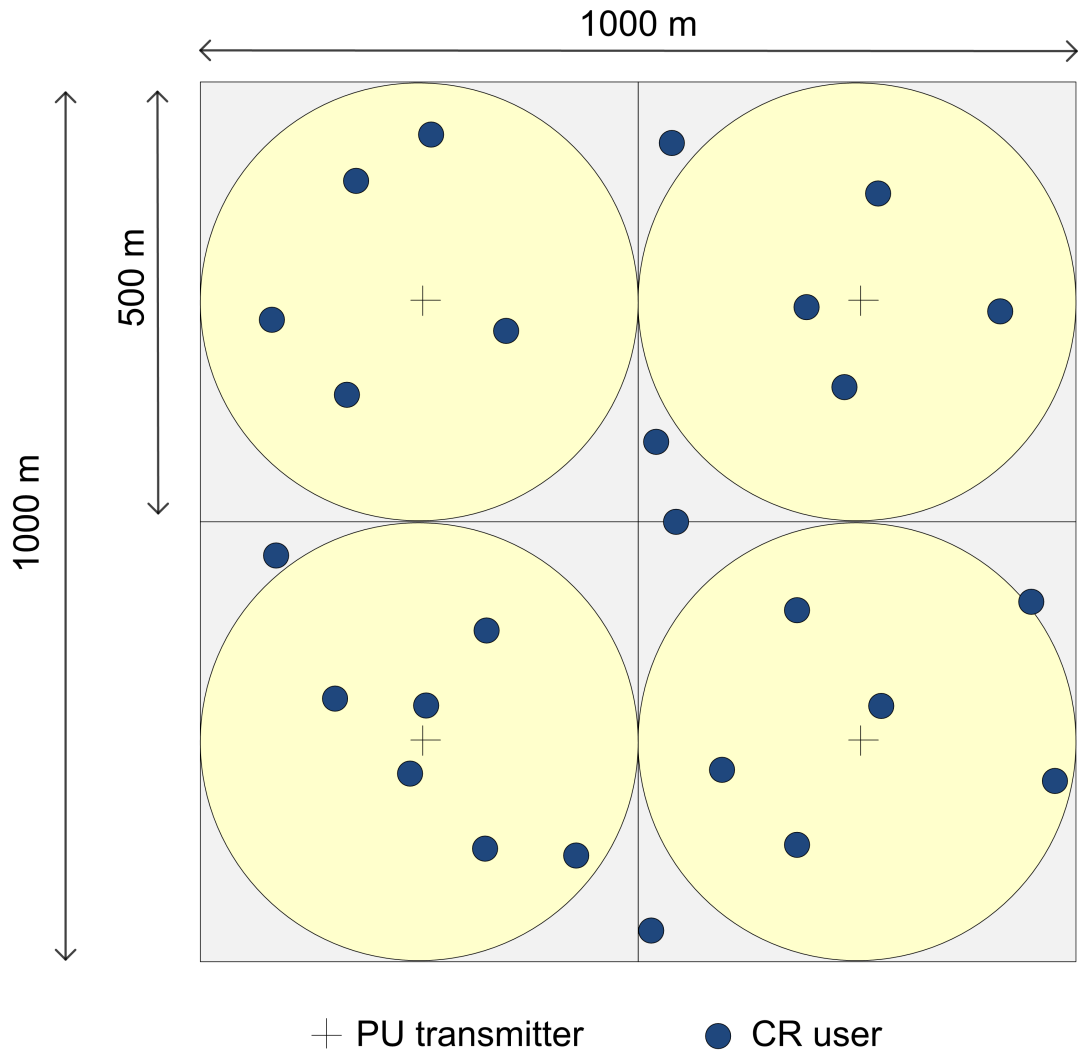


Figure 3.8: Topology used for performance evaluation.

CR powers and the time for which this power is detected by the primary nodes

(iii) Successful packet delivery ratio: the average number of packets successfully delivered in the network

(iv) CR network connectivity: the accumulative number of CR receivers per hop that successfully received the broadcast packet

In addition, we compare our work with the distributed broadcasting protocol (DBP) proposed in [43].

3.4.3 Protection to PU Receivers

In the first set of experiments, we are interested in comparing the performance of the proposed algorithms from the viewpoint of the PU-receiver protection. We define the interference probability as the ratio of the total number of times CR packets

collide with the PU receivers over the total number of broadcasting packets. It can be clearly seen from Figure 3.9, that our proposed protocol *MPUP* causes less harmful interference to the PU nodes. This is primarily because, in *MPUP*, the CR nodes opportunistically select the channel that causes the least overlap with the PU protected zone which in turn reduces the interference probability with PU receivers. *MPUP* reduced the interference collision by more than 24% for moderate PU activity and up to 40% for higher PU activity over the channels when compared to DBP. Although, *MCRC* does not consider the PU receivers that might exist in the PU protected zones, it always outperforms DBP by using the channel which has the lower probability of occupancy. It can be noted that the interference probability increases with PU activity. This is because more channels will be occupied by PUs which makes it difficult to find a channel that does not interfere with the PU communication.

The average CR transmitted power and the duration for which this power is observed at the PU receivers is measured to evaluate the interference risk of the proposed protocol onto locations inside the PU protected zones. We define the interference-time product for the PU receivers operating on the primary channel as the sum of the product of both the received CR powers and the time for which this power is detected by the primary nodes. The interference to PU receivers depends on the average overlapping area as well as the PU activity over the selected channel. As can be observed from Figure 3.10, the collision risk with the PU receivers is trivial for *MPUP*. This is due to the appropriate optimization metrics that result in selecting the proper channel for broadcasting which must avoid any overlapping with the PU receivers' protected area. It is observed that the proposed protocols have the best protection for PU communication, particularly *MPUP* which guarantees the protection for PU receivers in the PU zones. As shown in Figures 3.9 and 3.10, the proposed broadcast protocol outperforms other schemes in terms of less interference collision risk with PU receivers.

3.4.4 CR Performance

In this set of experiments, the packet delivery ratio and the CR network connectivity have been measured in order to evaluate the performance of the broadcast protocols from the viewpoint of the CR network.

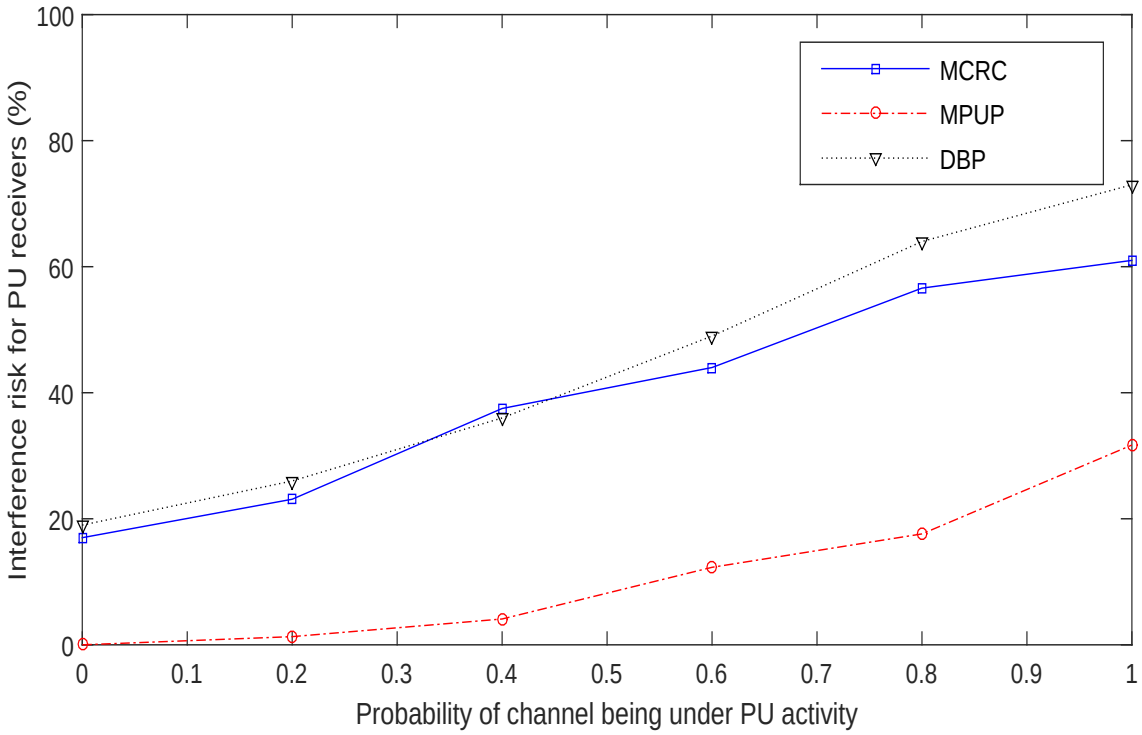


Figure 3.9: Probability of PU interference due to transmissions from CR users on occupied channel.

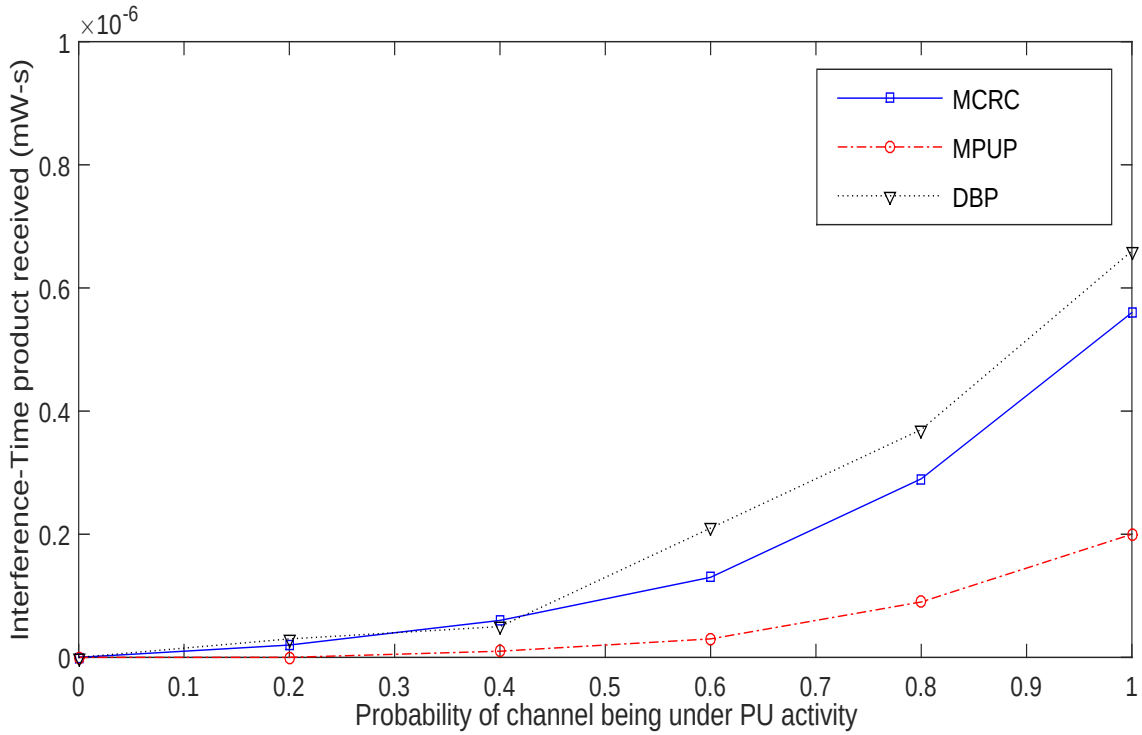


Figure 3.10: The effect of CR users transmissions on PU receivers.

We define the average delivery of packets as a metric to evaluate the process of data dissemination reliability. Figure 3.11 shows the percentage of messages received by CR nodes under varying channel availability. It is clear that *MCRC* outperforms other techniques for data delivery reliability. The packet delivery ratio for *MCRC* is nearly double the packet delivery ratio for *MPUP*. This is due to the fact that the main objective in *MCRC* is the CR network reachability. Hence, the CR users prefer to select the channel that offers the maximum connectivity with the CR nodes in their vicinity. On the other hand, avoiding interference to PUs is of paramount importance in *MPUP*. Consequently, CR nodes under the PU coverage zone for the chosen channel are no longer reachable by CR transmitter nodes. Nevertheless, *MCRC, MPUP* and *DBP* exhibit a gradual increase in the packet delivery ratio as the probability of the channel availability increases. This is due to the fact that lower PU activity increases the chances for CR nodes finding PU-free channels for their transmission. It is worth noting that the diversity in the channel availability and the PU activity will result in the creation of different CR topologies [106], which makes it hard to reach a higher number of CR nodes in the neighbourhood. By using the appropriate metrics and employing the same intelligent algorithms, we achieve better results.

Furthermore, we also consider the CR network connectivity as a metric to evaluate the CR performance of our proposed broadcasting algorithms. The CR connectivity is explained as the mean of accumulative receivers that successfully received the transmitted packet. Figure 3.12 represents the number of accumulative CR receivers for each algorithm. *MCRC* achieves better network connectivity compared to *MPUP*. As in *MCRC* the priority is to select the channel which offers the largest coverage area and connect the maximum number of CR nodes. Increasing the coverage area will increase the average number of CR nodes reached by a single transmission which results in better reachability. On the other hand, *MPUP* maintains the channel which guarantees extra protection to the PU receivers. Consequently, CR nodes under the PU coverage zone for the chosen channel are no longer reachable by CR transmitter nodes.

It is observed that at each new hop the ratio of CR receivers decreased. This is because the probability of collisions increases as the message propagates in the network. Therefore, for all the techniques, at each new hop, the CR connectivity decreases.

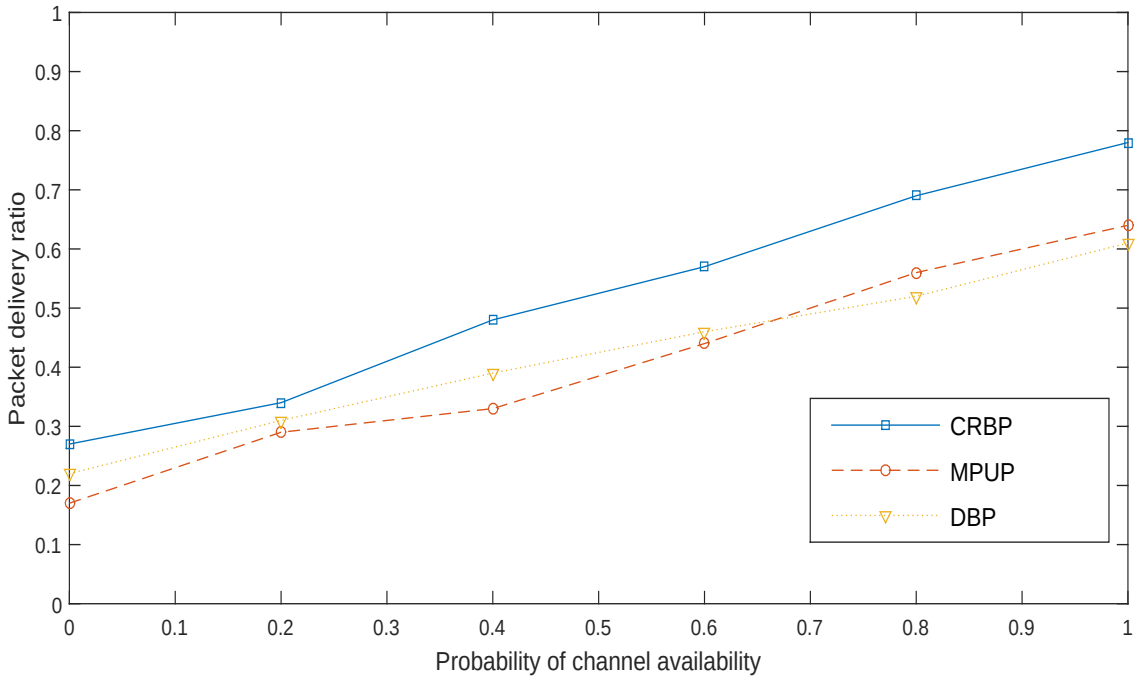


Figure 3.11: Successful broadcast ratio using different probabilities of channel availability.

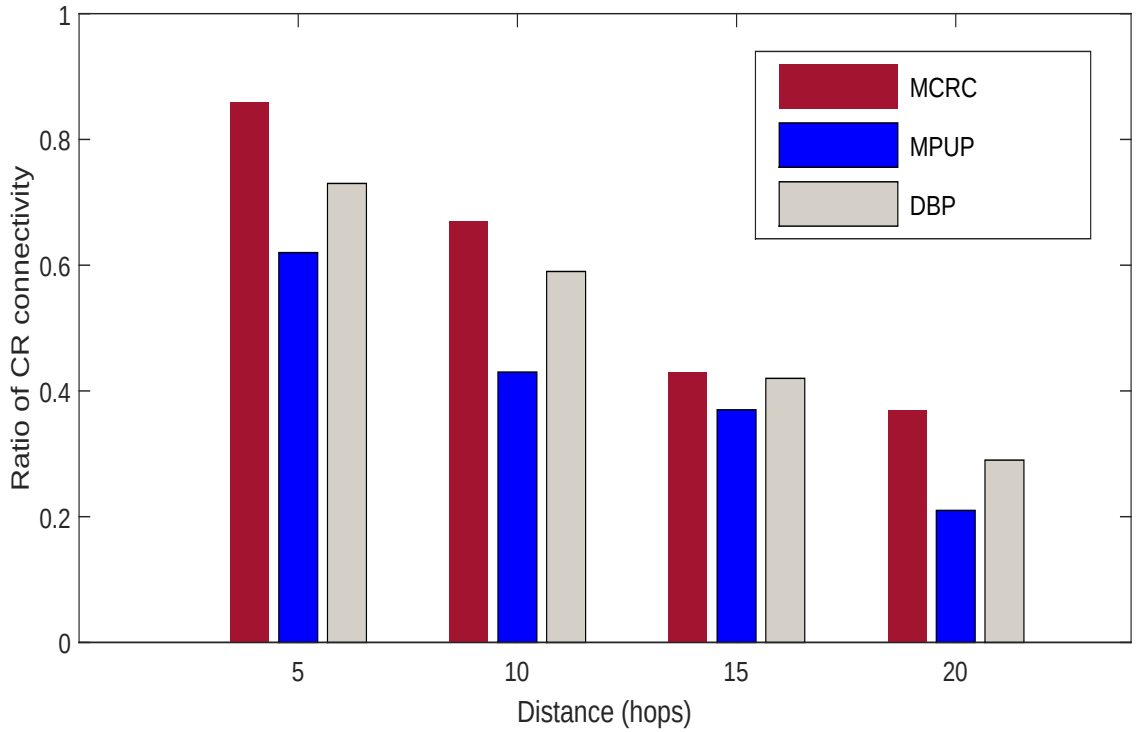


Figure 3.12: Ratio of average number of CR neighbours per hop that successfully receive the transmitted packet.

3.5 Conclusion

In this chapter, we proposed a fully-distributed broadcast protocol for CR ad hoc networks that makes the following contributions: i) alleviates the interference collision risk to PU communications; ii) guarantees protection to the PU receivers and iii) provides a high successful broadcast ratio. Furthermore, we consider practical scenarios in our design where no global network topology is known or no common control channel is assumed to exist. A key novelty of this work is the formulation of the broadcast issue from the viewpoint of protecting PU receivers, which is a distinctive feature in CR networks.

Chapter 4

Broadcast Protocol for Cognitive Radio Ad Hoc Networks

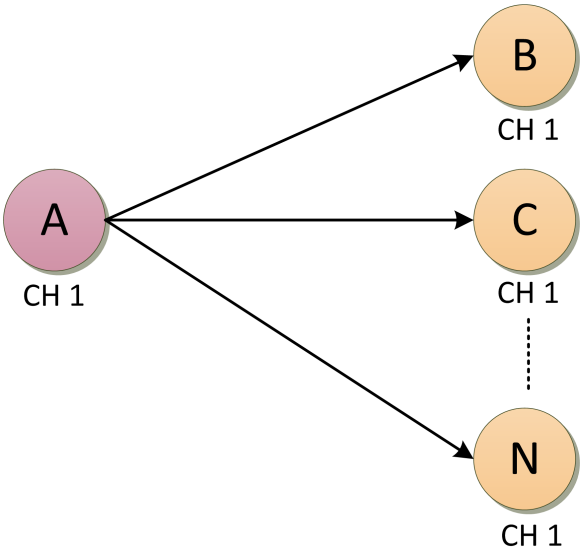
In this chapter, a distributed reliable Cognitive Radio Broadcast Protocol (CRBP) for cognitive radio ad hoc networks is proposed that makes the following contributions: (i) reliable data dissemination, (ii) joint transmitter-receiver channel selection, (iii) protection of primary users' communication and (iv) coordinating the broadcast process without the need for a common channel. A key novelty of the proposed CRBP is the formulation of the broadcast problem from the viewpoint of connecting different local topologies, which is a unique feature in cognitive radio networks. We jointly map the network topologies and the spectrum observations onto a bipartite graph which allows the channel selection undertaken at each node to capture the spectrum information and the environmental topologies of all the neighbouring nodes. This secures the network connectivity and reduces the interference with primary users. The reliability is ensured by connecting different topologies and synchronizing adjacent nodes. Furthermore, we believe that the consideration of different topologies in the same neighbourhood, transmitter-receiver synchronization and the coordination of the broadcast process without a common channel uniquely distinguishes CRBP from the other works in the literature.

This chapter starts by Section 4.1, which presents the unique challenge of successful broadcasting in CR networks. Then, the system model and assumptions are described in Section 4.2. The chapter continues with Section 4.3, which presents the proposed broadcast protocol for CR ad hoc networks. Performance evaluation is conducted in Section 4.4. Finally, Section 4.5 concludes the chapter.

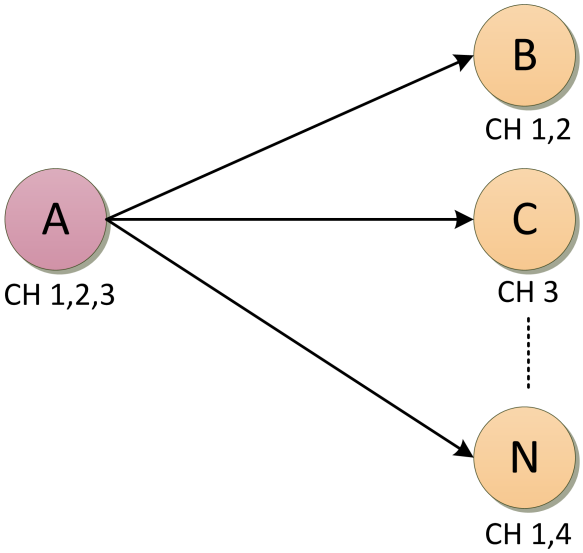
4.1 The Unique Challenge

In this section, we address the unique challenge of reliable broadcast in CR ad hoc networks. Since broadcast messages often need to be disseminated to all or most of the possible nodes, the broadcast protocol has to achieve a very high successful broadcast rate. In CR ad hoc networks, the broadcast channel for single-hop reliable broadcast may not always be one channel due to various reasons. Therefore, a CR node may not be able to deliver the broadcast message to its single-hop neighbouring node even if that node in the same transmission area. However, during the broadcast procedure, it may broadcast the packet via different channels to cover other CR nodes. This is different from the broadcast schemes in traditional ad hoc networks, whereby nodes usually broadcast messages on one channel. This feature imposes a unique challenge of identifying the broadcast channels that connect all neighbouring CR nodes to each CR node.

To further illustrate the challenges associated with broadcasting in CR ad hoc networks, we consider a simple single-hop network shown in Figure 4.1, where node A is the source node with N neighbours. In traditional single-channel or multi-channel ad hoc networks, all nodes follow the rules of a precise wireless standard. Due to uniform channel availability, broadcasting is easily implemented as all nodes can be tuned to a single common channel as shown in Figure 4.1(a). Thus, *node A* only needs to transmit over one channel to let all its neighbouring nodes receive the broadcast message. On the contrary, broadcasting in CR ad hoc networks is a challenging task and much more complicated. Allocating a single channel for broadcasting in CR networks makes the entire operation vulnerable to the PU user activity. CR users should immediately stop their transmission and vacate the channel once PU activity appears on the broadcast channel. This makes the broadcasting operation vulnerable to suspending as long as there is a PU node active on that channel. Furthermore, in CR networks different CR users might acquire different channels at different times. This prevents the allocation of one single channel for all network nodes, as shown in Figure 4.1(b), where *node A* may have to broadcast the message using different channels in order to deliver the broadcast message to all neighbours. In the worst case scenario, each neighbouring node may tune on a different channel, as a result, the source node has to broadcast over N channels. Indeed, the successful delivery of the broadcasted message for neighbouring nodes within a single hop in



(a) Traditional ad hoc network



(b) CR ad hoc network

Figure 4.1: An example demonstrating the unique challenge when selecting the broadcast channel

CR ad hoc networks relies on connecting different local topologies. The broadcast channel(s) should be carefully selected and dynamically allocated to guarantee the network operation.

4.2 System Model and Assumptions

In this section, we present the system model and the basic assumptions related to our proposed work.

4.2.1 Network Model

We consider a CR ad hoc network with no centralized coordinator. In this type of network setting, we assume network environment tasks like spectrum sensing, neighbour discovery, channel selection decision, etc., are accomplished by the CR nodes individually. The general network structure consists of a set of M Primary Radio (PU) nodes $\{PU_1, PU_2, ..., PU_m\}$ and a set of N Cognitive Radio (CR) nodes $\{CR_1, CR_2, ..., CR_n\}$ in the same geographical area. Primary nodes can access their designated licensed spectrum with no restriction. While, CRs can access licensed bands opportunistically, i.e. they are allowed to use the idle licensed bands only if they do not interfere with ongoing PU transmissions. Note that an idle state describes the temporal availability of a channel. To prevent interference, CR users are capable of sensing spectrum opportunities using energy detectors, cyclostationary feature extraction, pilot signals or cooperative sensing [7], [66], [69], [71] [72]. Our proposed protocol can work with any underlying MAC protocol or spectrum sensing techniques.

We consider the set of K non-overlapping orthogonal frequency channels ($C_{global} = C_1, C_2, ..., C_k$), which may be freely occupied by the PU. Each CR node knows the global channel set C_{global} and can operate on a subset C_{local} of this global channel set depending on the local channel availability at that node, where $C_{local} \subseteq C_{global}$. For simplicity, we assume that all channels have the same capacity. However, our protocol can be easily extended to channels of different capacities. In our model, we assume that CR nodes are equipped with half-duplex transceivers that can either receive or transmit (not both) on a single channel at any given time. Each CR can swiftly hop between channels using software defined radio (SDR) technology. The utilisation of a single transceiver lowers the operative cost of the CR device [108], and avoids any possible interference between adjacent transceivers due to their close proximity [109]. Each CR has a circular transmission range with a radius of CR_t. All CR nodes within the transmission range of the sender are considered as single-hop neighbouring nodes. In addition, every CR has a circular sensing range with a radius of CR_s. Moreover, the CR node is able to detect any PU who is currently active on the spectrum and within the sensing range of the corresponding CR. Since different CR users have different local sensing ranges which may include different PU activities, their acquired available channels may be different.

Table 4.1: Symbols used for CRBP description

Symbols	Descriptions
N	Set of CR nodes
C_{global}	Total number of channels
C_i	The available channel set of CR_i
N_i	Set of single-hop neighbours of CR_i
T_s	Spectrum sensing time for CR users
T_t	Transmission time for CR users
C^r_{PU}	Transmission range of PU users
C^r_{CR}	Transmission range of CR users
$\mathcal{G}(\mathcal{X}, \mathcal{Y}, \mathcal{E})$	Bipartite graph
$e(i, j)$	The link that connects CR_i and CR_j
BCS_i	Broadcast channel set of CR_i
TC_i	Tuning channel of CR_i

Throughout this chapter, we assume the channel status does not change in a short period of time, i.e., channel availability is relatively stable with respect to the protocol execution time. Therefore, this work is more suited to spatial spectrum underutilization and the case of temporal underutilization when the PU activities are not very dynamic. The main notations used in the chapter are summarized in Table 4.1 for easy reference.

In the rest of the chapter, we use the term "sender" to indicate a CR node that wants to issue a new broadcast or rebroadcast the received packet. In addition, we use the term "receiver" to indicate a CR that has not yet received the broadcast packet.

4.2.2 Spectrum Sensing

Spectrum sensing aims to identify the available spectrum and prevent any harmful interference to the primary users. We assume the cognitive radio nodes undertake spectrum sensing periodically in order to detect any PU activity and ensure up-to-date information regarding the spectrum occupancy. Furthermore, we assume all CR users are synchronized to the same sensing cycles. During the sensing period, all CR users must be silent and no transmission is allowed. Consequently, the time needed to disseminate a message in the network will be affected when the CR users are unable to transmit owing to the enforcement of the silent zone. The spectrum sensing and the transmission times for any CR user are T_s and T_t respectively. Where T_t is the effective duration of time for which transmission is allowed for any

CR node on any choice of free spectrum, while T_s is the duration of time that all CR nodes must be silent for the purpose of sensing. $T_s + T_t$ gives the frame time for each user when considered together.

4.2.3 Neighbour Discovery

In order to successfully deliver the broadcast messages to all the CR nodes in each neighbourhood, CRs must discover the network topology and the common idle channels that can be used to communicate among neighbours, these tasks are typically accomplished during the neighbour discovery. In the absence of a common control channel, discovering neighbours in CR ad hoc networks is undoubtedly a challenging task, we propose a neighbour discovery mechanism to address this issue. Initially, we assume that individual nodes are tuned to different channels and have no prior knowledge of their neighbours and the network topology. Furthermore, each CR node maintains the local idle channel list based on the information received from the spectrum sensing. At the beginning of constructing the network, each CR node has to beacon its information (node's I.D and available channels) on all the locally available channels, one-by-one. As a result, all single hop neighbours that are tuned to any idle channel may receive a copy of this message. Each CR node receives this beacon message and records the transmitter's CR node information in its single-hop neighbours list N_i. After forming and configuring the network, the CR nodes do not have to beacon messages unless there is a change in their channel availability.

4.3 CRBP Broadcast Protocol

In this section, we introduce CRBP, the proposed broadcast protocol for ad hoc cognitive radio networks. The main idea of the CRBP broadcast protocol is to let the sender broadcast on the most efficient subset of its available channels from the original available channel set in order to guarantee reliable broadcasting in CR ad hoc networks. The proposed protocol decomposes a complicated CR network into a simpler CR network so that the complexity of the original CR network can be reduced and an efficient selection of broadcast channels can be acquired. The aim of CRBP is to increase the reliability and the reachability of data dissemination over multi-hop ad hoc CR networks. The CRBP protocol adapts itself according

to the current network characteristics to guarantee successful broadcast operation. Thus, every CR node autonomously classifies the available channels based on local observations of PU activities over these channels. This classification is then refined by identifying the minimum set of channels that should be used for broadcasting. The tuning channel for a given node is selected from this set, which is the best channel in the set that has no PU activity and could serve a higher number of CR neighbours. The tuning channel selections of both the sender and the receiver are designed for guaranteed channel rendezvous.

The CRBP tries to converge CRs which have similar spectrum opportunities to the same tuning channel so as to increase the network connectivity, which in turn reduces the number of transmissions over multiple channels and the delay in packet dissemination. The reason for pursuing such a goal is twofold. Firstly, grouping CRs with similar available channels implicitly implements hard-decision cooperative sensing [76, 110]. Secondly, it reduces the size of the channel set required to connect all the neighbouring nodes. To ensure the packet is conveyed to all the neighbouring nodes for each packet transmission, the sender broadcasts the packet over a minimum set of idle channels that are common between the sender and the neighbouring nodes in its vicinity. Additionally, CR nodes with no data to transmit classify the channels based on the same criteria in order to tune to the best channel for data reception.

Using the same criteria for all nodes in the network, allows CR users in close geographic areas to select, with high probability, the same channel set. It is likely that CR nodes in the sender's vicinity have the same PU activity, hence channels available to a CR sender are also available to its neighbours with high probability [111]. Therefore, CRBP increases the probability of creating a connected topology. Once a packet is received, every intermediate CR receiver undergoes the same procedure again to convey the message to its neighbours. CRBP is designed with the following properties in mind: (i) decentralization: distributed implementation of channel allocation, (ii) convergence: CR users with the same available channels individually converge to the same channel decisions, (iii) delay and communication efficient: channel allocation is achieved with no exchange of messages and (iv) adaptability: reallocation is required only in the case where there is a change in the network topology.

4.3.1 Probability of Channel Availability

The performance of CR networks is closely related to the activities of the licensed users over the licensed channels. Therefore, the estimation of these activities plays an essential role in the performance of any cognitive radio protocol. The primary user traffic can be modelled as an alternating renewal process consisting of *on* (busy) and *off* (idle) periods [7,101,102]. This PU activity model has been used very widely in the literature [36, 100–105]. The *on* time represents the period where the channel is occupied by a primary user, while the *off* time indicates the channel is free and can be used for cognitive radio transmission without causing any harmful interference to PU nodes. In this model, the *on* and *off* periods of the primary users are assumed to be independent and identically distributed (i.i.d.), where the alternating renewal process is modelled as a two state birth-death process with death rate μ_{off} and birth rate μ_{on} [102]. Since each PU node arrival is independent, the lengths of the *on* and *off* periods are exponentially distributed with mean value equal to β_n and α_n, respectively [101, 112].

Let $\frac{1}{\mu_{on}}$ and $\frac{1}{\mu_{off}}$ be the average *on* and *off* times of the k^{th} channel. The *on* time represents the period where the channel is occupied by a primary user, while the *off* time indicates the channel is free and can be used for cognitive radio transmission without causing any harmful interference to PU nodes. Let Φ_k^{busy} denote the probability of finding the k^{th} channel to be busy, then Φ_k^{busy} is given by

$$\Phi_k^{busy} = \frac{\mu_{off}}{\mu_{on} + \mu_{off}}, \tag{4.1}$$

where $1 \leq k \leq K$ (the total number of channels). Therefore, the probability of the k^{th} channel being idle is:

$$\Phi_k^{idle} = 1 - \Phi_k^{busy} = \frac{\mu_{on}}{\mu_{on} + \mu_{off}}. \tag{4.2}$$

Let λ^k represent the set of channels that meet the user requirements, i.e. channels that have a probability of availability equal to or greater than the threshold probability Φ_{th}^{idle}. From equation (4.2), for each CR candidate-forwarding node the set of channels λ^k is chosen such that:

$$\Phi_k^{idle} \geq \Phi_{th}^{idle}, \forall k \in \lambda^k : 1 \leq k \leq K. \tag{4.3}$$

The channel set accessibility probability $\Psi(\lambda^k)$ at each CR node can be calculated based on the availability of the chosen channel set as given below:

$$\Psi(\lambda^k) = \prod_{i \in k} \Phi_i^{idle}. \tag{4.4}$$

4.3.2 Bipartite Graph Formation

In this section, the idea of formulating the local network topology by a bipartite graph is introduced. A bipartite graph constructed by a CR node is represents both single-hop neighbours and available spectrum bands over which it can communicate. Based on the constructed graph, a CR node can select the minimum set of channels through which it can reach all its neighbours on all different local topologies. Details of constructing such a graph are explained below. In addition, an example is given to illustrate the process of the proposed protocol.

4.3.2.1 Construction of the Local Network Topology

Based on the joint temporal and spatial distribution of licensed spectrum availability, different CR nodes might observe different sets of available channels as well as different neighbours. In order to start communicating with other nodes, each CR node has to identify its idle channels, discover the neighbouring nodes in its vicinity and information about their channels. Once the CR node becomes aware of its single-hop neighbours information, it can build up its local view of the network topology.

Let $\mathcal{G}(\mathcal{V}, \mathcal{E})$ denotes the topology of a CR ad hoc network, where the set of all CR nodes in the network is denoted by $\mathcal{V}$ and the set of all links in the network is denoted by $\mathcal{E}$. The problem of selecting the best set of channels for reliable broadcast is described as: given a CR ad hoc network topology $\mathcal{G}(\mathcal{V}, \mathcal{E})$, what is the minimum set of channels that successfully connects all CR nodes of $\mathcal{G}(\mathcal{V}, \mathcal{E})$?

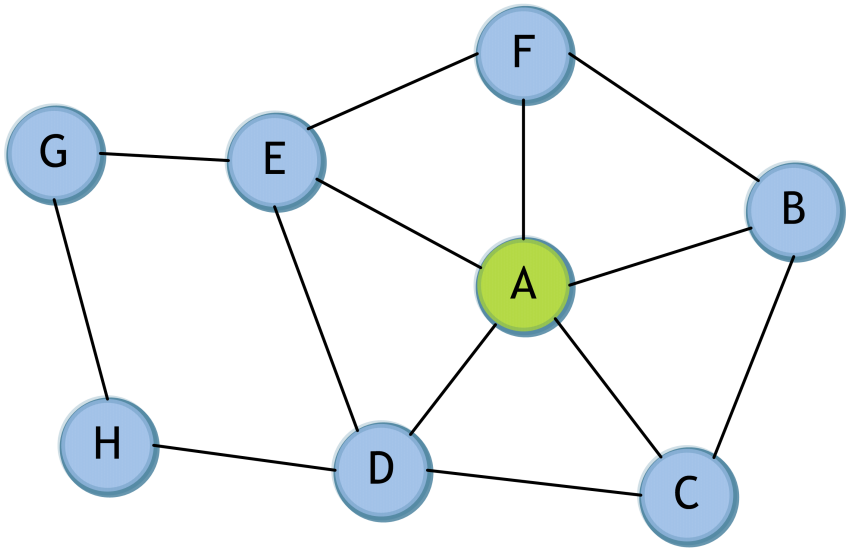
Connecting different local topologies in CR ad hoc network may not be possible through a single broadcasting channel due to various reasons. Therefore, a CR user may not be able to deliver the broadcast message to all its single-hop neighbours. However, it may broadcast the message on different channels during the broadcast procedure. This is different from traditional ad hoc networks, where nodes usually broadcast messages on only one channel. This feature imposes an exceptional

challenge of identifying the set of broadcasting channels that connects all the local topologies, especially for complex network topologies.

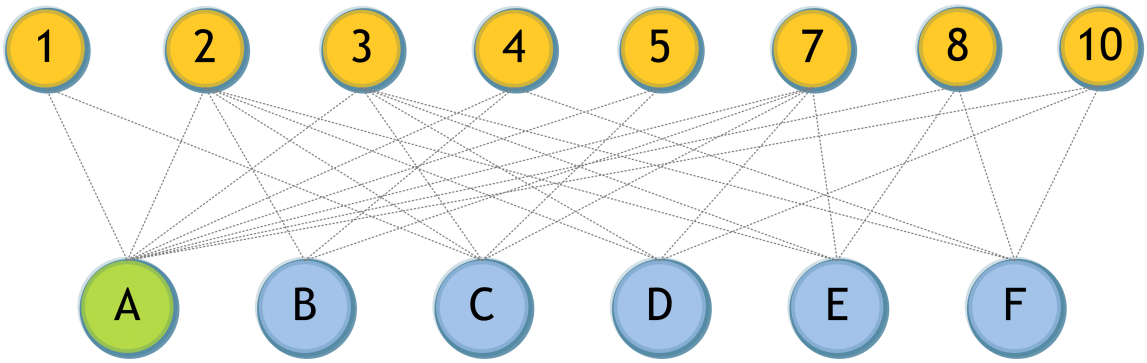
The CR network topology and the set of shared idle channels among neighbouring nodes can be jointly modelled as a bipartite graph [50]. A graph $\mathcal{G}(\mathcal{V}, \mathcal{E})$ is called a bipartite graph $\mathcal{G}(\mathcal{X}, \mathcal{Y}, \mathcal{E})$ if the set of vertices $\mathcal{V}$ can be divided into two disjoint sets $\mathcal{X}$ and $\mathcal{Y}$ with $\mathcal{X} \cup \mathcal{Y} = \mathcal{V}$, such that each edge in $\mathcal{E}$ has one endpoint in $\mathcal{X}$ and the other in $\mathcal{Y}$. As each CR_i senses a free channel set λ_i and receives information from a set of single-hop neighbours N_i on their idle channels, then it can construct an undirected bipartite graph which jointly represents the similarities between its own idle channels and the idle channels of its neighbours. For our purposes, a bipartite graph $\mathcal{G}_i(\mathcal{X}_i, \mathcal{Y}_i, \mathcal{E}_i)$ is constructed by CR_i, where the set of vertices $\mathcal{X}_i$ represents the one-hop neighbours N_i plus CR_i, the set of vertices $\mathcal{Y}_i$ represents the set of available channels λ_i, while the set of vertices $\mathcal{E}_i$ represents the common available channels between CR_i and its single-hop neighbours. An edge (x, y) exists between vertex $x \in \mathcal{X}_i$ and a vertex $y \in \mathcal{Y}_i$ if and only if $y \in \lambda_j$, i.e., channel y is in the idle channel set of both CR_i and CR_j. Note that CR_i is connected to all vertices in $\mathcal{Y}_i$, since $\mathcal{Y}_i = \lambda_i$. The graph model is then used as the basis for computing the broadcast channel set.

4.3.2.2 An Illustrative Example

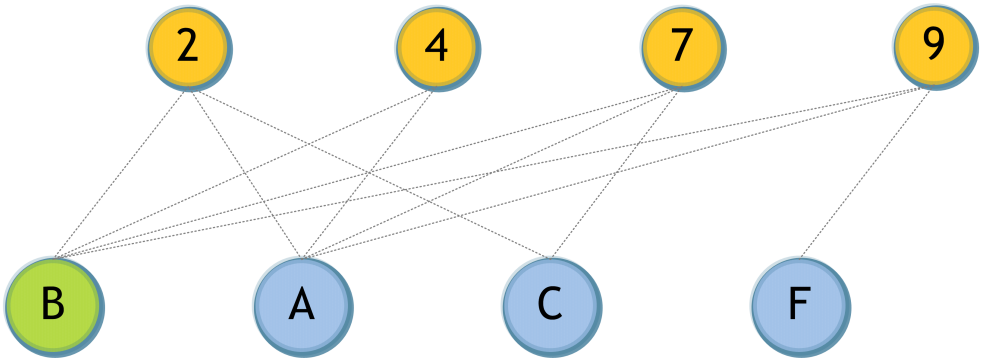
We use the example shown in Figure 4.2 to illustrate the process of constructing the bipartite graph. Figure 4.2(a) shows that the topology graph for the original CR ad hoc network consists of eight nodes. The idle channel sets for each CR node are as follows: $\lambda_A = \{1, 2, 3, 4, 5, 7, 8, 10\}$, $\lambda_B = \{2, 4, 7, 9\}$, $\lambda_C = \{1, 2, 3, 5, 6, 7\}$, $\lambda_D = \{2, 3, 7, 10\}$, $\lambda_E = \{2, 3, 7, 8, 9\}$, $\lambda_F = \{3, 4, 6, 8, 9\}$, $\lambda_G = \{3, 6, 8, 9\}$ and $\lambda_H = \{2, 3, 6, 8, 9\}$. In Figure 4.2(b), we show the bipartite graph $\mathcal{G}_A(\mathcal{X}_A, \mathcal{Y}_A, \mathcal{E}_A)$ constructed by CR_A. The set of vertices $\mathcal{X}_A$ correspond to CR_A plus its single-hop neighbours N_A, $\mathcal{X}_A = \{A, B, C, D, E, F\}$, while the set of vertices $\mathcal{Y}_A$ corresponds to the set of idle channels $\lambda_A = \{1, 2, 3, 4, 5, 7, 8, 10\}$. Note that CR_A is connected to all vertices in $\mathcal{Y}_A$, since $\mathcal{Y}_A = \lambda_A$. In Figure 4.2(c), we present the bipartite graph $\mathcal{G}_B$ constructed by CR_B, for the same topology of Figure 4.2(a). Note that $\mathcal{G}_A \neq \mathcal{G}_B$ despite the fact that CR_A and CR_B are one-hop neighbours. This holds true because $N_A \neq N_B$ and with different physical locations it is expected that $\lambda_A \neq \lambda_B$.



(a) 8-node CR network



(b) Bipartite graph constructed by node A



(c) Bipartite graph constructed by node B

Figure 4.2: The connectivity graph and the construction of the bipartite graph.

4.3.3 Broadcast Channel Set Computation

The minimum number of channels through which a CR node can reach all its single-hop neighbours has to be chosen to reduce the total number of broadcasts and the overall congestion in the network. Therefore, based on its own bipartite graph $\mathcal{G}_i(\mathcal{X}_i, \mathcal{Y}_i, \mathcal{E}_i)$, every CR computes the minimum Broadcast Channels Set (BCS_i) and assigns the best channel as the Tuning Channel (TC_i). The problem of finding the minimum broadcasting channels set for each CR node can be modelled as the set cover problem.

The set cover problem is as follows: given a set of n elements called the universe $\mathcal{U} = \{\mathcal{U}_1, \mathcal{U}_2, ..., \mathcal{U}_n\}$ and a collection of m sets of $\mathcal{U}$, $\mathcal{S} = \{\mathcal{S}_1, \mathcal{S}_2, ..., \mathcal{S}_m\}$, find the smallest sub-collection $\mathcal{C}$ of $\mathcal{S}$ such that $\mathcal{C}$ covers all elements in $\mathcal{U}$ [113]. $\mathcal{C}$ is a set cover if and only if $\bigcup_{\mathcal{S}_i \in \mathcal{C}} \mathcal{S}_i = \mathcal{U}$.
For our purpose, finding the minimum but the most effective BCS, we represent the *universe* by the set of vertices $\mathcal{X}$, the *collection* by the set of vertices $\mathcal{Y}$ and the inclusion of elements in sets as edges. We have now transformed $\mathcal{Y}$ into a set of subsets of $\mathcal{X}$ and the task now is to find a minimum cardinality subset of $\mathcal{Y}$ vertices which covers the entire vertices of $\mathcal{X}$. Finding the minimum set cover is an NP-complete problem [114]. For a bipartite graph of small size, an exhaustive search may be feasible. However, the space of possible solutions grows exponentially with the cardinality of the vertex set. Hence, a greedy heuristic algorithm for finding a cover set with a minimum number of channels has been developed in Algorithm 4.1.

Algorithm 4.1 iteratively examines a single channel and chooses the channel which covers the largest number of uncovered nodes in each round. The vector BCS holds the indexes of the channels that have already been chosen, while $\mathcal{U}$ holds the set of CRs that are not covered yet by the channels in the BCS. Initially, BCS is empty while $\mathcal{U} = \mathcal{X}_i$ and $\mathcal{S} = \mathcal{Y}_i$. In each iteration, we find the channel $\mathcal{S}_i$ from $\mathcal{S}$ which has the highest overlap with $\mathcal{U}$. We then add $\mathcal{S}_i$ to BCS, remove it from $\mathcal{S}$, remove CR users covered by $\mathcal{S}_i$ from $\mathcal{U}$. The process terminates when $\mathcal{U}$ is empty. Accordingly, all single-hop CR nodes are now connected with the source node by at least one of the selected channels. The list of selected channels is updated accordingly after each iteration. The output is the broadcast channels set BCS, ranked in descending order based on the number of the neighbours served per channel. The idea behind prioritising channels in descending order is twofold; first:

to enable the CR node to pick the first channel in the list as the TC which guarantees the maximum connectivity with its neighbouring nodes, second: when transmitting, the source node will guarantee the maximum number of its neighbouring nodes is achieved at the first transmission, the second highest number of neighbours is achieved at the second transmission, and so on. The pseudo-codes of the proposed algorithm for calculating the broadcast channel set and the tuning channel is shown in Algorithm 4.1.

4.3.4 Protocol Flow Chart

This section outlines the procedure of the proposed CRBP protocol. The flow chart of the proposed broadcast protocol is illustrated in Figure 4.3. As shown in Figure 4.3, before broadcasting any message, every CR node first identifies its own available channels and discovers its single-hop neighbouring CR nodes. Whether it is the source node or not, the CR node uses its local network information, the set of available channel λ^k and the list of neighbours N_i to construct the bipartite graph based on Algorithm 4.1. Then, it computes the BCS. Finally, if this node is the source node, it hops and broadcasts the message on each channel of the broadcast channel list according to the priority list. On the other hand, if this CR node is not the transmitter, it is by default a receiver node. Then, it assigns the best channel as the TC. If the intermediate-node receives the broadcast message from another sender, it rebroadcasts this message using the channels calculated based on Algorithm 4.1.

4.4 Performance Evaluation

We have implemented CRBP with the NS-2 simulator, where a total of 100 CR nodes are randomly deployed within a square region of sides 1000 m, each having sensing and transmission times given by $T_S = 0.1$ s and $T_t = 0.6$ s respectively. Simulations run for 100 s. A total of 100 packets were sent, where each packet is sent by a randomly selected node after 1 s. Each group of simulations is repeated 100 times and the results are the average values over 100 times. We set the communication range of each PU node $C^r_{PU} = 250$ m, moreover, the CR user has a transmission range $C^r_{CR} = 150$ m.

Algorithm 4.1 *Calculation of the broadcast channel set and the tuning channel*

Require: $\mathcal{G}_i(\mathcal{X}_i, \mathcal{Y}_i, \mathcal{E}_i)$

$\mathcal{U} \leftarrow \mathcal{X}_i$, $\mathcal{S} \leftarrow \mathcal{Y}_i$, $BCS \leftarrow \emptyset$, $TC \leftarrow \emptyset$

while $\mathcal{U} \neq \emptyset$ **do**

  for $i = 1$ to $|\mathcal{S}|$ **do**

    Find $\mathcal{S}_i \in \mathcal{S}$, such that $|\mathcal{S}_i \cap \mathcal{U}|$ is max

    if there is more than one $\mathcal{S}_i \in \mathcal{S}$ achieve the same goal **then**

      choose $\mathcal{S}_i$ which has the highest probability of channel availability

    end if

    if $TC = \emptyset$ **then**

      $TC = \mathcal{S}_i$

    end if

  end for

  $BCS \leftarrow BCS \cup \mathcal{S}_i$

  $\mathcal{S} \leftarrow \mathcal{S} \setminus \mathcal{S}_i$

  $\mathcal{U} \leftarrow \mathcal{U} - \mathcal{S}_i \cap \mathcal{U}$

end while

return BCS, TC

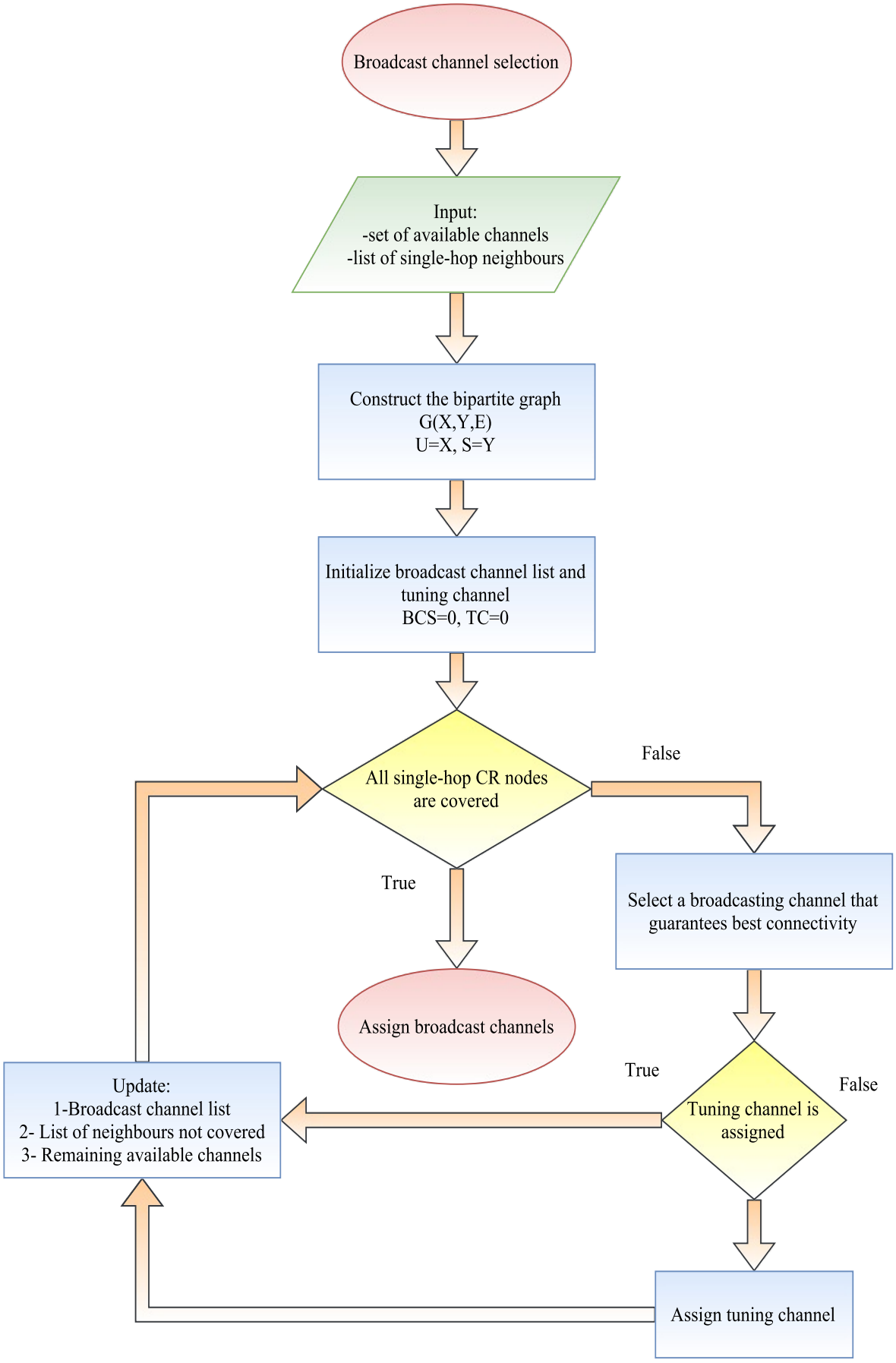


Figure 4.3: Cognitive radio broadcast protocol operation flowchart

As a point of reference, we compare the performance of our CRBP protocol against three broadcasting protocols: (a) random strategy (RS), (b) selective broadcasting (SB) presented in [38] and (c) SURF strategy proposed in [37]. We suggested RS strategy because it is the simplest one and no information is required. In RS, channels are randomly picked to be used by CR nodes for transmission and/or receiving, without any consideration of the ongoing PU and CR activity over these channels. In SB, a CR node broadcasts the information over a selected group of channels instead of a single channel. In this approach, the node might need to listen to more than one channel. SB does not provide any synchronization between transmitter and receiver nodes. However, SURF classifies the channels on the basis of PU unoccupancy and CR occupancy, then selects the best one for transmission. Since the transmission is done over a single channel, any CR node within the transmission range of the sender and overhearing on a different channel will not be able to receive the transmitted information.

Since, our goals are to: i) protect the PU communication from potential interference, ii) efficiently broadcast the data across the network, and iii) merge neighbouring nodes to the same channel decision, we have defined five metrics to evaluate the performance of CRBP:

1) *Potential Interference Ratio (PIR)*: It is defined as the ratio of the total number of times the selected channel is unavailable due to the PU activity after the channel selection decision is taken over the total number of times the channel selection decision taken. This metric outlines the potential interference with the ongoing transmission of PU nodes over the selected channel(s).

2) *Network Connectivity Ratio (NCR)*: This metric evaluates the connectivity of the network as well as the data dissemination process. It represents the proportion of total number of nodes successfully received the message (actual number of receivers) over the total number of the CR nodes in the network.

3) *Packet Delivery Ratio (PDR)*: It represents the ratio of the packets received by a particular CR node over the total number of packets sent on the network. This metric is used to effectively analyse the packet dissemination process.

4) *Decision Convergence Ratio (DCR)*: This metric is used to compare the convergence of the channel decision by a particular CR node with its single-hop

neighbours. It is the ratio of the total number of CR neighbours that share the same channel for overhearing over the entire number of neighbouring nodes.

5) *Channel Set Size (CSS)*: This metric is defined as the number of the channels used by the source node for broadcasting a packet toward its single-hop neighbours. The lesser the size of the channel set, the more efficient the algorithm.

4.4.1 PU Communication Protection

In this section, we characterize the Probable Interference Ratio (PIR) caused by CR nodes to PU nodes due to an inappropriate channel decision from CRBP, RS, SB, and SURF. Figure 4.4 clearly shows that CRBP causes less interference to PU nodes, compared to RS, SB, and SURF. This is primarily because, in CRBP, the CR nodes opportunistically use the unutilized channels for transmission based on real-time sensing, which reduces the interference with the PU communications. Note that in CRBP, at the time of transmission, if there is no idle channel due to PU activity over all the channels the CR will not transmit the data. Figure 4.4 shows a tiny PIR value for CRBP, which demonstrates the instances where there is no idle channel and a potential interference would be caused if a transmission continued. It can be clearly seen from fig. 4.4, that the PIR value decreases once the number of channels increases. When the number of channels Ch = 10, the value of PIR is lower than when Ch = 5. This is because a higher number of channels increases the probability for nodes to find PU-free channels for CR transmission. Accordingly, CRBP alleviates collisions with primary communication, which provides better protection for the on-going PU transmission.

4.4.2 Reliability and Reachability of the Data Dissemination Process

In this section, we evaluate the performance of CRBP from the viewpoint of CR network connectivity. Network connectivity ratio (NCR) is defined as the proportion of accumulative CR receivers over the total number of the CR nodes in the network. Figure 4.5 compares the network connectivity ratio for RS, SB, SURF and CRBP. It is worth noting the diversity in terms of the channel availability and the PU activity as well as the distributed channel decision result in the creation of different

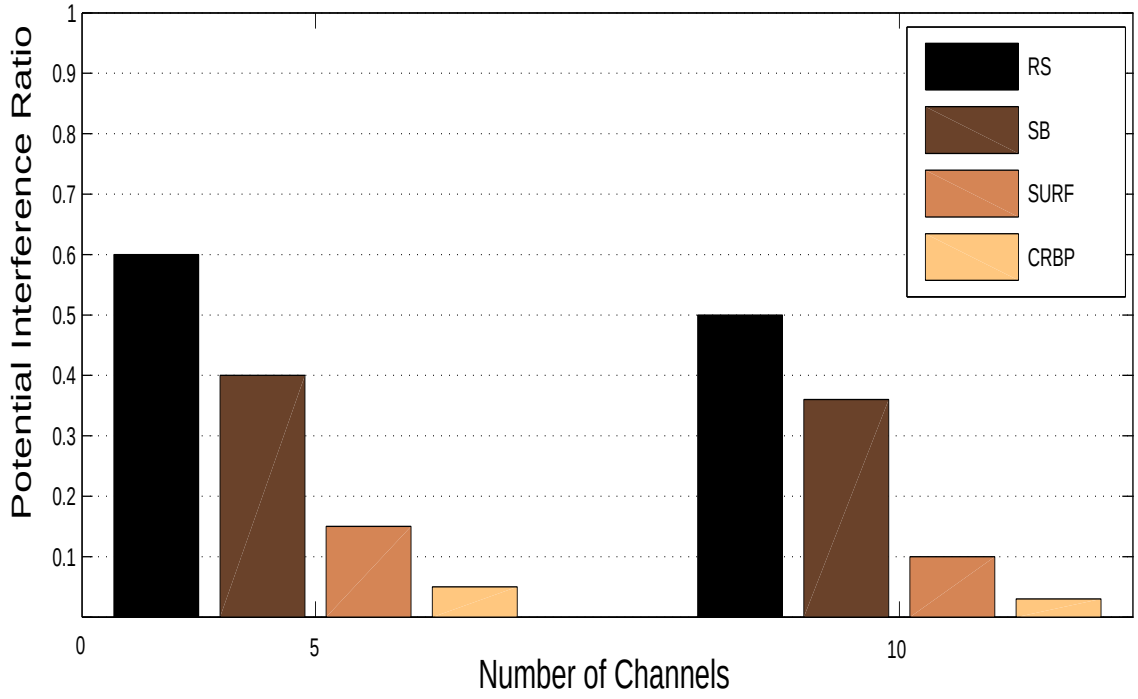


Figure 4.4: The effect on PU nodes due to transmissions by the CR users on the occupied channel

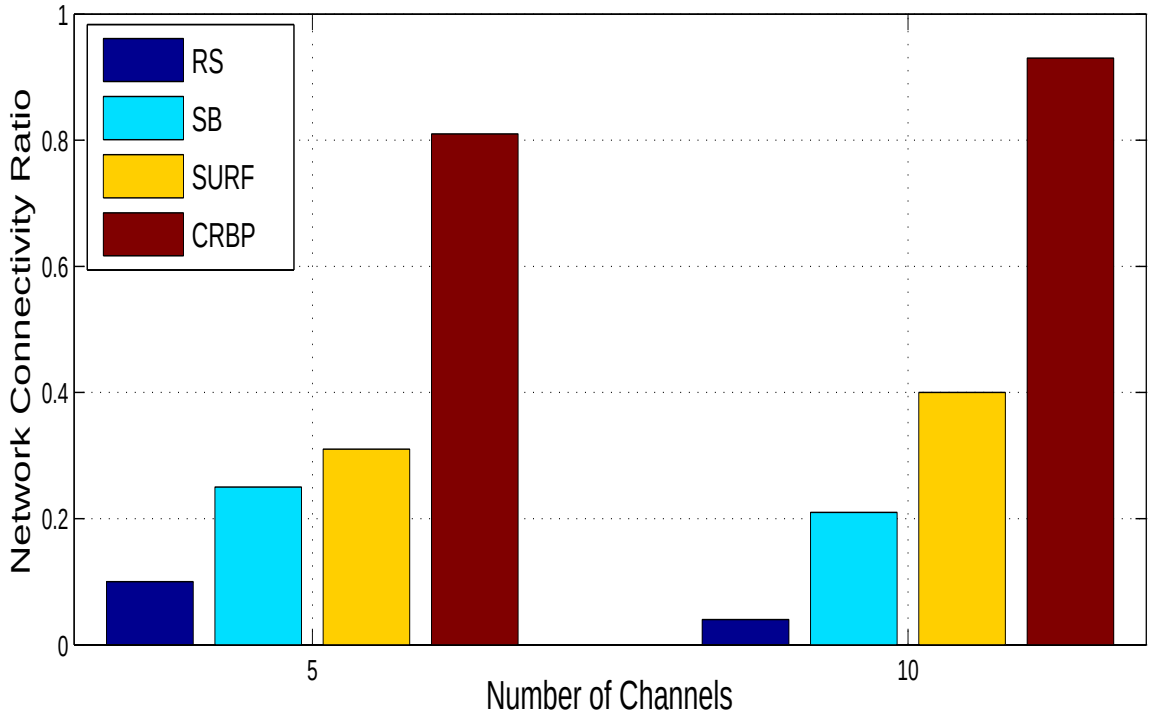


Figure 4.5: Comparison of the network connectivity ratio

network topologies (clusters) at each CR node. CRBP beats this problem by creating communication links to other topologies through transmitting over the minimum set of channels to cover all the CR nodes in its vicinity. It can be clearly seen that CRBP outperforms the other protocols in term of network connectivity. CRBP is intelligent to create linked network topology of 81% (Ch = 5) and 89% (Ch = 10) CR receivers. SURF could produce a connected network topology of 38% (Ch = 5) and 41% (Ch = 10) CR receivers. SB can make a connected network topology of 25% (Ch = 5) and 21% (Ch = 10) CR receivers. While RS is only able to produce a connected network topology of 6% (Ch = 5) and 3% (Ch = 10) CR receivers. It is worth mentioning that with the increase of the number of channels, CRBP performance is also slightly enhanced. This result is not unreasonable, since adding more channels spreads nodes over more channels and makes rendezvousing neighbours harder. Nevertheless, by employing the proper metric and utilising the same algorithm at both CR sender and receiver, CRBP attains finer results when the number of channels increase. This is because with extra channels, the chances of finding a free-PU channel increased.

4.4.3 Packet Delivery Ratio

The Packet Delivery Ratio (PDR) of RS, SB, SURF and CRBP are shown in Figures 4.6 and 4.7, where total number of channels(Ch) is Ch = 5 and Ch = 10 respectively. CRBP performed very well compared to other protocols and it significantly increases the packet delivery ratio. In particular, CRBP guarantees approximately a 76% packet delivery ratio for Ch = 5, while in RS, it is almost 3%, 21% in SB and 32% in the case of SURF. While when Ch = 10, CRBP provides almost an 83% packet delivery ratio, compared to almost 1% in the case of RS, 17% for SB and 29% for SURF. Table 4.2 shows the simulation results of the successful packet delivery ratio under different number of channels. It is worth noting that the diversity in terms of the channel availability and PU activity result in the creation of different network topologies (clusters) at each CR node. As shown in Table 4.2, CRBP overcomes this problem by creating communication links to other topologies by transmitting over the minimum set of channels to cover all the CR nodes in its vicinity, which in turn maximizes the reachability of the broadcast messages.

As a matter of fact, RS does not guarantee that the selected channel is free from PU activity for its transmission, thus causing a harsh reduction in the delivery ratio.

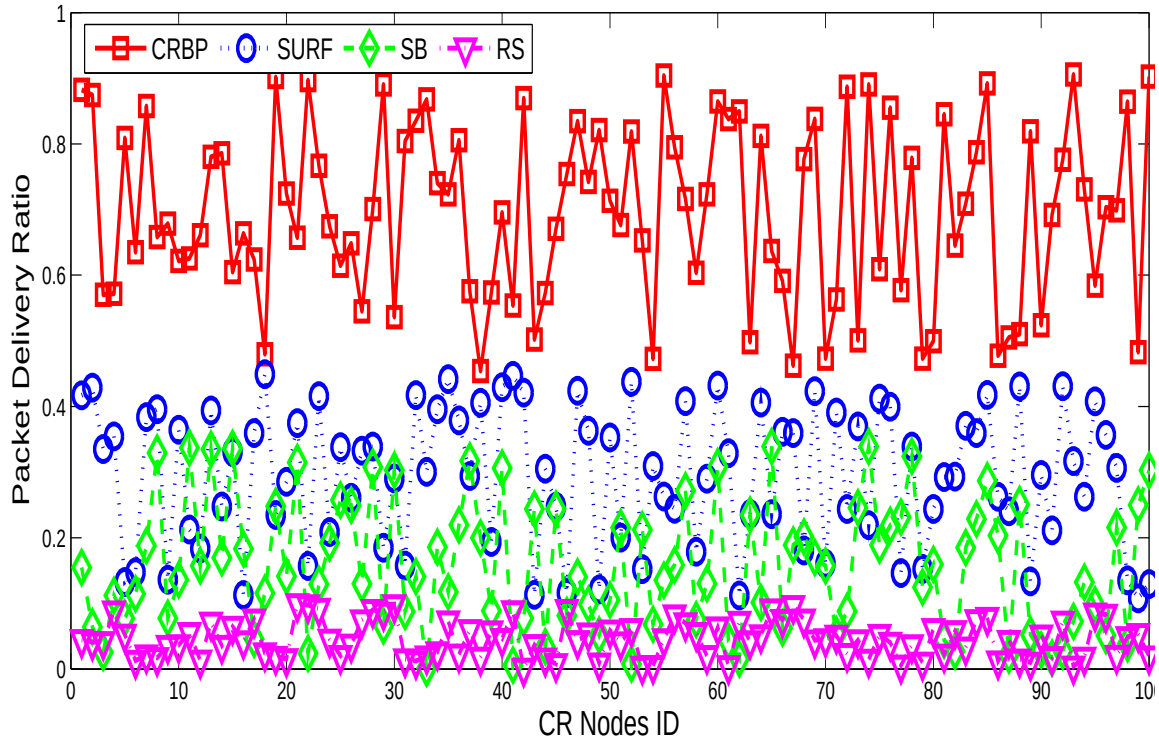


Figure 4.6: CR nodes and successful packet delivery ratio, Ch=5

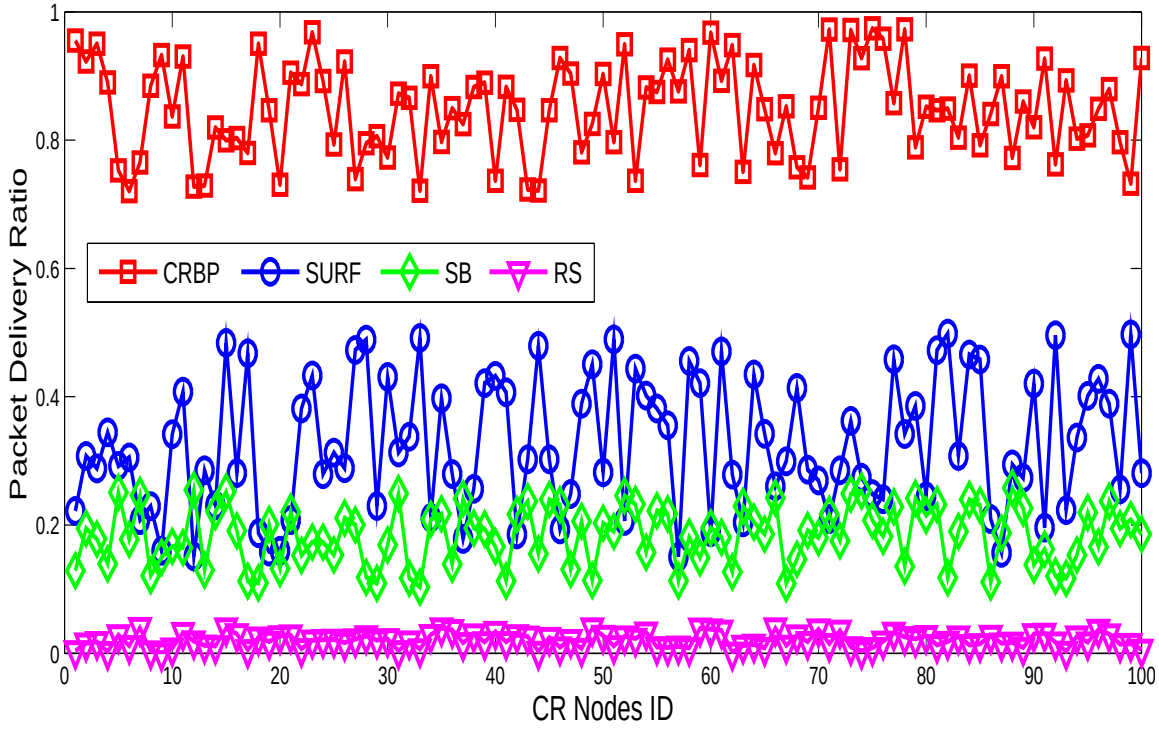


Figure 4.7: CR nodes and successful packet delivery ratio, Ch=10

Table 4.2: Successful packet delivery ratio

Broadcast Technique	Packet Delivery Ratio	
	ch=5	ch=10
Cognitive Radio Broadcast Protocol (CRBP)	76%	83%
SURF	32%	29%
Selective Broadcasting (SB)	21%	17%
Random Strategy (RS)	3%	1.2%

In SB, although the transmission is achieved through multiple channels, it provides a reduced delivery ratio compared to CRBP. In some cases, the transmitter may not have any effective receivers due to lack of transmitter/receiver synchronization between nodes (i.e., the overhearing channel is selected randomly). In the case of SURF, the transmission occurs over a single channel which means only the nodes tuning to that channel and within the transmission range of the source node will receive the message. While in CRBP, each CR node delivers the message to all the neighbours through selecting channels that provide high probability for connectivity, which in turn maximises the reachability of the broadcast messages. It is worthy remembering that for all the techniques, with the message replication and propagation at each new hop, the chances of collisions enlarges and accordingly, the packet delivery ratio decreases. In summary, based on results obtained and shown in Figures 4.5, 4.6 and 4.7, CRBP guarantees the best network connectivity by increasing the data dissemination reliability in multi-hop cognitive radio ad hoc networks. It is important to highlight that with an increase in the number of channels, CRBP performance is also slightly enhanced. This result is not unreasonable, since adding more channels spreads nodes over more channels. However, by using the proper metric and mainly employing the same algorithm at the sender and the receiver, CRBP achieves better results when more channels are available.

4.4.4 Decision Convergence Ratio

In this section, we evaluate and characterize the merging between neighbouring nodes to the same channel decisions. The Decision Convergence Ratio (DCR) has been defined as a metric for this purpose. Grouping the CR nodes with similar channel decision increases the probability of effective and reliable data dissemination, reducing the number of channels required to connect all the neighbouring nodes

and implicitly implement cooperative spectrum sensing. Figure 4.8 compares the ratio of total number of neighbours sharing the same receiving channel over the total number of CR neighbours for the four protocols: RS, SB, SURF and CRBP. CRBP has almost equal ratio of similar neighbours tuning decision to SURF, while higher numbers of neighbours sharing the same tuning decision compared to RS, and SB. This is primarily because both algorithms CRBP and SURF employ the same algorithm at the sender and the receiver that select the channel that offers best group-level connectivity (i.e., the channel that connect a higher number of neighbours) as the receiving channel. This will result in providing a good synchronization between the neighbouring nodes. Since, CRBP also provides best network-level connectivity (i.e., links up other neighbours who tune onto other channels). Therefore, the majority of neighbouring nodes will receive the transmission message successfully which provides a good connectivity. In addition, this causes an increase in the ratio of accumulative receivers and the packet delivery ratio in the network as shown in Figures 4.5, 4.6 and 4.7.

4.4.5 Channel Set Size

In this section, we evaluate and compare the Channel Set Size (CSS) used by CR nodes to broadcast the message for the four protocols. The CSS is defined as the number of channels used by the transmitter for broadcasting a packet to its single-hop neighbours. Figure 4.9 compares the CSS with respect to the number of available channels for RS, SB, SURF and CRBP. It can be observed that SB uses most of the available channels for broadcasting. In addition, the channel set size increases when the number of available channels increases. This is because, with an increase in the number of idle channels, CR nodes are spread over more channels. As a result, the CR node needs to transmit over more channels. However, the CSS in the case of CRBP is reasonable. Furthermore, the number of used channels does not have too much of an affect with the increase in number of the available channels. This is obtained thanks to CRBP which uses proper metrics to prevent CR nodes from scattering over all available channels and merges the neighbouring nodes to the same channel decision, which in turn results in a dramatic reduction in the channel set size. RS and SURF use only a single channel for the transmission regardless of the number of available channels. Due to the non-uniform channel availability, especially

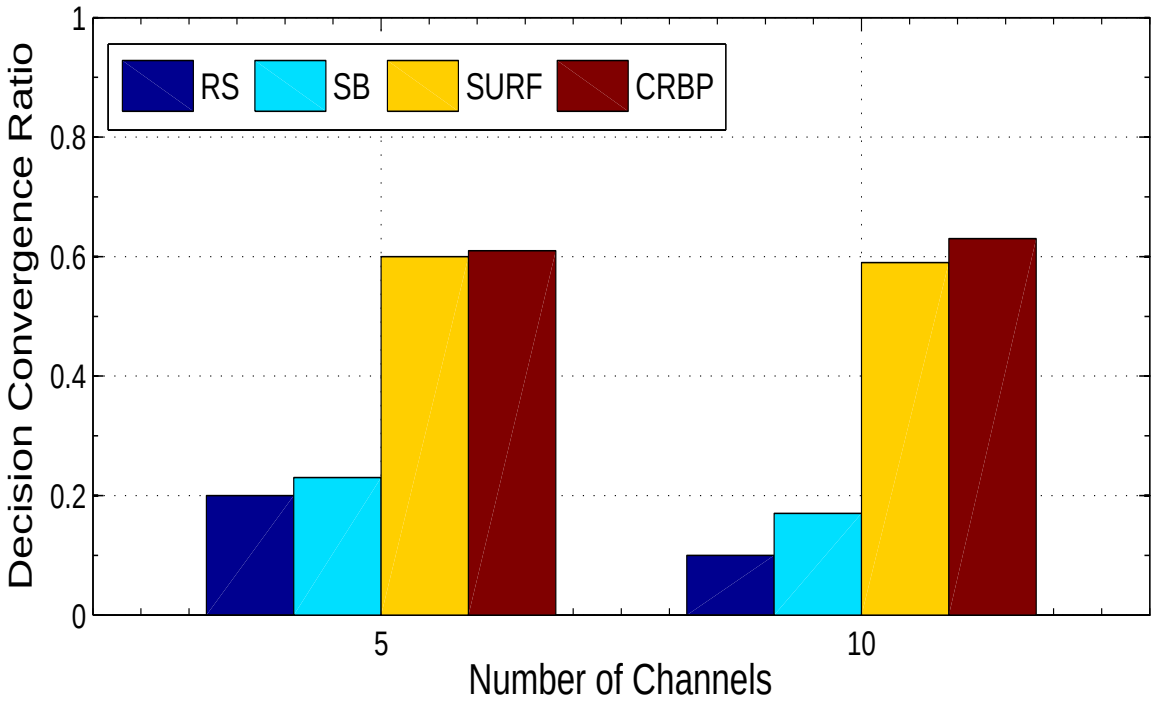


Figure 4.8: Ratio of average number of neighbours tuning on the same channel over the total number of neighbours

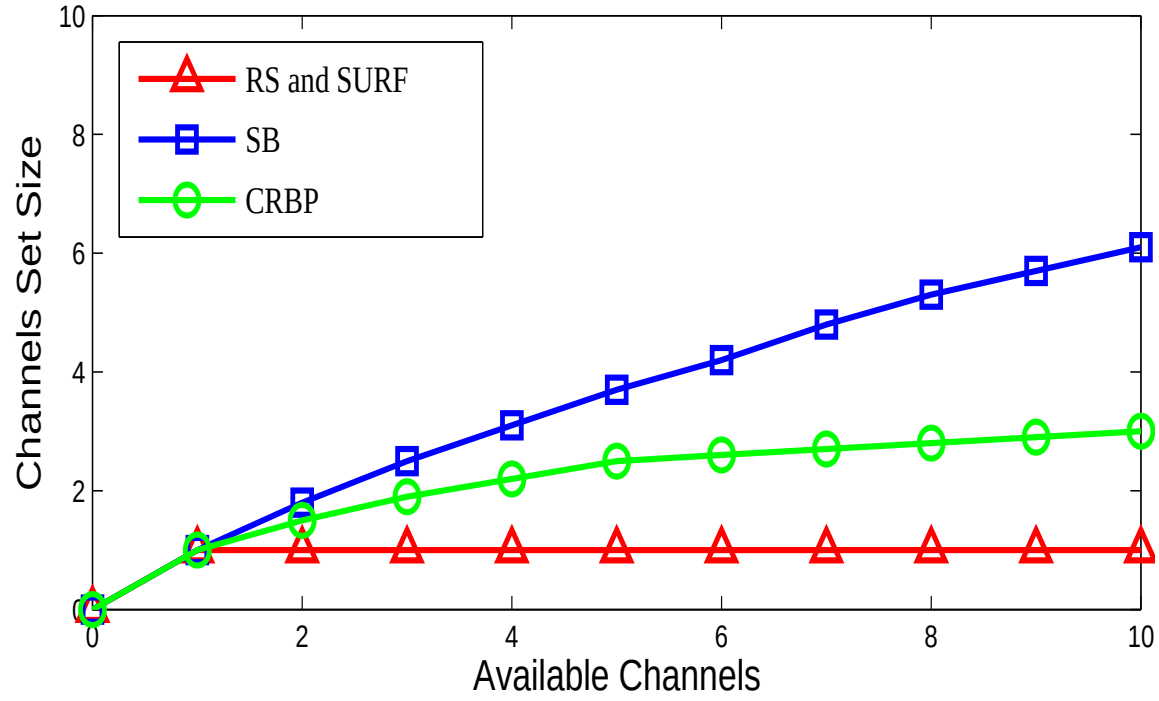


Figure 4.9: Channel availability among the nodes and the average number of used channels for broadcast per node

the possibility of the unavailability of a global common channel, it is hard to use a single channel for broadcasting in CR networks. Since CRBP also connects other topologies in the vicinity, the majority of the CR neighbouring nodes will receive the transmitted message successfully, which results in an increase in the packet delivery ratio.

4.4.6 Packet Ratio Description

In the traditional single channel wireless network, when nodes broadcast packets, all the single-hop neighbouring nodes will receive that packet due to all nodes working on the same channel. There is only one reason that may result in the loss of the transmitted packet, and this is collision. This is not the only reason to lose a packet in CR networks. Many other reasons cause the loss of the transmitted packet in CR networks, like interruption with PU communication, CR nodes tuned to different channels and collision between CR nodes.

In this section, we evaluate the performance of our broadcast protocol. We have defined four different types of packet ratio (the ratio of delivered packets, the ratio of misplaced packets, the ratio of collided packets and the ratio of interrupted packets) as performance metrics to analyse and evaluate the performance of our proposed protocol.

1) *Delivered packet ratio:* It represents the proportion of the CR nodes that successfully received the broadcast packets over the total number of neighbouring nodes. This ratio is used to quantify the data dissemination accomplishment.

2) *Misplaced packets ratio:* It represents the proportion of CR nodes that lost the packets because they tuning on channel different from the transmitter over the total number of neighbouring nodes. This ratio measures the packets lost due to CR node listening on the wrong channel.

3) *Collided packets ratio:* It is defined as the total number of CR nodes that did not receive the transmitted packets owing to collisions with CR nodes over the total number of neighbouring nodes. This ratio is used to quantify the collided packets with the CR nodes.

4) *Interrupted packets ratio:* It represents the ratio of the CR nodes that did not receive the broadcast packets owing to the interruption with PU nodes over

the total number of neighbouring nodes. This ratio is used to quantify the interrupted packets with the PU nodes.

Two comparisons for the packet ratio of RS, SB, SURF and CRBP, when Ch = 5 and Ch = 10, have been demonstrated in Figures 4.10 and 4.11 respectively. The different packet ratios have been measured in a single-hop context and multiple sources have been taken into consideration throughout the multi-hop network. It can be clearly seen, as expected, CRBP provides higher packet delivered ratio compared to RS, SB, and SURF. This is primarily because CRBP emphasize on connecting all nodes in the neighbourhood. If the number of available channels is large, the probability that two neighbouring nodes select the same channel is fairly high. However, when the number of channels is high, this leads the other protocols to scatter CR nodes among most of the available channels. On the other hand, opposite behaviour can be seen in the misplaced packets ratio. There are fewer lost packets in CRBP compared to the other works. This is due to the fact that CRBP selects the channels that provide higher connectivity with the neighbours as the receiving channel, while RS and SB select the tuning channel randomly. It is noted that when the total number of channels increases from Ch = 5 to Ch = 10, the ratio of lost packet for both RS and SB increases. This is because when more channels are available, the CR neighbours are scattered over new channels and when nodes broadcast to the channels, there is more chance of CR neighbours being overheard on a different channel. Figures 4.10 and 4.11 show that due to the PU interruption, RS and SB lost the highest number of packets in comparison with SURF and CRBP. This is due to CRBP considers real time sensing for the PU activity when selecting the channel for broadcasting. Moreover, in CRBP, with more available channels, the interrupted packet ratio decreases. This is due to the fact that when the number of channels increase, CRBP gets a better chance of finding unoccupied channels. Finally, the collided packet ratio increases with the increase in the number of successful transmissions for all the techniques. Both the ratio of delivered packets and the ratio of lost packets (misplaced, collided, interrupted) demonstrate that CRBP achieves better packet delivery to the neighbouring nodes, compared to RS, SB, and SURF protocols.

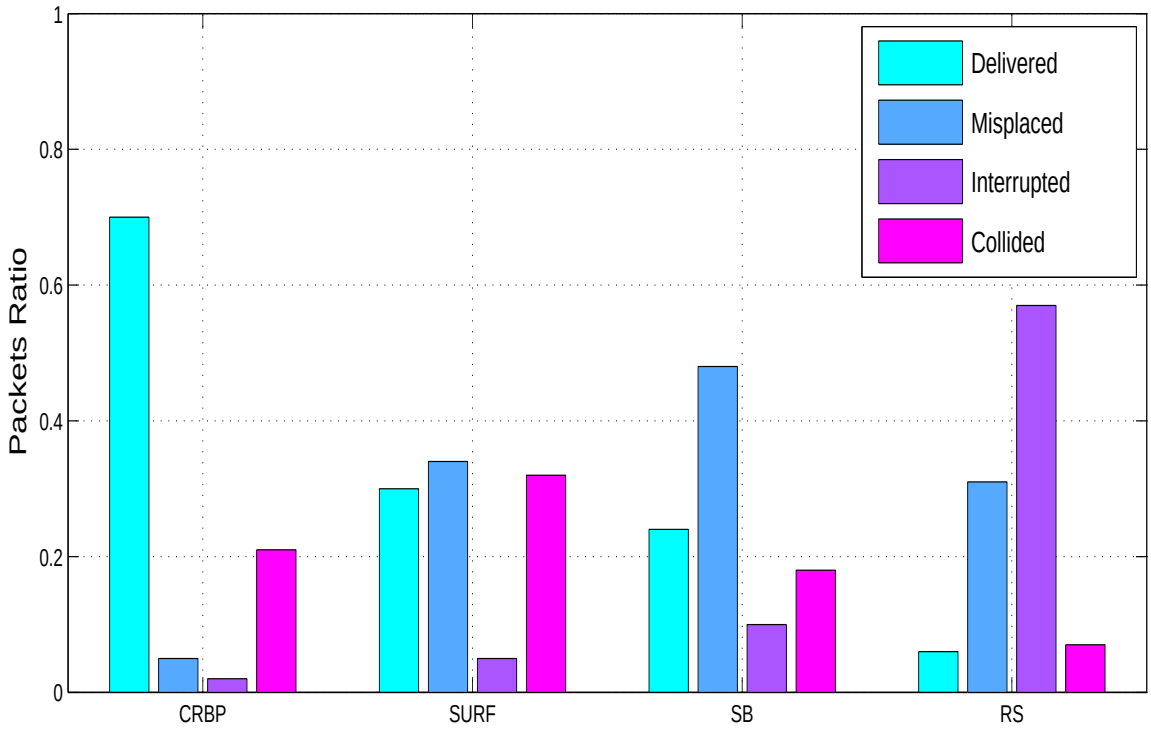


Figure 4.10: Packet ratio description (Delivered, Misplaced, Interrupted, Collided), when Ch=5

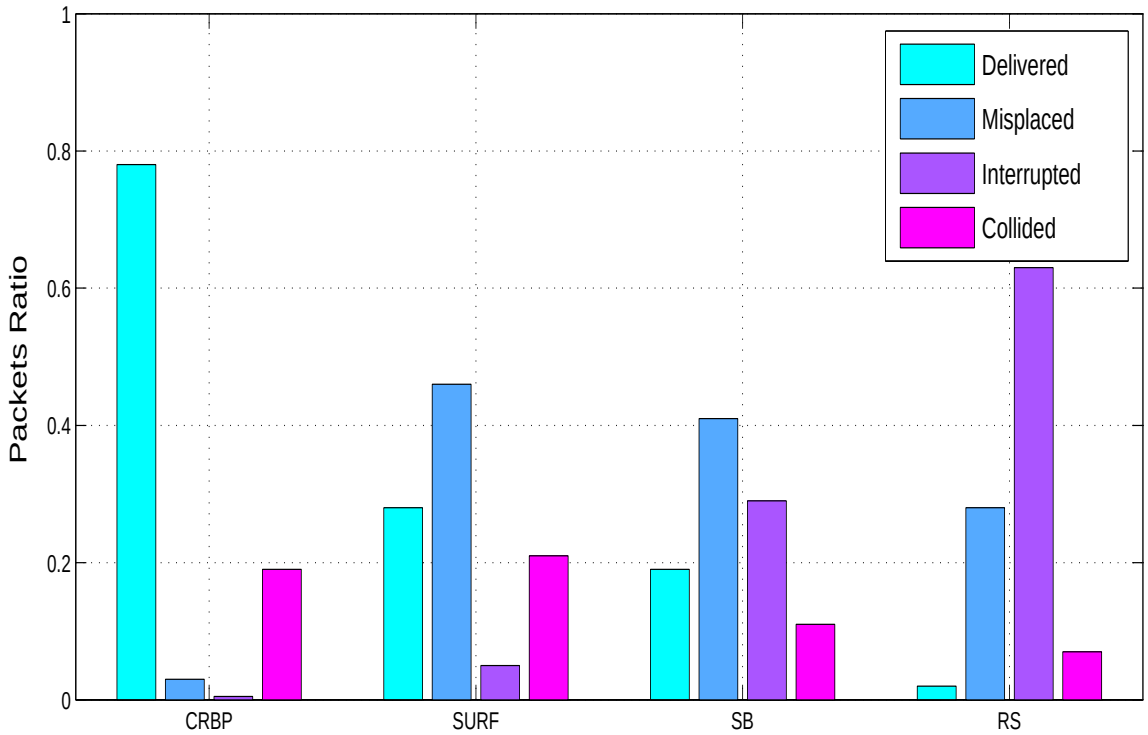


Figure 4.11: Packet ratio description (Delivered, Misplaced, Interrupted, Collided), when Ch=10

4.5 Conclusion

In this chapter, we have proposed and investigated CRBP, a distributed and intelligent broadcasting protocol for reliable packet dissemination in CR ad hoc networks. The main design objective of CRBP is to reliably disseminate the control information through connecting different local topologies, which is a unique feature in cognitive radio networks. By jointly mapping the network topologies and the spectrum observations onto a bipartite graph, CRBP allows each node to capture the spectrum information and the environmental topologies of all the neighbouring nodes. This secures the network connectivity and reduces the interference with primary users. The reliability is ensured by connecting different topologies and synchronizing adjacent nodes. Simulation results attest that CRBP is superior in reliable broadcasting compared to random broadcasting, selective broadcasting and SURF broadcasting protocols. Furthermore, we show that different from other techniques, CRBP achieves better results when the number of channels increases. This is owing to the intelligent channel selection mechanism.

Chapter 5

Reliable Collaborative Spectrum Sensing for Cognitive Radio Networks in Malicious Environments

Cognitive radio is a promising technology where CR users can opportunistically access the under-utilized spectrum. However, CR networks face new threats due to their unique characteristics. Malicious CR nodes could adversely degrade the performance of collaborative spectrum sensing through providing false local sensory reports to the fusion centre which lead to incorrect sensing decisions. Developing an efficient security mechanism and model for secure spectrum sensing is a challenging task due to the new classes of security threats and challenges in CR networks. In this chapter, we present the Reliable Collaborative Spectrum Sensing Scheme (RCSSS), a novel and robust defence scheme to counter the SSDF attacks in cognitive radio wireless networks. The proposed scheme can significantly improve the reliability and the accuracy of collaborative spectrum sensing in adversarial environments. In the proposed scheme, when a CR node generates a sensing report based on local observations, it creates a unique signature using its own secret key and collects some signatures from different neighbouring CR nodes in its vicinity. Before sending to the FC, the final report is encrypted using the cell's key. Once the message reaches the FC, it is certified as valid sensory data only if it passes the three-tier verification process (i- the report must be signed by the unique secret key belonging to the

sender, ii- different signatures of CR users from the same cell must be included, iii- the report must be sealed by the trusted nodes). In addition, we use an efficient and fast reputation-based classification scheme to further analyse the behaviour of each node. Malicious CR nodes should be easily classified. Their false reports along with their negative effects will be cautiously removed from collaborative sensing decisions in a very short time span.

This chapter is organized as follows: In Section 5.1, we describe the system model and assumptions. In Section 5.2, we present RCSSS, the proposed security framework and the detection strategy. We analyse the defence scheme against SSDF attacks and present simulation results in Section 5.3. Finally, we conclude the chapter in Section 5.4.

5.1 System Model

We consider an infrastructure-based CR network where the channel sensing measurements reported from multiple CR nodes are combined at the central entity, namely the Fusion Centre (FC), in order to make reliable sensing decisions. We virtually divide the CR network into multiple cells where the information of each CR node inside a particular cell is bounded to the cell's key. It is assumed that the CR network is well-connected and dense enough to support collaborative sensing in the presence of primary users. It is likely that CR nodes in the same vicinity have the same PU activity. Hence, sensing measured by a CR node can be detected by multiple neighbours with high probability [106]. Based on its local observation, every CR user decides whether a specific channel is occupied or free of use by the primary user and forwards its report to the FC. It is assumed that the FC is equipped with efficient storage and computation capabilities to serve as a data collection centre. Hence, the final decision on channel availability is made by the FC after fusing all local decisions received from the CR users.

The FC is assumed to be secured and well-protected. In addition, during the short time of bootstrapping, we assume that no CR nodes can be compromised. In an ideal CR network where all CR users are honest, most of the local decisions match the global decisions. However, in some practical situations a CR network might be subjected to numerous attacks, like eavesdropping, jamming and SSDF attacks. In this chapter, we consider the problem that malfunctioning or malicious

CR nodes exist and can severely degrade the performance of collaborative spectrum sensing through SSDF attack.

An attacking scenario is shown in Figure 5.1, where a malicious node manipulates the sensing results by injecting tampered data in order to mislead neighbouring CR nodes and the FC to make a wrong decision regarding the spectrum availability. We assume that there is a probability β that each CR user may be controlled by an adversary and become an SSDF attacker. Here, we use β as an indicator of the network vulnerability to SSDF attacks. The higher the value of β, the higher the vulnerability of the CR network. We consider a Clairvoyant case in this work and we assume that the FC already has knowledge of the network vulnerability and is aware of the precise value of β. In practical situations, when there is no knowledge of the value of β, a cautious estimation can be used at the cost of spectrum utilization efficiency. We further assume that the status of each CR user is independent from other CR users in the network, whether or not it is a SSDF malicious node. Let N and M denote the number of all CR nodes and malicious nodes in the network, respectively. Then, the number of honest CR nodes can be easily obtained as $H = N - M$. According to the Law of Large Numbers, when the number of total CR users in the network is large enough, the network vulnerability can be computed as $\beta \approx M/N$. In contrast to honest users, the main goal of malicious users is to undermine the operation of the network through poisoning the FC by tampered data which may or may not meet their actual sensing measurements. The unique secret key (sk_{CR_i}) and the unique coefficient (α_i) are assumed to be set before deployment. The main notations used in this chapter are summarized in Table 5.1 for easy reference.

5.2 The Proposed System

In collaborative sensing, all CR nodes share their sensing data with nodes within their vicinity to jointly determine which spectrum bands are indeed available. Meanwhile, malicious nodes might even enjoy the utilization of free channels by modifying the sensing data, which significantly degrades the performance of collaborative sensing. By manipulating the radio sensing information, an adversary can affect the beliefs of a cognitive radio, and consequently its behaviour. In this chapter, we present RCSSS, a novel multi-layer defence scheme based on a reputation evaluation

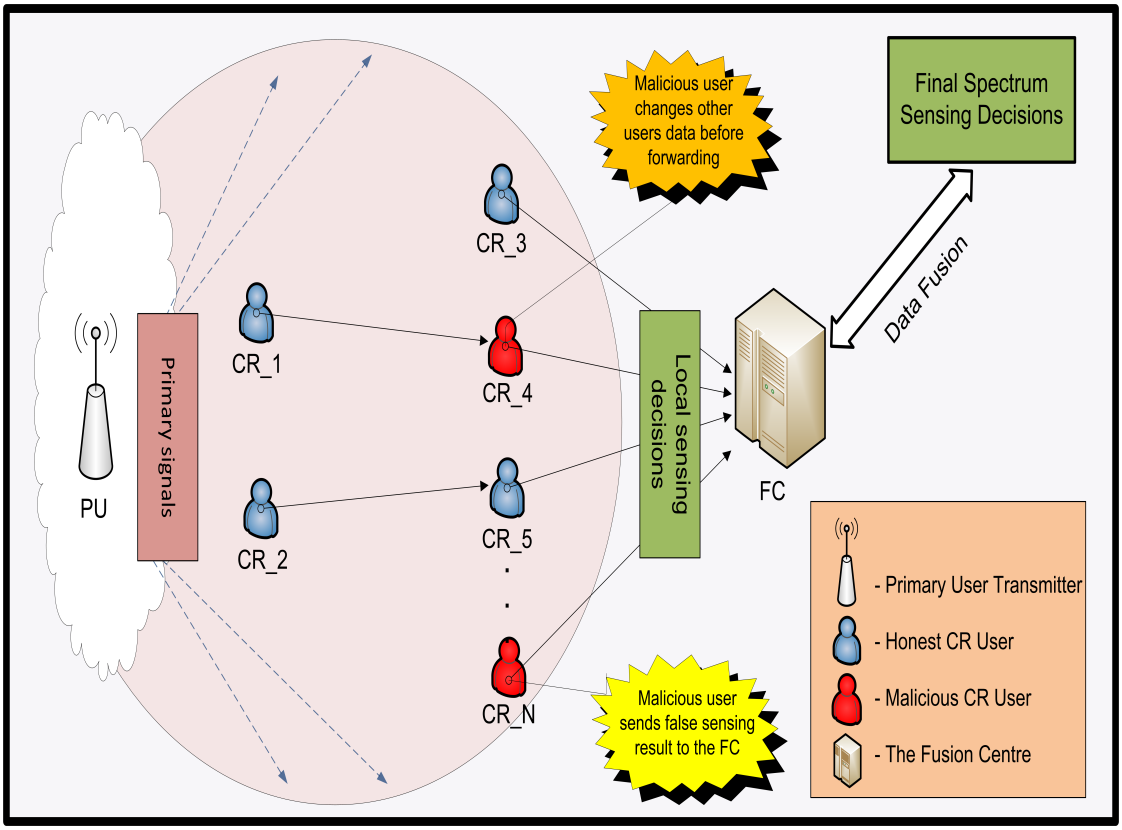


Figure 5.1: Collaborative spectrum sensing model in a CR network where CRs sense PU signal and send local decisions to the FC where the final decision is made while malicious attackers may inject tampered data or change other users reports to degrade the fusion performance.

algorithm to thwart attacks targeting availability, authenticity and confidentiality of critical and vital sensing information. The proposed scheme uses two keys to encrypt the messages between CR nodes and the FC: *i) Unique secret key:* shared only between the CR node and the FC, this key is used to provide node authentication. *ii) Cell key:* shared only between CR nodes in the same cell and the FC, this key is used to provide cell authentication. The encryption technique prevents any node from outside the cell from disclosing the sensing information. Furthermore, by dynamically updating the reputation of each CR user according to its historical behaviour, the FC securely classifies CR nodes and makes a trusted nodes list with the objective of checking the reliability of the sensing data as well as detecting malicious users.

In existing security models, compromising nodes which are not involved in generating a particular sensing report may result in compromising that report as well. Therefore, the novel design of our model successfully eliminates the effects of adversaries on the reliability of spectrum sensing data. In the following sections, we further detail the proposed defence scheme, starting with the collaborative sensing management, construction of the virtual cells and exchanging local sensing messages. This is followed by the report generation, the process of data fusion and the message verification process at the FC. We also discuss the procedure of selecting the trusted CR nodes that play an important role in the verification of sensory data at the FC.

5.2.1 Collaborative Sensing Management

It is highly probable that CR nodes in closed geographical areas sense the same PU activity. Hence, inside a cell of n CR nodes, a sensing report must be collaboratively agreed by at least s ($1 \leq s \leq n$) CR nodes in order to be accepted by the FC [98]. Accordingly, any report generated from a cell must hold s different signatures of CR nodes. Multiple signatures make the system more reliable against threats, since the validity of the created report can be ensured even if some malicious nodes participate in the report generation.

Table 5.1: Symbols used for RCSSS description

Symbols	Descriptions
β	Probability of network vulnerability
C	Encrypted report
CH	Primary user channel
CV_i^k	Correlation value between CR_i and the FC on k^{th} channel
d	Number of trusted nodes
E_k	The encryption function
H	Number of honest CR nodes
$H(.)$	The hash function
K_{cell}^A	Authentication cell key shared among all CR nodes in cell A
l	Side length of the cell
M	Number of malicious CR nodes
MAC_k	The message authentication code
N	Toal number of CR nodes in the network
n	Number of CR nodes inside a cell
NB_i	Neighbours list of CR_i
P	Large prime number
Q_F	Probability of a false alarm
Q_{MD}	Probability of missed detection
Q_{SSDF}	Probability of SSDF attack
R	Sensing report
s	Threshold number of signatures required to create a report
S_i	Signature of CR_i computed through a LSSS
sk_{CR_i}	Unique secret key of CR_i
S_{pack}	Group of s signatures from the neighbours of CR_i
TRi	Trustworthiness value of CR_i
x_{cell}^A, y_{cell}^A	Coordination of cell A
x_{cr}, y_{cr}	CR user coordination
x_{fc}, y_{fc}	FC coordination

5.2.2 Construction of the Virtual Grid

We simply divide the CR network into several virtual square cells. Two important parameters, the location of the FC as well as the cell side length l, are set before the deployment. We assume that each CR user has self-localization ability and is equipped with a GPS (Global Positioning System) unit. In addition, the localization scheme in [115] might be used by a CR node to obtain its geographic location. We denote the cell containing CR_i by A_{cell}, which is also known by the home cell of that CR node. The associated coordinates represents the centre of the cell by (x^A_{cell}, y^A_{cell}). Each CR node calculates the centre location of its current cell using the FC as a reference point as follows:

$$x^A_{cell} = 0.5\left\lceil \frac{x_{cr} - x_{fc}}{l} \right\rceil, \tag{5.1}$$

$$y^A_{cell} = 0.5\left\lceil \frac{y_{cr} - y_{fc}}{l} \right\rceil. \tag{5.2}$$

After calculating the virtual cell coordinates, CR_i localized in a particular cell sends its cell location to the FC requesting the corresponding cell authentication key. Once the FC receives a request, it sends the cell key alongside the following parameters (s, p) to the related node encrypted by the unique secret key (sk_{CR_i}), which is only known by the i^{th} CR node and the FC.

$$FC \longrightarrow CR_i = E_{sk_{CR_i}}\{K^A_{cell}, s, p\}, \tag{5.3}$$

where K^A_{cell} is the authentication key of a given cell, p is a large prime number over the finite field $GF(p)$ and s is the minimum number of required nodes that should participate in the report generation.

5.2.3 Neighbour Discovery

Each CR node broadcasts a HELLO message containing the CR node's ID and the location of the current cell (x^A_{cell}, y^A_{cell}). This message is encrypted by the cell authentication key (K^A_{cell}), as this key is shared only between the FC and the CR nodes in that particular cell, hence the cell privacy is protected. We adopt the broadcasting scheme and the sensing cycle proposed by [106] for neighbour discovery

and network construction,

$$CR_i \longrightarrow * : E_{K^A_{cell}}\{CR_i, (x^A_{cell}, y^A_{cell})\}. \tag{5.4}$$

Using the cell authentication key, each CR node within the same cell decrypts the message and responds by an acknowledgement (ACK) message including its node ID. Assuming CR_j is in the same cell (A_{cell}) as CR_i, then it can use the cell key (K^A_{cell}) to decrypt the message and reply with an ACK message:

$$CR_j \longrightarrow CR_i : E_{K^A_{cell}}\{ACK, CR_i||CR_j\}. \tag{5.5}$$

Based on the received acknowledgement messages, each node creates its CR neighbours list (NB) containing the IDs of CR nodes within its vicinity and that share the same cell. Moreover, to authenticate the cell's members, each CR node inside the cell has to send its neighbour list *(NB)* to the FC via a Message Authenticated Code (MAC) using the node's unique key (sk_{CR_i}), that is

$$CR_i \longrightarrow FC = MAC_{sk_{CR_i}}(NB, (x^A_{cell}, y^A_{cell})). \tag{5.6}$$

Finally, this message is decrypted at the FC. If a uniform message is received from all the nodes of that cell, this certifies that the cell constitution is free from malicious nodes. However, if a malicious node is found, the FC can eliminate that node and alert the other nodes about the adversary node.

5.2.4 Report Generation

Each CR user $CR_i \in N$ performs its spectrum sensing on the primary channels at time t and sends the encrypted sensing report to the FC. The sensing measurements of PU activity in a particular cell have to be agreed by s CR nodes of that cell before generating a valid report. The sensing report (R) usually contains information about channel ID, cell ID, duration of channel occupancy and time stamp, etc. Then, every participating CR node encrypts R using the cell key (K^A_{cell}). As all the generated reports are encrypted by the cell's key, any node outside that cell will not be able

to disclose R. The encrypted report is given as

$$C = H(.)\ K_{cell}^{A}\ R. \tag{5.7}$$

In order to prevent any malicious users from forging and injecting fake information, the sensing report should be authenticated before the FC considers its measurements. In RCSSS, any sensing report from any CR node must hold two types of authentication: i) a unique signature of the CR node that generates the report and ii) s signatures from different CR nodes sharing the same cell. For the first tier of authentication, we compute a unique signature S_i from the encrypted report C using a univariate polynomial of degree $s-1$ over the finite field $GF(p)$ and the node's unique secret key and coefficient sk_{CR_i}, α_i, respectively [116] as,

$$S_i = F(sk_{CR_i}) = \sum_{u=0}^{s-1} \alpha_u (sk_{CR_i})^u \mod p. \tag{5.8}$$

The polynomial is evaluated using the node's unique secret key sk_{CR_i}, which is known only by the CR_i and the FC. Hence, the authenticity of CR_i can only be verified by the FC using the uniquely generated S_i. Finally, CR_i collects $s-1$ corresponding signatures from same cell neighbouring nodes namely, S_{pack} and computes the MAC over the collected s signatures, as a second tier of authentication to the report as $MAC_{K_{cell}^{A}}(S_{pack})$. Thus, the construction of the final report is finished and CR_i sends $\{CR_i,\ C,\ MAC_{K_{cell}^{A}}(S_{pack})\}$.

5.2.5 Sensing Measurements Fusion Process

All the CR nodes make their own decisions about the availability of spectrum bands and forward this information to the FC. The fusion centre verifies the messages and monitors the decisions regarding the PUs presence/absence. In order to improve the reliability of the collaborative sensing process, the FC selects a group of d CR nodes from each cell to be the trusted nodes of that cell. By adopting $d = n-s+i,\ (i \geq 1)$, CR nodes as trusted nodes in each cell, we guarantee that at least one trusted node participates in any report generation process. Only reports that have been approved by the trusted nodes will be considered by the FC as valid reports.

Adopting the trusted nodes' participation as a third tier of report verification enhances the security of the system and makes it more difficult for the attacker

to inject fabricated sensing report into the data collector. Moreover, neither the adversaries or the CR nodes have knowledge of the trusted nodes, as it is the FC's responsibility to select the trusted nodes and it does not share this information with other users. Hence, compromising any number of CR nodes in the network will not lead to disclosing the trusted nodes because compromising the FC is the only way to discover them. For this reason, the adversary node needs to compromise all the cell's trusted nodes in addition to s or more nodes from a particular cell in order to successfully generate a bogus report.

5.2.6 Verifying the Sensory Data at the FC

All the sensing reports must be verified and checked by the FC before they are considered reliable sensing measurements. Therefore, for each sensing report the FC has to verify: i) Node authenticity: the availability of a unique signature. The FC verifies the unique signature (S_i) of the i^{th} CR node using the unique secret key owned only by the FC and that CR node, ii) Cell authenticity: no less than s CR nodes have definitely participated in the report generation. The FC uses the corresponding cell key of the received report to decrypt S_{pack} and verify the authenticity of all s nodes and iii) The trusted nodes' participation: whether the report is certainly approved by at least one of the trusted nodes. Once the original report is recovered by the FC, the validation of the report is confirmed as only CR nodes inside that cell have the corresponding cell key. Furthermore, each user has its unique secret key and only the FC is aware of the trusted CR nodes of each cell.

5.2.7 Trusted CR Nodes List Formation

After collecting all the sensing information from the CR nodes, the FC verifies these measurements and calculates the final status of the perceived channels. Then, the FC compares the final status of the channels with the local observations received from each CR user. Based on the correlation between the concluded channel status and the local channel observation of each node, the FC updates the trustworthiness value of each CR user which is denoted by TR and initialised by μ. We denote the consistency and inconsistency between the FC information and the information of $CR_i(t)$ by $CON_i(t) = 1$ and $CON_i(t) = 0$, respectively. If the received sensing measurement is similar to the one verified and concluded by the FC, then $TR_i(t)$

will be increased. Otherwise, we decrease the value $TR_i(t)$. In particular, the higher the trustworthiness value, the more honest the CR node, resulting in promotion to the cells list of trusted nodes.

Any CR node whose $TR_i(t)$ goes below a certain threshold will be identified as a malicious node and will be excluded by the FC from the trusted node list. We update the trustworthiness of the CR users at time t based on historical reputation and the recent value of the consistency function $CON_i(t)$ as follows;

$$TR_i(t) = (1 - \lambda)TR_i(t-1) + \lambda CON_i(t). \tag{5.9}$$

We update $TR_i(t)$ in two different ways in order to distinguish between a malicious and honest CR user in the network. Therefore, we use two different values of λ, λ_1 and λ_2 that are relatively small and large respectively, where λ_1 , $\lambda_2 \in (0, 1)$. By doing so, the trustworthiness evolution $TR_i(t)$ for the honest node will increase slowly but it will fall fast for malicious nodes and attackers. When $CON_i(t) = 0$, this means an attacker is trying to share fake data with the FC. In this case, the FC uses λ_2 to update the node reputation which will decrease $TR_i(t)$ quickly and the node will be easily identified. On the other hand, when $CON_i(t) = 1$, this means CR_i is an honest node and a relatively small λ_1 prevents $TR_i(t)$ from increasing quickly. The update process of both cases for $TR_i(t)$ is:

$$TR_i(t) = \begin{cases} (1 - \lambda_1)TR_i(t-1) + \lambda_1 CON_i(t), \text{ if } CON_i(t) = 1, \\ (1 - \lambda_2)TR_i(t-1) + \lambda_2 CON_i(t), \text{ if } CON_i(t) = 0. \end{cases} \tag{5.10}$$

This update mechanism is very efficient against periodic attacking, since $TR_i(t)$ decreases quickly as the attacking time elapses. Consequently, the malicious nodes can be easily excluded from the trusted node list if their $TR_i(t)$ fall below a certain threshold δ.

5.3 Performance Analysis and Discussion

In this section, we investigate the security strength of RCSSS under random node capture attacks. Our concern here is to evaluate how a specific fraction of malicious nodes would affect the security of the network. We consider a multi-channel

CR network comprising of 1000 CR nodes, all randomly deployed. In the following sections, we analyse the security strength of the proposed defence scheme with respect to two aspects of the design goals, i.e., security of the system against SSDF attacks and system end-to-end security regarding data confidentiality and integrity. We compare the performance of our proposed protocol with LEDS [99], BAIS [86] and COOPON [93].

5.3.1 Spectrum Sensing Data Falsification Attacks

Malicious CR nodes may want to insert bogus sensing reports with non-existing or false sensory information in order to spoof the FC. Hence, a full cell is considered under SSDF attack if any of the malicious CR nodes are able to forge a false sensing report to the FC regarding that cell. Assume that there are N CR nodes in the network, n average number of nodes in each cell, s endorsement nodes, d trusted CR nodes and m malicious CR nodes. Then, there are $\binom{N}{m}$ different ways for the attacker to compromise m CR nodes and $\binom{n}{s}$ different ways for each cell to select s CR nodes from n CR nodes in the network to participate in the report generation. Thus, the product of the aforementioned terms, i.e., $\binom{N}{m}\binom{n}{s}$ is the total number of different ways that an attacker can compromise m CR nodes and the cell selects s CR nodes to sign the generated report. This is based on the assumption that the adversary compromises b CR nodes out of the s endorsement nodes for the entire network. Since s CR nodes are needed to generate a report of any cell, then $(m-b)$ out of $(N-s)$ nodes must be compromised. Thus, the probability that none of the s CR nodes is captured by the attacker (i.e., the cells are secured) can be obtained by;

$$P_{s\{0\}} = \left[\frac{\binom{N-s}{m}}{\binom{N}{m}} \right]. \tag{5.11}$$

In order for a bogus report to successfully pass the verification process and be accepted by the FC, the adversary has to compromise at least s endorsement nodes and all the trusted nodes d in the corresponding cell.

Notice that, if the adversary succeeds in compromising a cell in the worst case scenario, only sensory information of that cell can be forged due to the location-aware property of the underlying verification. Hence, when compromising m CR

nodes, the probability that a particular cell is under SSDF attack (i.e., sends a faulty report to the FC endorsed by at least s CR nodes and the d trusted CR nodes) is a conditional probability and is calculated as;

$$\begin{aligned} Q_{SSDF} &= \sum_{i=1}^{s} P_{s\{i\}} \sum_{i=1}^{d} P_{d\{i\}}, \\ Q_{SSDF} &= \sum_{i=1}^{s} \left[\frac{\binom{s}{i}\binom{N-s}{m-i}}{\binom{N}{m}} \right] \sum_{i=1}^{d} \left[\frac{\binom{d}{i}\binom{N-d}{m-i}}{\binom{N}{m}} \right], \end{aligned} \tag{5.12}$$

where $P_{\{s\}} = \sum_{i=1}^{s} P_{s\{i\}}$ is the probability of compromising s CR nodes, while $P_{\{d\}} = \sum_{i=1}^{d} P_{d\{i\}}$ is the probability of compromising all d trusted CR nodes.

In Figure 5.2, we compare the security strength of the proposed scheme RCSSS against SSDF attacks with three different strategies. Our main concern here is to show the effect of the SSDF attacks on the network for different fractions of malicious CR nodes. It is evident that the proposed RCSSS performs better than other techniques in confronting SSDF attacks. This is due to the efficient verification process at the FC and the trusted node selection procedure, which makes it very difficult for the attacker to break the verification process and inject faulty sensory data. However, COOPON and BAIS find that the probability of spoofing the FC increases with increasing malicious CR nodes. This is mainly because increasing the number of malicious nodes will decrease the accuracy of detection in COOPON. However, for the BAIS strategy, when 50% or more nodes are malicious, the FC becomes completely blind, i.e., the probability of identifying an SSDF attacker becomes zero. It is clear even under a huge proportion of attackers (50%), the RCSSS performs better than the other schemes in thwarting the SSDF attacks.

5.3.2 Security Strength Regarding End-to-End Data Confidentiality and Integrity

In RCSSS, every report is encrypted using the corresponding cell key. Hence, compromising any CR node from a particular cell would not affect the confidentiality of the generated report. The content of the report is revealed and can be obtained only by a CR node inside the cell. Hence, the confidentiality of the sensory report is guaranteed even when a number of nodes outside a particular cell are compromised.

The adversary may obtain the content of the report only if a CR node participating in the generation of the corresponding report is compromised. In addition, the integrity of the sensing report should not be compromised as long as its cell nodes are not compromised. Therefore, the attacker needs to control s CR nodes of that particular cell in order to use their unique keys to modify the sensing data and create new signatures (S_{Pack}) that could pass the FC verification process. Accordingly, controlling intermediate nodes would not result in multiple gains and does not allow the adversary to break the confidentiality or the integrity of other cells. Hence, assume the attacker compromised b nodes from a total of s endorsement nodes. It is required to compromise $(m-b)$ CR nodes from the remaining $(N-s)$ CR nodes in the network in order to compromise that particular cell. As s nodes are picked randomly from N CR nodes in the network, there are $\binom{N}{s}\binom{s}{b}\binom{N-s}{m-b}$ different ways that the attacker could compromise b nodes from s CR nodes that signed the report. As a result, the probability that an attacker compromises the confidentiality is,

$$P_{s\{b\}} = \left[\frac{\binom{N}{s}\binom{s}{b}\binom{N-s}{m-b}}{\binom{N}{m}\binom{N}{s}}\right] = \left[\frac{\binom{s}{b}\binom{N-s}{m-b}}{\binom{N}{m}}\right]. \tag{5.13}$$

Lastly, the adversary needs to compromise k CR nodes from the cells trusted nodes d, only known by the FC, in order to successfully compromise a particular cell in terms of integrity,

$$P_{d\{b\}} = \left[\frac{\binom{N}{d}\binom{d}{b}\binom{N-d}{m-b}}{\binom{N}{m}\binom{N}{d}}\right] = \left[\frac{\binom{d}{b}\binom{N-d}{m-b}}{\binom{N}{m}}\right]. \tag{5.14}$$

Accordingly, in line with Baye's theorem [117], the probability of a given cell being secure with respect to data confidentiality and integrity can be calculated as a conditional probability;

$$P_{E2E\{s|d\}} = \left[1 - \frac{\binom{s}{b}\binom{N-s}{m-b}}{\binom{N}{m}}\right]\left[1 - \frac{\binom{d}{b}\binom{N-d}{m-b}}{\binom{N}{m}}\right]. \tag{5.15}$$

Figure 5.3 shows the performance enhancement achieved by the proposed scheme with respect to end-to-end security of data confidentiality and integrity. RCSSS significantly outperforms other schemes regarding the fraction of secure cells in the entire network. By adopting the location-aware feature, the impact of the compromised nodes on the entire network can be reduced to their vicinity without affecting

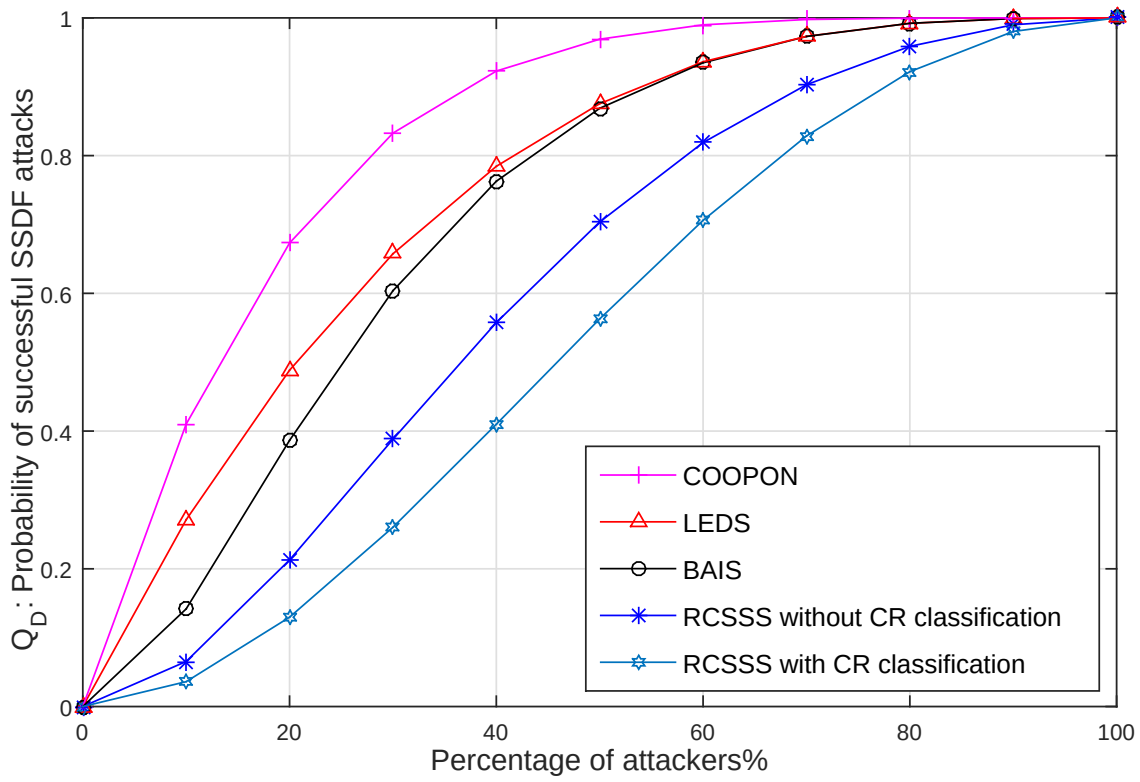


Figure 5.2: Probability of the network being under SSDF attacks versus the fraction of malicious CR users in the network

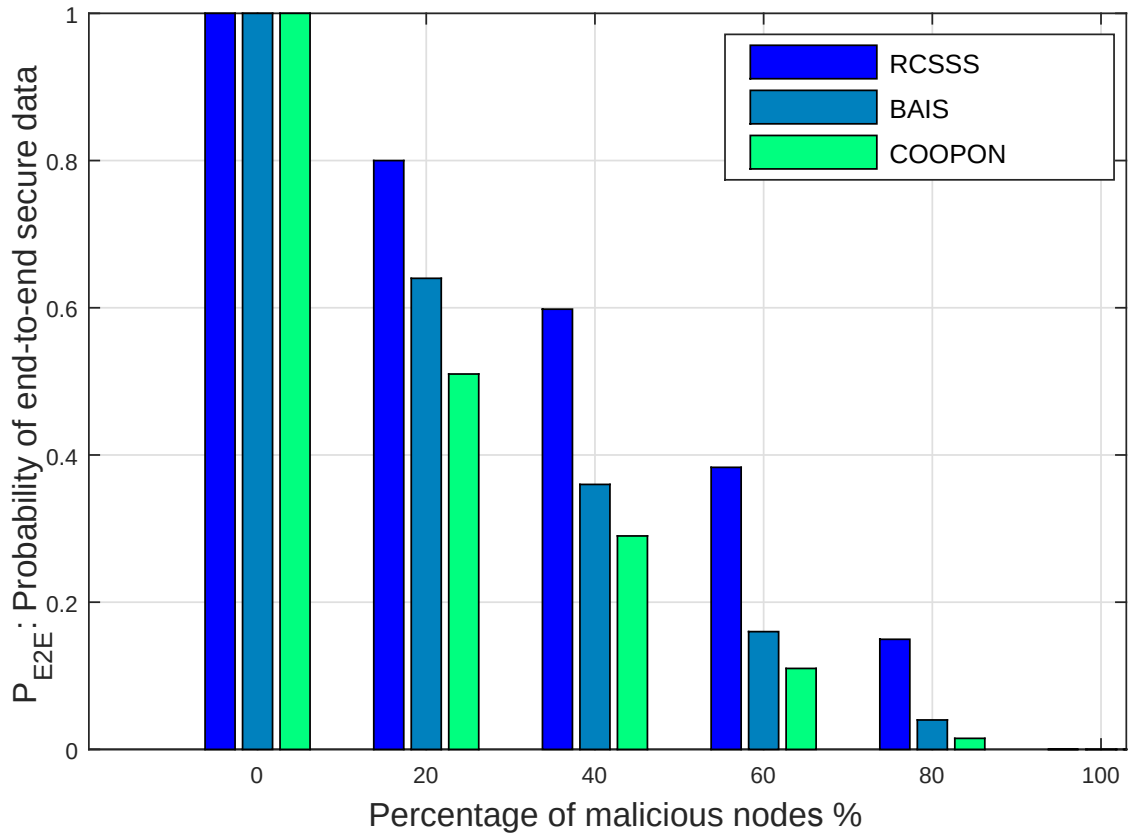


Figure 5.3: Comparison of the system's end-to-end security in terms of confidentiality and integrity

the end-to-end security of other sensing data. It clearly shows that, as the number of malicious nodes increases, the performance degradation of all systems also increases. BAIS performs well only when the number of attackers is less than or equal to 30% of the total CR nodes. On the other hand, our proposed scheme mitigates the effect of attackers even with a higher ratio of attackers. The participation of trusted nodes and the verification process of the FC makes it difficult for the attacker to compromise the security of a particular cell as it needs to control d trusted CR nodes in addition to s endorsement CR nodes in order to be able to modify the contents of the sensory data and make it pass the FC verification process.

5.3.3 The Probability of False Alarm and Missed Detection

In this section, we consider the performance of the trusted node selection in terms of its false alarm probability (Q_F) (i.e. a trusted CR node is wrongly identified as a malicious node) and missed detection probability (Q_{MD}) (i.e, a malicious CR node is wrongly identified as a trusted node). Let $\hat{P}_f$ and $\hat{P}_{md}$ denote the average probability of false alarm and missed detection for any CR node, respectively. We assume P_f^T, P_{md}^T and P_f^M, P_{md}^M are the false alarm and missed detection probabilities for the trusted and the malicious CR nodes, respectively. Based on the analysis in [118], the probability that a trusted CR_i status on the k^{th} channel, namely CH_i^k, is different from the one concluded by the FC (CH_{FC}^k) is Q_f^k,

$$\begin{aligned} Q_f^k &= Pr\{CH_i^k \neq CH_{FC}^k \mid CR_i \textit{ is a trusted node}\} \\ &= \Big[P_f^T(1-\hat{P}_f) + (1-P_f^T)\hat{P}_f\Big]P_{idle}^k \\ &\quad + \Big[(1-P_{md}^T)\hat{P}_{md} + P_{md}^T(1-\hat{P}_{md})\Big]P_{busy}^k, \end{aligned} \tag{5.16}$$

where P_{idle}^k is the probability of the k^{th} channel being idle concluded by the FC, given as,

$$P_{idle}^k = Pr\{CH_{FC}^k = idle\} = \frac{\sum_{j=1}^{L} CH_j^k}{n}. \tag{5.17}$$

Here, L is the number of reports verified by the FC out of n reports received from a particular cell.

P_{busy}^k is the probability of the channel k being busy concluded by the FC, given

as,

$$P_{busy}^{k} = Pr\{CH_{FC}^{k} = busy\} = 1 - P_{idle}^{k}, \\ = 1 - \Big(\frac{\sum_{j=1}^{L} CH_{j}^{k}}{n}\Big). \tag{5.18}$$

Furthermore, we denote by CV_i^k, the correlation value of channels status between CR_i and the FC, given by [118],

$$CV_{i}^{k} = \sum_{t=1}^{W} \mid CH_{i}^{k}(t) - CH_{FC}^{k}(t) \mid, \tag{5.19}$$

where t is the sensing time slot of a collection period W, $(t = 1, 2, ..., W)$. We assume all the channels are independent and follow a Bernoulli distribution with identical probability Q_f^k. Based on the or-rule, the CR user whose CV goes above a certain threshold θ is identified as malicious. By assuming these variables are large enough, the correlation value CV_i^k can be approximated to be a Gaussian distribution by using the Central Limit Theorem (CLT) [119],

$$CV_{i}^{k} \sim \mathcal{N}\left(WQ_{f}^{k}, WQ_{f}^{k}\left(1 - Q_{f}^{k}\right)\right). \tag{5.20}$$

Hence, with a given θ, the probability of a false alarm for a trusted CR node is,

$$Q_{f}^{k} = 1 - \Phi\left(\frac{\theta - WQ_{f}^{k}}{\sqrt{WQ_{f}^{k}\left(1 - Q_{f}^{k}\right)}}\right). \tag{5.21}$$

Finally, based on the or-rule the probability of a trusted node identified as malicious can be written as follows,

$$Q_{F} = 1 - \prod_{k=1}^{K}\left(1 - Q_{f}^{k}\right). \tag{5.22}$$

For the or-rule, the FC infers the presence of a malicious node when at least one local channel measurement does not match with the FC results. It can be seen that the or-rule is very conservative for the CR nodes to be selected as trusted nodes.

Similarly, the probability that a malicious CR_i status on channel k, namely CH_i^k, matching the one concluded by the FC (CH_{FC}^k) is Q_{md}^k,

$$\begin{aligned} Q_{md}^k &= Pr\{CH_i^k = CH_{FC}^k \mid CR_i \textit{ is a malicious node}\} \\ &= 1 - \Big\{ \Big[P_f^M(1-\hat{P}_f) + (1-P_f^M)\hat{P}_f \Big] P_{idle}^k \\ &\quad + \Big[(1-P_{md}^M)\hat{P}_{md} + P_{md}^M(1-\hat{P}_{md}) \Big] P_{busy}^k \Big\}. \end{aligned} \tag{5.23}$$

Then, by using the CLT, the correlation value CV_i^k can be approximated to be a Gaussian distribution,

$$CV_i^k \sim \mathcal{N}\left(W\left(1-Q_{md}^k\right), WQ_{md}^k\left(1-Q_{md}^k\right)\right). \tag{5.24}$$

Hence, with a given θ, the probability of missed detection for a malicious CR node is,

$$Q_{md} = \Phi\left(\frac{\theta - W\left(1-Q_{md}^k\right)}{\sqrt{WQ_{md}^k\left(1-Q_{md}^k\right)}}\right). \tag{5.25}$$

Finally, the probability of a malicious node identified as a trusted node can be written as follows,

$$Q_{MD} = \prod_{k=1}^{K} Q_{md}^k. \tag{5.26}$$

Figure 5.4 and Figure 5.5 show the performance of the trusted node selection strategy. It is clearly demonstrated that both the probability of false alarm Q_F and the probability of missed detection Q_{MD} are considerably influenced by the probability of network vulnerability β. In addition, selecting a proper threshold for the correlation value could enhance the performance of the system. The higher false alarm probability means that there is a higher probability to misjudge trusted CR nodes as malicious users. However, the higher missed detection probability means an increased presence of malicious CR nodes in the trusted list, which will result in wrong spectrum decisions.

It is worth noting that the performance of the node classification technique is influenced by the sensing information accuracy. Moreover, the presence of the trustworthiness threshold δ could significantly reduce the probability of false alarm (Q_F)

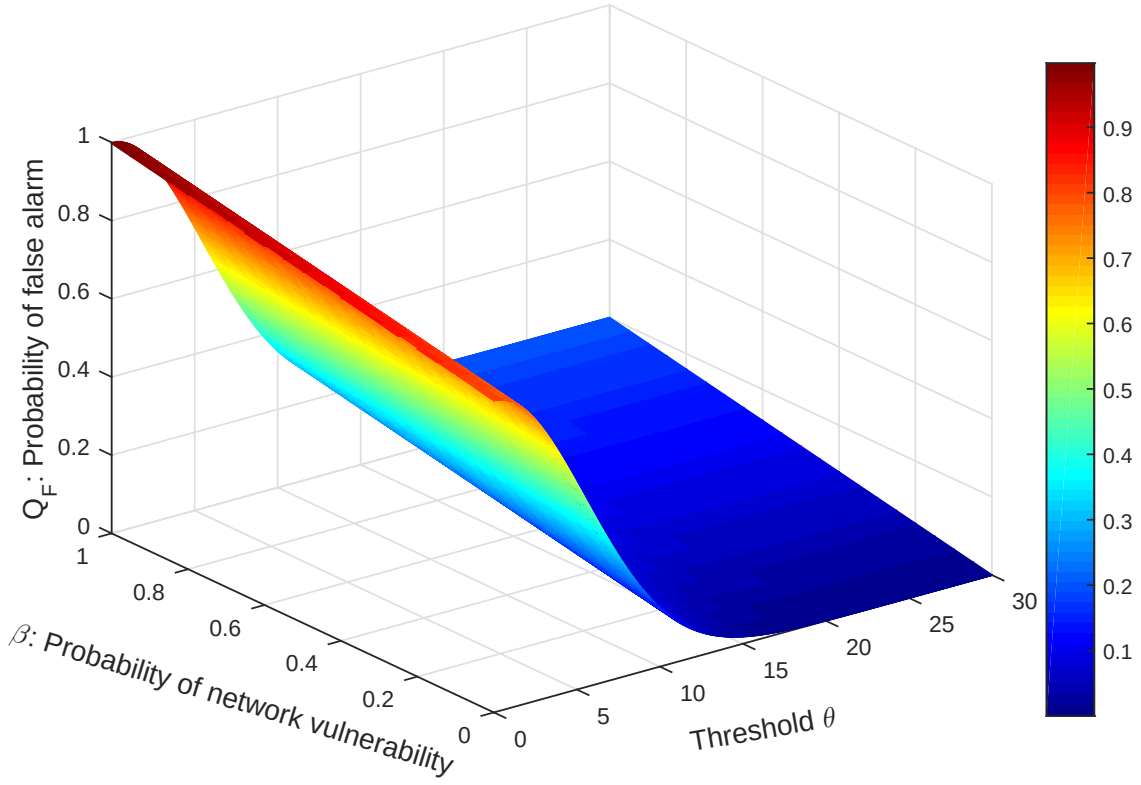


Figure 5.4: Probability of a trusted CR node wrongly identified as a malicious node

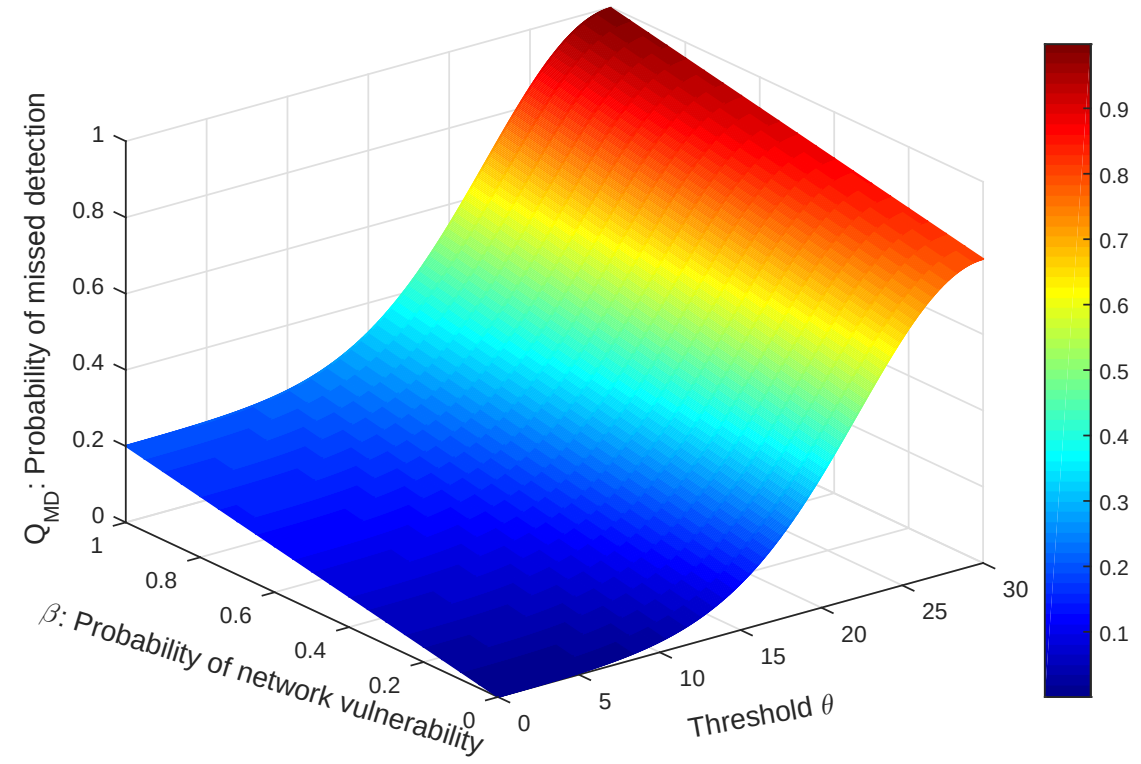


Figure 5.5: Probability of a malicious CR node wrongly identified as a trusted node

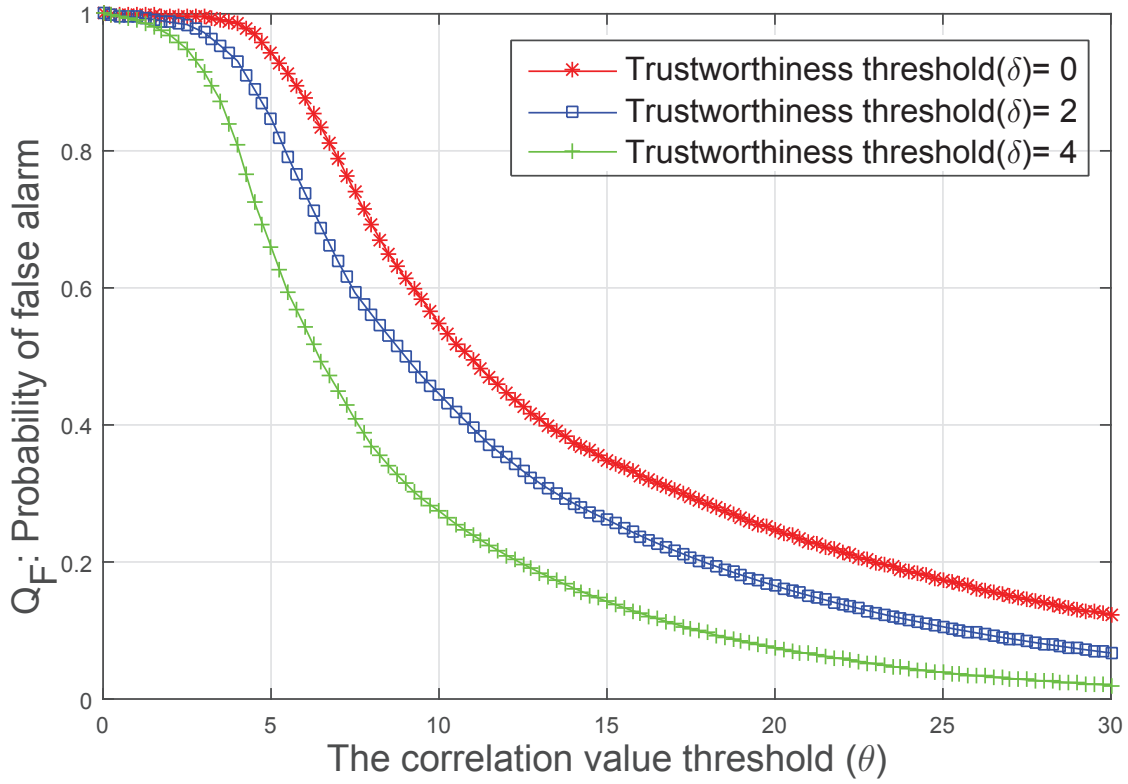


Figure 5.6: False alarm probability vs. δ and θ

and missed detection (Q_{MD}). This primarily improves the efficiency of the selection strategy used in picking up the trusted nodes and the classification of CR nodes as shown in Figure 5.6 and Figure 5.7. The probability of CR exclusion from the trusted node list is presented in Figure 5.8. We employ a reputation-based metric to counter SSDF attacks by excluding those malicious users from the sensing data fusion process. It can be noticed that the suspension probability of malicious CR nodes ($P_M^{Exclusion}$) reduces as the density of attackers rises, while the suspension probability of honest CR nodes ($P_H^{Exclusion}$) increases at the FC. When the network is under huge attack, the system will not be able to exclude malicious CR nodes from the list. In addition, it will mistakenly consider honest nodes as attackers. In this case, the system will not be of any use.

5.3.4 Identification of Malicious Nodes

Figure 5.9 compares the performance of the dynamic reputation update algorithm for different users. The behaviour of three different users, periodic attacker, intermittent attacker and honest node is considered. For the periodic attack, when the malicious node starts attacking (round four), the system reputation quickly decreases. This

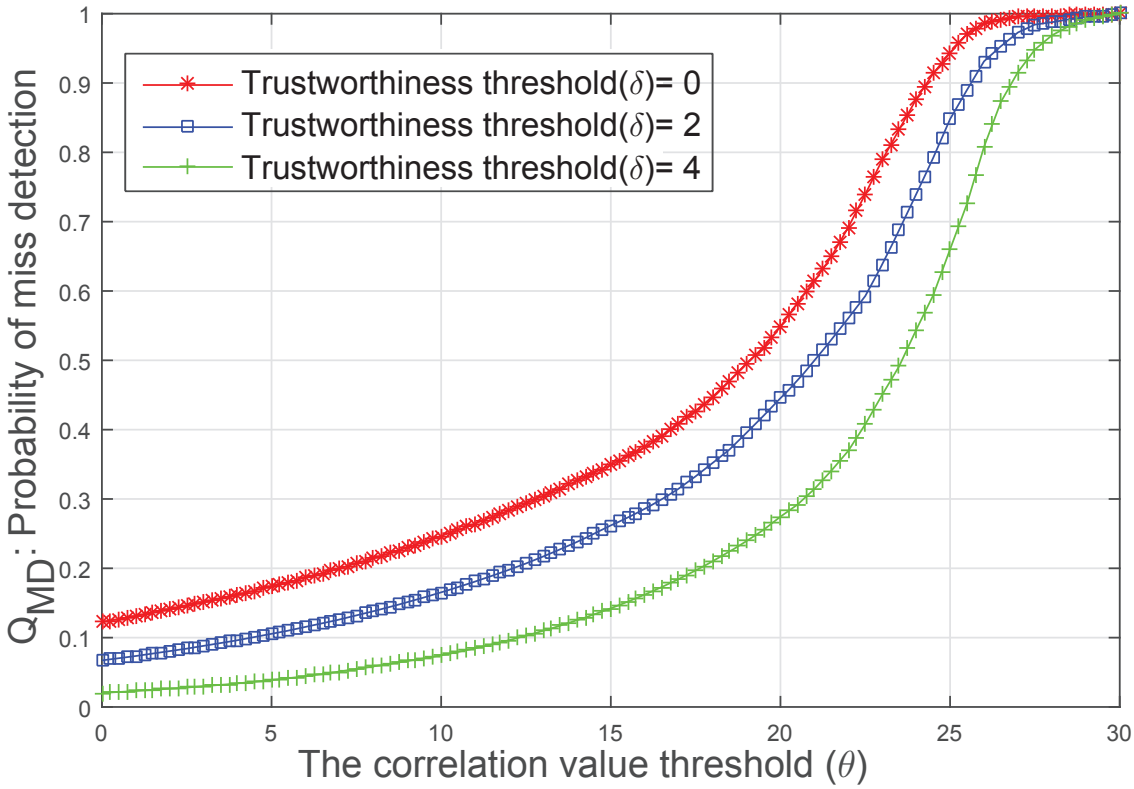


Figure 5.7: Probability of missed detection vs. δ and θ

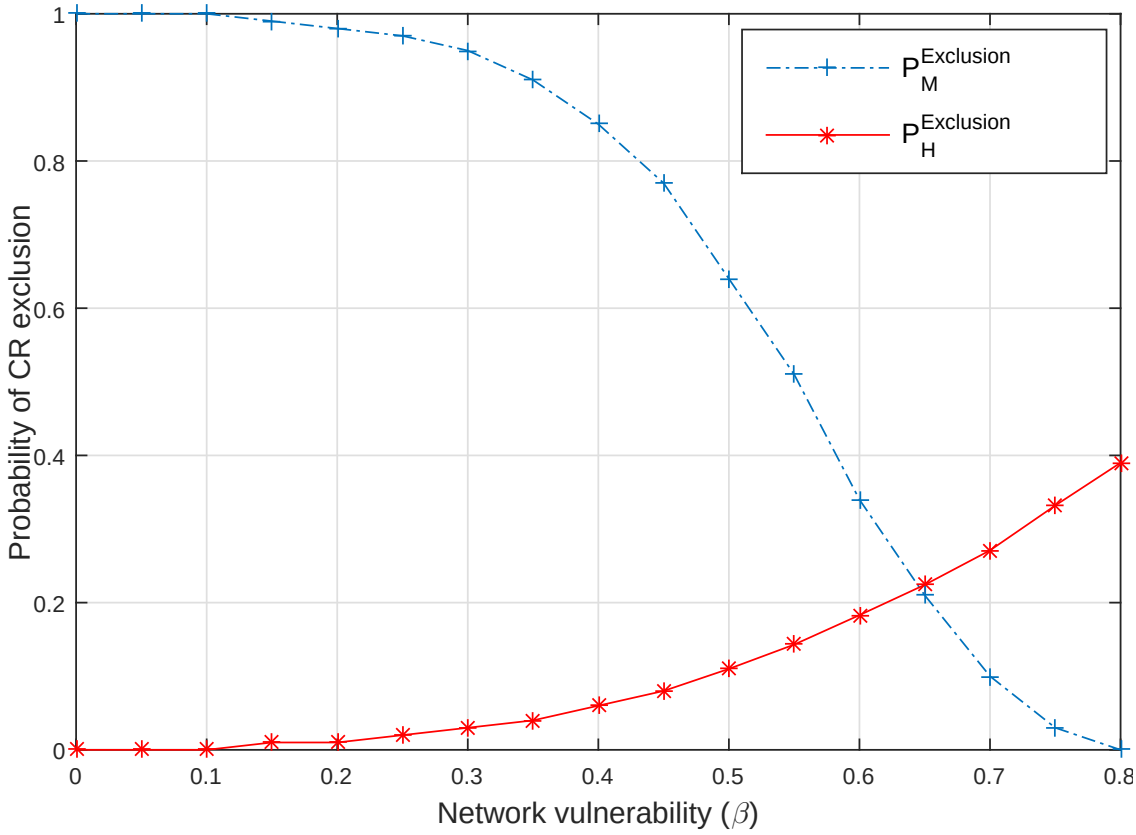


Figure 5.8: The probability of CR exclusion from the list of trusted nodes

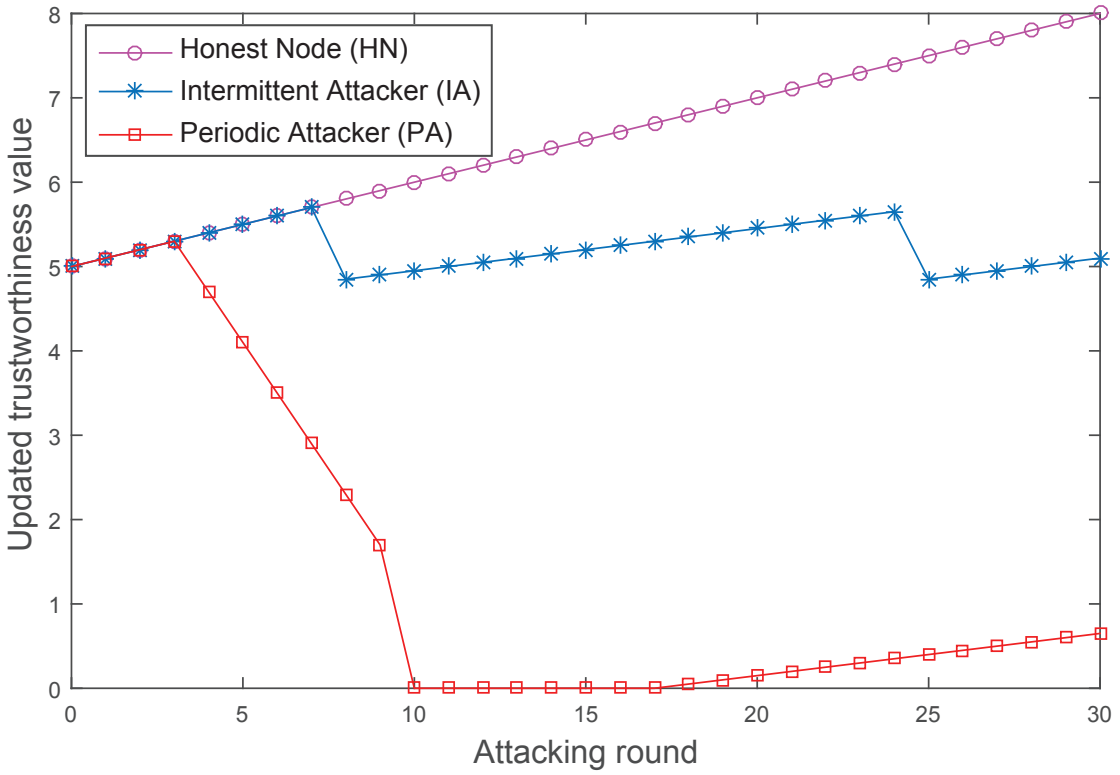


Figure 5.9: The dynamic reputation update process for different behaviours of CR users

continues as the node sends false sensing information. When the node's TR goes below a certain threshold δ, it will be excluded from the list of trusted nodes. In the case of an occasional attack, the node's reputation will decrease quickly by λ_2 when providing faulty sensing data, but will increase slowly by λ_1 when it behaves normally. Finally, the honest nodes' reputation will increase steadily with a relatively small λ_1. It is worth mentioning that adopting different weights λ_1 and λ_2 in the reputation update algorithm allows us to deal with honest nodes and malicious nodes in different ways which result in enhancing the system's performance. The proposed strategy allows fast exclusion of malicious nodes from the trusted node list. Although, it tolerates some nodes that occasionally provide wrong sensory information in order for them to correct their decisions.

5.4 Conclusion

Collaborative spectrum sensing is considered as an efficient strategy to enhance the accuracy of spectrum sensing in CR networks. However, when some nodes in the network are corrupted by adversaries, the efficiency of collaborative sensing may be

reduced considerably. In this chapter, we present a novel defence scheme against fraudulent spectrum sensing data reported by malicious CR users. Multi-levels of defence are used to maintain an adequate level of protection. First, we employ a secure authentication protocol between the FC and the collaborative nodes. Second, three tiers of verification, the unique signature of the node, the cell-mates signatures and the seal of the trusted nodes have to be checked by the FC to validate the received sensory data. Finally, an efficient reputation-based fusion scheme is used as a third level of defence, enabling the FC to select trusted nodes with the objective of ensuring the reliability of the received sensory information.

Mathematical analysis and simulation results show that our proposed scheme performs well against SSDF attacks as well as considerably enhancing the end-to-end security which enables the decision maker to obtain more reliable and accurate sensing results in an adversarial environment. The proposed framework is flexible and can be easily extended to detect various kinds of attacks in addition to SSDF attacks. The results of this work will help in minimizing the potential security vulnerabilities in the design and implementation of CR networks.

Chapter 6

Conclusion and Further Research

CR emerges as a revolutionary technology to deal with the disparity between the continuously increasing demand for wireless radio spectrum and the spectrum underutilization by licensed users. Although the operational aspects of CR networks have attracted considerable research attention, research on spectrum management techniques is still in its infancy. In this thesis, three intelligent spectrum management techniques for CR networks are addressed: 1) distributed intelligent primary receiver-aware message exchange in CR ad hoc networks; 2) distributed reliable broadcasting for CR ad hoc networks; and 3) an efficient protocol to defend particular network security attacks in CR networks. The issues investigated in this research have crucial impact on the establishment, functionality, performance and security of CR networks. Furthermore, many of the unique spectrum management challenges in CR networks are addressed for the first time in this thesis. These challenges have vital effects on the network performance and functionality and particularly difficult to solve due to the unique characteristics of CR networks. The research in this thesis is fundamental for laying the foundations of CR networks and operating networking protocols for reliable communications in CR networks. Furthermore, it provides essential visions for future protocol design in CR networks. This chapter summarizes the main contributions and highlights the major advances that have been accomplished. In addition, it sheds light on directions and suggestions for further research.

6.1 Conclusion

We started by discussing the broadcast issue and the challenges it brings in CR ad hoc networks. We then studied and discussed two straightforward broadcasting schemes. Based on the outcomes of investigating different broadcasting strategies, we obtain some important insights for designing an efficient and robust broadcasting protocol for CR ad hoc networks. Additionally, we highlighted the security threats in CR networks, specifically the SSDF attacks and its effect on the performance of the CR network. Furthermore, a survey of existing research related to the broadcasting protocols and the defending schemes against SSDF attacks is provided. The main contributions presented in this thesis are listed below:

- The control-message exchange challenges in CR ad hoc networks with PU receivers collision avoidance have been addressed for the first time. The problem is formulated by investigating the trade-off between maximizing successful CR broadcast and maximizing PU receiver protection. Two distributed broadcasting algorithms, *maximize PU protection (MPUP)* and *maximize CR connectivity (MCRC)* are proposed under practical scenarios where no global network topology is known and no common control channel is assumed to exist. The major objective of *MPUP* is the protection of the primary users, explicitly to protect PU receivers that are not detected during spectrum sensing. On the other hand, the priority of *MCRC* is to increase the packet delivery ratio by increasing the CR network connectivity. A key novelty of this work is the formulation of the broadcast issue from the viewpoint of protecting PU receivers, which is a distinctive feature in CR networks. Simulation results show that our proposed broadcasting schemes achieve higher measure of safeguarding of PU nodes whilst providing a high successful broadcast ratio. *MPUP* offers the best protection for PU communications, particularly PU receivers in the PU zones. While *MCRC* achieves a high successful broadcast ratio through connecting the maximum number of CR nodes.

- An intelligent and fully-distributed broadcasting protocol for reliable data dissemination in CR ad hoc networks named CRBP is introduced. The main design objective of CRBP is to reliably disseminate the control information through connecting different local topologies, a unique feature in cognitive

radio networks, and to synchronise both transmitter and receiver without a common control channel. The proposed protocol decomposes a complicated CR network into a simpler one so that the complexity of the original CR network can be reduced and an efficient selection of broadcast channels can be acquired. By jointly mapping the network topologies and the spectrum observations onto a bipartite graph, CRBP allows each node to capture the spectrum information and the local topologies of all the neighbouring nodes. This secures the network connectivity and reduces the interference with primary users. The reliability is ensured by connecting different topologies and synchronizing adjacent nodes. A key novelty of the proposed CRBP is the formulation of the broadcast problem from the viewpoint of connecting different local topologies, which is a unique feature in cognitive radio networks. Simulation results confirm that CRBP outperforms other broadcasting schemes in terms of reliable data dissemination and network connectivity.

- A malicious type of security threat in CR networks named the spectrum sensing data falsification is investigated. CR nodes corrupted by adversaries inject false sensory information into the central data collector during the fusion process so that the FC may make incorrect sensing decisions about spectrum availability. Furthermore, an intermediate malicious CR node could manipulate the received message before forwarding it to the FC. This attack is so difficult to detect and may seriously exacerbate the spectrum access probability. A novel and robust defence scheme to counter the SSDF attacks in CR networks is presented. Multi-levels of defence are used to maintain an adequate level of protection:i) a secure authentication protocol between the FC and the collaborative nodes is employed; ii) three tiers of verification, the unique signature of the node, the cell-mates signatures and the seal of the trusted nodes have to be checked by the FC to validate the received sensory data; iii) an efficient reputation-based fusion scheme is used as a third level of defence, which enables the FC to select trusted nodes with the objective of ensuring the reliability of the received sensory information. Mathematical analysis and simulation results show that the proposed scheme performs well against SSDF attacks as well as considerably enhancing the end-to-end security which enables the decision maker to obtain more reliable and accurate

sensing results in an adversarial environment.

6.2 Further Research

In this research, we have investigated some challenges and developed techniques for spectrum management in CR networks. However, we have only scratched the surface of this new wireless communication paradigm. There are many research issues that have not yet been investigated, particularly concerning spectrum management techniques used to fulfil the expected potential of CR wireless networks. Some recommendations for further research directions that would build on the work presented in this thesis are summarised as follows:

- Primary user activity model: We have studied the performance of the proposed broadcasting protocols based on mapping the primary network channel availability as the PU activity model for *MPUP*, *MCRC* and *CRBP* broadcasting protocols developed in Chapters 3 and 4. The primary network channel availability can be represented with different channel activity models, such as Bernoulli Process, General Distribution and Deterministic Process. It would be interesting to test and analyse the proposed protocols using different PU activity models. In fact, PU activity in a real wireless environment is much more complicated. For a practical scenario, large scale experimental tests need to be done to provide sold benchmarks for the aforementioned issue.

- Dynamic spectrum access: There are three DSA models: 1) underlay DSA model, 2) overlay DSA model and 3) interweave DSA model. Throughout this thesis, we have adopted the interweave DSA model. One potential possible direction is to extend current work while taking both underlay and overlay DSA models into account.

- Broadcast latency: Future works on this topic may focus on the investigation of how multiple CR node have to broadcast data with different priorities. In addition, we would like to measure the broadcast latency in various interference environments.

- Distributed decision: One potential improvement to the proposed defence scheme could be realized by combining the artificial neural network with the

verification module for knowledge adaptation and fusion, which might be used to deal with more challenging scenarios in CR ad hoc networks where no central entity is available.

- Extending the detecting scheme: Further research is needed to investigate more effective methods of identifying adversaries and to understand when malicious nodes collude in various groups to increase their goal of degrading the collaborative spectrum sensing. The proposed framework is flexible and can be easily extended to detect various kinds of attacks in addition to SSDF attacks.

References

[1] I. F. Akyildiz, W. Y. Lee, and K. R. Chowdhury, "Spectrum management in cognitive radio ad hoc networks," *IEEE Netw.*, vol. 23, no. 4, pp. 6–12, July 2009.

[2] FCC, "Spectrum policy take force (SPTF) report," *Federal Communications Commission Tech. Rep ET Docket No. 02-135*, November 2002.

[3] N. Zhang, H. Liang, N. Cheng, Y. Tang, J. W. Mark, and X. S. Shen, "Dynamic spectrum access in multi-channel cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2053–2064, November 2014.

[4] N. Tadayon and S. Aissa, "Modeling and analysis framework for multi-interface multi-channel cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 935–947, Feb 2015.

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

[6] M. Luis, R. Oliveira, R. Dinis, and L. Bernardo, "Characterization of the opportunistic service time in cognitive radio networks," *IEEE Trans. Cogn. Commun. Net.*, vol. PP, no. 99, pp. 1–1, 2016.

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

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

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

[10] F. K. Jondral, "Software-defined radio—basics and evolution to cognitive radio," *EURASIP Journal on Wireless Communications and Networking*, vol. 2005, no. 3, p. 652784, 2005. [Online]. Available: http://dx.doi.org/10.1155/WCN.2005.275

[11] J. O. Neel, J. H. Reed, and R. P. Gilles, "Convergence of cognitive radio networks," in *2004 IEEE Wireless Communications and Networking Conference (IEEE Cat. No.04TH8733)*, vol. 4, March 2004, pp. 2250–2255 Vol.4.

[12] FCC, "In the matter of facilitating opportunities for flexible, efficient, and reliable spectrum use employing cognitive radio technologies, authorization and use of software defined radios," December 2003.

[13] I. Poole, "What exactly is... cognitive radio?" *Communications Engineer*, vol. 3, no. 5, pp. 42–43, Oct 2005.

[14] "Ieee standard for information technology–telecommunications and information exchange between systems wireless regional area networks (wran)–specific requirements - part 22: Cognitive wireless ran medium access control (mac) and physical layer (phy) specifications: Policies and procedures foroperation in the tv bands amendment 1: Management and control plane interfaces and procedures and enhancement to the management information base (mib)," *IEEE Std 802.22a-2014 (Amendment to IEEE Std 802.22-2011)*, pp. 1–519, May 2014.

[15] F. Granelli, P. Pawelczak, R. V. Prasad, K. P. Subbalakshmi, R. Chandramouli, J. A. Hoffmeyer, and H. S. Berger, "Standardization and research in cognitive and dynamic spectrum access networks: Ieee scc41 efforts and other activities," *IEEE Communications Magazine*, vol. 48, no. 1, pp. 71–79, January 2010.

[16] A. N. Mody, M. J. Sherman, R. Martinez, R. Reddy, and T. Kiernan, "Survey of ieee standards supporting cognitive radio and dynamic spectrum access," in

MILCOM 2008 - 2008 IEEE Military Communications Conference, Nov 2008, pp. 1–7.

[17] "Ieee standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 5: Television white spaces (tvws) operation," *IEEE Std 802.11af-2013 (Amendment to IEEE Std 802.11-2012, as amended by IEEE Std 802.11ae-2012, IEEE Std 802.11aa-2012, IEEE Std 802.11ad-2012, and IEEE Std 802.11ac-2013)*, pp. 1–198, Feb 2014.

[18] M. S. Song, G. Ko, and S. Hwang, "Standardization of cognea on tv white spaces," in *2009 9th International Symposium on Communications and Information Technology*, Sept 2009, pp. 820–823.

[19] Y. Al-Mathehaji, S. Boussakta, M. Johnston, and J. Hussein, "Primary receiver-aware opportunistic broadcasting in cognitive radio ad hoc networks," in *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*, July 2016, pp. 30–35.

[20] G. Resta, P. Santi, and J. Simon, "Analysis of multi-hop emergency message propagation in vehicular ad hoc networks," in *Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing.* ACM, 2007, pp. 140–149.

[21] F. Ingelrest, D. Simplot-Ryl, and I. Stojmenovic, "Broadcasting in hybrid ad hoc networks," in *Second Annual Conference on Wireless On-demand Network Systems and Services*, Jan 2005, pp. 131–138.

[22] D. Zhao and K.-W. Chin, "Approximation algorithms for interference aware broadcast in wireless networks," in *2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, June 2013, pp. 1–9.

[23] D. Kim, C.-K. Toh, J. C. Cano, and P. Manzoni, "A bounding algorithm for the broadcast storm problem in mobile ad hoc networks," in *2003 IEEE Wireless Communications and Networking, 2003. WCNC 2003.*, vol. 2, March 2003, pp. 1131–1136 vol.2.

[24] J. Hong, J. Cao, W. Li, S. Lu, and D. Chen, "Sleeping schedule-aware minimum latency broadcast in wireless ad hoc networks," in *2009 IEEE International Conference on Communications*, June 2009, pp. 1–5.

[25] M. Chekhar, K. Zine-Dine, M. Bakhouya, and A. Aaroud, "A dynamic threshold-based probabilistic scheme for broadcasting in ad hoc networks," in *2015 15th International Conference on Intelligent Systems Design and Applications (ISDA)*, Dec 2015, pp. 511–516.

[26] Z. J. Haas, J. Y. Halpern, and L. Li, "Gossip-based ad hoc routing," *IEEE/ACM Transactions on Networking*, vol. 14, no. 3, pp. 479–491, June 2006.

[27] M. Song, J. Wang, and Q. Hao, "Broadcasting protocols for multi-radio multi-channel and multi-rate mesh networks," in *2007 IEEE International Conference on Communications*, June 2007, pp. 3604–3609.

[28] I. Chlamtac and S. Kutten, "On broadcasting in radio networks - problem analysis and protocol design," *IEEE Transactions on Communications*, vol. 33, no. 12, pp. 1240–1246, December 1985.

[29] C. Qiu, H. Shen, L. Yu, and S. Soltani, "Low-latency multi-flow cooperative broadcast in fading wireless networks," *IEEE Transactions on Computers*, vol. 65, no. 6, pp. 1802–1815, June 2016.

[30] J. Wu and F. Dai, "Broadcasting in ad hoc networks based on self-pruning," in *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428)*, vol. 3, March 2003, pp. 2240–2250 vol.3.

[31] T. Y. Wu, W. Liao, and C. S. Chang, "Cach: Cycle-adjustable channel hopping for control channel establishment in cognitive radio networks," in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, April 2014, pp. 2706–2714.

[32] H. Ohize and M. Dlodlo, "Ant colony system based control channel selection scheme for guaranteed rendezvous in cognitive radio ad-hoc network," in *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Sept 2016, pp. 1–7.

[33] R. Paul and Y. J. Choi, "Adaptive rendezvous for heterogeneous channel environments in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 11, pp. 7753–7765, Nov 2016.

[34] C. Cormio and K. R. Chowdhury, "An adaptive multiple rendezvous control channel for cognitive radio wireless ad hoc networks," in *2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, March 2010, pp. 346–351.

[35] Y. Zhang, G. Yu, Q. Li, H. Wang, X. Zhu, and B. Wang, "Channel-hopping-based communication rendezvous in cognitive radio networks," *IEEE/ACM Transactions on Networking*, vol. 22, no. 3, pp. 889–902, June 2014.

[36] K. R. Chowdhury and I. F. Akyildiz, "Crp: A routing protocol for cognitive radio ad hoc networks," *Selected Areas in Communications, IEEE Journal on*, vol. 29, no. 4, pp. 794–804, 2011.

[37] M. H. Rehmani, A. C. Viana, H. Khalife, and S. Fdida, "Surf: A distributed channel selection strategy for data dissemination in multi-hop cognitive radio networks," *Computer Communications*, vol. 36, no. 10, pp. 1172–1185, 2013.

[38] Y. R. Kondareddy and P. Agrawal, "Selective broadcasting in multi-hop cognitive radio networks," in *IEEE Sarnoff Symposium*. IEEE, 2008, pp. 1–5.

[39] C. J. L. Arachchige, S. Venkatesan, R. Chandrasekaran, and N. Mittal, "Minimal time broadcasting in cognitive radio networks," in *Distributed Computing and Networking*. Springer, 2011, pp. 364–375.

[40] J. Qadir, A. Misra, and C. T. Chou, "Minimum latency broadcasting in multi-radio multi-channel multi-rate wireless meshes," in *Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, SECON'06*, vol. 1. IEEE, 2006, pp. 80–89.

[41] K. Bian, J.-M. Park, and R. Chen, "Control channel establishment in cognitive radio networks using channel hopping," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 689–703, April 2011.

[42] N. Theis, R. Thomas, and L. DaSilva, "Rendezvous for cognitive radios," *IEEE Transactions on Mobile Computing*, vol. 10, no. 2, pp. 216–227, Feb 2011.

[43] Y. Song and J. Xie, "A distributed broadcast protocol in multi-hop cognitive radio ad hoc networks without a common control channel," in *in Proce. IEEE INFOCOM*, March 2012, pp. 2273–2281.

[44] Z. Htike and C. S. Hong, "Broadcasting in multichannel cognitive radio ad hoc networks," in *Wireless Communications and Networking Conference (WCNC), 2013 IEEE*. IEEE, 2013, pp. 733–737.

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

[46] C. Campolo, A. Molinaro, A. Vinel, and Y. Zhang, "Modeling prioritized broadcasting in multichannel vehicular networks," *Vehicular Technology, IEEE Transactions on*, vol. 61, no. 2, pp. 687–701, 2012.

[47] J. Chen and Y.-D. Chen, "Amnp: Ad hoc multichannel negotiation protocol for multihop mobile wireless networks," in *Communications, 2004 IEEE International Conference on*, vol. 6. IEEE, 2004, pp. 3607–3612.

[48] Y. Zhang, Q. Li, G. Yu, and B. Wang, "Etch: Efficient channel hopping for communication rendezvous in dynamic spectrum access networks," in *2011 Proceedings IEEE INFOCOM*, April 2011, pp. 2471–2479.

[49] A. Ghasemi and E. S. Sousa, "Opportunistic spectrum access in fading channels through collaborative sensing," *Journal of communications*, vol. 2, no. 2, pp. 71–82, 2007.

[50] L. Lazos, S. Liu, and M. Krunz, "Spectrum opportunity-based control channel assignment in cognitive radio networks," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on*. IEEE, 2009, pp. 1–9.

[51] C. Cormio and K. R. Chowdhury, "Common control channel design for cognitive radio wireless ad hoc networks using adaptive frequency hopping," *Ad Hoc Networks*, vol. 8, no. 4, pp. 430 – 438, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870509001127

[52] I. Chuang, H. Y. Wu, K. R. Lee, and Y. H. Kuo, "Alternate hop-and-wait channel rendezvous method for cognitive radio networks," in *2013 Proceedings IEEE INFOCOM*, April 2013, pp. 746–754.

[53] J. Mo, H. S. W. So, and J. Walrand, "Comparison of multichannel mac protocols," *IEEE Transactions on Mobile Computing*, vol. 7, no. 1, pp. 50–65, Jan 2008.

[54] Y. Song and J. Xie, "QB^{2}IC: A qos-based broadcast protocol under blind information for multihop cognitive radio ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 3, pp. 1453–1466, March 2014.

[55] R. Simon, L. Huang, E. Farrugia, and S. Setia, "Using multiple communication channels for efficient data dissemination in wireless sensor networks," in *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005.*, Nov 2005, pp. 10 pp.–439.

[56] L. Anantharamu, B. S. Chlebus, D. R. Kowalski, and M. A. Rokicki, "Deterministic broadcast on multiple access channels," in *2010 Proceedings IEEE INFOCOM*, March 2010, pp. 1–5.

[57] A. Asterjadhi, R. Kumar, T. L. Porta, and M. Zorzi, "Broadcasting in multi channel wireless networks in the presence of adversaries," in *2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, June 2011, pp. 377–385.

[58] A. S. Al-Mogren, "Energy adaptive approach in a multi-channel dissemination-based network," in *2008 New Technologies, Mobility and Security*, Nov 2008, pp. 1–6.

[59] W. f. Lv, F. l. Wang, and T. y. Zhu, "A greedy strategy of data dissemination over multi-channel in mobile computing environments," in *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*, vol. 5, Aug 2010, pp. V5–322–V5–326.

[60] L. Sun and W. Wang, "On distribution and limits of information dissemination latency and speed in mobile cognitive radio networks," in *2011 Proceedings IEEE INFOCOM*, April 2011, pp. 246–250.

[61] D. Starobinski and W. Xiao, "Asymptotically optimal data dissemination in multichannel wireless sensor networks: Single radios suffice," *IEEE/ACM Transactions on Networking*, vol. 18, no. 3, pp. 695–707, June 2010.

[62] C. J. L. Arachchige, S. Venkatesan, R. Chandrasekaran, and N. Mittal, "Minimal time broadcasting in cognitive radio networks," in *Distributed Computing and Networking*. Springer, 2011, pp. 364–375.

[63] K. Hamdi, W. Zhang, and K. B. Letaief, "Opportunistic spectrum sharing in cognitive mimo wireless networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 8, pp. 4098–4109, August 2009.

[64] A. K. Mir, A. Akram, E. Ahmed, J. Qadir, and A. Baig, "Unified channel assignment for unicast and broadcast traffic in cognitive radio networks." in *LCN Workshops*, 2012, pp. 799–806.

[65] M. Chraiti, H. Hakim, W. Ajib, and H. Boujemaa, "Spectrum sharing techniques for broadcast cognitive radio networks," 2013.

[66] V. K. Bhargava and E. Hossain, *Cognitive Wireless Communication Networks*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2007.

[67] N. Muchandi and R. Khanai, "Cognitive radio spectrum sensing: A survey," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, March 2016, pp. 3233–3237.

[68] L. Doyle, "Essentials of cognitive radio," 2009.

[69] D. Cabric, A. Tkachenko, and R. W. Brodersen, "Spectrum sensing measurements of pilot, energy, and collaborative detection," in *MILCOM 2006 - 2006 IEEE Military Communications conference*, Oct 2006, pp. 1–7.

[70] R. Tandra and A. Sahai, "Snr walls for feature detectors," in *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, April 2007, pp. 559–570.

[71] A. Tkachenko, D. Cabric, and R. W. Brodersen, "Cyclostationary feature detector experiments using reconfigurable bee2," in *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, April 2007, pp. 216–219.

[72] S. Helif, R. Abdulla, and S. Kumar, "A review of energy detection and cyclostationary sensing techniques of cognitive radio spectrum," in *2015 IEEE Student Conference on Research and Development (SCOReD)*, Dec 2015, pp. 177–181.

[73] H. Li, X. Cheng, K. Li, C. Hu, N. Zhang, and W. Xue, "Robust collaborative spectrum sensing schemes for cognitive radio networks," *IEEE Trans. Parallel Distr. Syst.*, vol. 25, no. 8, pp. 2190–2200, Aug 2014.

[74] A. Tukmanov, Z. Ding, S. Boussakta, and A. Jamalipour, "On the impact of network geometric models on multicell cooperative communication systems," *IEEE Wireless Commun.*, vol. 20, no. 1, pp. 75–81, February 2013.

[75] Z. Gao, H. Zhu, S. Li, S. Du, and X. Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 6, pp. 106–112, December 2012.

[76] S. M. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative sensing among cognitive radios," in *Communications, 2006. ICC'06. IEEE International Conference on*, vol. 4. IEEE, 2006, pp. 1658–1663.

[77] S. S. N, C. Cordeiro, and K. Challapali, "Spectrum agile radios: utilization and sensing architectures," in *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, Nov 2005, pp. 160–169.

[78] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio networks," in *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, Nov 2005, pp. 137–143.

[79] W. Lin, Y. Wang, and W. Ni, "Cluster-based cooperative spectrum sensing in two-layer hierarchical cognitive radio networks," in *2013 IEEE Global Communications Conference (GLOBECOM)*, Dec 2013, pp. 1082–1087.

[80] N. Ahmed, D. Hadaller, and S. Keshav, "Guess: Gossiping updates for efficient spectrum sensing," in *Proceedings of the 1st International Workshop on Decentralized Resource Sharing in Mobile Computing and Networking*, ser. MobiShare '06. New York, NY, USA: ACM, 2006, pp. 12–17. [Online]. Available: http://doi.acm.org/10.1145/1161252.1161256

[81] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 1023–1043, Secondquarter 2015.

[82] H. Ma, L. Zheng, X. Ma, and Y. luo, "Spectrum aware routing for multi-hop cognitive radio networks with a single transceiver," in *2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*, May 2008, pp. 1–6.

[83] Y. Song and J. Xie, "A qos-based broadcast protocol for multi-hop cognitive radio ad hoc networks under blind information," in *2011 IEEE Global Telecommunications Conference - GLOBECOM 2011*, Dec 2011, pp. 1–5.

[84] J. Li and J. Xie, "Rendezvous scheme without a predetermined sender or receiver in cognitive radio ad-hoc networks," in *2016 IEEE Global Communications Conference (GLOBECOM)*, Dec 2016, pp. 1–6.

[85] M. R. Kim and S. J. Yoo, "Distributed coordination protocol for common control channel selection in multichannel ad-hoc cognitive radio networks," in *2009 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, Oct 2009, pp. 227–232.

[86] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *IEEE Trans. Signal Process.*, vol. 59, no. 2, pp. 774–786, Feb 2011.

[87] J. Wei and X. Zhang, "Two-tier optimal-cooperation based secure distributed spectrum sensing for wireless cognitive radio networks," in *INFOCOM IEEE Conference on Computer Communications Workshops , 2010*, March 2010, pp. 1–6.

[88] S. Liu, Q. Liu, J. Gao, and J. Guan, "Attacker-exclusion scheme for cooperative spectrum sensing against SSDF attacks based on accumulated suspicious level," in *Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2011 IEEE International Conference on*, March 2011, pp. 239–243.

[89] S. Sodagari, A. Attar, V. Leung, and S. Bilen, "Denial of service attacks in cognitive radio networks through channel eviction triggering," in *Global*

Telecommunications Conference (GLOBECOM 2010), 2010 IEEE, Dec 2010, pp. 1–5.

[90] K. Zeng, P. Paweczak, and D. Cabric, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Commun. Lett.*, vol. 14, no. 3, pp. 226–228, March 2010.

[91] L. Wang, L. Zhang, and X. Chen, "A dynamic threshold strategy against ssdf attack for cooperative spectrum sensing in cognitive radio networks," in *2015 International Conference on Wireless Communications Signal Processing (WCSP)*, Oct 2015, pp. 1–5.

[92] C. S. Hyder, B. Grebur, L. Xiao, and M. Ellison, "Arc: Adaptive reputation based clustering against spectrum sensing data falsification attacks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 8, pp. 1707–1719, Aug 2014.

[93] M. Jo, L. Han, D. Kim, and H. P. In, "Selfish attacks and detection in cognitive radio ad-hoc networks," *IEEE Netw.*, vol. 27, no. 3, pp. 46–50, May 2013.

[94] L. Lai, H. Jiang, and H. Poor, "Medium access in cognitive radio networks: A competitive multi-armed bandit framework," in *Signals, Systems and Computers, 2008 42nd Asilomar Conference on*, Oct 2008, pp. 98–102.

[95] Q. Wang, K. Ren, and P. Ning, "Anti-jamming communication in cognitive radio networks with unknown channel statistics," in *Network Protocols (ICNP), 2011 19th IEEE International Conference on*, Oct 2011, pp. 393–402.

[96] C. Chen, M. Song, C. Xin, and M. Alam, "A robust malicious user detection scheme in cooperative spectrum sensing," in *2012 IEEE Global Communications Conference (GLOBECOM)*, Dec 2012, pp. 4856–4861.

[97] C. S. Hyder, B. Grebur, and L. Xiao, *Defense against Spectrum Sensing Data Falsification Attacks in Cognitive Radio Networks*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 154–171. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-31909-9_9

[98] H.-W. Ferng, J. Nurhakim, and S.-J. Horng, "Key management protocol with end-to-end data security and key revocation for a multi-BS wireless sensor

network," *Wireless Networks*, vol. 20, no. 4, pp. 625–637, 2014. [Online]. Available: http://dx.doi.org/10.1007/s11276-013-0627-4

[99] K. Ren, W. Lou, and Y. Zhang, "Leds: Providing location-aware end-to-end data security in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 7, no. 5, pp. 585–598, May 2008.

[100] M. H. Rehmani, A. C. Viana, H. Khalife, and S. Fdida, "Surf: A distributed channel selection strategy for data dissemination in multi-hop cognitive radio networks," *Computer Communications*, vol. 36, no. 10, pp. 1172–1185, 2013.

[101] W.-Y. Lee and I. F. Akyildiz, "Optimal spectrum sensing framework for cognitive radio networks," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 10, pp. 3845–3857, 2008.

[102] H. Kim and K. G. Shin, "Efficient discovery of spectrum opportunities with mac-layer sensing in cognitive radio networks," *Mobile Computing, IEEE Transactions on*, vol. 7, no. 5, pp. 533–545, 2008.

[103] G. Yuan, R. C. Grammenos, Y. Yang, and W. Wang, "Performance analysis of selective opportunistic spectrum access with traffic prediction," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 4, pp. 1949–1959, 2010.

[104] L. Yang, L. Cao, and H. Zheng, "Proactive channel access in dynamic spectrum networks," *Physical communication*, vol. 1, no. 2, pp. 103–111, 2008.

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

[106] Y. Al-Mathehaji, S. Boussakta, M. Johnston, and H. Fakhrey, "Crbp: A broadcast protocol for cognitive radio ad hoc networks," in *IEEE International Conference on Communications (ICC)*, June 2015, pp. 7540–7545.

[107] "The network simulator ns-2," [Online; accessed 15-April-2017].

[108] H. Harada, "A small-size software defined cognitive radio prototype," in *Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on.* IEEE, 2008, pp. 1–5.

[109] H. Kim, C. Cordeiro, K. Challapali, and K. G. Shin, "An experimental approach to spectrum sensing in cognitive radio networks with off-the-shelf ieee 802.11 devices," in *IEEE Consumer Communications and Networking Conference (CCNC)*, 2007.

[110] A. Ghasemi and E. S. Sousa, "Opportunistic spectrum access in fading channels through collaborative sensing," *Journal of communications*, vol. 2, no. 2, pp. 71–82, 2007.

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

[112] K. Sriram and W. Whitt, "Characterizing superposition arrival processes in packet multiplexers for voice and data," *Selected Areas in Communications, IEEE Journal on*, vol. 4, no. 6, pp. 833–846, 1986.

[113] D. S. Hochbaum, "Approximation algorithms for the set covering and vertex cover problems," *SIAM Journal on computing*, vol. 11, no. 3, pp. 555–556, 1982.

[114] R. M. Karp, *Reducibility among combinatorial problems*. Springer, 1972.

[115] S. Capkun and J.-P. Hubaux, "Secure positioning in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 221–232, Feb 2006.

[116] A. Shamir, "How to share a secret," *Comm., ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[117] J. Pitman, "Introduction," *Springer Texts in Statistics*, vol. 5576, no. book section 1, p. 4749, 1993.

[118] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE Trans. Wireless Commun.*, vol. 9, no. 8, pp. 2488–2497, August 2010.

[119] X. Huang, Y. Zou, B. Shen, and Q. Chen, "Dynamic suspicious reputation based collaborative sensing in cognitive radio networks," in *Communications*

and Information Technologies (ISCIT), 2014 14th International Symposium on, Sept 2014, pp. 112–116.