2014-06-04

Security Issues in Cognitive Radio Networks

Zhang, Tongjie

UNIVERSITY OF CALGARY

Security Issues in Cognitive Radio Networks

by

Tongjie Zhang

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF COMPUTER SCIENCE

CALGARY, ALBERTA

May, 2014

Abstract

Cognitive radio is an emerging trend to solve the problem of scarce spectrum resources in the prosperous area of wireless communication. By dynamically utilizing unoccupied spectrums of primary (licensed) users, secondary (unlicensed) users can meet their own communication requirements. While traditional security attacks on wireless networks still exist, the cognitive radio technologies bring unique security challenges. Current literature on solving these problems assume a central authority, which, for example, assumes the role of a fusion centre. Dynamic wireless environments are composed of users from different competing wireless operators, and assuming the existence of a central authority is a major restriction. We propose approaches that do not rely on these centralized assumptions, and are thus more applicable to practical cognitive radio networks.

Cooperative sensing is an effective solution to improve sensing accuracy and robustness in the presence of fading and shadowing that make individual sensing less reliable. However, when an adversary can corrupt some nodes in the network, the effectiveness of cooperative sensing may degrade dramatically. We design the first fully distributed security scheme, *ReDiSen*, to defend such attacks in cooperative sensing. We apply reputation generated from exchanged sensing results as an aid to restrict the impact of malicious behaviours. Both theoretical analysis and simulation results indicate that *ReDiSen* provides an effective countermeasure against security attacks by enabling secondary users to obtain more accurate cooperative sensing results in an adversarial environment. *ReDiSen* does not rely on a central authority, and is therefore more applicable in dynamic cognitive radio networks.

In a cognitive radio network, selfish secondary users may not voluntarily contribute to the desired cooperative sensing process. We design the first fully distributed scheme to incentivize node participation in cooperative sensing, by connecting sensing and spectrum allocation, and offering incentive from the latter to the former. Secondary users who are more

active and report more accurate sensing values are given higher reputation values, which in turn lead to lower prices in the spectrum allocation phase. Theoretical analysis and simulation results indicate that the proposed method effectively incentivizes sensing participation, and rewards truthful and accurate reporting. Our proposed system is fully distributed and does not rely on a central authority, and so is more applicable in dynamic cognitive radio networks in practice. We also show how to improve the robustness of reputation when malicious nodes report spurious reputation.

VCG (Vickrey-Clarke-Groves) spectrum auctions represent a classic type of truthful spectrum allocation method in cognitive radio networks. While security and privacy issues recently start to draw attention in such spectrum auctions, there exists little work that examines the scenario where the auctioneer is not fully trustworthy. We present the first verifiable VCG spectrum auction that allows verification of the winner determination and pricing phases of the VCG auction. We use maximal independent set enumeration and secure multiparty computation to solve the verification problem, while protecting privacy of wireless users. We propose different methods in different steps of the verification scheme, and analyze the effectiveness, information leakage, and efficiency. Our scheme does not rely on a third party, does not alter the auction process, and by using an offline verification process, does not introduce extra delay to the auction process.

Acknowledgements

It is my great pleasure to thank all those who helped me in various ways during my graduate studies in the University of Calgary.

I would like to thank my supervisors Dr. Rei Safavi-Naini and Dr. Zongpeng Li. They have helped me in all means through my PhD years. Their invaluable insights and directions enlightened my academic thinking. Their guidance through regular meetings ensures my research was on the right trail. No result in this thesis would have come into light without the strong support from them.

I would like to thank my other two supervisory committee members: Dr. Carey Williamson and Dr. Michael Locasto; my external examiners Dr. Ali Ghorbani and Dr. Abraham Fapojuwo; and the two examiners for my Candidacy Exam: Dr. Philip Fong and Dr. Majid Ghaderi.

I would like to thank Ms. Deb Angus and Ms. Kay Koshin for their administrative support during my research.

I would like to thank the Department of Computer Science, led by Dr. Ken Barker and Dr. Carey Williamson. The staff in our Department offered me strong support through their daily hard work on maintaining my research agenda. Thank you, Mary, Lorraine, Craig, Britta, Katie, Camille, Susan, Maryam, Beverley, Erin, Tim, Darcy, Mark, Jennifer and Coral.

I would like to thank Dr. Payman Mohassel, Dr. Mike Jacobson, Dr. John Aycock, Dr. Marina Gavrilova, Dr. Jon Rokne, Dr. Jeffrey Boyd, Dr. Rob Kremer, Dr. Frank Maurer, Dr. Faramaz Samavati for their help on research collaboration, teaching and graduate affairs governance.

I would like to thank the Faculty of Graduate Studies and the Graduate Students' Association, especially Dr. Lisa Young, Ms. Valerie McGillivray and Ms. Gillian Robinson for

their great work on helping graduate students.

I would like to thank my colleagues in the ISPIA (Institute for Security, Privacy and Information Assurance) and Networks Group: Ashraful, Ajay, Song, Mina, Tuan, Hadi, Islam, Hoi, Mohammad, Masoud, Cheng, Fatemeh, Nashad, Raul, Pengwei, Setareh, Xifan, Rashmi, Asadulla, Xiaowei, Ahmad, Zahra, Jayalakshmi, Arif, Zain, Arash, Ebrahim, Mona, Mohsen, Saeed, Pooya, Hossein, James, Kris, Mod, Ida, Sumanta, Gaven, Mahavir, Kassam, Mingwei, Hanan, Nissan, Xunrui, Fajun, Maxim, Emir, Ruiting, Ashwathi, Marian, Ali, Faisal, Ibrahim, Aniket, Shambhavi, Tang, Linquan, Ming, Yang, Maryam, Yao, Haoming, Shreya, Arsham, Brad, Michel, Narges, Tauhid, Saikar, Reza, Mostafa, Robin, Sarah, Sutapa, Daniel, Negin, Ostap, Sebastian, Anton, Hasib and Benedict.

Table of Contents

List of Tables

List of Figures and Illustrations

List of Symbols, Abbreviations and Nomenclature

Symbol	Definition
ACM	Association for Computing Machinery
ATP	Association of Tennis Professionals
BGW	Ben-Or-Goldwasser-Wigderson
BMR	Beaver-Micali-Rogaway
BS	Base Station
CCC	Common Control Channel
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CR	Cognitive Radio
CRN	Cognitive Radio Networks
DARPA	Defense Advanced Research Projects Agency
dBm	Decibels of the measured power referenced to one milliwatt
DSA	Dynamic Spectrum Access
DSP	Digital Signal Processor
DST	Dempster-Shafer Theory
EA	Exploitation Attack
FCC	Federal Communications Commission
FPGA	Field-Programmable Gate Array
GVA	Generalized Vickrey Auction
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IRIS	robust cooperatIve sensing via iteRatIve State estimation
km	Kilometre

MAC	Media Access Control
MANETs	Mobile Ad-Hoc Networks
MIS	Maximal Independent Set
MIT	Massachusetts Institute of Technology
mW	Milliwatt
NRT	Neighbor-Reputation-Table
PDA	Personal Digital Assistant
PHY	Physical Layer
PS-TRUST	Provably Secure solution for TRUST
PU	Primary User
PUE	Primary User Emulation
PU-NT	Primary User Not Transmitting
PU-T	Primary User Transmitting
QoS	Quality of Service
RAN	Regional Area Network
ReDiSen	*Re*putation-based *Di*stributed *Sen*sing
RF	Radio Frequency
RSS	Received Signal Strength
SDR	Software Defined Radio
SFDL	Secure Function Definition Language
SNR	Signal-to-Noise Ratio
SMC	Secure Multiparty Computation
SPRT	Sequential Probability Ratio Test
SSDF	Spectrum Sensing Data Falsification
SU	Secondary User
SVDD	Support Vector Data Description

TRUST	TRuthful doUble Spectrum aucTions
TTP	Trusted Third Party
UE	User Equipment
VA	Vandalism Attack
VCG	Vickrey-Clarke-Groves
VHDL	VHSIC Hardware Description Language
VHSIC	Very High Speed Integrated Circuit
VoIP	Voice over IP
WNaN	Wireless Network after Next
WRAN	Wireless Regional Area Network
WRC	World Radiocommunication Conference
WSPRT	Weighted Sequential Probability Ratio Test
XG	neXt Generation radio
XT	Crosstalk

Chapter 1

INTRODUCTION

1.1 Cognitive Radio Networks

To resolve the disparity between the escalating demand of wireless radio frequency and spectrum under-utilization by license holders (primary users), the concept of an intelligent wireless communications system, *Cognitive Radio Network (CRN)*, has been proposed [4]. CRN represents an emerging trend for mitigating the spectrum scarcity problem faced in the growing area of wireless communications. A cognitive radio is aware of its environment, and adapts to new network scenarios based on its previous experiences. In CRNs, unlicensed users (secondary users) can lease spectrum from the license holders (primary users) if no harmful interference is incurred to the latter. Compared to the traditional fixed, static spectrum allocation, CRNs bring more efficient usage of radio frequency for wireless communication [4].

1.2 Spectrum Sensing and Allocation

To minimize potential interference with the primary users, secondary users first sense whether the spectrum of interest is occupied before attempting to access it. Spectrum sensing involves the detection of the presence of a transmitted signal of interest, and is crucial for CRN performance. In the sensing process, secondary users that operate cognitive radios should not introduce harmful interference to the primary users [4]. It is sometimes challenging for a cognitive radio to carry out reliable spectrum sensing. Signals suffer from *shadow fading* and *multi-path fading*. A secondary user may also falsely detect a primary user because of noise or interference. These problems can be addressed by coordinating multiple secondary users to cooperate with each other in spectrum sensing [111]. Each secondary user acts as a sensing terminal that conducts local spectrum sensing. In the centralized cooperative sensing process, individual nodes send their local sensing data to a central authority (fusion centre), where data are processed about a final sensing decision.

Cooperative sensing can provide more accurate decision-making process, reduce amortized resource consumption at individual nodes, improve the network throughput, and overcome performance degradation [4]. Cooperative sensing is also helpful in accelerating the sensing of many channels by assigning different secondary users to sense different channels. After the cooperative sensing process, if the group decision on the spectrum state indicates that the primary users are idle, then the secondary users execute spectrum allocation protocols to decide which of them may access the fallow spectrum.

The cooperative spectrum sensing and spectrum allocation processes introduced above are implemented by the secondary users themselves without the involvement of the primary users. Considering that no sensing result can reflect the primary user state perfectly, the primary users can also actively play a role during the spectrum allocation process. Spectrum opportunities can be announced by primary users rather than detected by secondary users, if collaboration between primary users and secondary users is established [117].

Spectrum auction was proposed to efficiently share spectrum among secondary users in interference-limited systems, while the primary users can generate additional profit in the process [26]. In such a secondary spectrum market, an *auctioneer* periodically announces the fallow spectrum to be auctioned. Then the interested secondary users act as *bidders* to place their *bids*. The auctioneer implements the auction by collecting bids from the bidders and computing the winners and their prices. The auctioneer publishes the list of winners to all bidders and communicates the prices to the winners. A winner of the auction can lease the spectrum from the primary user on a short-term basis with a price charged.

A spectrum auction can have multiple winners due to spatial reuse of a wireless channel. In contrast to commodity auctions, a spectrum auction allows multiple winning bidders as long as no interference is incurred among them. The presence/absence of interference depends on the physical location and the transmission power of the secondary users. Two secondary users are connected by an edge in the *conflict graph* if their transmissions interfere with each other. VCG auctions are designed for multiple items where bidders can submit arbitrary bids for every subset of items. Considering the spatial reusability of radio spectrums, VCG auctions can be applied to implement spectrum auctions in cognitive radio networks.

1.3 Motivations

While traditional security attacks on wireless networks still exist, cognitive radio technologies bring unique security challenges. In an adversarial network environment, an adversary may compromise and control a subset of nodes to attack the cooperative sensing protocol, *e.g.*, by reporting false sensing results that aim to affect the final group decision. Such attacks are known as *Spectrum Sensing Data Falsification (SSDF)* attacks. Studies in the literature suggest that the performance of cooperative sensing can degrade significantly due to the falsified reports from malicious nodes [71].

Existing research on SSDF attacks typically assumes the existence of a fusion centre that collects local measurements, and makes the final decision on primary users' presence or absence [1,17,20,26,27,37,42,48,56,69,70,84,90,109,117,125]. The requirement of a fusion centre has its own problems:

1. The centralized schemes usually incur heavy communication overhead between the fusion centre and the cognitive radios. The reporting channels between the fusion centre and the secondary users are subject to fading, thus the results become less reliable.

2. All spatial-correlation-based detection systems imply that the geo-locations of all the cognitive radios are acquired by the fusion centre, prior to the sensing

process. We observe that the cognitive radio networks are managed by different wireless operators. The existence of a global location database amongst competing operators may be unlikely, and cannot be assumed.

3. Malicious nodes can aim to compromise the fusion centre, and hence paralyze the entire system. The fusion centre, carrying so much information, is an attractive target of attack for privacy snoopers. The single point of failure may incur a disaster of private information leakage.

4. All secondary users need to establish a connection with the fusion centre. While nodes are moving, such constant connection requires extensive usage of network protocols.

5. Another downside is the leak of private location information in some security schemes [27, 48, 69], while it is often desirable to protect location privacy in CRNs.

The existence of selfish secondary users is another problem in CRNs. Not all secondary users are willing to participate in the cooperative sensing process, which requires individual sensing and interaction with neighbouring nodes, and hence consumes energy and CPU (Central Processing Unit) cycles. In distributed CRNs, the secondary users may belong to different operators with different base stations, potentially pursuing selfish goals and making independent decisions towards whether to cooperate with other secondary users, to act alone, or even to become a free-rider. To implement fairness in the network and help honest secondary users obtain better sensing results, effective control of such selfish behaviour is important. How to incentivize the non-malicious but selfish secondary users to participate in the cooperative sensing process is therefore an interesting and important topic to investigate. The incentivizing method for cooperative sensing also needs to be fully distributed without a central authority.

In VCG auctions, the auctioneer first implements winner determination by comparing the total valuations of the different independent sets in the conflict graph [38]. The auctioneer then calculates the price for each winner in the winning independent set. In particular, the price charged to a winning secondary user is set as the externality it exerts on the other bidders. The auctioneer then publishes the winners as well as their individual prices to be charged. Existing literature mostly assumes that the auctioneer is trustworthy throughout the spectrum auction process. This is a rather strong assumption. In practice, the auctioneer may be compromised in the winner determination and/or pricing phases of a VCG auction. First, the auctioneer may announce a falsified set of winners, with whom it may have a collusion. Second, the auctioneer can charge prices to the winners that are different than what a VCG auction prescribes, for potentially gleaning a higher revenue.

For the first time in the literature, this thesis aims to detect such misbehaviours of the auctioneer. The goals of our verification mechanism design include enabling both the winning and losing secondary users in a VCG spectrum auction to discover whether the auction has been truthfully implemented by the auctioneer, including both in winner selection and in spectrum pricing. At the same time, the bidders' privacy must be protected to the maximum possible extent. For example, whenever possible, revealing direct or indirect information about a user's bid to other users should be avoided.

Another limitation in the literature is the breach of privacy of primary and secondary users in some security schemes [27, 47, 48]. In wireless networks, privacy is usually required, which is particularly important in the heterogeneous environments such as CRNs. Information shall not be disclosed to a service or application without pre-approval. The location privacy is important to be protected in CRNs. In addition, the privacy of the bidders shall be protected during the verification process of VCG auctions.

1.4 Contributions

The main contributions of this thesis are summarized below.

1. We design the first fully distributed secure spectrum sensing scheme - *ReDiSen*, where nodes only exchange information with their neighbours, to secure cooperative sensing. *ReDiSen* uses reputation to weight received values from neighbours according to their trustworthiness. With the removal of the fusion centre, the reputation system provides a mechanism to restrict the harm to the network inflicted by malicious nodes, and to help secondary users correctly identify the state of the primary user. *ReDiSen* can improve the robustness against falsified reports from malicious neighbours. More specifically, if malicious nodes report falsified values, reputation can improve the performance by adjusting the cooperative sensing values closer to the real state of the primary user. Legitimate secondary users in a distributed CRN can identify the presence/absence of primary users with high accuracy, despite the existence of malicious users who may report bogus sensing results with significant errors. *ReDiSen* also protects the location privacy of secondary users. Nodes do not need to report their geographic location to either a central authority, as required by schemes based on spatial correlation [27, 48, 69], or any other neighbour. From examining messages transmitted in the system, one cannot infer the precise location of a particular node.

2. We design the first fully distributed scheme to address the problem of incentivizing cooperation in spectrum sensing. We design a reputation-based pricing method to offer strong incentive for secondary users to pursue a lower price in the spectrum allocation process. Such connection brings more effective incentives for secondary users to participate in the cooperative sensing process,

compared to offering incentives from spectrum sensing only. With the help of a fully distributed algorithm, the secondary users can compute the global reputation value on sensing accuracy as public knowledge. To better reflect the behaviours of secondary users, we model a reputation update process that takes both previous behaviours and recent behaviour into account, while discounting previous behaviours. To countermeasure attacks on the reputation fusion process with spurious reputation from malicious nodes, we design the first fully distributed algorithm to improve the robustness of reputation. The accuracy of the public knowledge is improved, therefore, the incentives are more robust for non-malicious but selfish secondary users.

3. We design the first verifiable VCG auction that protects against mis-behaviour of the auctioneer. We show how an auctioneer can prove to the bidders that the spectrum auction was conducted correctly. Our verification scheme protects the privacy of bidders, without disclosing unnecessary information about the actual bids placed by them. The verification scheme does not rely on a trusted third party, and is hence more applicable to dynamic cognitive radio networks. Our verification scheme does not modify or interfere with the VCG auction itself. The verification process is an optional and offline plug-in module. System availability is guaranteed even with application of the verification.

1.5 Thesis Organization

This thesis is organized as follows.

In Chapter 2, we introduce the background about CRNs. Section 2.1 introduces the reason why CRNs are proposed. Section 2.2 introduces the concept of CRNs. Section 2.3 and Section 2.4 introduce spectrum sensing and cooperative sensing. Section 2.5 discusses the SSDF attacks to be counter-measured in Chapter 5. Section 2.6 discusses the selfish behaviours and consequences in CRNs to be counter-measured in Chapter 6. Section 2.7 overviews different kinds of reputation systems. Section 2.8 introduces VCG spectrum auctions to be verified in Chapter 7 through *secure multiparty computation (SMC)* introduced in Section 2.9.

In Chapter 3, we outline the related work of securing distributed cooperative sensing, incentivizing spectrum sensing, as well as verifying VCG spectrum auctions to be discussed in Chapters 5, 6, and 7. We also introduce some papers on other unique security attacks in CRNs.

In Chapter 4, we introduce the network model and attack models for Chapters 5, 6, and 7.

In Chapter 5, we present our contribution on securing distributed cooperative sensing in CRNs. Section 5.1 introduces the *ReDiSen* scheme, which can improve the cooperative sensing accuracy in adversarial environments. Section 5.3 extends Section 5.1 to multiple sensing sessions through introducing the reputation update process. Section 5.4 discusses the simulation objective, outline and results. Section 5.5 concludes Chapter 5 by discussing the assumptions, simulation parameter selections, limitations and possible future directions.

In Chapter 6, we present our contribution on incentivizing cooperative sensing in CRNs with reputation-based pricing. Section 6.1 presents the reputation-based pricing method. Section 6.2 is on reputation generation through sensing participation, sensing accuracy, and reputation update. Section 6.3 introduces the method for defending attacks in the reputation generation process. Section 6.4 presents simulation results. Section 6.5 concludes Chapter 6 by discussing the assumptions, simulation parameter selections, limitations and possible future directions.

Chapter 7 presents our contribution on verifying VCG spectrum auctions in CRNs. Section 7.1 and Section 7.2 describe the verification methods in the winner determination and pricing phases through SMC, and discuss information leakage in different methods.

Section 7.3 and 7.4 analyze the sufficiency and incentives during the verification process. Section 7.5 evaluates the efficiency and information leakage of the verification scheme. Section 7.6 concludes Chapter 7 by discussing the assumptions, limitations and possible future directions.

We conclude the thesis with the summary of contributions, limitations, and possible future research directions in Chapter 8.

Chapter 2

BACKGROUND

In this Chapter, we introduce the background related to this thesis, including the motivation behind the proposal of CRNs, the concept of CRNs, spectrum sensing, cooperative sensing, SSDF attacks, selfish behaviours and consequences, reputation systems, VCG spectrum auctions, and *Secure Multiparty Computation (SMC)*.

2.1 Why Cognitive Radio?

Wireless communication is carried by radio waves in the physical layer. Radio waves are characterized according to their frequency. A radio spectrum is divided into a number of frequency bands, each possessing particular characteristics, which determine the usage appropriate to that band. Spectrum in a country can either be purchased or allocated via government decree.

The number of wireless users and applications have grown rapidly in recent years. As the usage of small portable devices such as smart phones increases, Web surfing and data accessing from sites such as YouTube through wireless networks are becoming more common. Consequently, the volume of wireless traffic rises. This requires more spectrum bandwidth to provide satisfactory services. However, there is only a fixed amount of spectrum allocated to license holders (primary users). Each license holder maintains exclusive rights to its allocated spectrum, and unlicensed devices are not permitted to transmit in licensed bands. Spectrum is becoming increasingly crowded.

The official regulatory provisions that pertain to frequency allocations in Canada are given in the Canadian Table of Frequency Allocations and the related spectrum policies [43]. Figure 2.1 is based on the 2014 version of the table, which was developed from decisions of

World Radiocommunication Conference (WRC). Figure 2.1 provides a graphic representation of Canadian electromagnetic spectrum allocations between 9 Hz and 275 GHz. Most of the spectrums are already occupied by primary users.

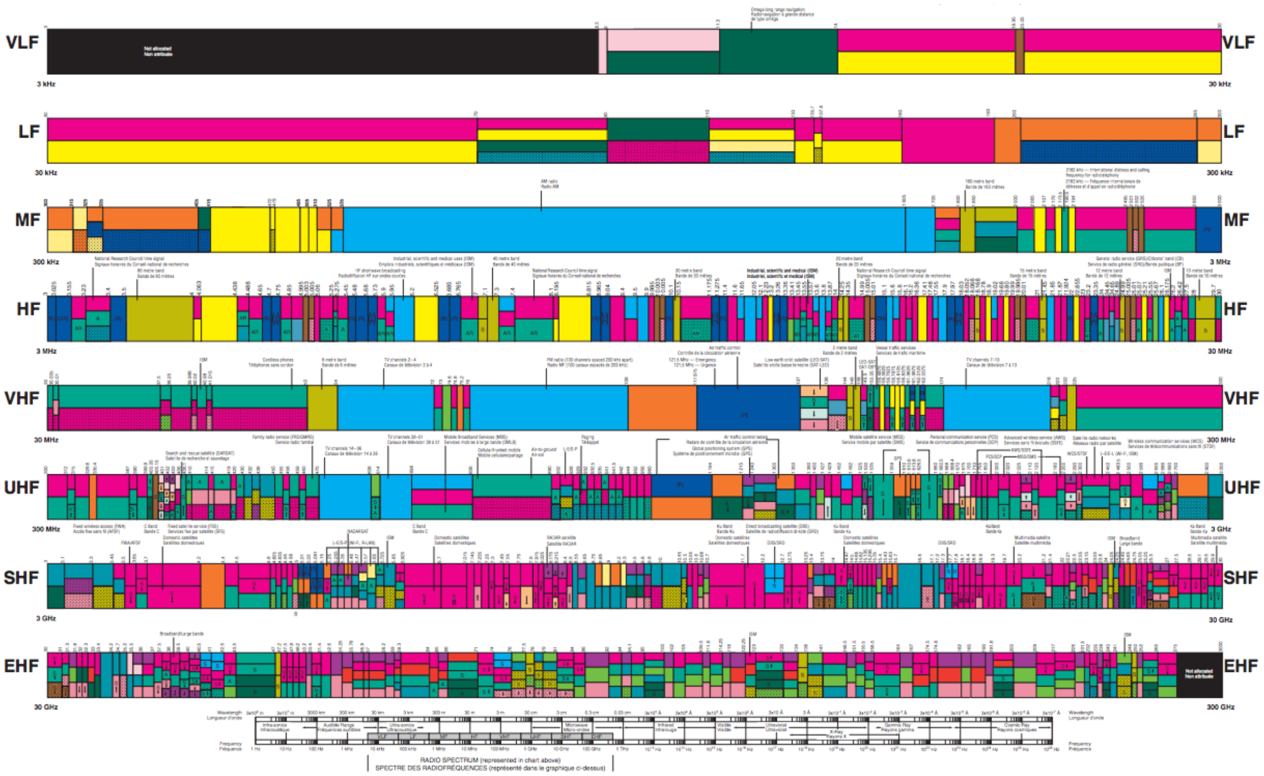


Figure 2.1: 2014 Canadian Table of Frequency Allocations

The traditional static spectrum allocation strategy is inefficient. There are a lot of opportunities in spectrum allocation strategy. Measurement studies have shown that spectrum is under-utilized in both temporal and spatial domains. Many sections of the radio frequency owned by federal agencies are unused, which leads to artificial spectrum scarcity [99]. Figure 2.2 shows the average spectrum occupancy by band in the Town of Vienna, Virginia, USA measured by the Shared Spectrum Company [91]. We can see most of the spectrums are utilized less than 20%. These unoccupied spectrums are normally referred to as *White Spaces*.

Due to jurisdictional and organizational disparities, there are different wireless frequencies, standards, and technologies for a wide range of applications. In some emergency situ-

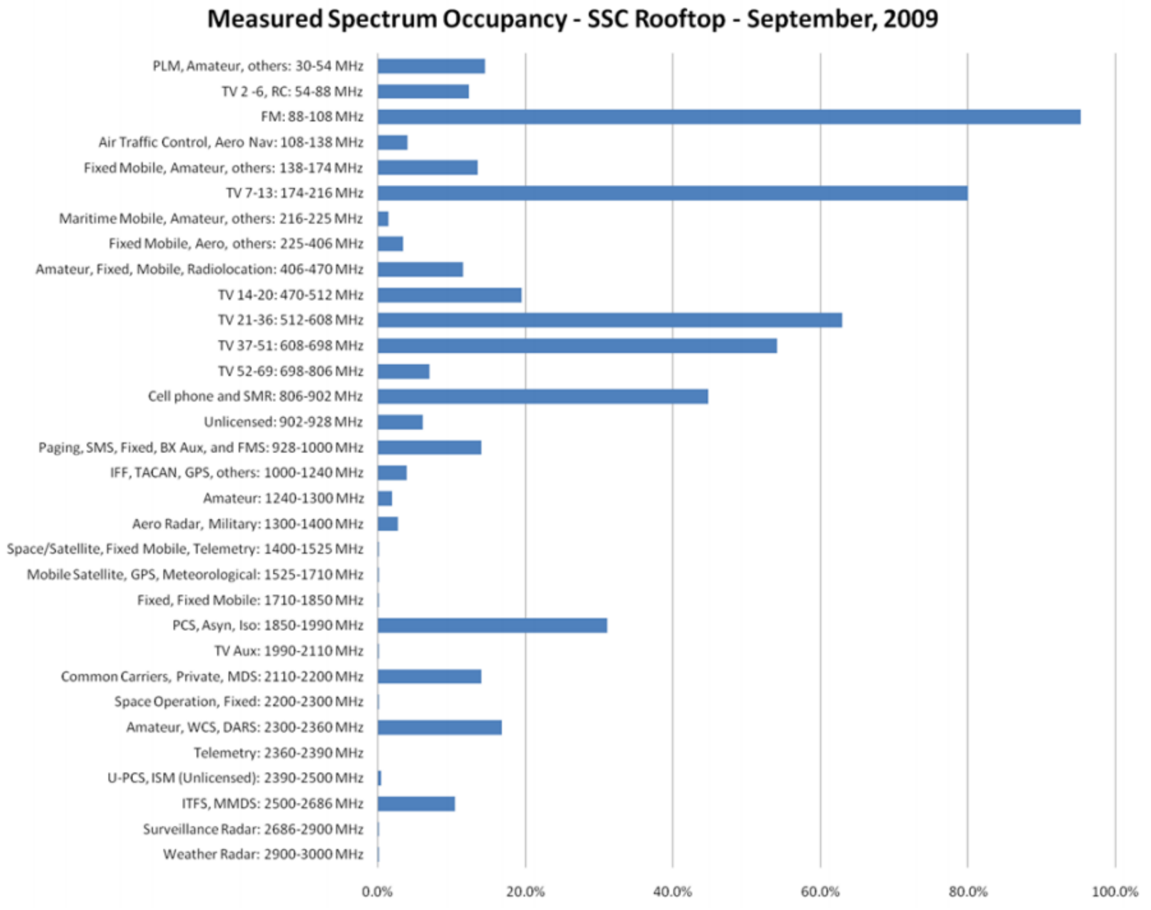


Figure 2.2: Measured Spectrum Occupancy

ations, many public safety groups such as ambulance service, police service, and fire service cannot easily communicate with each other. Figure 2.3 illustrates an emergency environment, where different public service vehicles cannot communicate with each other directly because of different radio frequencies. Communication through the *Base Stations (BSs)* of each service suffers from delay of synchronization, and security vulnerabilities in the communication of multiple paths. The public safety community is in need of extra spectrum to enable direct communication.

In this kind of heterogeneous network, reliable communication across platforms employing different communication standards is necessary.

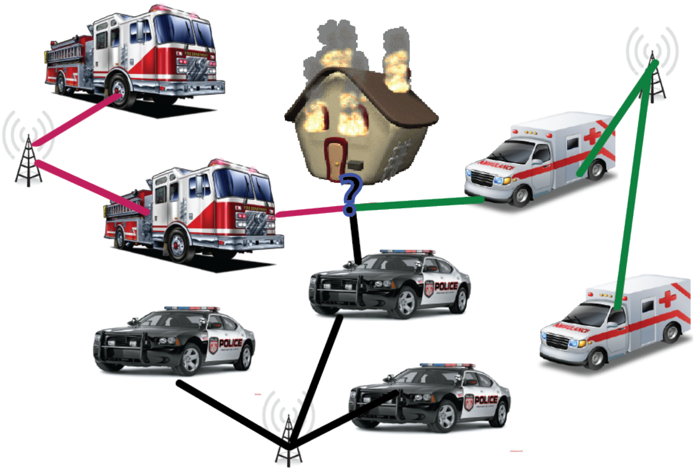


Figure 2.3: An Example of Emergency Environment

2.2 Cognitive Radio Networks

Due to the above reasons, the concept of an intelligent wireless communications system, *Cognitive Radio (CR)*, was proposed. A cognitive radio is aware of its environment (radio frequency, spectrum occupancy, network traffic, transmission quality, and so forth), and adapts to new scenarios based on its previous experiences. The two primary objectives are highly reliable communication whenever needed, and efficient utilization of radio spectrum. Given the availability of non-contiguous spectrum holes, it is possible for unlicensed users (secondary users) to lease spectrum from primary users while respecting their rights. Cognitive radio is an emerging networking technology that enables wireless devices to use spectrum much more efficiently than previous technologies. Another anticipated benefit of cognitive radio technology is that it will enable lower cost Internet access by reducing the substantial cost component associated with the purchase of spectrum. In the USA, the *Federal Communications Commission (FCC)* is planning to make wireless providers share the under-utilized spectrum with TV broadcasters. They aim to provide wireless services to 98% of Americans [28]. This is a tremendous market for cognitive radio technology.

The term *cognitive radio* was first used by Joseph Mitola III in his dissertation: *The point in which wireless personal digital assistants (PDAs) and the related networks are sufficiently* *computationally intelligent about radio resources and related computer-to-computer communications to detect user communication needs as a function of use context, and to provide radio resources and wireless services most appropriate to those needs* [73]. The FCC's definition is: *A Cognitive Radio is a radio that can change its transmitter parameters based on the interaction with the environment in which it operates. The majority of cognitive radios will probably be SDRs (Software Defined Radio) but neither having a software nor being field programmable are requirements of a cognitive radio.* SDR, sometimes abridged as software radio, is generally a multi-band radio that supports multiple air interfaces and protocols, and is reconfigurable through software running on a *digital signal processor (DSP), field-programmable gate array (FPGA)*, or general-purpose microprocessors [72]. CR, usually built upon an SDR platform, is a context-aware intelligent radio capable of autonomous reconfiguration by learning from and adapting to the surrounding communication environment [74]. CRs are capable of perceiving and sensing their *radio frequency (RF)* environment, learning about their radio resources, *user equipment (UE)*, and application environment, and adapting their configuration and behaviour accordingly [66]. Although there exist different definitions regarding the scope of cognitive radios, two features are considered essential: *re-configurability* and *intelligent adaptive behaviour* [114]. In general, the cognitive radio functionality requires sensing, learning, adapting, and being flexible and agile. A cognitive radio normally consists of several major functional blocks: sensing and detection of environment, parameter configuration, re-configurable *Media Access Control (MAC)* layer, network-layer procedures, self-organized communication/networking coordinator and radio frequency [18].

CRNs are networks where nodes are equipped with cognitive radios. A cognitive radio network can sense the operating environment and adapt the implementation to achieve the best performance. The operating environment of a CRN is broad, including the signal propagation environment, node density, traffic load, mobility, and available spectrum. CRNs can be deployed in centralized, distributed, ad-hoc, or mesh network environments. Many wireless device manufacturers, telecommunication operators and chip makers have started to invest in the research and development of CRNs [114]. DARPA (Defense Advanced Research Projects Agency) started the *neXt Generation (XG) radio* program and the *Wireless Network after Next(WNaN)* [2,68,85]. Figure 2.4 illustrates a cognitive radio network. The TV base stations have a primary user network in one spectrum. The smart-phones can communicate using the same spectrum frequency while it is unoccupied. These secondary users form a cognitive radio network. The primary user spectrum is not always occupied by the primary users. In the unoccupied time intervals, the secondary users can detect the absence of primary users and use the spectrum for their own communication. An adversary may control some of the secondary users as illustrated in the figure.

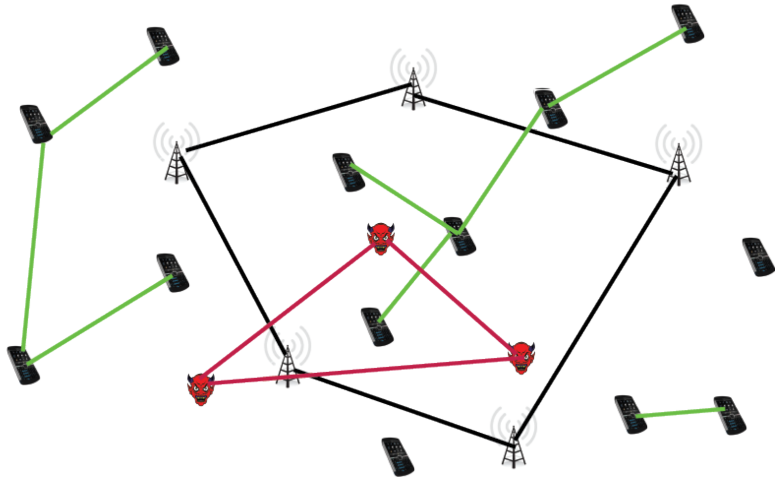


Figure 2.4: Illustration of A Cognitive Radio Network

Launched in November 2004, IEEE 802.22 (*Cognitive Wireless RAN Medium Access Control and Physical Layer specifications: Policies and procedures for operation in the TV Bands*) is the first communication standard for TV frequency spectrum using cognitive radio technology. The development of the IEEE 802.22 *Wireless Regional Area Network (WRAN)* standard is aimed at using cognitive radio techniques to allow sharing of geographically unused spectrum allocated to the *Television Broadcast Service*, on a non-interfering basis, to bring broadband access to hard-to-reach areas with low population density. It has the potential for wide usage worldwide [75]. IEEE 802.22 is the first international standard, so it can become a touchstone for the potential of cognitive radio technology.

The IEEE 802.22 working group has representatives from commercial industry, broadcasters, government, regulators, and academia. The core technology is the cognitive radio technology based spectrum usage to be operated in the TV white spaces (unoccupied spectrums) from 54-862 MHz, on a non-interfering basis for the primary users. It provides three mechanisms for the protection of primary users: sensing, database access, and specially designed beacon [75]. IEEE 802.22 specifies that the system will be formed by base stations and *Customer Premises Equipment (CPE)*. The CPEs will be attached to a base station via a wireless link. The base stations will control the medium access for all the CPEs attached to it. A key feature of the WRAN Base Stations is that they will be capable of performing distributed sensing. The CPEs will be sensing the spectrum and will be sending periodic reports to the base station, informing it about what they sense. The physical layer is optimized for long channel response times and highly frequency-selective fading channels [75].

2.3 Spectrum Sensing

Cognitive radio allows sharing wireless spectrum among many different types of devices and services. It is designed to avoid interference between the devices and services sharing the spectrum. Sharing the spectrum allows everyone to access more spectrum. Users benefit as it increases wireless bandwidth availability. Wireless networks benefit as well, as it increases the network capacity.

Spectrum sensing is crucial for CRN performance. In broad terms, spectrum sensing involves the detection of the presence of a transmitted signal of interest [23]. In the sensing process, the cognitive radio users shall not cause harmful interference to the primary users [4]. Furthermore, cognitive radio users shall efficiently identify and exploit the unoccupied spectrum for required throughput. The sensing process can be implemented by an individual secondary user or cooperatively by a group of secondary users.

A secondary user is able to decide whether a signal from a primary user is present or not within a certain time and spectrum band. The sensing methods can be categorized into different classes. *Energy detection* is the most widely adopted sensing scheme due to its simplicity, low energy consumption, and short sensing time [4]. Other detection methods include *matched filter detection* where stationary Gaussian noise is detected. This can maximize the received *signal-to-noise ratio (SNR)* [88]. This method requires a *priori* knowledge of the primary user signal such as the modulation type, the pulse shape, and the packet format. Hence, if this information is not accurate, the matched filter performs poorly. Another detection method is *cyclostationary feature detection*. Modulated signals are in general coupled with sine wave carriers, pulse trains, repeating spreading, hopping sequences, or cyclic prefixes, which result in built-in periodicity. These modulated signals are characterized as cyclostationarity since their mean and autocorrelation exhibit periodicity [101]. However, it is computationally complex and requires significantly longer observation times.

In individual energy sensing, a secondary user i decides whether a signal from a primary user is present or not within a certain time window and a certain spectrum band. When the primary user is transmitting, the sensed power E_i can be expressed by the signal propagation model as

$$E_i = E_0 - 10\gamma \log_{10}(\frac{d_i}{d_0}) - S_i - MP_i \quad \mathrm{d}Bm, \tag{2.1}$$

where E_0 is the transmit power of the primary user, γ is the path-loss exponent, d_0 is the reference distance. d_i denotes the distance from the secondary user i to the primary user. S_i represents the power loss effect due to shadow fading. MP_i represents the multi-path fading effect [118]. We use dBm for decibels of the measured power referenced to one milliwatt.

2.4 Cooperative Sensing

It is a challenge for a cognitive radio to carry out reliable spectrum sensing. In a wireless channel, signal fading can cause a secondary user to fail to detect the existence of an operating primary user. Signals suffer from different kinds of fading in cognitive radio networks. A large obstruction such as a hill or a large building obscures the main signal path between the transmitter and the receiver. This is called *shadow fading*. Another fading is called *multi-path fading*. Multi-path is the propagation phenomenon that results in radio signals reaching the receiving antenna by two or more paths. Causes of multi-path include atmospheric ducting, ionospheric reflection and refraction, and reflection from water bodies and terrestrial objects such as mountains and buildings. It is also possible for a secondary user to falsely detect a primary user because of noise or interference in the wireless environment. Figure 2.5 illustrates some examples of fading and interference. Secondary user 1 (SU1) is suffering both multi-path fading and shadow fading. Secondary user 2 (SU2) cannot detect the existence of any primary user because it is not within their transmission ranges. Secondary user 3 (SU3) also cannot detect the transmission of primary users, and so may incur interference with the primary users. These problems can be addressed by requiring multiple secondary users to cooperate with each other in the spectrum sensing.

Cooperative sensing is proposed to enhance the sensing performance by exploiting the spatial diversity of the observations of spatially distant cognitive radio users. Each secondary user acts as a sensing terminal that conducts local spectrum sensing. Then data fusion is conducted to determine the final result of spectrum sensing. Cooperative sensing can make more accurate decisions, cost less resources of individual nodes, improve the sensitivity, improve the throughput by reducing the sensing time, and overcome the performance degradation due to fading and shadowing [4]. Cooperative detection among secondary users is more accurate since the uncertainty in a single user can be reduced [31].

In distributed cooperative sensing without central authority, each secondary user obtains

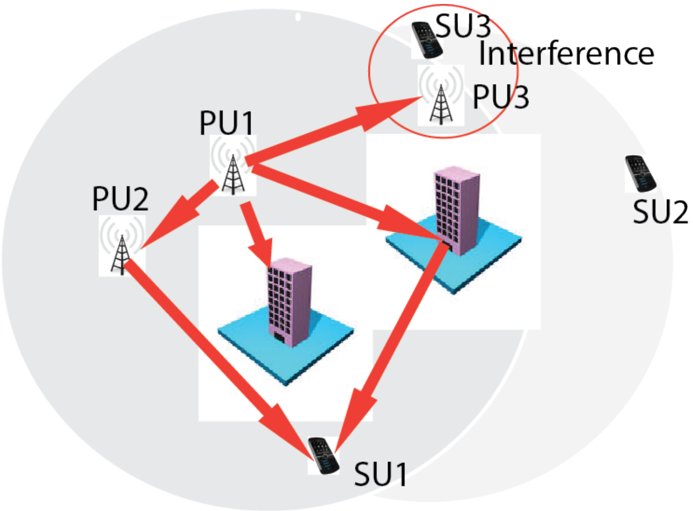


Figure 2.5: Fading and Interference

a local measurement in a time interval T. After a sensing session, a series of value update sessions are executed by the secondary users. Let $V_{i,j}^t$ be the value that a transmitter i sends to a receiver j during the update session t. We assume that $T \gg t$. If the node i is honest, then $V_{i,j}^t = E_i$. V_j^t is the value of receiver j during the update session t. All secondary users exchange their local measurements of the primary user energy with their neighbours, and update their own values based on the received values. For the honest nodes, the initial values are the sensed values of the primary user energy. The malicious nodes may report arbitrary values aiming to achieve their malicious goals. When a consensus is achieved through the cooperate sensing process, a secondary user can locally compare the consensus result with a pre-determined threshold to decide whether the primary user signal is absent or present in the monitored frequency band.

2.5 SSDF Attacks

In cognitive radio networks, attackers can generate signals that are observed by the cognitive radio, with the purpose of confusing the latter. Attackers can raise the noise floor in the vicinity of a cognitive radio, making it impossible to detect signals that shall normally be detected. Attackers can physically tamper with stored data such as policy databases. Attackers can physically jam or congest communication channels. Attackers can spoof false sensor information, resulting in non-optimal decision making. Attackers can manipulate the parameters in the learning algorithms of cognitive radios. The security issues related to cognitive radio technologies span software engineering and artificial intelligence, in addition to security. We focus on the security issues that are unique to cognitive radio networks.

Compared with individual spectrum sensing, cooperative sensing can enhance sensing accuracy, while reducing the need for sensitive and expensive sensing technology. In the cooperative sensing process, individual nodes send their local sensing data to a fusion centre or other nodes, then the data is processed to make a final sensing decision. However, the adversary may control some nodes to report false sensing results to the fusion centre or other nodes, aiming to degrade the final group decision. This is called a SSDF attack. In SSDF attacks, false spectrum sensing data are intentionally reported, with an aim of affecting the accuracy of the sensing decision. Figure 2.6 illustrates a SSDF attack. Previous studies have shown that the performance of cooperative sensing can degrade significantly due to such falsified sensing reports from malicious nodes [71].

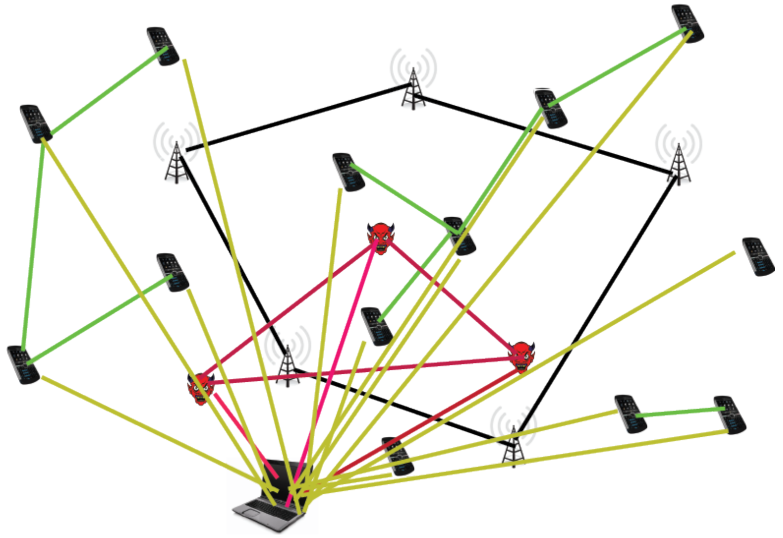


Figure 2.6: Illustration of an SSDF Attack

2.6 Selfish Behaviours and Consequences

Secondary users in a distributed CRN are subject to restrictions in weight and form-factor of the devices, which in turn limits their power supply. Since frequent battery replacement is not always practical, energy efficiency is in general an important goal. The power consumed by an active sensor is 24 mW compared to merely 0.4 mW by an inactive sensor [52]. As a result, a secondary user has a natural incentive not to sense by itself, but to act as a free-rider by passively receiving the cooperative sensing results from other honest nodes. That is, it can join the network and listen to the communication channel, without implementing the local sensing algorithm. Such selfish behaviour has no direct harm to other secondary users. However, the lack of honest neighbours' participation will compromise the level of robustness and accuracy of the cooperative sensing results.

Another reason for selfish behaviour of honest secondary users is the energy consumption and delay incurred by the iterative algorithms themselves [76]. Compared with individual sensing, the iterative algorithms proposed in the existing literature delay the decision making process. The cost of additional energy consumption in reporting sensed values to a neighbour is also non-negligible. Weighting the cost and delay from the cooperative sensing process, some honest nodes may choose not to participate in the entire process, but to perform local sensing only. If these secondary users have better sensing technologies by themselves, it is conceivable for them not to participate and share their data. Apparently, such selfish behaviour also has a negative impact on the overall well-being of the distributed CRN.

A recent work showed that honest secondary users can obtain more accurate cooperative sensing reports in an adversarial environment, as long as more than half of the neighbours correctly report sensed values [123]. This was based on the assumption that all honest secondary neighbours actively participate in the entire cooperative sensing process. However, some honest neighbours may not actively participate in the process. More honest secondary users can help the secondary user network to obtain a more accurate cooperative sensing result. The selfish behaviours of some of the honest nodes however may result in less accurate cooperative sensing results at other secondary users, which will degrade the performance of the distributed cooperative sensing. This loss of accuracy will adversely affect all nodes and in particular the selfish secondary users who will use the cooperative sensing results generated from the active secondary users. This can incentivize the honest secondary users to participate in the cooperative sensing process. However, the incentive from the cooperative sensing process itself does not apply to the cases where honest nodes choose to sense by themselves but not to report.

2.7 Reputation Systems

Reputation systems are used to cope with liars holding false positive/negative opinions [14]. The concept of reputation has been widely used in economics, ecology, anthropology and other social sciences. A rich body of literature has been devoted to the investigation of different reputation systems for computer networks [77,119].

Reputation can be computed via different approaches. In a centralized scheme, a central authority sets up and updates the reputation for other nodes. In a distributed environment, nodes can only generate reputation of their neighbours through mutual communication. There exist different models of reputation in distributed algorithms.

Evidential Model is widely adopted by online business systems, such as *eBay* and *Amazon* [50,81,120,121]. The general scenario of this model can be described as follows: a node may estimate the trustworthiness of a given party based on its own past interactions with it or may consult other trusted nodes who have directly interacted with that party. These trusted nodes are *witnesses*. There are two kinds of *beliefs* - *local belief* and *total belief*. A node's local belief about another node is from direct interactions with it, and can be propagated to others upon request. A node's total belief about another node combines the local belief (if any) with testimonies received from all witnesses reached (if any). Total belief can be used for deciding whether the node being considered is trustworthy.

In the *Broker Model*, every node is associated with a broker who represents multiple users [8, 62]. A broker collects for its users the distributed reputation ratings about any service. In return, a node provides its broker the transaction rating after every transaction with any service in order to build up the reputation database on all services. In addition, brokers form a trust network where they collect and exchange reputation data about services. A broker is a *de facto Trusted Third Party (TTP)*.

In the *Local Leader Model*, a leader is elected through a *secure leader selection* process [86]. Then the leader updates the reputation of its own neighbours, and keeps a table of the reputation values. No second-hand data is used. At each time step, each node receives an instantaneous reputation rating from the leader. The instantaneous rating is combined with its ratings from the previous time steps to form an overall reputation for the node. Observations from a node are then weighted by this overall reputation when data fusion is done by the leader.

In the *One-hop Model*, each node monitors its one-hop neighbourhood for misbehaving nodes and accordingly updates the reputation of them in the *Neighbor-Reputation-Table (NRT)* [96]. Then they publish their NRT to their 1-hop neighbourhood. Others use this second-hand information published in NRT for updating the reputation of their neighbours after it passes a deviation test.

The basic idea of the *Neural Network Model* is to aggregate a node's multiple local reputations through a neural network to approximate the node's global reputation [95]. In this setting, there is still a *Master Agent*. So this is not a truly distributed system.

In our work, we apply local belief in the Evidential Model for the reputation to be calculated to secure the fully distributed cooperative sensing, as well as total belief for the reputation calculation in the incentive methods for cooperative sensing.

2.8 VCG Auction

VCG Auction, also known as *Generalized Vickrey Auction (GVA)*, is a classical auction mechanism for selling a set of goods to a group of bidders [22, 33, 103]. In VCG auctions, a bidder i can submit arbitrary bids b_i for every subset of items. A VCG auction has two phases: winner determination and pricing. In the winner determination phase, the auctioneer computes the maximum total utility $\sum_{i=1}^{n} v_i$ over all feasible allocations, where v_i is the valuation of bidder i of the spectrum being auctioned. If i is truthful, then i's bid $b_i = v_i$. The maximum total utility feature is called economic efficiency or social welfare. The maximum total utility for a VCG auction can be solved as a Maximum Independent Set problem.

Given an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, a subset of nodes $\mathcal{S} \subseteq \mathcal{V}$ is an independent set if there is no edge in $\mathcal{E}$ between any two nodes in $\mathcal{S}$. The Maximum Independent Set problem is the following: given a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, find an independent set in $\mathcal{G}$ of maximum cardinality. The concept of a Maximum Independent Set is different from that of a Maximal Independent Set, which is defined as an independent set for which no node can be further included without violating independence. In the Weighted Maximum Independent Set case, each node $i \in \mathcal{V}$ has an associated non-negative weight $W(i)$ and the goal is to find a maximum weight independent set. In VCG spectrum auctions, the weight is the bid of the bidder i.

After winner determination, the auctioneer allocates the goods to bidders accordingly. In the pricing phase, the price p_i charged to a bidder i is the opportunity cost its presence introduces to the other bidders. The price is calculated as the difference between the total valuation of the winners, and the total valuation of the first rejected independent set who would have been allocated if i were absent from the auction

$$p_i = \max \sum_{i=1}^{n} v_i - \max_{j \neq i} \sum_{j=1}^{n-1} v_j, \tag{2.2}$$

where maximum is taken over all feasible allocations to the $n - 1$ bidders other than i.

The VCG price is equal to the 'damage' caused to other bidders by the winner's presence. VCG prices are non-negative. The utility of a truth-telling bidder in a VCG auction is always non-negative (the auction is individual rational). VCG auctions are strategy-proof. For every bidder, even if it knows the full bids of all other bidders, it maximizes its utility by bidding truthfully.

2.9 Secure Multiparty Computation (SMC)

Secure multiparty computation enables different parties to compute a function of their private inputs without revealing any information except for the output of the function. The computation is performed by the parties jointly, without a trusted authority. The basic technique for performing secure computation is: any function can be represented as a Boolean circuit and/or an algebraic circuit. Then each gate in the circuit can be securely evaluated.

FairplayMP [10] is the extension of Fairplay [67], the first implementation framework to implement arbitrary secure computation in a high level language. Programs in FairplayMP are specified in a high-level programming language, the Secure Function Definition Language (SFDL), which shares some similarity to the VHDL (Very High Speed Integrated Circuit Hardware Description Language). The FairplayMP compiler translates these programs into a garbled circuit, which is executed in a special runtime environment written in Java.

Every player has a function file that needs to be evaluated and a configuration file about the computation settings. All the participants compile the function file using the FairplayMP compiler to obtain a low level representation of a Boolean circuit. The input players share their input using the Ben-Or-Goldwasser-Wigderson (BGW) protocol [11]. The BGW protocol uses Shamir's secret sharing scheme to implement secure multiparty computation over an arithmetic circuit. Then the computation players use the input with the description of the Boolean circuit to create a garbled circuit according to the Beaver-Micali-Rogaway (BMR) protocol [9], and send the garbled circuit to the result players. Finally the result players evaluate the garbled circuit to receive their output. The FairplayMP protocol combines both arithmetic and Boolean circuit representations, and use each one where it is most efficient.

Chapter 3

RELATED WORK

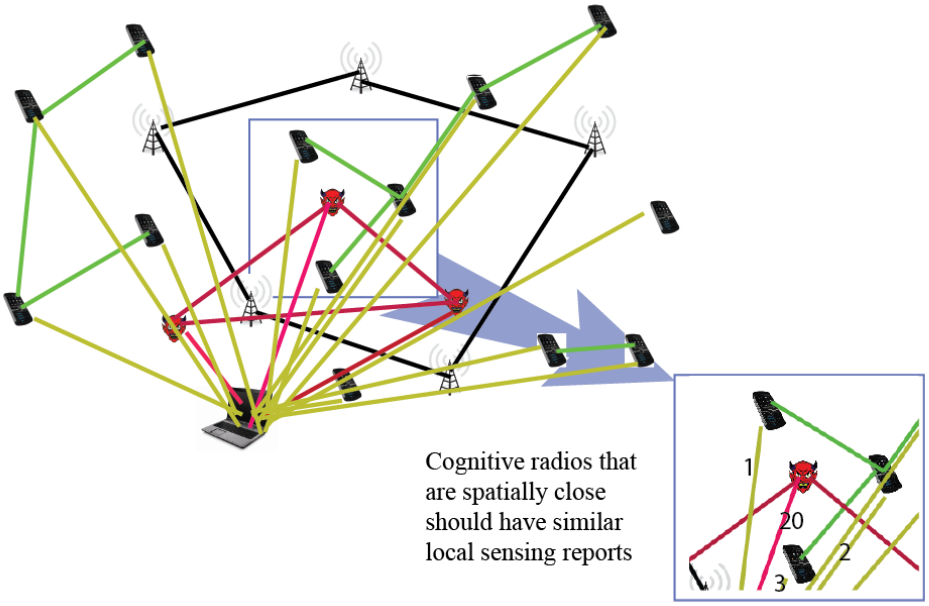
In this Chapter, we overview the key papers related to the fields of securing distributed cooperative sensing, incentivizing spectrum sensing, as well as verifying VCG spectrum auctions. We also introduce some related works on the security issues in CRNs that are not covered by this thesis. Some survey papers have explored this field more comprehensively [7, 29, 83].

3.1 Securing Distributed Cooperative Sensing

3.1.1 Spatial-correlation-based Schemes

Some schemes use location as an additional factor to identify malicious nodes. The intuition is that *cognitive radios that are spatially close to each other shall have similar local sensing reports*. Malicious nodes have to be aggressive in raising or lowering the reported signals or decisions to influence the outcome of the final cooperative sensing decision. However, any secondary user that reports significantly different sensing results from their neighbouring nodes is deemed as malicious or malfunctioning, and those sensing results will be discarded [27, 47, 48, 69]. Figure 3.1 illustrates a scenario of this kind of scheme, where malicious nodes report very different sensing values compared to that of their neighbours; they shall be detected as attackers.

Fatemieh *et al.* identified outlier measurements inside each equally divided square space cell, as well as corroboration among neighbouring cells in a hierarchical structure to identify cells with a significant number of malicious nodes [27]. The reports of individual nodes in a cell are pairwise compared. Once the outlier threshold is met or surpassed, the node is flagged as an outlier and excluded from future calculation. A weighted approach is also presented for those that are flagged as outliers by the central authority. They are assigned a



Cognitive radios that
are spatially close
should have similar
local sensing reports

Figure 3.1: Illustration of A Spatial-Correlation-Based Scheme

low or *high* label. If the average value at an outlier cell is considered too low compared to its peers, it is flagged as a *low-outlier*, otherwise a *high-outlier*. After the outlier detection and averaging is performed, the weights of nodes are updated. This work provides a framework for taking inherent uncertainties into consideration. However, it assumes that both the legitimate and malicious nodes are deployed uniformly. When malicious nodes collude to change the distribution, the system will be compromised.

Min *et al.* proposed to group sensors in close proximity into clusters, and use correlation-based filters to exclude or minimize the effect of abnormal reports [69]. Their work elegantly considers shadow-fading correlation among nearby sensors. A sensor report that significantly deviates from the neighbouring sensing reports is deemed suspicious, and will be discarded or penalized by the fusion centre. However, the system works only when attackers constitute less than $\frac{1}{3}$ of the nodes in a cluster, and is not able to detect regions that are dominated by attackers.

Kaligineedi *et al.* proposed a simple outlier detection scheme to pre-filter the extreme values in sensing data [48]. It uses an *average combination scheme* to simplify the decision process at the fusion centre. However, it has limited detection capability, and only extreme malicious reports can be filtered, with *Always Yes* users and *Always No* users identified. The extension of this method re-examines the outlier factors and proposes different kinds of strategies to improve the detection of malicious users. They also proposed using the observations from closest neighbours in a neighbourhood to further improve the detection. If the spatial information of the users is available at the fusion centre, the outlier factor can be assigned to each node based on the energy-detector outputs of its closest spatial neighbours. However, it cannot detect malicious users who can manipulate their distribution and density in the cognitive radio networks, either.

As discussed before, the geo-locations of all sensing nodes are not likely to be gathered by the fusion centre. The previous schemes assume that all cognitive radios are stationary. A development trend of cognitive radio networks is to cover mobile devices to improve the dynamic and flexible spectrum access for mobile communication [69]. While most users in a cognitive radio network tend to be mobile in both infrastructure-based or ad-hoc networks, it is hard to maintain a large database of all node locations. Spatial-correlation-based schemes where location information is not used in the detection process are more desirable. The privacy of nodes also needs to be protected. The movement of nodes shall not impact the final decision in the whole process, either.

3.1.2 Other Centralized Schemes

There are other centralized schemes for defending SSDF attacks. Wang *et al.* analyzed the impact of the malicious node population in a system, and transferred the problem to an optimization problem deciding the number of sensing reports collected under the requirement of QoS [106]. This is a passive solution without any countermeasure against the attacks. In addition, it assumes that all users have independent and identically distributed fading. This is often not realistic since signal fading of neighbouring nodes is correlated.

Chen *et.al.* proposed a weighted, reputation-based data fusion technique based on a sequential probability ratio test [19]. The test is composed of two steps: reputation maintenance and hypothesis test. Reputation is determined by the consistency of the local sensing report with the final sensing decision. The hypothesis testing is an improved version of *Sequential Probability Ratio Test (SPRT)* - *Weighted Sequential Probability Ratio Test (WSPRT)*. The idea of WSPRT is to modify the likelihood of SPRT so that the reputations of individual nodes are also taken into account. This scheme depends on *a priori* knowledge of the reported radio values. It also does not count for spatial variability of spectrum availability. It only focuses on detection in a small region. In addition, malicious users are not removed from the sensing process even if their reputation weights are low. The speed to arrive at a stable state is also unsatisfactory. Another limitation is that it can only be used for hard fusion, where secondary users only report binary results of whether the primary user is transmitting or not, but not soft fusion, where secondary users report the sensed value of the primary user energy. This limitation decreases the accuracy of the final decision.

Wang *et al.* proposed a malicious user detection algorithm that calculates the suspicion level of secondary users based on their past reports [109]. However, the assumption on *Vandalism Attack (VA)*, where malicious users report primary users absent while they are in fact present, cannot correctly reflect the effect of the attack. They only define a *false alarm attack* and a *false alarm and miss detection attack*. The false alarm attack is the same as *Exploitation Attack (EA)*, where malicious users report the presence of a primary user when there is none. However, false alarm and miss detection attack is a combination of EA and VA. If the sensed energy is higher than the detection threshold, the attacker reports a lower energy level; otherwise, it reports a higher energy level. While the primary user exists, malicious users cannot make false alarms by increasing the level of sensing reports. The scenarios of false alarm and miss detection need to be analyzed in two different cases.

Li *et al.* proposed an abnormality detection approach to detect malicious secondary users [56]. They proposed a *double-sided neighbour distance algorithm* to identify outlier users who are far away from most secondary users in the history space. However, their approach assumes $M \ll N$, *i.e.*, most nodes are honest. In addition, it assumes that if the history of a secondary user is too close to that of others, its behaviour is also abnormal. This assumption will identify the normal spatial correlation as attacks, thus cannot be applied in cognitive radio networks. This checking cannot be used in dynamic networks where the detection history of different nodes are not close to each other.

Min *et al.* proposed a *robust cooperative sensing via iteRatIve State estimation (IRIS)* attack detection framework [70]. This approach takes the network topology into consideration. However, the network topology is prone to change in most cognitive radio networks, and so the proposed approach is not always practically promising.

3.1.3 Distributed Schemes

All the above solutions assume the existence of fusion centres, and cannot operate in a fully distributed cognitive radio network. Li *et al.* proposed to remove the fusion centre by having all cognitive radios update their local measurements with neighbouring nodes iteratively to arrive at consensus [59]. A secondary user needs to communicate only with its direct neighbours. Each secondary user conducts energy detection to obtain a local measurement of the primary user's signal. These measurements are then exchanged with neighbours. A secondary user updates its value based on its own value and those received from all its neighbours. The updated values are then exchanged. This iterative process continues until a consensus is reached asymptotically among all secondary users [80]. The scheme focuses primarily on how to arrive at a consensus without considering possibly falsified local measurements. Figure 3.2 illustrates this distributed scheme. There is no centralized authority playing the role of the fusion centre. Nodes establish connections by themselves to exchange their sensing results.

Yan *et al.* discuss a number of attacks in the distributed cooperative sensing process [118]. They propose a security scheme that is still not fully distributed, as it contains a hash-based

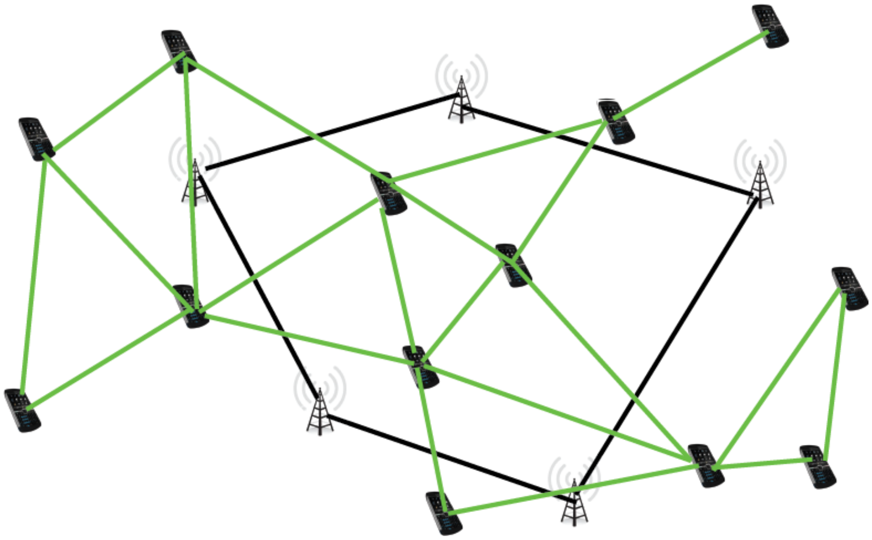


Figure 3.2: Illustration of A Distributed Scheme

verification implemented by a centralized root node.

3.2 Incentivizing Cooperative Sensing

Selfishness in collaborative sensing has recently attracted much attention. Song *et al.* first studied this problem and proposed incentive strategies [93]. Mukherjee further discussed this problem in a partially-connected network with imperfect information [76]. However, both works consider only the utility (payoff) function for secondary users as improved sensing accuracy compared to individual sensing, which is only from the spectrum sensing process. Wang *et al.* studied how secondary users can collaborate through an evolutionary game [104]. A recent work considers another selfish behaviour where secondary users report arbitrary information as their sensing results or simply copy other secondary users' reports, to save sensing energy [58]. However, both works only consider hard fusion with binary results of the primary user state, which is less fine-grained compared to soft fusion where real values from the sensed information of the primary users are exchanged. El-Sherif *et al.* discussed the joint design of spectrum sensing and spectrum allocation [24], but only considered individual spectrum sensing without cooperation.

There are a number of models for spectrum allocation. Some assume the existence of a central authority who controls and coordinates the spectrum allocation [45, 97, 100, 108, 115, 116]. The problem of allocating spectrum based on the *Quality of Service (QoS)* requirements of secondary users has been recently studied [45, 115, 116]. Some secondary users require minimum-rate guaranteed services such as *Voice over IP (VoIP)*, while some only require best effort service such as WiFi data services. These works all assume a single base station as the central authority to allocate spectrum resources to secondary users.

A number of solutions propose distributed spectrum allocation methods [16,92,105,122], where each secondary user makes its own decision about the spectrum access strategy, mainly based on local observation of the spectrum dynamics. A hybrid method, called distributed-centralized spectrum allocation, enables the secondary users to elect a leader randomly from either the secondary users or the primary users to act as the central authority [116].

3.3 Verifying VCG Spectrum Auctions

A plethora of mechanisms for spectrum auctions in cognitive radio networks have been proposed, with different targets [34–36, 39, 44, 112, 126–130]. We briefly introduce some milestone papers in this field. VERITAs is the first single-sided truthful spectrum auction [126]. TRUST is the first truthful double spectrum auction that enables spectrum reuse [127]. Huang *et al.* proposed two spectrum auction schemes to deal with wireless interference constraints. Jia *et al.* proposed a spectrum auction scheme that computes approximately maximum revenue as an alternative goal to maximize social welfare. Wu *et al.* proposed a semi-definite programming based solution that is resistant to collusion. Zhu *et al.* proposed spectrum auction for networked secondary users [128]. Gopinathan *et al.* focused on the guarantee of truthfulness through bid independent prices [36]. However, most of them do not provide security guarantee for the spectrum auctions.

Some recent works explore security issues in the spectrum auction [21, 41, 82]. Huang *et* *al.* proposed an auction agent between the auctioneer and the bidders to protect privacy [41]. Chen *et. al.* extended TRUST into PS-TRUST, to protect the privacy of bidders [21]. PS-TRUST also introduced a third party as the auction agent. Their focus is protecting the privacy of the bidders, and is thus orthogonal to the focus of this thesis.

A verification scheme for Vickrey or second price auction has been recently proposed [5]. The Vickrey auction rule is: the bidder with the highest bid wins the item, and pays an amount equal to the second highest bid. Vickrey auction is designed for one-item-one-winner auctions. No previous work has investigated the verification for VCG spectrum auctions in cognitive radio networks.

3.4 Other Unique Security Attacks

There are other attacks that are unique to CRNs. The adversary may emulate the characteristics of a primary user in attempting to gain priority over other secondary users. This is known as a *primary user emulation (PUE)* attack. Li *et al.* modelled the game between attackers and defenders in a multichannel cognitive radio system as a dogfight game [57]. Liu *et al.* used a helper node close to a primary user to enable a secondary user to verify cryptographic signatures carried by signals of the helper node, and then obtain the authentic link signatures of the helper node to verify primary user signals [63].

Bian *et al.* first analyzed security vulnerabilities in the spectrum allocation of IEEE 802.22. The security sub-layer protects network control information by attaching message authentication codes to the management messages. However, the security sub-layer only protects *intra-cell* management messages and does not protect *inter-cell* beacons [12].

CRN users usually coordinate with each other by using a common medium for control message exchange. This common medium is known as a common control channel (CCC) [2, 3, 64, 65]. For jamming into the common control channel, Tague *et al.* proposed to use random assignment of cryptographic keys to hide the location of common control channels [102]. Lazos *et al.* proposed a randomized distributed scheme that allows nodes to establish a new control channel using frequency hopping [54]. Safdar *et al.* proposed a new framework for providing common control channel security by authenticating secondary users and exchanging secure key in the transactions [87].

Chapter 4

SYSTEM MODEL

We introduce the network model and attack models in this chapter. The glossary of notations in this Chapter is listed as Table 4.1

Symbol	Description
N	Number of Secondary Users
K	Number of Orthogonal Frequency Channels
Ω_N	Set of Secondary Users
Ω_K	Set of Channels
$\mathcal{G}$	Graph
$\mathcal{V}$	Set of Vertices
$\mathcal{E}$	Set of Edges
m_i	Number of i's Neighbours who Report Falsified Values
n_i	Number of i's Neighbours who Report Correct Values
$\mathbf{P}_i$	Transmission Power Vector of i over all Channels
P_i^k	Transmission Power of i on Channel k

Table 4.1: Glossary of Notations in Chapter 4

4.1 Network Model

We consider a hybrid network consisting of several primary user networks and a secondary user network. There are N secondary users. The total radio spectrum consists of K orthogonal frequency channels where *crosstalk (XT)* between the channels is eliminated. XT is a phenomenon where a signal transmitted on one channel creates an undesired effect in another channel. The primary users are located relatively far away from the secondary users. Each primary user network operates over a predetermined channel with high transmission power, and are abstracted as a single virtual node. Let $\Omega_N = \{1, 2, \ldots, N\}$ and $\Omega_K = \{1, 2, \ldots, K\}$ denote the sets of secondary users and channels, respectively.

Each secondary user is equipped with a cognitive radio. They utilize omnidirectional antennas to communicate with each other. The network formed by the secondary users is modelled as an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. The set of secondary users are the nodes $\mathcal{V}$, and the set of edges is $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$. A node j is a neighbour of a node i if $(i, j) \in \mathcal{E}$, indicating that i and j can directly communicate. The neighbours of a node i are denoted by $\{j|(i, j) \in \mathcal{E}\} \subset \mathcal{V}$. Secondary users are located within the transmission range of the primary users, and can individually sense the environment to detect the existence of the primary users.

We use the energy sensing method in the cooperative sensing process for a secondary user to detect primary users' presence. An active secondary user measures the primary user energy in a sensing session. Each sensing session is followed by a series of value update sessions, where active secondary users exchange local measurements with neighbours, and update their own values based on received values. For honest nodes, the initial values are the sensed values of the primary user energy. The malicious nodes may report arbitrary values aiming to achieve their malicious goals.

In a given sensing round, a secondary user i has m_i neighbours who report falsified values (including attacking malicious neighbours and honest nodes that sense falsely due to severe fading or system failure), and n_i neighbours who report correct values (including honest nodes that sense correctly and non-attacking malicious nodes), each equipped with a cognitive radio. They are located within the transmission range of primary users, and can individually sense the environment to detect the existence of primary users. The secondary users share a single identity system, where the identities of neighbours are resistant to *Sybil* attacks, where a node illegitimately claims multiple identities [79].

If the cooperative sensing results indicate that the primary users are not transmitting on certain channels, the secondary users can transmit on these unoccupied channels. The secondary users are able to transmit or receive over multiple channels simultaneously. They can also share a particular channel with different transmission power, which leads to a corresponding level of interference. The transmission power vector of a secondary user i over all channels is denoted by $\mathbf{P}_i = (P_i^1, P_i^2, \ldots, P_i^K)$, where P_i^k is the transmission power of i on channel k. There is an upper-bound for the total transmission power of a secondary user over all the channels.

In VCG spectrum auctions, we assume that the primary user acts as the auctioneer, and sells its wireless spectrum. The secondary users are the bidders. A conflict graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ models interference among the set of bidders. Two bidders $i, j \in \mathcal{V}$ interfere if $(i, j) \in \mathcal{E}$. The topology of G is public knowledge. The auctioneer implements a VCG auction that allocates the wireless spectrum in an interference-free manner, and charges prices based on the VCG pricing rule.

4.2 Adversary Model

We now present the adversary models that will be studied in Chapters 5, 6, and 7.

4.2.1 Securing Distributed Cooperative Sensing

A malicious node can identify, and communicate with, other malicious nodes in each attack. We assume malicious nodes will follow one of the following attack strategies based on their attacking frequency and output values:

1. *Always Attack*: The malicious nodes attack in all sensing sessions. They always report falsified values: the lowest possible value (thermal noise) while the primary user is transmitting, and the highest possible value (primary user transmission power) while the primary user is not transmitting.

2. *Intermittent Attack*: The malicious nodes attack in some selected sessions. They report falsified sensed values to the honest neighbours in attacking sessions, and truthful sensed values in non-attacking sessions. We define the *attack intensity* as the percentage of sessions when falsified values are reported.

3. *Random Attack*: The malicious nodes may not participate in the sensing process in *Random Attack*, compared to *Always Attack* and *Intermittent Attack* where they sense the primary user state. They just report random values within a rational range to other honest neighbours, no matter whether the primary user is transmitting or not.

4. *Camouflaged Attack*: Other than the falsified values or random values, the malicious nodes report the attenuated signal strength on its location when the primary user is not transmitting. They report values that appear reasonable and are similar to the local measurements of honest nodes from previous sensing sessions when the primary user was transmitting. This attack strategy is especially preferred by the adversary in a light fading environment, where honest nodes have better knowledge of the distance to the primary user.

In *Always Attack*, *Intermittent Attack*, and *Camouflaged Attack*, the malicious nodes first sense the primary user energy, and then decide what values to report to their neighbours based on the primary user state. In *Random Attack*, the malicious nodes report random values without sensing first. The adversary can be either *selfish*, aiming to have exclusive access to the primary user spectrum, or *vandalic*, aiming to incur severe interferences among the primary users and other secondary users.

4.2.2 Incentivizing Cooperative Sensing

There are three kinds of nodes in the network:

1. *Always active honest nodes*, who participate in all the cooperative sensing processes, and report their sensed results and reputation vectors;

2. *Honest but selfish nodes*, who may choose not to participate in the cooperative sensing process at all the channels. When they decide to participate, they report their sensed value to neighbours;

3. *Malicious nodes*, who may or may not participate in the cooperative sensing process, and report falsified values when participating.

We assume malicious nodes participate in the pricing game with fraudulent information. During the reputation fusion process, malicious nodes may report low reputation values for honest nodes and high reputation values for themselves, aiming at lower prices in the spectrum allocation process.

4.2.3 Verifying VCG Spectum Auctions

The following adversarial behaviours of the spectrum auctioneer are considered.

1. *Winner falsification*: The auctioneer chooses a set of bidders that is not social welfare maximizing.
2. *Price falsification*: The auctioneer charges a winning bidder a price that is different from its VCG price.

The bidders (spectrum buyers) are assumed to be semi-honest but curious. They follow the prescribed protocol, but are interested in learning private information about other bidders. There is no collusion among bidders.

Chapter 5

SECURING DISTRIBUTED COOPERATIVE SENSING

It is desirable to design a secure, scalable, and distributed cooperative sensing scheme without fusion centre, which can still secure distributed cooperative sensing in CRNs with malicious attackers. The fusion centre is an essential component to implement the existing secure cooperative sensing solutions, which do not allow a straightforward extension to a distributed solution. While there exists work in the literature that discusses security issues in distributed cooperative sensing, some centralized mechanisms, *e.g.*, root nodes, are still required [118]. A distributed scheme where secondary users exchange with their neighbours and update their value iteratively without a central authority does not consider the security attacks in the cooperative sensing process [59]. In this thesis, we propose *ReDiSen*, a *Re*putation-based *Di*stributed *Sen*sing scheme that is the first fully distributed cooperative spectrum sensing scheme with security assurance against malicious behaviour of a subset of nodes. This thesis introduces the distributed method to help secondary users obtain more accurate cooperative sensing results through an iterative update algorithm [123]. A secondary user reliably exchanges information with neighbours within its communication range. The set of neighbours of a node may evolve as nodes move around in the network. *ReDiSen* is applicable to dynamic yet adversarial CRN environments.

The glossary of notations in this Chapter is listed as Table 5.1

Symbol	Description
T	Sensing Session
t	Value Update Session
$V_{i,j}^t$	Value i Sends to j during Update Session t
V_j^t	Value of Receiver j during Update Session t
$R_{j,i}^{(VD)}$	Reputation Value of i generated by j based on Value Differences
m_i	Number of i's Neighbours who Report Falsified Values
n_i	Number of i's Neighbours who Report Correct Values
θ	Discount Factor
$\bar{V}_j^{t+1}$	Value from the System without Reputation
$R_{j,i}^{(RV)}$	Reputation Value of i generated by j based on Received Values
A_j	Average Difference from the Average Value of j's Neighbours
δ	Discount Factor
σ	Standard Deviation for Fading
E_0	Primary User Transmission Power
d_0	Reference Distance

Table 5.1: Glossary of Notations in Chapter 5

5.1 Reputation Requirements

We use a reputation system to weight the information received by a node from its neighbour, with higher weights for honest neighbours that are trusted, and lower weights for neighbours that are less trusted. Reputation systems have been previously used to cope with malicious behaviours [14]. In *ReDiSen*, nodes monitor behaviours of their neighbours and use such information to assign reputation values to them.

5.1.1 Updating Values Based on Value Differences

After the first round of exchanging the sensed energy values of the primary user, an honest node calculates the reputation of its neighbours based on their reported values and its own value. The calculation of reputation can be based on different methods. We use $R_{j,i}^{(VD)}$ to denote the reputation value of the transmitter i generated by the receiver j based on value differences. Then, all secondary users update their values and exchange their updated values with their neighbours as described in Algorithm 1. θ is a discount factor that is smaller than but close to 1 [59].

Algorithm 1 *ReDiSen*: Value Update Algorithm Based on Value Differences (Input: The sensed value of a node j and received values from j's neighbours. Output: The converged value)

```
A node $j$ individually senses the primary user energy at sensing session $T$
while $i$ is a neighbour of $j$ do
    Receive local measurements $V_{i,j}^{t}$
    Send local measurement $V_{j,i}^{t}$
    Calculate reputation $R_{j,i}^{(VD)}$
    while The converged value is not obtained do
        Update value:
            $V_j^{t+1} = V_j^t + \sum_{i=1}^{m_j+n_j+1} (1-\theta) R_{j,i}^{(VD)} (V_{i,j}^t - V_j^t) \quad (5.1)$
    end while
end while
```

In this algorithm, nodes only interact with their neighbouring nodes as Figure 5.1 illustrates.

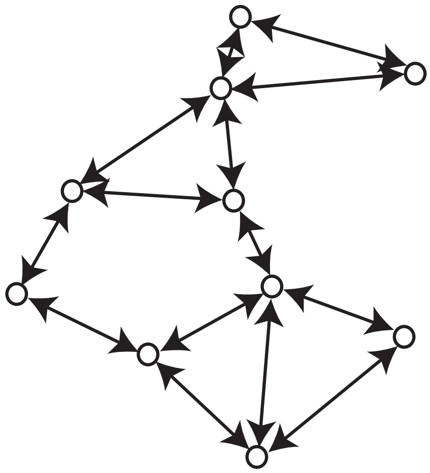


Figure 5.1: Secondary Users Only Exchange Values with Their Neighbours

When the updated value has no distinguishable difference from the previous update session, a converged value is obtained. To form a neighbourhood, nodes have to be situated within each others' communication range. However, the location privacy is protected since no exact location is reported to either a central authority or another node.

We explore general reputation requirements that are required for *ReDiSen* to produce better results than that of a reputation-less scheme. The reputation system for *ReDiSen* is *sound* if it outputs a higher value than the reputation-less scheme while the primary user is transmitting, and a lower value otherwise, assuming a subset of nodes report falsified values. The requirement can be formalized as Proposition 1.

Proposition 1. *Suppose an honest node j can assign reputation $R_{i_M}^{(VD)} < 1$ to a neighbour that reports falsified values, and $R_{i_N}^{(VD)} > 1$ to a neighbour that reports correct values. Then in* ReDiSen *j can update its value to the value V_j^{t+1} which, when compared to $\bar{V}_j^{t+1}$, the value from the system without reputation, is higher when the primary user is transmitting, and lower when the primary user is not transmitting.*

Proof. The value update scheme in the reputation-less scheme from the literature [59] has the same value update algorithm, except that in each value update session, the values are updated as:

$$\bar{V}_j^{t+1} = \bar{V}_j^t + \sum_{i=1}^{m_j+n_j+1} (1-\theta)(\bar{V}_{i,j}^t - \bar{V}_j^t), \tag{5.2}$$

with initial value $\bar{V}_j^0 = \bar{V}_j$ [3].

Note that since $V_{j,j}^t = V_j^t$, in the superscripts of this subsection, $m_j + n_j + 1$ is logically equal to $m_j + n_j$ in this scenario. For an honest node j, we denote with $R_{i_N}^{(VD)}$ the reputation of a neighbour i that reports a correct value, and with $R_{i_M}^{(VD)}$ the reputation of a node i that reports a falsified value. Hereby, the two value update schemes can be formulated as

$$V_j^{t+1} = V_j^t + (1-\theta)[\sum_{i=1}^{m_j} R_{i_M}^{(VD)}(V_{i,j}^t - V_j^t) + \sum_{i=m_j+1}^{m_j+n_j} R_{i_N}^{(VD)}(V_{i,j}^t - V_j^t)], \tag{5.3}$$

and

$$\bar{V}_j^{t+1} = \bar{V}_j^t + (1-\theta)[\sum_{i=1}^{m_j}(V_{i,j}^t - V_j^t) + \sum_{i=m_j+1}^{m_j+n_j}(V_{i,j}^t - V_j^t)]. \tag{5.4}$$

Therefore, the comparison between these methods is

$$V_j^{t+1} - \bar{V}_j^{t+1} = (1-\theta)[\sum_{i=1}^{m_j}(R_{i_M}^{(VD)} - 1)(V_{i,j}^t - V_j^t) + \sum_{i=m_j+1}^{m_j+n_j}(R_{i_N}^{(VD)} - 1)(V_{i,j}^t - V_j^t)] \tag{5.5}$$

An honest node j may sense correctly or falsely in a sensing session. However, it does not know whether its sensed value is correct or not.

If j senses correctly, $V_{i,j}^t \approx V_j^t$ for a neighbour i that also reports a correct value, $V_j^{t+1} - \bar{V}_j^{t+1} \approx \sum_{i=1}^{m_j}(R_{i_M}^{(VD)} - 1)(V_{i,j}^t - V_j^t)$. While the primary user is transmitting, we have $V_{i,j}^t < V_j^t$ for a neighbour i that reports a falsified value. So, as long as $\sum_{i=1}^{m_j}(R_{i_M}^{(VD)} - 1) < 0$ for an *SSDF* attack, we have $V_j^{t+1} > \bar{V}_j^{t+1}$, which indicates *ReDiSen* can help j obtain a higher value. While the primary user is not transmitting, $V_{i,j}^t > V_j^t$ for a neighbour i that reports a falsified value and so as long as $\sum_{i=1}^{m_j}(R_{i_M}^{(VD)} - 1) < 0$, we have $V_j^{t+1} < \bar{V}_j^{t+1}$, which indicates *ReDiSen* can help j obtain a lower value. Thus the first requirement, for the case when j senses correctly, is that $\sum_{i=1}^{m_j}(R_{i_M}^{(VD)} - 1) < 0$ for a neighbour i reporting a falsified value.

If j senses falsely, $V_{i,j}^t \approx V_j^t$ for a neighbour i that also reports a falsified value, $V_j^{t+1} - \bar{V}_j^{t+1} \approx \sum_{i=m_j+1}^{m_j+n_j}(R_{i_N}^{(VD)} - 1)(V_{i,j}^t - V_j^t)$. While the primary user is transmitting, for a neighbour i that reports a correct value, we have $V_{i,j}^t > V_j^t$. So, as long as $\sum_{i=m_j+1}^{m_j+n_j}(R_{i_N}^{(VD)} - 1) > 0$, we have $V_j^{t+1} > \bar{V}_j^{t+1}$. This indicates that *ReDiSen* can help j obtain a higher value. While the primary user is not transmitting, for a neighbour i that reports a correct value, we have $V_{i,j}^t < V_j^t$ and so as long as $\sum_{i=m_j+1}^{m_j+n_j}(R_{i_N}^{(VD)} - 1) > 0$, we have $V_j^{t+1} < \bar{V}_j^{t+1}$. This indicates *ReDiSen* can help j obtain a lower value. Thus the second requirement, for the case when j senses falsely, is that $\sum_{i=m_j+1}^{m_j+n_j}(R_{i_N}^{(VD)} - 1) > 0$ for a neighbour i that reports a correct value.

Note $V_j^{t+1} > \bar{V}_j^{t+1}$ indicates that the honest nodes obtain cooperative sensing results that are closer to the transmitting state of the primary user, and $V_j^{t+1} < \bar{V}_j^{t+1}$ indicates that the honest nodes obtain results that are closer to the non-transmitting state of the primary user. This means that under the above conditions, the requirements for reputation in *ReDiSen* are $R_{i_M}^{(VD)} < 1$ and $R_{i_N}^{(VD)} > 1$. □

A method for generating the desired reputation is introduced in Section 5.2.1.

5.1.2 Updating Values Based on Received Values

Instead of assigning reputation to the value differences, we can alternatively assign reputation to received values from neighbours directly. In this method, all nodes first implement individual sensing to obtain local measurements. Then they exchange values in the subsequent value update sessions. A straightforward method with no security assurance is to assign uniform weights as reputation to all neighbours. This method essentially calculates the average value of all nodes in the neighbourhood $\bar{V}_j^{t+1} = \sum_{i=1}^{m_j+n_j+1} \frac{1}{m_j+n_j+1} V_{i,j}^t$ as the cooperative sensing result. $V_{j,j}^t = V_j^t$ indicates the local measurement of node j itself. $R_{j,i}^{(RV)}$ denotes the reputation node j assigns to i based on received values. $R_{j,j}^{(RV)}$ denotes the weight node j assigns to itself.

We propose to use reputation in this process, too. After receiving the exchanged values from neighbours, an honest node can calculate the weighted combination of values from all neighbours as well as its own value, as described in Algorithm 2. Again, location privacy is protected in the algorithm.

Algorithm 2 *ReDiSen*: Value Update Algorithm based on Received Values (Input: The sensed value of a node j and received values from j's neighbours. Output: The converged value)

```
A node $j$ individually senses the primary user energy at sensing session $T$
while $i$ is a neighbour of $j$ do
    Receive local measurements $V_{i,j}^t$
    Send local measurement $V_{j,i}^t$
    Calculate weight $R_{j,i}^{(RV)}$
    while The converged value is not obtained do
        Update value as
            $$V_j^{t+1} = \sum_{i=1}^{m_j+n_j+1} R_{j,i}^{(RV)} V_{i,j}^t \qquad (5.6)$$
    end while
end while
```

The requirement for the reputation can be formalized as Proposition 2.

Proposition 2. *Higher weights to correctly reported values and lower weights to falsely reported values can help an honest node j obtain a cooperative sensing result that is closer to the real state of the primary user.*

Proof. After receiving the exchanged values from neighbours, an honest node can assign different weights as reputation values based on the received values to improve the cooperative sensing performance, rather than simply averaging them. Compared with the uniform weight method

$$\bar{V}_j^{t+1} = \sum_{i=1}^{m_j+n_j+1} R_{j,i}^{(RV)} V_{i,j}^t = \sum_{i=1}^{m_j+n_j+1} \frac{1}{m_j+n_j+1} V_{i,j}^t, \tag{5.7}$$

we require a lower weight $R_{j,k}^{(RV)} < \frac{1}{m_j+n_j+1}$ to be assigned to a node k if $V_{k,j}^t$ is a falsified value; and a higher weight $R_{j,l}^{(RV)} > \frac{1}{m_j+n_j+1}$ to be assigned to a node l if $V_{l,j}^t$ is a correct value. Then, the updated value V_j^{t+1} based on the differentiated weights $V_j^{t+1} > \bar{V}_j^{t+1}$ when the primary user is transmitting, $V_j^{t+1} < \bar{V}_j^{t+1}$ when the primary user is not transmitting. □

We will compare these two methods of assigning reputation on value differences and received values in the simulation. A method for generating the desired reputation is introduced in Section 5.2.2.

5.2 Generating Reputation

5.2.1 Generating Reputation Based on Value Differences

Reputation values in *ReDiSen* are generated once for each sensing session as follows:

$$R_{j,i}^{(VD)} = 2 - \frac{|V_{i,j} - \tilde{V}_j|}{\frac{\sum_{l=1}^{m_j+n_j+1} |V_{l,j} - \tilde{V}_j|}{m_j+n_j+1}} = 2 - \frac{(m_j+n_j+1)|V_{i,j} - \tilde{V}_j|}{\sum_{l=1}^{m_j+n_j+1} |V_{l,j} - \tilde{V}_j|}, \tag{5.8}$$

where $\tilde{V}_j = \frac{\sum_{l=1}^{m_j+n_j+1} V_{l,j}}{m_j+n_j+1}$ is the average value of all the nodes in the neighbourhood. We can observe that $0 \leq R_{j,i}^{(VD)} \leq 2$.

If the majority of the neighbourhood reports correctly sensed values, we can use the average value of all the nodes in the neighbourhood $\tilde{V}_j^t$ to improve the uniform method. In this case, the correct reported values are closer to the average value than the falsified values are. Hereby, we can define the average difference of all nodes in the neighbourhood

$$A_j = \frac{\sum_{l=1}^{m_j+n_j+1} |V_{l,j}^t - \tilde{V}_j^t|}{m_j+n_j+1}. \tag{5.9}$$

As long as there are more neighbours that report correct values, the distance from the value of a node that senses correctly to the average value will be smaller than the average distance to the average value, and *vice versa.* This intuition leads to Theorem 1:

Theorem 1. *Equation (5.8) assigns reputation* $0 < R_{i_M} < 1$ *for a neighbour that reports falsified values, and* $R_{i_N} > 1$ *for a neighbour that reports correct values, which will help honest nodes obtain better cooperative sensing results than the reputation-less scheme, assuming that the majority of neighbours are either correctly sensing honest nodes or non-attacking malicious nodes.*

Proof. For a neighbour that reports falsified values, the distance to the average value is larger than the average distance from the average value: $|V_{i,j} - \tilde{V_j}| > \frac{\sum_{l=1}^{m_j+n_j+1} |V_{l,j} - \tilde{V_j}|}{m_j+n_j+1}$. Since both $m_j + n_j + 1 > 0$ and $\sum_{l=1}^{m_j+n_j+1} |V_{l,j} - \tilde{V_j}| > 0$, we can derive $\frac{(m_j+n_j+1)|V_{i,j}-\tilde{V_j}|}{\sum_{l=1}^{m_j+n_j+1} |V_{l,j}-\tilde{V_j}|} > 1$, which is equivalent to $2 - \frac{(m_j+n_j+1)|V_{i,j}-\tilde{V_j}|}{\sum_{l=1}^{m_j+n_j+1} |V_{l,j}-\tilde{V_j}|} < 1$. According to (5.8), we have $0 < R_{i_M}^{(VD)} < 1$.

For a neighbour that reports correct values, the distance to the average value is smaller than the average distance from the average value. $|V_{i,j} - \tilde{V_j}| < \frac{\sum_{l=1}^{m_j+n_j+1} |V_{l,j} - \tilde{V_j}|}{m_j+n_j+1}$. Since both $m_j + n_j + 1 > 0$ and $\sum_{l=1}^{m_j+n_j+1} |V_{l,j} - \tilde{V_j}| > 0$, we can derive $\frac{(m_j+n_j+1)|V_{i,j}-\tilde{V_j}|}{\sum_{l=1}^{m_j+n_j+1} |V_{l,j}-\tilde{V_j}|} < 1$, which is equivalent to $2 - \frac{(m_j+n_j+1)|V_{i,j}-\tilde{V_j}|}{\sum_{l=1}^{m_j+n_j+1} |V_{l,j}-\tilde{V_j}|} > 1$. According to (5.8), we have $R_{i_N}^{(VD)} > 1$.

These two cases can justify that the proposed reputation-generating method in (5.8) enables honest nodes assign $0 < R_{i_M}^{(VD)} < 1$ for neighbours that report falsified values, $R_{i_N}^{(VD)} > 1$ for neighbours that report correct values. According to Proposition 1, (5.8) can help honest nodes obtain better cooperative sensing results than the reputation-less scheme. □

If an honest node suffers from severe fading, then the value it transmits always indicates that the primary user is not transmitting. Thus, its reputation value is lower since its behaviour is similar to that of the malicious nodes when the primary user is transmitting. However, the honest node can move to other locations to rebuild its reputation.

5.2.2 Generating Reputation Based on Received Values

If the difference between the reported value of a neighbour i and the average value is lower than the average difference ($|V_{i,j}^t - \tilde{V}_j^t| < A_j$), then i is recognized as reporting a correct value, and is thus assigned a higher weight than $\frac{1}{m_j+n_j+1}$. If the difference between the reported value of a neighbour i and the average value is higher than the average difference ($|V_{i,j}^t - \tilde{V}_j^t| > A_j$), then i is perceived as reporting a falsified value, and is thus assigned a lower weight than $\frac{1}{m_j+n_j+1}$. We can normalize $1 - \frac{|V_{i,j}^t - \tilde{V}_j^t|}{\sum_{l=1}^{m_j+n_j+1} |V_{l,j}^t - \tilde{V}_j^t|}$ to calculate the weights that can meet the requirements in Proposition 2.

The improved method for a node to assign different weights as reputation can be described as:

$$R_{j,i}^{(RV)} = \frac{1 - \frac{|V_{i,j}^t - \tilde{V}_j^t|}{\sum_{l=1}^{m_j+n_j+1} |V_{l,j}^t - \tilde{V}_j^t|}}{\sum_{k=1}^{m_j+n_j+1}(1 - \frac{|V_{i,j}^t - \tilde{V}_j^t|}{\sum_{l=1}^{m_j+n_j+1} |V_{l,j}^t - \tilde{V}_j^t|})} = \frac{1 - \frac{|V_{i,j}^t - \tilde{V}_j^t|}{\sum_{l=1}^{m_j+n_j+1} |V_{l,j}^t - \tilde{V}_j^t|}}{(m_j+n_j+1) - \sum_{k=1}^{m_j+n_j+1}(\frac{|V_{i,j}^t - \tilde{V}_j^t|}{\sum_{l=1}^{m_j+n_j+1} |V_{l,j}^t - \tilde{V}_j^t|})}$$
$$= \frac{1 - \frac{|V_{i,j}^t - \tilde{V}_j^t|}{\sum_{l=1}^{m_j+n_j+1} |V_{l,j}^t - \tilde{V}_j^t|}}{(m_j+n_j+1) - \frac{\sum_{l=1}^{m_j+n_j+1} |V_{l,j}^t - \tilde{V}_j^t|}{\sum_{l=1}^{m_j+n_j+1} |V_{l,j}^t - \tilde{V}_j^t|}} = \frac{1 - \frac{|V_{i,j}^t - \tilde{V}_j^t|}{\sum_{l=1}^{m_j+n_j+1} |V_{l,j}^t - \tilde{V}_j^t|}}{m_j+n_j} \tag{5.10}$$

These two cases indicate that as long as a node reports a value that has a smaller difference from the average value than the average difference A_j, it is assigned a higher weight. If a node reports a value that has a larger difference from the average value than the average difference A_j, it is assigned a lower weight. This result leads to Theorem 2:

Theorem 2. *Using weights generated in equation (5.10) as reputation can help honest nodes obtain better cooperative sensing results than the reputation-less scheme, given the condition that the majority of neighbours are either correctly sensing honest nodes or non-attacking malicious nodes.*

Proof. To evaluate the improved weight assigning method (5.10) with the uniform weight method, we calculate the difference between the weights calculated from two methods:

$$\begin{aligned} R^{(\bar{RV})}{}_{j,i} - R^{(RV)}_{j,i} &= \frac{1}{m_j+n_j+1} - \frac{1-\frac{|V^t_{i,j}-\tilde{V}^t_j|}{\sum_{l=1}^{m_j+n_j+1}|V^t_{l,j}-\tilde{V}^t_j|}}{m_j+n_j} \\ = \frac{(m_j+n_j)-(m_j+n_j+1)+\frac{(m_j+n_j+1)|V^t_{i,j}-\tilde{V}^t_j|}{\sum_{l=1}^{m_j+n_j+1}|V^t_{l,j}-\tilde{V}^t_j|}}{(m_j+n_j+1)(m_j+n_j)} &= \frac{(m_j+n_j+1)\frac{|V^t_{i,j}-\tilde{V}^t_j|}{\sum_{l=1}^{m_j+n_j+1}|V^t_{l,j}-\tilde{V}^t_j|}-1}{(m_j+n_j+1)(m_j+n_j)} \end{aligned} \tag{5.11}$$

Since $(m_j+n_j+1)(m_j+n_j) > 0$, we can derive:

$$\begin{aligned} &R^{(\bar{RV})}{}_{j,i} < R^{(RV)}_{j,i} \Leftrightarrow R^{(\bar{RV})}{}_{j,i} - R^{(RV)}_{j,i} < 0 \Leftrightarrow (m_j+n_j+1)\frac{|V^t_{i,j}-\tilde{V}^t_j|}{\sum_{l=1}^{m_j+n_j+1}|V^t_{l,j}-\tilde{V}^t_j|} < 1 \\ &\Leftrightarrow (m_j+n_j+1)|V^t_{i,j}-\tilde{V}^t_j| < \sum_{i=1}^{m_j+n_j+1}|V^t_{i,j}-\tilde{V}^t_j| \Leftrightarrow |V^t_{i,j}-\tilde{V}^t_j| < \frac{\sum_{l=1}^{m_j+n_j+1}|V^t_{l,j}-\tilde{V}^t_j|}{m_j+n_j+1} \end{aligned} \tag{5.12}$$

which is $|V^t_{i,j}-\tilde{V}^t_j| < A_j$ according to the definition of A_j in (5.9), and

$$\begin{aligned} &R^{(\bar{RV})}{}_{j,i} > R^{(RV)}_{j,i} \Leftrightarrow R^{(\bar{RV})}{}_{j,i} - R^{(RV)}_{j,i} > 0 \Leftrightarrow (m_j+n_j+1)\frac{|V^t_{i,j}-\tilde{V}^t_j|}{\sum_{l=1}^{m_j+n_j+1}|V^t_{l,j}-\tilde{V}^t_j|} > 1 \\ &\Leftrightarrow (m_j+n_j+1)|V^t_{i,j}-\tilde{V}^t_j| > \sum_{i=1}^{m_j+n_j+1}|V^t_{i,j}-\tilde{V}^t_j| \Leftrightarrow |V^t_{i,j}-\tilde{V}^t_j| > \frac{\sum_{l=1}^{m_j+n_j+1}|V^t_{l,j}-\tilde{V}^t_j|}{m_j+n_j+1} \end{aligned} \tag{5.13}$$

which is $|V^t_{i,j}-\tilde{V}^t_j| > A_j$ according to the definition of A_j in (5.9).

According to Proposition 2, (5.10) can help honest nodes obtain better cooperative sensing results than the reputation-less scheme does.

□

In the above discussions on the improved weight assigning method based with the reputation generated as (5.10), we take an honest node j itself into consideration. If the values of j itself is removed from the process when generating reputation, the majority rule needs to be elevated by adding one extra honest node into the system.

5.3 Reputation Update Process

Our discussion so far has been focused on comparison within a single sensing session. The calculations and comparisons all happen in one sensing session and restart in the next sensing session. However, a realistic cognitive radio network is dynamic. The nodes, both honest and malicious, may move to different locations in different sensing sessions. Their neighbourhood can be different in different sensing sessions. In some sensing sessions, the majority of the neighbourhood may not be dominated by nodes that report correct values.

We can extend the previous method based on value differences to a reputation update process, which can reflect the behaviour changes of the neighbours. The reputation update process can be designed as:

$$\begin{aligned} R_{j,i}^{(VD)T} &= \delta R_{j,i}^{(VD)T-1} + (1-\delta)(2 - \frac{|V_{i,j}^{T-1} - \tilde{V}_j^{T-1}|}{A_j^T}) \\ &= \delta R_{j,i}^{(VD)T-1} + (1-\delta)(2 - \frac{(m_j+n_j+1)|V_{i,j}^{T-1} - \tilde{V}_j^{T-1}|}{\sum_{i=1}^{m_j+n_j+1}|V_{i,j}^{T-1} - \tilde{V}_j^{T-1}|}), \end{aligned} \tag{5.14}$$

with initial value $R_{j,i}^{(VD)0} = 2 - \frac{|V_{i,j}^0 - \tilde{V}_j^0|}{\frac{\sum_{i=1}^{m_j+n_j+1}|V_{i,j}^0 - \tilde{V}_j^0|}{m_j+n_j+1}} = 2 - \frac{(m_j+n_j+1)|V_{i,j}^0 - \tilde{V}_j^0|}{\sum_{i=1}^{m_j+n_j+1}|V_{i,j}^0 - \tilde{V}_j^0|}$, where δ is a discount factor of previous reputation values in $(0,1)$. We can observe that $0 \leq R_{j,i}^{(VD)} \leq 2$.

We can derive the value of $R_{j,i}^{(VD)T}$ as

$$\begin{aligned} &R_{j,i}^{(VD)T} = (\delta)^T(2 - \frac{(m_j+n_j+1)|V_{i,j}^0 - \tilde{V}_j^0|}{\sum_{i=1}^{m_j+n_j+1}|V_{i,j}^0 - \tilde{V}_j^0|}) + (\delta)^{T-1}(1-\delta)(2 - \frac{(m_j+n_j+1)|V_{i,j}^1 - \tilde{V}_j^1|}{\sum_{i=1}^{m_j+n_j+1}|V_{i,j}^1 - \tilde{V}_j^1|}) \\ &+ \cdots + \delta(1-\delta)(2 - \frac{(m_j+n_j+1)|V_{i,j}^{T-2} - \tilde{V}_j^{T-2}|}{\sum_{i=1}^{m_j+n_j+1}|V_{i,j}^{T-2} - \tilde{V}_j^{T-2}|}) \\ &+(1-\delta)(2 - \frac{(m_j+n_j+1)|V_{i,j}^{T-1} - \tilde{V}_j^{T-1}|}{\sum_{i=1}^{m_j+n_j+1}|V_{i,j}^{T-1} - \tilde{V}_j^{T-1}|}) \\ &= 2 - (\delta)^T \frac{(m_j+n_j+1)|V_{i,j}^0 - \tilde{V}_j^0|}{\sum_{i=1}^{m_j+n_j+1}|V_{i,j}^0 - \tilde{V}_j^0|} - (\delta)^{T-1}(1-\delta)\frac{(m_j+n_j+1)|V_{i,j}^1 - \tilde{V}_j^1|}{\sum_{i=1}^{m_j+n_j+1}|V_{i,j}^1 - \tilde{V}_j^1|} \\ &- \cdots - \delta(1-\delta)\frac{(m_j+n_j+1)|V_{i,j}^{T-2} - \tilde{V}_j^{T-2}|}{\sum_{i=1}^{m_j+n_j+1}|V_{i,j}^{T-2} - \tilde{V}_j^{T-2}|} - (1-\delta)\frac{(m_j+n_j+1)|V_{i,j}^{T-1} - \tilde{V}_j^{T-1}|}{\sum_{i=1}^{m_j+n_j+1}|V_{i,j}^{T-1} - \tilde{V}_j^{T-1}|} \\ &= 2 - (\delta)^T \frac{|V_{i,j}^0 - \tilde{V}_j^0|}{A_j^0} - (\delta)^{T-1}(1-\delta)\frac{|V_{i,j}^1 - \tilde{V}_j^1|}{A_j^1} \\ &- \cdots - \delta(1-\delta)\frac{|V_{i,j}^{T-2} - \tilde{V}_j^{T-2}|}{A_j^{T-2}} - (1-\delta)\frac{|V_{i,j}^{T-1} - \tilde{V}_j^{T-1}|}{A_j^{T-1}} \end{aligned} \tag{5.15}$$

Recall that the reputation requirement is $0 < R_{i_M}^{(VD)} < 1$ for neighbours that report falsified values, and $R_{i_N}^{(VD)} > 1$ for neighbours that report correct values. For the updated reputation $R_{j,i}^{(VD)T}$ in sensing session T, this requirement turns to be $(\delta)^T \frac{|V_{i,j}^0 - \tilde{V}_j^0|}{A_j^0} - (\delta)^{T-1}(1-$

$\delta)\frac{|V_{i,j}^{1}-\tilde{V}_{j}^{1}|}{A_{j}^{1}}-\cdots-\delta(1-\delta)\frac{|V_{i,j}^{T-2}-\tilde{V}_{j}^{T-2}|}{A_{j}^{T-2}}-(1-\delta)\frac{|V_{i,j}^{T-1}-\tilde{V}_{j}^{T-1}|}{A_{j}^{T-1}} > 1$ for neighbours that report falsified values, and $(\delta)^{T}\frac{|V_{i,j}^{0}-\tilde{V}_{j}^{0}|}{A_{j}^{0}}-(\delta)^{T-1}(1-\delta)\frac{|V_{i,j}^{1}-\tilde{V}_{j}^{1}|}{A_{j}^{1}}-\cdots-\delta(1-\delta)\frac{|V_{i,j}^{T-2}-\tilde{V}_{j}^{T-2}|}{A_{j}^{T-2}}-(1-\delta)\frac{|V_{i,j}^{T-1}-\tilde{V}_{j}^{T-1}|}{A_{j}^{T-1}} < 1$ for neighbours that report correct values. This requirement can be met probabilistically based on $\frac{|V_{i,j}^{T}-\tilde{V}_{j}^{T}|}{A_{j}^{T}}$ and the value of δ.

For the neighbours of node j, $\frac{|V_{i,j}^{T}-\tilde{V}_{j}^{T}|}{A_{j}^{T}} < 1$ when there are more neighbours that report correct values; $\frac{|V_{i,j}^{T}-\tilde{V}_{j}^{T}|}{A_{j}^{T}} > 1$ when there are more neighbours that report falsified values. For neighbours that report falsified values, $\frac{|V_{i,j}^{T}-\tilde{V}_{j}^{1}|}{A_{j}^{T}} > 1$ when there are more neighbours that report correct values; $\frac{|V_{i,j}^{T}-\tilde{V}_{j}^{T}|}{A_{j}^{T}} < 1$ when there are more neighbours that report falsified values. To improve the cooperative sensing performance, by assigning higher reputation to nodes that report correct values and lower reputation to nodes that report falsified values, a good node j wishes to be in a neighbourhood that has a larger fraction of neighbours reporting correct values.

To discuss the impact of δ, let us first examine the relations between different factors in different sensing sessions. It is easy to observe that $(\delta)^{T-1}(1-\delta) < (\delta)^{T-2}(1-\delta) < \cdots < \delta(1-\delta) < (1-\delta)$. So the most recent observation is more important than the previous ones, starting from the second sensing session. To compare the discount factor $(\delta)^{T}$ for the first sensing session with the factors of other sensing sessions, we can solve the inequalities $(\delta)^{T} > (\delta)^{T-\mathcal{T}}(1-\delta) \Leftrightarrow \mathcal{T} < \log_{\delta}(1-\delta)$, and $(\delta)^{T} < (\delta)^{T-\mathcal{T}}(1-\delta) \Leftrightarrow \mathcal{T} > \log_{\delta}(1-\delta)$. The results indicate: the higher $\log_{\delta}(1-\delta)$ is, the more important the first sensing session is for a node j to assign reputation to the neighbours in the future sensing sessions.

For the method of assigning reputation to received values, the results and discussions about the reputation update process are similar, and are omitted.

5.4 Performance Evaluation

5.4.1 Simulation Objective and Outline

We perform simulation studies in *Matlab* to examine whether *ReDiSen* converges to better sensed values at secondary users, compared to reputation-less schemes, *i.e.*, the honest nodes should update to higher values while the primary user is transmitting, and *vice versa*.

In our simulations, E_0 is $80dBm$, which is the typical transmission power of a FM radio station. The transmission power is attenuated while arriving at secondary users. We consider the reference distance d_0 as $1m$. If the primary user is not transmitting, the secondary users can only sense the thermal noise floor $-111dBm$. Each secondary user has the same capacity to communicate with other secondary users in the proximity. We simulate a network of secondary users in the area of $1km \times 1km$.

In the following figures, solid lines indicate the updated value or average updated value of honest secondary users in *ReDiSen*. Dashed lines indicate the updated values or average updated value in the reputation-less scheme. When the results from these two schemes are the same, we use dotted line to illustrate the indistinguishable values.

5.4.2 Value Update Process

We first simulate the value update process for the method of assigning reputation to the value differences. We simulate the scenarios where a primary user is located at (a) $5km$ away; (b) $2.5km$ away from the centre of the secondary user network. The communication range of a secondary user is $750m$. In Figures 5.2 and 5.3, the malicious nodes implement the *Always Attack* strategy. Honest nodes implement *ReDiSen* with reputation values generated from the average value of neighbours. The final outputs are the updated values in the two equations (5.1) and (5.2) with the reputation generated as the equation (5.8) after 150 value update rounds. There are 7 honest secondary users in a CRN of 10 secondary users. We assume that all honest nodes report correct values in the simulation process. The standard deviation for shadow fading σ is $3dB$. θ is 0.995.

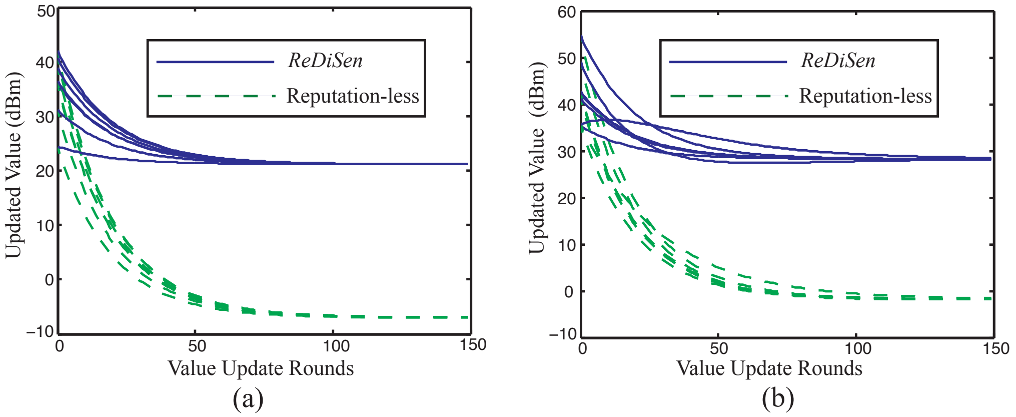


Figure 5.2: Value Update Process when Honest Nodes Assign Reputation to the Value Differences. The Primary User is Transmitting and Located (a) 5 km, (b) 2.5 km Away from the Secondary User Network.

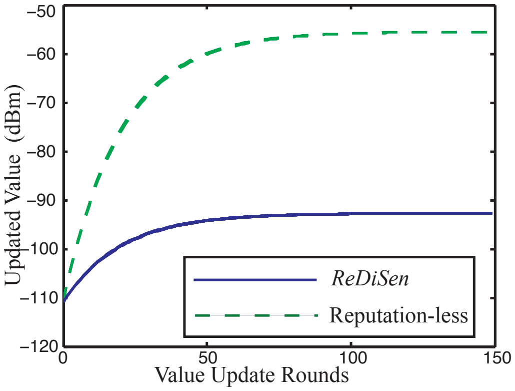
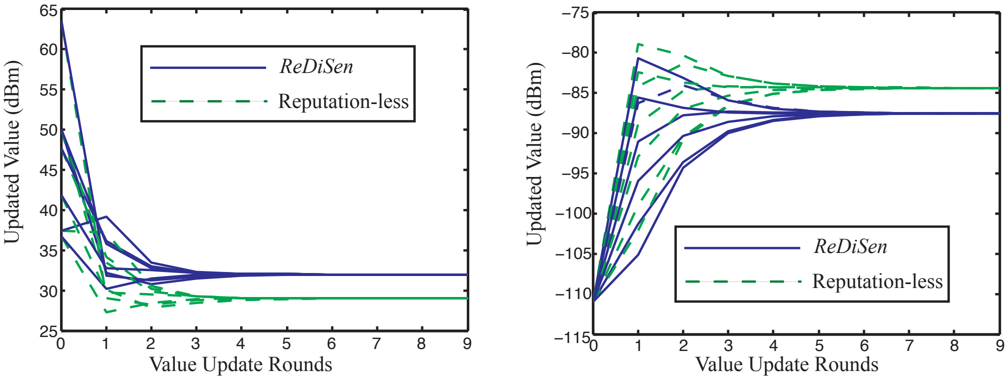


Figure 5.3: Value Update Process when Honest Nodes Assign Reputation to the Value Differences. The Primary User is Not Transmitting. The Malicious Nodes Implement the *Always Attack* Strategy.

While the primary user is transmitting, the honest nodes obtain higher updated values (approximately $30dBm$) than in the reputation-less scheme. While the primary user is not transmitting, the honest nodes obtain lower updated values (approximately $37dBm$) than in the reputation-less scheme. Since honest nodes all start from the same noise floor, their value update processes are close to each other, which makes the lines almost overlapping. Both scenarios indicate that *ReDiSen* can achieve better cooperative sensing results compared to the reputation-less scheme. The updated values of honest nodes converge to a value that is closer to the truthful state of the primary user than the converged value in the reputation-less scheme.

We next simulate the value update process for assigning reputation to the received values with the same parameters. The primary user is located $5km$ away. Figure 5.4 illustrates the value update process. The final outputs are the updated values in equation (5.6) with reputation generated with uniform weight and equation (5.10). While the primary user is transmitting, honest nodes obtain higher updated values (approximately $4dBm$) than the reputation-less scheme. While the primary user is not transmitting, the honest nodes obtain lower updated values (approximately $4dBm$) than the reputation-less scheme. Figure 5.4 justifies that applying differentiated weights to the received values can help the honest nodes arrive at better cooperative sensing results. The effects are not as significant as the method of assigning reputation to the value differences.



(a)

(b)

Figure 5.4: Value Update Process when the Honest Nodes Assign Reputation to the Received Values. The Primary User is (a) Transmitting, (b) Not Transmitting.

We also simulate *Camouflaged Attack* scenario where there is light shadow fading $\sigma = 1dB$. Since honest nodes are aware of the light fading environment, they can easily identify irrational values received from neighbours. Consequently, the malicious nodes are more likely to adopt the *Camouflaged Attack* strategy. The malicious nodes instead report attenuated primary user signal strength while the primary user is not transmitting.

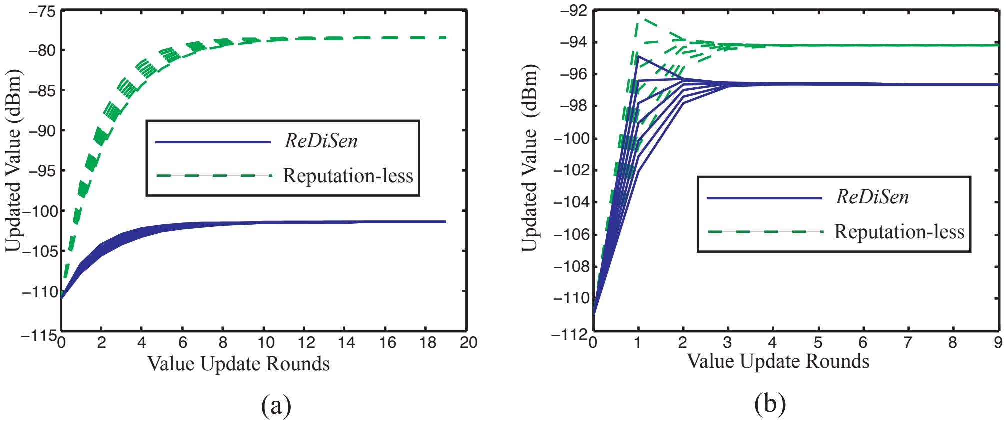


Figure 5.5: Value Update Process when the Honest Nodes Assign Reputation to (a) Value Differences, (b) Received Values. The Primary User is Not Transmitting. Malicious Nodes Implement the *Camouflaged Attack* Strategy.

Figure 5.5 illustrates the value update process. Honest nodes output lower updated values (approximately $35dBm$ when the honest nodes assign reputation to value differences, $2dBm$ when the honest nodes assign reputation to received values) than the reputation-less scheme. Figure 5.5 justifies that applying differentiated weights as reputation to the received values can help honest nodes obtain better cooperative sensing results. The camouflaged attacks are less effective for the adversary since honest nodes can achieve lower values when the primary user is not transmitting.

Figures 5.2 - 5.5 together suggest that using reputation can help honest nodes obtain higher cooperative sensing results when the primary user is transmitting, lower cooperative sensing results when the primary user is not transmitting, in both methods of assigning reputation on value differences and received values, with different distances from the primary user, as long as the majority of neighbours report correctly sensed values. Assigning reputation to received values is less effective compared to assigning reputation to value differences, since the improvements are less significant. However, assigning reputation to received values can help honest nodes converge to a decision much faster.

We next discuss the impact of the percentage of malicious nodes, density of nodes and communication range in Section 5.4.3, 5.4.4, and 5.4.5.

5.4.3 Percentage of Malicious Nodes

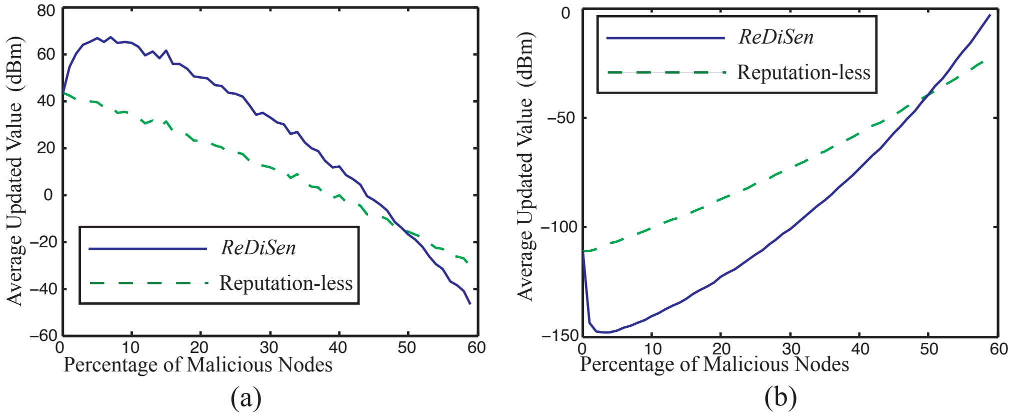


Figure 5.6: Average Updated Values in the *Always Attack* Strategy.

Figure 5.6 uses the average value of all honest nodes as the indicator of performance in *Aways Attack*. We average the values of all honest nodes to compare with the convergence values in the reputation-less scheme. We simulate the impact of the malicious node percentage in a network of 100 nodes. The standard deviation for fading and shadowing σ is $3dB$. If the secondary users are deployed uniformly in a grid model, each secondary user occupies a cell of $100m \times 100m$. The primary user is located $5km$ away. The communication range of a secondary user is $750m$. Figure 5.6(a) illustrates the comparisons of *ReDiSen* and the reputation-less scheme while the primary user is transmitting. As long as the adversary corrupts less than 49% of the whole CRN, *ReDiSen* can obtain better (higher) average values than the reputation-less scheme. Figure 5.6(b) illustrates the comparisons while the primary user is not transmitting. *ReDiSen* can obtain better (lower) average values than the reputation-less scheme with less than 49% malicious nodes. Note that when the percentage of malicious nodes is low, the system generates higher reputation values (closer to 2) for the honest neighbours who report correct sensed value -111 dBm, which makes the average updated value even lower than -111 dBm.

Malicious nodes can attack in all sensing sessions by reporting falsified values. They can also implement the *Random Attack* strategy or the *Intermittent Attack* strategy. For the *Intermittent Attack* strategy, we simulate the scenario where the malicious nodes attack with 67% intensity. Figure 5.7 and Figure 5.8 illustrate the simulation results in the *Random Attack* and *Intermittent Attacks* strategies. The primary user is also located $5km$ away.

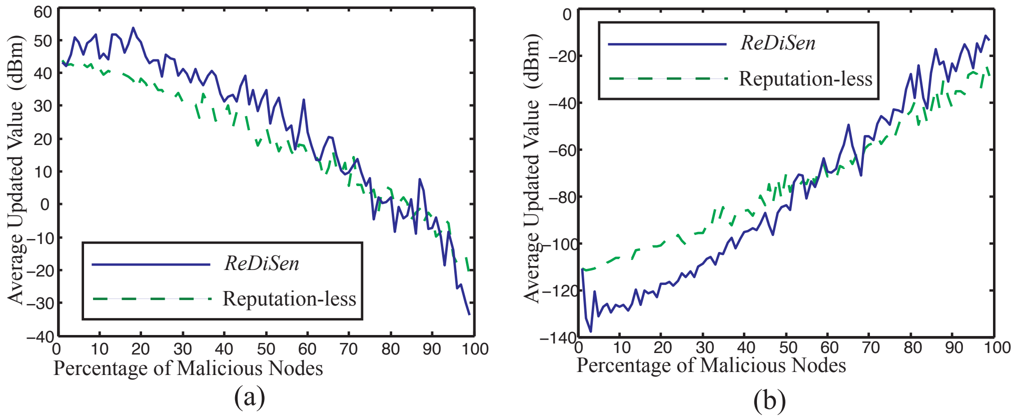


Figure 5.7: Average Updated Values in the *Random Attack* Strategy.

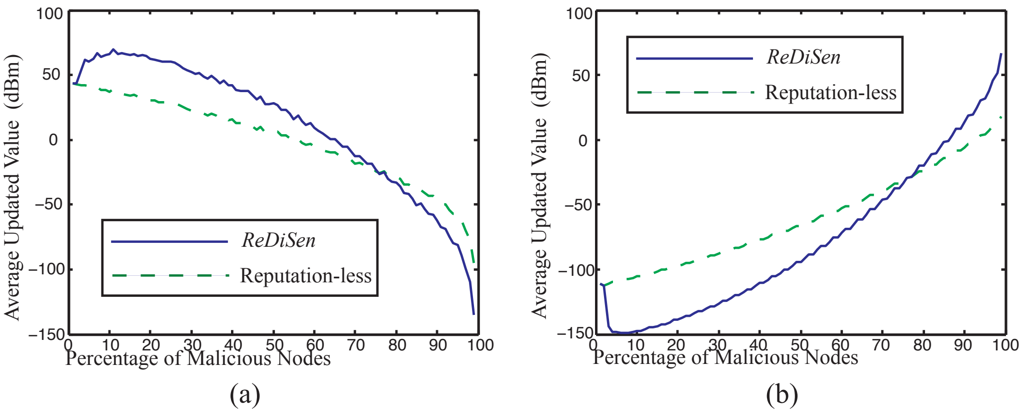


Figure 5.8: Average Updated Values in the *Intermittent Attack* Strategy with 67% Intensity.

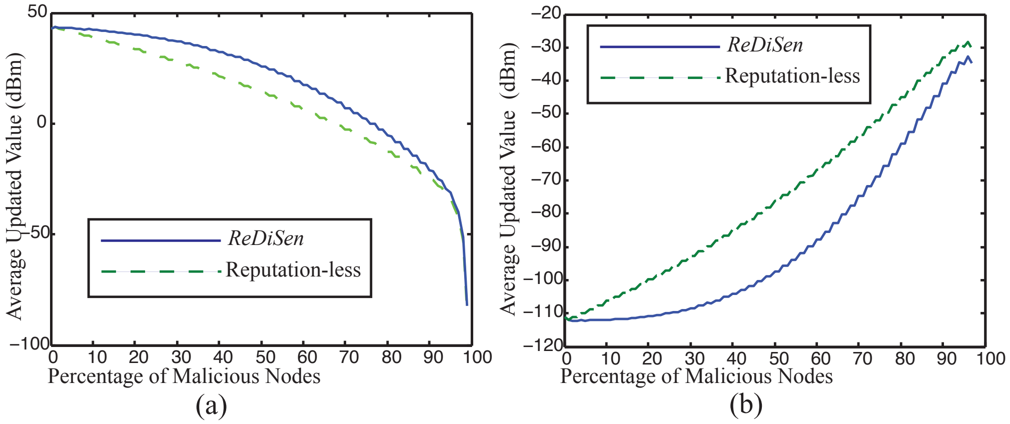


Figure 5.9: Average Updated Values in the *Intermittent Attack* Strategy with 50% Intensity.

We simulate the differences between *ReDiSen* and the reputation-less scheme in the *Random Attack* strategy and *Intermittent Attack* strategy, as illustrated in Figure 5.7, 5.8, and 5.9. A malicious node randomly chooses a number between $-111dBm$ to $80dBm$ to report. The simulation results indicate that: no matter whether the primary user is transmitting or not, *ReDiSen* is better than the reputation-less scheme by updating the values of the honest nodes closer to the truthful state of the primary user even when there are 68% malicious nodes. Figure 5.8 illustrates the effect in the *Intermittent Attack* strategy with 67% attack intensity, which can tolerate up to 75% malicious nodes. Figure 5.9 illustrates the effect in the *Intermittent Attack* strategy with 50% attack intensity, which can tolerate up to 95% malicious nodes.

Figure 5.6, Figure 5.7, Figure 5.8, and Figure 5.9 together verify that *ReDiSen* can obtain better cooperative sensing results under different attack strategies. We observe that the *Always Attack* strategy is the most effective strategy for the malicious nodes. This is because the malicious nodes may behave as the honest nodes in some sessions in the *Random Attack* strategy or the *Intermittent Attack* strategy.

5.4.4 Density of Nodes

We examine the effect of network density in Figure 5.10. Compared to Section 5.4.2, we simulate 70 honest secondary users in a CRN of 100 secondary users. The primary user is located $5km$ away. With the other parameters remaining intact, we can observe that the honest nodes have similar cooperative sensing results in different densities of networks under attacks from the same percentage of malicious nodes of Figure 5.2(a). The honest nodes can still obtain higher updated values (approximately $30dBm$) than the reputation-less scheme.

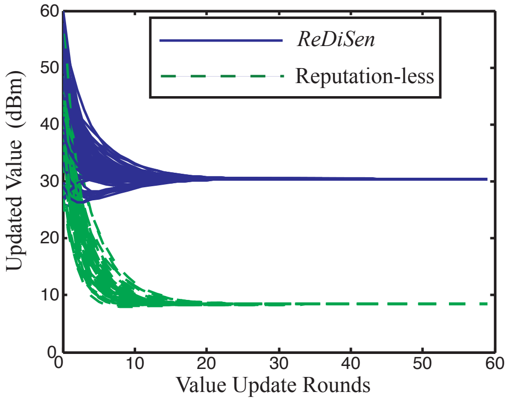


Figure 5.10: Value Update Process when the Honest Nodes Assign Reputation to the Value Differences.

5.4.5 Communication Range

We then study the impact of the communication range of a secondary user. The communication range plays an important role regarding the connections between secondary users. A higher communication range incurs a higher connectivity for the secondary user network, which will eventually help secondary users receive more assistances from other honest users. In a network where connectivity is low, convergence may not even happen, since some honest nodes may be isolated from other honest nodes because they are surrounded by many malicious neighbours. In this situation, there are multiple networks rather than only one network in the whole system. Compared to Section 5.4.2, we simulate a network with the communication range of a secondary user as $250m$ and $500m$. The primary user is transmitting.

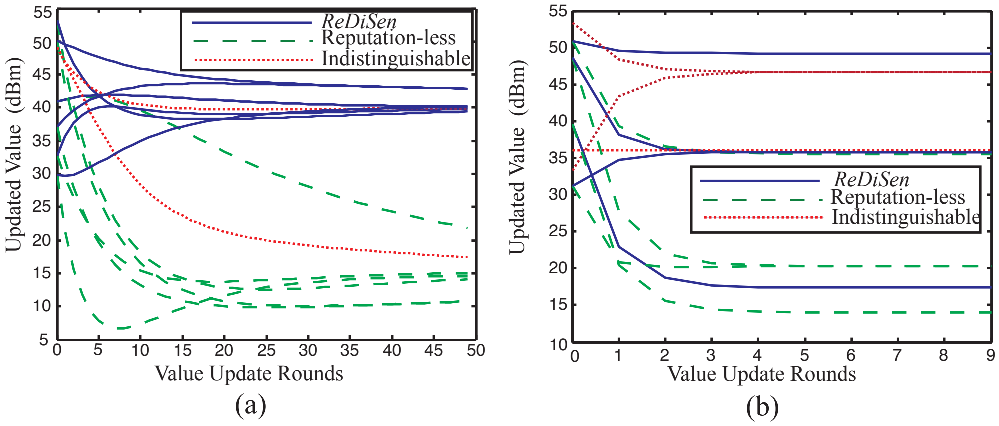


Figure 5.11: Value Update Process when the Honest Nodes Assign Reputation to (a) Value Differences, (b) Received Values. The Primary User is Transmitting. The Malicious Nodes Implement the *Random Attack* Strategy. The Communication Range of a Secondary User is 250 m. There is No Convergence in Either Case.

Figure 5.11 illustrates the value update process when the the communication range of a secondary user is $250m$, which reduces the chances for the secondary users to communicate. There is no converged value for honest nodes in either case of assigning reputation on received values or value differences. Figure 5.12 illustrates the value update process when the communication range is $500m$. There is no converged value for honest nodes when assigning reputation to received values. Convergence does happen when assigning reputation to value differences. No matter whether convergence is achieved, *ReDiSen* can help honest nodes obtain higher cooperative sensing results than the reputation-less scheme.

From the simulation results in Figure 5.11 and Figure 5.12, we can observe that assigning reputation to the received values can help honest nodes arrive at convergence faster than assigning reputation to the value differences, if convergence is possible at all. When secondary users have a smaller communication range, convergence may not happen. There is a higher probability that assigning reputation to value differences can help honest nodes

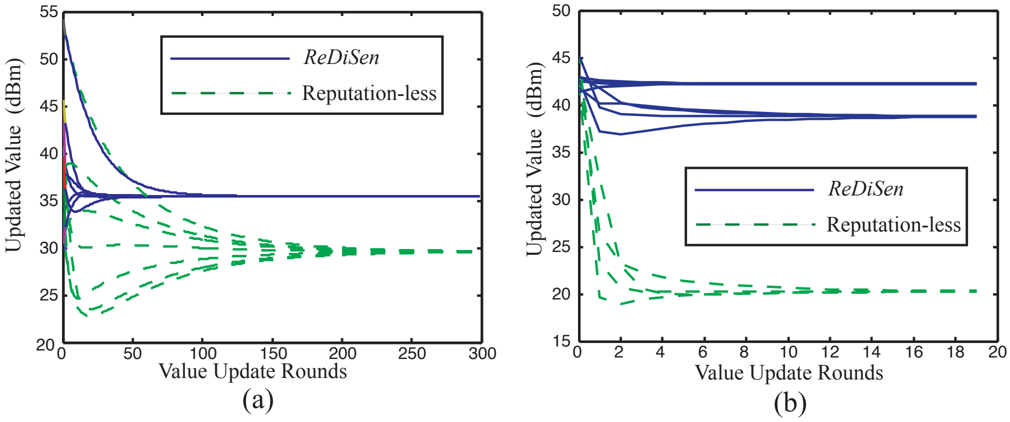


Figure 5.12: Value Update Process when the Honest Nodes Assign Reputation to (a) Value Differences, (b) Received Values. The Primary User is Transmitting. The Malicious Nodes Implement the *Random Attack* Strategy. The Communication Range of a Secondary User is 500 m. Convergence Happens in (a) but Not in (b).

obtain convergence than assigning reputation to received values. These two methods each have their own benefits and disadvantages.

5.4.6 Impact of θ on Convergence Speed

We then study the different factors that can have impact on the convergence speed. We first simulate the impact of θ on the convergence speed of the system. Figure 5.13 illustrates the value update processes with $\theta = 0.997$ and $\theta = 0.999$, and other parameters the same as Figure 5.2 (a). The simulation results indicate that the higher value θ is, the more rounds it takes for the updated values to converge.

5.4.7 Impact of CRN Sizes on Convergence Speed

We then simulate the impact of CRN sizes on the convergence speed of the system. Figure 5.14 illustrates the relations between the number of nodes in a CRN and the number of rounds towards convergence. The percentage of malicious nodes remains the same in all sizes of CRNs (30%). The simulations results indicate that the higher the network density

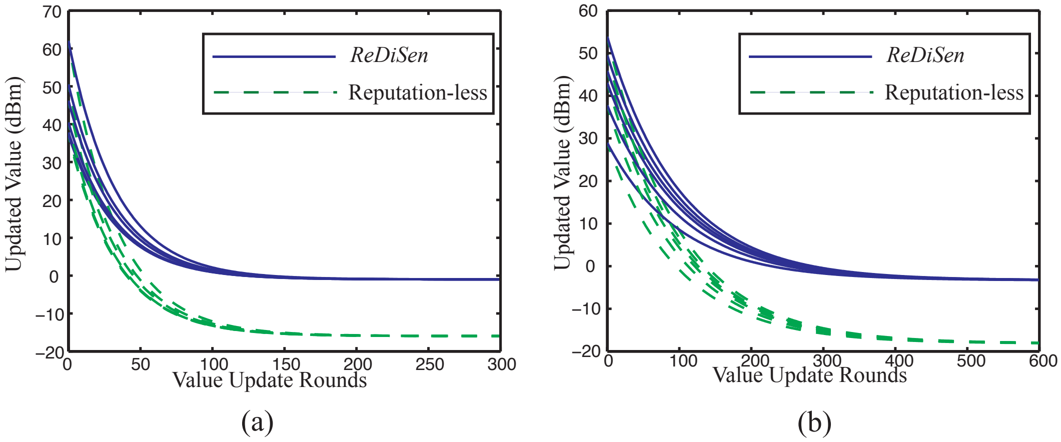


Figure 5.13: Value Update Process with (a) $\theta = 0.997$, (b) $\theta = 0.999$.

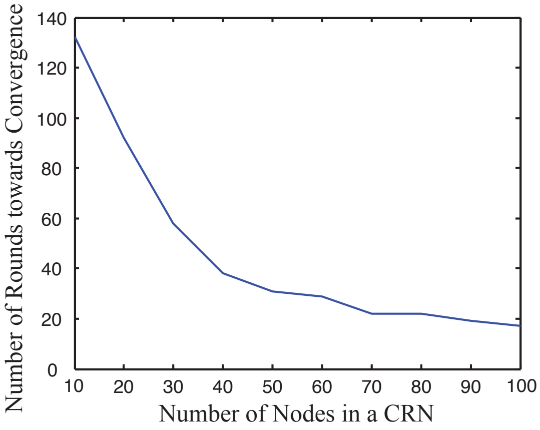


Figure 5.14: Relations between the Number of Nodes in a CRN and the Number of Rounds towards Convergence

is, the faster a converged value can be obtained for honest nodes.

5.4.8 Impact of Malicious Nodes on Convergence Speed

We then simulate the impact of malicious nodes on the convergence speed of the system. Figure 5.15 illustrates the relations between the number of malicious nodes and the number of rounds towards convergence. We simulate a network of 21 secondary users. The number of malicious nodes increases from 1 to 10. The simulations results indicate that the number of malicious nodes does not have a definite impact on the convergence speed. Figures 5.2, 5.14, and 5.15 together verify that the convergence speed depends on the parameters of θ

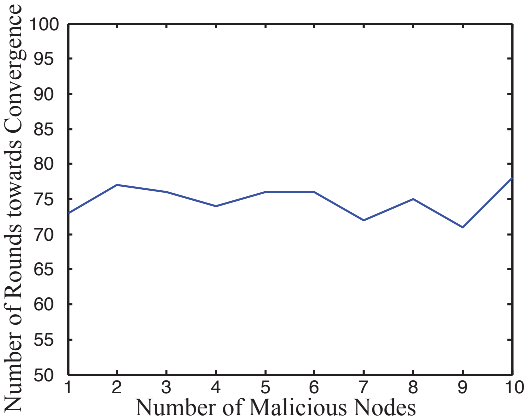


Figure 5.15: Relations between the Number of Malicious Nodes and the Number of Rounds towards Convergence

and the density of nodes, but not the number of malicious nodes.

5.4.9 Reputation Update Process

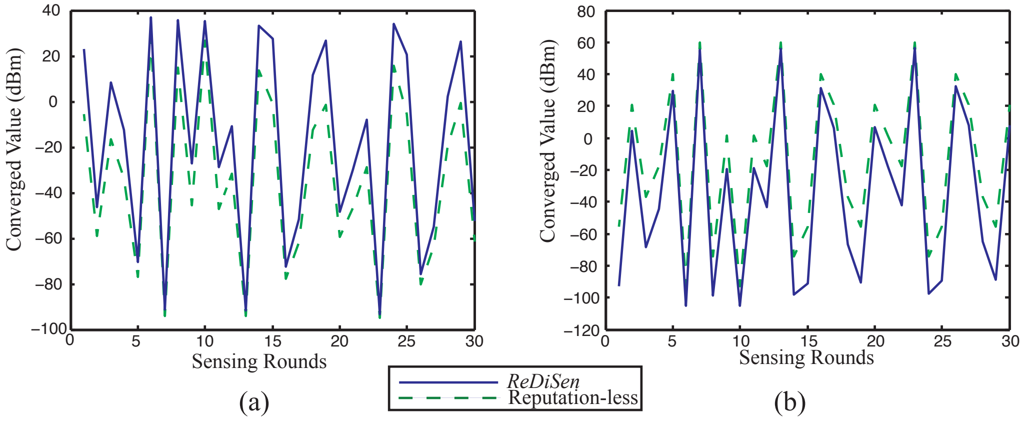


Figure 5.16: Reputation Update Process. The Primary user is (a) Transmitting, (b) Not Transmitting.

Section 5.4.2, 5.4.3, 5.4.4, and 5.4.5 all illustrate the memory-less reputation values discussed in Section 5.1. We next simulate the reputation update process described in Section 5.3. We simulate 30 sensing sessions with other parameters the same as Section 5.4.3. In the first sensing session, honest nodes generate reputation using method (5.1). In the next 29 sensing sessions, they update reputation using method (5.14). The neighbourhoods of the honest nodes change in every sensing session. Such neighbourhood change leads to the change of the percentage of malicious nodes. In the 30 sensing sessions, 16 of them are sessions with more honest neighbours while 14 of them are with more malicious neighbours. In the first sensing session, there are 30% malicious nodes on average in a neighbourhood.

Figure 5.16 illustrates that, using the reputation update method (5.14), *ReDisen* can still help honest nodes obtain better cooperative sensing results in 90% of sensing sessions, even though there are more malicious nodes in the neighbourhood in 47% sensing sessions. This simulation demonstrates that the proposed reputation update method can help honest nodes countermeasure SSDF attacks in a dynamic CRN environment.

5.5 Concluding Remarks

In this Chapter, we proposed the first fully distributed security scheme *ReDiSen* to secure cooperative sensing results in adversarial CRNs. In *ReDiSen*, we assume that a single identity system exists among all the secondary users. We also assume that all the secondary users use an out-of-band communication system to exchange control messages. In our adversary model, we assume that the malicious users attack in the same manner during a sensing session without collusion.

In our simulation process, we only implemented *ReDiSen* in a small scale. A future direction to extend this work can be a thorough experimental study in a real CRN, with different kinds of devices as primary and secondary users. During the experimental study, the parameters about the primary user power depends on the nature of primary users; the distances between the primary users and the secondary users, as well as the density of secondary users, depends on how the network elements are deployed; the noise floor and the stand deviation for shadow fading depend on the communication media; the selection of θ depends on how fast the secondary users want to converge their values to a consensus.

Another future direction to extend this work can be a study on more sophisticated malicious behaviours, such as

1. The malicious users may not attack in the same manner during an attack. For example, some of the malicious users may adopt *Random Attack* strategy, while the others adopt *Intermittent Attack* strategy.

2. The malicious users may adopt different attack intensities with some pre-calculated distribution, aiming to maximize their attack goals when reducing the probabilities of being detected.

3. The malicious users can collude to coordinate how to attack the system rotationally, so that their reputation values are kept above a certain level to avoid the detection from the honest secondary users.

4. The malicious users can attack the whole distributed spectrum sensing and allocation process together, including the work presented in Chapter 6 and Chapter 7.

5. The malicious users can implement other security attacks to a CRN, such as primary user emulation attacks and jamming attacks into the control channels, as described in Section 3.4.

Chapter 6

INCENTIVIZING COOPERATIVE SENSING

We model the spectrum sensing and spectrum allocation processes as a non-cooperative game to incentivize cooperative sensing. A previous distributed spectrum allocation scheme considers this non-cooperative game model for secondary users to arrive at a consensus spectrum allocation result iteratively without a central authority [105]. However, they did not discuss how the weight of each secondary user is calculated and utilized. We propose to use reputation values as weights in the distributed spectrum allocation process. In our system, reputation values that reflect sensing participation and sensing accuracy are used to offer incentive in the pricing function used in the spectrum allocation process. To obtain a lower price for utilizing fallow spectrum, a secondary user needs to participate more actively in the spectrum sensing process, and report accurate sensing reports. We propose a method to calculate global reputation values for the secondary users, that can incentivize them to participate in the cooperative sensing processes with more accurate results on more channels. In the reputation fusion process, the adversary may also compromise some secondary users to report spurious reputation values, aiming to improve their pricing factors in the spectrum allocation process. We design a distributed algorithm to countermeasure this kind of attacks.

The glossary of notations in this Chapter is listed as Table 6.1

6.1 Incentive Method

To offer stronger incentives for honest nodes to participate in the cooperative sensing process, we connect sensing participation to the reputation in a distributed spectrum allocation process through a user-dependent pricing function in a spectrum allocation game. In the distributed spectrum allocation process, some secondary users behave selfishly to maximize

Symbol	Description
$\mathcal{G}$	Non-Cooperative Game
Ω	Set of Players
$\mathcal{P}$	Action Space
$\mathcal{P}_i$	Action Set for i
U_i	Utility Function of i
λ_i^k	Pricing Factor of i on Channel k
c_i^k	Cost Incurred by Cooperative Sensing for i on Channel k
P_i^k	Transmission Power of i on Channel k
K_i	Number of Channels i Senses in a Sensing Session
T_i	Number of Sensing Sessions i Participates
C_i	Total Sensing Cost of i
$PU\text{-}NT$	Primary User is not Transmitting
$PU\text{-}T$	Primary User is Transmitting
G_{ii}^k	Channel Gain on Channel k of the Source to an Intended Destination
G_{ji}^k	Channel Gain on Channel k between i and an Unintended User j
M_i^k	Noise at i
β	SNR gap
α	Probability of Primary User not Transmitting
$R_i^{(SP)}$	Reputation of i about Sensing Participation
$R_i^{(SA)}$	Reputation of i about Sensing Accuracy
μ	Discount Factor
ϵ	Linear Combination Parameter
η	Linear Combination Parameter
δ	Discount Factor
$\omega_{j,i}^{(SA)k}$	Credibility of i generated by j on Channel k
s_i	Number of i's Neighbours who Transmit Spurious Reputation
c_i	Number of i's Neighbours who Transmit Truthful Reputation

Table 6.1: Glossary of Notations in Chapter 6

their own performance. A well designed pricing mechanism can elicit socially efficient behaviour from them.

We adopt the non-cooperative game among secondary users proposed in recent literature [105]. The game $\mathcal{G}$ is expressed as $\mathcal{G} = \{\Omega, \mathcal{P}, \{U_i\}\}$, where $\Omega = \{1, 2, \ldots, N\}$ is a finite set of players; $\mathcal{P} = \mathcal{P}_1 \times \mathcal{P}_2 \times \cdots \times \mathcal{P}_N$ is the action space with $\mathcal{P}_i$ being the action set for player i; and U_i is the utility function of player i, which depends on the strategies of all players, which are the secondary users. They can select different transmission powers on different channels. Higher transmission powers may bring higher achievable data rate. At the same time, higher prices are also incurred. Secondary users select their transmission powers to maximize their respective utility functions, and under certain conditions, they eventually reach a Nash Equilibrium after a number of iterations [105].

The utility function of a secondary user i when the primary user is not transmitting in a sensing session can be considered as the achievable data rate received by i from the network, $\log_2(1 + \frac{\beta G_{ii}^k P_i^k}{\sum_{j \in \Omega_N, j \neq i} G_{ji}^k P_j^k + M_i^k})$, subtracting the cost associated with the pricing function and the cooperative sensing process. Only when the primary user is not transmitting, the cost brought by the pricing function is incurred for a secondary user who is interested to transmit on this channel. We use a linear pricing mechanism [105] to describe the cost incurred by the pricing function, where the price $\lambda_i^k P_i^k$ increases monotonically with transmission power P_i^k. On each channel k, we denote the cost incurred by cooperative sensing for each secondary user as c_i^k. The total cost C_i from cooperative sensing for a node i depends on the number of channels K_i it senses in a sensing session, and the number of sensing sessions it participates in T_i, $C_i = \sum_{T=1}^{T_i} \sum_{k=1}^{K_i} c_i^k$. We denote the state where the primary user is not transmitting as $PU\text{-}NT$, and the state where the primary user is transmitting as $PU\text{-}T$. The utility function when the primary user is not transmitting is defined as:

$$\begin{aligned}
&\tilde{U}_i^{(PU-NT)}(\mathbf{P}_i, \mathbf{P}_{-i}) \\
&= \sum_{k \in \Omega_K} \tilde{u}_i(P_i^k) \\
&= \sum_{k \in \Omega_K} u_i(P_i^k) - \sum_{k \in \Omega_K} \alpha \lambda_i^k P_i^k - \sum_{k=1}^{K_i} c_i^k \\
&= \sum_{k \in \Omega_K} [\log_2(1 + \frac{\beta G_{ii}^k P_i^k}{\sum_{j \in \Omega_N, j \neq i} G_{ji}^k P_j^k + M_i^k}) - \lambda_i^k P_i^k] - \sum_{T=1}^{T_i} \sum_{k=1}^{K_i} c_i^k
\end{aligned} \tag{6.1}$$

where $\lambda_i P_i^k$ is the user-dependent linear pricing function that can drive the Nash Equilibrium close to a Pareto optimal solution. G_{ii}^k is the channel gain on channel k of the source to an intended destination, G_{ji}^k is the channel gain on channel k between the secondary user i and an unintended user j, M_i^k is the noise at i, β is the SNR gap that is needed to reach a certain channel capacity between practical implementation and information theoretical results [78].

The utility function when the primary user is transmitting is negative, defined as the cost from the cooperative sensing process:

$$\tilde{U}_i^{(PU-T)}(\mathbf{P}_i, \mathbf{P}_{-i}) = -\sum_{T=1}^{T_i} \sum_{k=1}^{K_i} c_i^k \tag{6.2}$$

We assume that for T sensing sessions, the primary user does not transmit in αT of them, and transmits in $(1-\alpha)T$ of them. Hereby, the average utility function per sensing session can be defined as:

$$\begin{aligned} &\tilde{U}_i(\mathbf{P}_i, \mathbf{P}_{-i}) \\ &= \frac{1}{T}(\alpha T(\tilde{U}_i^{(PU-NT)}(\mathbf{P}_i, \mathbf{P}_{-i})) + (1-\alpha)T\tilde{U}_i^{(PU-T)}(\mathbf{P}_i, \mathbf{P}_{-i})) \\ &= \sum_{k \in \Omega_K} \alpha[\log_2(1 + \frac{\beta G_{ii}^k P_i^k}{\sum_{j \in \Omega_N, j \neq i} G_{ji}^k P_j^k + M_i^k}) - \lambda_i^k P_i^k] - \frac{\sum_{T=1}^{T_i} \sum_{k=1}^{K_i} c_i^k}{T} \end{aligned} \tag{6.3}$$

The social optimization problem is to maximize a weighted sum of the achievable data rates of all secondary users in a sensing session:

$$\max_{\mathbf{P}} \sum_{i \in \Omega_N} R_i \sum_{k \in \Omega_K} \alpha \log_2(1 + \frac{\beta G_{ii}^k P_i^k}{\sum_{j \in \Omega_N, j \neq i} G_{ji}^k P_j^k + M_i^k}) \tag{6.4}$$

where R_i is the reputation of secondary user i, assigned to i to reward active participation and to punish idle behaviour in the cooperative sensing process. When a secondary user has a better reputation, it shall gain a higher utility in the social optimization problem, and *vice versa*.

We adopt the methodology as in [105] to derive the optimal pricing factor for the secondary users, described in (6.5). The pricing factor depends on the reputation values of all the secondary users in the network. We can observe that the higher reputation value a node i has, the lower reputation values its neighbours have (including both malicious and selfish secondary users), and the lower price i has to pay in the spectrum allocation process. This effect can offer a strong incentive for a secondary user i to improve its reputation.

$$
\begin{aligned}
\lambda_i^k &= -\frac{\sum_{j\in\Omega_N, j\neq i} R_j \frac{\partial u_j(P_j^k)}{\partial P_i^k}}{R_i} \\
&= -\frac{\sum_{j\in\Omega_N, j\neq i} R_j \frac{\partial[\alpha \log 2(1+\frac{\beta G_{jj}^k P_j^k}{\sum_{i\in\Omega_N, i\neq j} G_{ij}^k P_i^k + M_j^k})]}{\partial P_i^k}}{R_i} \\
&= -\frac{\sum_{j\in\Omega_N, j\neq i} R_j \frac{\partial[\alpha \log 2(1+\frac{\beta G_{jj}^k P_j^k}{G_{ij}^k P_i^k + \sum_{l\in\Omega_N, l\neq j, i\neq j} G_{ij}^k P_i^k + M_j^k})]}{\partial P_i^k}}{R_i} \\
&= -\frac{\sum_{j\in\Omega_N, j\neq i} R_j \frac{\alpha}{\ln 2} \frac{\frac{\partial(\frac{\beta G_{jj}^k P_j^k}{G_{ij}^k P_i^k + \sum_{l\in\Omega_N, l\neq j, i\neq j} G_{ij}^k P_i^k + M_j^k})}{\partial P_i^k}}{1+\frac{\beta G_{jj}^k P_j^k}{G_{ij}^k P_i^k + \sum_{l\in\Omega_N, l\neq j, i\neq j} G_{ij}^k P_i^k + M_j^k}}}{R_i} = \frac{\sum_{j\in\Omega_N, j\neq i} R_j \frac{\alpha}{\ln 2} \frac{\frac{G_{ij}^k \beta G_{jj}^k P_j^k}{(G_{ij}^k P_i^k + \sum_{l\in\Omega_N, l\neq j, i\neq j} G_{ij}^k P_i^k + M_j^k)^2}}{1+\frac{\beta G_{jj}^k P_j^k}{G_{ij}^k P_i^k + \sum_{l\in\Omega_N, l\neq j, i\neq j} G_{ij}^k P_i^k + M_j^k}}}{R_i} \\
&= \frac{\sum_{j\in\Omega_N, j\neq i} R_j \frac{\alpha}{\ln 2} \frac{\frac{G_{ij}^k \beta G_{jj}^k P_j^k}{(\sum_{i\in\Omega_N, i\neq j} G_{ij}^k P_i^k + M_j^k)^2}}{1+\frac{\beta G_{jj}^k P_j^k}{\sum_{i\in\Omega_N, i\neq j} G_{ij}^k P_i^k + M_j^k}}}{R_i} = \frac{\sum_{j\in\Omega_N, j\neq i} R_j \frac{\alpha}{\ln 2} \frac{\frac{G_{ij}^k \beta G_{jj}^k P_j^k}{\sum_{i\in\Omega_N, i\neq j} G_{ij}^k P_i^k + M_j^k}}{\sum_{i\in\Omega_N, i\neq j} G_{ij}^k P_i^k + M_j^k + \beta G_{jj}^k P_j^k}}{R_i} \\
&= \frac{\alpha\beta}{R_i \ln 2} \sum_{j\in\Omega_N, j\neq i} \frac{R_j G_{ij}^k P_j^k G_{jj}^k}{(\sum_{i\in\Omega_j, i\neq j} G_{ij}^k P_i^k + M_j^k)(\sum_{i\in\Omega_j, i\neq j} G_{ij}^k P_i^k + M_j^k + \beta G_{jj} P_j^k G_{ij}^k)}
\end{aligned}
\tag{6.5}
$$

After receiving transmission power P_i^k, the noise M_i^k from the neighbours, measuring G_{ii}^k and G_{ij}^k from the received signal power, and obtaining the reputation values (Section 6.2), each secondary user first adjusts its linear pricing factor over all channels according to (6.5), and then determines its best action, including the optimal channel selection and the transmission rate on each channel. The goal of user i is to maximize its individual utility function (6.1). The same procedure happens at all secondary users in the network. The Pareto optimal Nash Equilibrium is reached when all secondary users converge to the best response. The secondary users can update their best responses according to the best responses of their neighbours iteratively, using Jacobi (parallel), Gauss-Seidel (sequential) schemes [105], or asynchronous schemes [6, 89].

6.2 Generating Reputation

When discussing the spectrum allocation game, we established a reputation-based pricing scheme for secondary users to reach Nash Equilibrium. A user with higher reputation is assigned a lower price in the game. The next step is to design an appropriate mechanism for generating reputation.

6.2.1 Sensing Participation

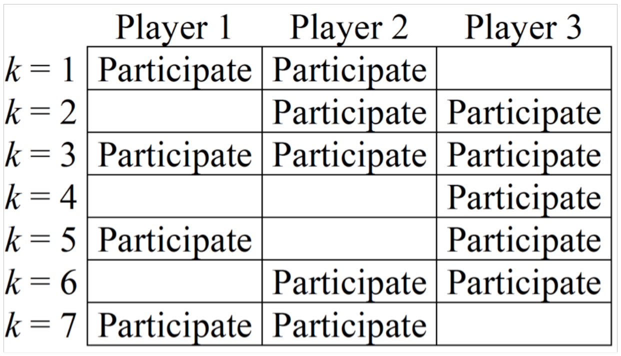
A natural way of generating R_i is to make public knowledge secondary user i's sensing participation $R_i^{(SP)}$. $R_i^{(SP)}$ is a parameter relevant to the number of channels a secondary user actively senses in a cooperative sensing session. K_i is observable by the neighbours of i.

We use the percentage of sensed channels of i for the optimization: $R_i^{(SP)} = \frac{K_i}{K}$. The higher $R_i^{(SP)}$ is, the better price i will obtain in the spectrum allocation process, which can be used as an incentive for i to increase K_i by participating in more channels. To calculate K_i, each node in the network monitors its neighbours' activity on channel k. We describe this process in Algorithm 3.

Algorithm 3 Calculating Sensing Participation. (Input: The channels a secondary user j participates in. Output: Reputation about sensing participation $R^{(SP)}$ for all the secondary users.)

```
$j$ participates in a subset of all channels
$j$ observes the other participants in every channel
while There is a secondary user $i$ participating on the same channel do
    $j$ broadcasts its observed channel participation information $K_{j,i}$ for another node $i$
    $j$ receives the observed channel participation information $K_{1,i}, K_{2,i}, K_{3,i}, \ldots$ for another node $i$ from its neighbours
    $j$ calculates $K_i = |K_{1,i} \cup K_{2,i} \cup \cdots \cup K_{j,i} \cup \ldots|$
    $i$ calculates $R_i^{(SP)} = \frac{K_i}{K}$
end while
```

Consider the sensing participation in Figure 6.1. Player 1 participates in channels $\{1, 3, 5, 7\}$. Player 2 participates in channels $\{1, 2, 3, 6, 7\}$. Player 3 participates in channels $\{2, 3, 4, 5, 6\}$. Since channel 4 is only sensed by Player 3, Player 3 has to do individual



	Player 1	Player 2	Player 3
$k = 1$	Participate	Participate	
$k = 2$		Participate	Participate
$k = 3$	Participate	Participate	Participate
$k = 4$			Participate
$k = 5$	Participate		Participate
$k = 6$		Participate	Participate
$k = 7$	Participate	Participate	

Figure 6.1: Observation on the Sensing Participations of Neighbours

sensing on channel 4. The activity of Player 3 on channel 4 is not counted towards its participation in cooperative sensing. To obtain K_i, Players 2 and 3 each observe the channels where they are active. They each record the other players on a channel: $K_{1,2} = \{1, 3, 7\}$, $K_{1,3} = \{3, 5\}$, $K_{2,1} = \{1, 3, 7\}$, $K_{2,3} = \{2, 3, 6\}$, $K_{3,1} = \{3, 5\}$, $K_{3,2} = \{2, 3, 6\}$. They broadcast the observations to neighbours. Each player then calculates the cardinality of the union set for each individual neighbour. $K_1 = |K_{2,1} \cup K_{3,1}| = 4$, $K_2 = |K_{1,2} \cup K_{3,2}| = 5$. In this case, $K_3 = |K_{1,3} \cup K_{2,3}| = 4$ rather than $K_3 = 5$. Hereby, $R_1^{(SP)} = R_3^{(SP)} = \frac{4}{7}$, $R_2^{(SP)} = \frac{5}{7}$.

6.2.2 Sensing Accuracy

The above method incentivizes users with reputation to participate in channel sensing. Considering that malicious nodes can be active in the cooperative sensing process to achieve their malicious goals, the reputation shall be further improved to reflect the sensing accuracy, besides level of participation.

We improve the sensing accuracy and participation by both identifying falsified sensing reports and incentivizing the participation of honest secondary users. This idea is similar to the *Elo* rating system for chess and *ATP (Association of Tennis Professionals) Rankings* for tennis, where the more an athlete plays, and the better an athlete performs, the higher her or his rating is. When connecting spectrum sensing with the spectrum allocation process, reputation can reflect both sensing accuracy and sensing participation of the secondary users. If a user participates more actively, or senses and reports the primary user state more accurately, it is rewarded with a lower price in the spectrum allocation process.

In a given sensing interval, a secondary user i has m_i neighbours who report falsified values (including attacking malicious neighbours and honest nodes sensing incorrectly due to severe fading or system failure), and n_i neighbours who report correct values (including honest nodes sensing correctly and non-attacking malicious nodes). We use $R_{j,i}^{(SA)k}$ to denote the reputation of transmitter i generated by receiver j to reflect the sensing accuracy of i. Each user j maintains a reputation vector of its neighbours, on a channel k: $\{R_{j,1}^{(SA)k}, R_{j,2}^{(SA)k}, \ldots, R_{j,m_j+n_j}^{(SA)k}\}$. All secondary users update their values and exchange their updated values with their neighbours. $V_{i,j}$ is the value that a transmitter i sends to a receiver j. After the first round of sensing value exchange, an honest node calculates the reputation of its neighbours based on their reported values and its own value. The reputation values reflecting sensing accuracy $R_{j,i}^{(SA)k}$ are generated on channel k as follows:

$$R_{j,i}^{(SA)k} = 2 - \frac{(m_j + n_j + 1)|V_{i,j}^k - \tilde{V}_j^k|}{\sum_{l=1}^{m_j+n_j+1} |V_{l,j}^k - \tilde{V}_j^k|} \tag{6.4}$$

where $\tilde{V}_j^k = \frac{\sum_{l=1}^{m_j+n_j+1} V_{l,j}^k}{m_j+n_j+1}$ is the average value of all the nodes in the neighbourhood on channel k [123]. The value of $R_{j,i}^{(SA)k}$ falls into $[0, 2]$.

This reputation generating method can assign reputation $R_{j,i}^{(SA)k} < 1$ for a neighbour that reports falsified values, and $R_{j,i}^{(SA)k} > 1$ for a neighbour that reports correct values, which will help honest nodes obtain better cooperative sensing results than the reputation-less scheme, assuming that the majority of neighbours are either correctly sensing honest nodes or non-attacking malicious nodes [123].

6.2.3 Reputation Fusion

Reputation values reflecting sensing accuracy of a secondary user are generated individually by its peers, and are fused into a global reputation value for use in the pricing factor of the spectrum allocation process. The reputation fusion process is a distributed scheme without a central authority. Upon detection of an idling primary user, the secondary users exchange their reputation vectors with each other iteratively towards a converged global reputation. Such agreed-upon reputation values become public knowledge in spectrum allocation.

Inspired by the distributed algorithm for cooperative sensing [59], we design a distributed algorithm for secondary users to achieve consensus on global reputation, as described in Algorithm 4. $\mu \in (0,1)$ is a discount factor. t indicates the reputation update session.

Algorithm 4 Distributed Reputation Fusion Algorithm on Channel k. (Input: Reputation vector of a node j: $R_{j,1}^{(SA)k}, R_{j,2}^{(SA)k}, \ldots, R_{j,i}^{(SA)k}, \ldots, R_{j,m_j+n_j}^{(SA)k}$ and received reputation vectors from j's neighbours. Output: The converged reputation vector.)

```
while $i$ is a neighbour of $j$ do
    $j$ receives reputation vectors from a neighbour $i$: $R_{i,1}^{(SA)k}, R_{i,2}^{(SA)k}, \ldots, R_{i,m_i+n_i}^{(SA)k}$
    $j$ sends its own reputation vector to a neighbour $i$: $R_{j,1}^{(SA)k}, R_{j,2}^{(SA)k}, \ldots, R_{j,i}^{(SA)k}, \ldots, R_{j,m_j+n_j}^{(SA)k}$
    while The converged reputation vector is not obtained do
        $j$ updates its reputation vector as
            $R_{j,i}^{(SA)k(t+1)} = R_{j,i}^{(SA)kt} + \sum_{l=1}^{m_j+n_j} \mu(R_{l,i}^{(SA)kt} - R_{j,i}^{(SA)kt}) \quad (6.5)$
    end while
end while
```

In the distributed reputation fusion algorithm, the consensus reputation value $R_i^{(SA)k}$ for i on channel k is the average reputation value from all secondary users in the network $R_i^{(SA)k} = \frac{\sum_{j \in \Omega_N, j \neq i} R_{j,i}^{(SA)k}}{N_i}$ [80]. Since a node can sense on multiple channels, the reputation value $R_i^{(SA)}$ about a node i can be described as $\frac{1}{K_i} \sum_{k \in \Omega_K, P_i^k > 0} R_i^{(SA)k}$. The higher $R_i^{(SA)k}$ it obtains, the lower price i faces in the spectrum allocation process, which can be used as another incentive for i to contribute more accurate sensing results. This statement also implies that a malicious node is less incentivized to attack with falsified sensing results.

The method of generating and fusing $R_i^{(SP)}$ has been discussed before as $R_i^{(SP)} = \frac{K_i}{K}$, which falls into the range of $[0,1]$. The two reputation vectors can be linearly combined together with parameters ϵ and η, to form the final global reputation R_i to be used in the pricing factor in the spectrum allocation process. Considering the different value ranges of $R_i^{(SA)}$ and $R_i^{(SP)}$, the global reputation value of node i is:

$$\begin{aligned}
R_i &= \epsilon R_i^{(SA)} + 2\eta R_i^{(SP)} \\
&= \epsilon \frac{1}{K_i} \sum_{k\in\Omega_K, P_i^k>0} R_i^{(SA)k} + 2\eta \frac{K_i}{K} \\
&= \frac{\epsilon}{K_i N_i} \sum_{k\in\Omega_K, P_i^k>0} \sum_{j\in\Omega_N, j\neq i} (2 - \frac{(m_j+n_j+1)|V_{i,j}^k - \tilde{V}_j^k|}{\sum_{l=1}^{m_j+n_j+1} |V_{l,j}^k - \tilde{V}_j^k|}) \\
&+ \frac{2\eta K_i}{K}
\end{aligned} \tag{6.6}$$

where $0 < \epsilon < 1, 0 < \eta < 1, \epsilon + \eta = 1$.

6.2.4 Role of Reputation

For the linear combination of $R_i^{(SA)}$ and $R_i^{(SP)}$, we now analyze the effect of the parameters towards incentivizing secondary user participation. In the reputation value R_i, $\frac{2\eta K_i}{K}$ offers incentive for both malicious and honest neighbours, while $\frac{\epsilon}{K_i}\sum_{k\in\Omega_K, P_i^k>0} R_i^{(SA)k}$ offers incentive to honest neighbours only. To differentiate secondary users in the spectrum allocation process, we propose the requirement that is consistent with the requirement for sensing accuracy. We require that $R_i < 1$ for a malicious neighbour i, and $R_i > 1$ for an honest neighbour i.

For an honest neighbour i, the requirement is $\frac{\epsilon}{K_i}\sum_{k\in\Omega_K, P_i^k>0} R_i^{(SA)k} > \frac{K-2\eta K_i}{K}$. Since $\epsilon + \eta = 1$, the requirement translates to $\frac{\epsilon}{K_i}\sum_{k\in\Omega_K, P_i^k>0} R_i^{(SA)k} > \frac{K-2\eta K_i}{K(1-\eta)}$.

Since $\frac{\epsilon}{K_i}\sum_{k\in\Omega_K, P_i^k>0} R_i^{(SA)k} > 1$, an honest node has to meet the requirement of $\frac{K-2\eta K_i}{K(1-\eta)} < 1$ to obtain a reputation value $R_i > 1$. This requirement can be transformed to $K_i > \frac{K}{2}$. Hereby, as long as it participates in more than half of the channels and reports correctly sensed values, the requirement is satisfied. In this case, the system can incentivize the honest nodes to participate in at least half of the channels. Again, the more channels it participates in, the lower price it can gain in the spectrum allocation process.

For a malicious neighbour i, the requirement is $\frac{\epsilon}{K_i}\sum_{k\in\Omega_K, P_i^k>0} R_i^{(SA)k} < \frac{K-2\eta K_i}{K}$. Since

$\epsilon + \eta = 1$, the requirement translates to $\frac{\epsilon}{K_i} \sum_{k \in \Omega_K, P_i^k > 0} R_i^{(SA)k} < \frac{K - 2\eta K_i}{K(1-\eta)}$.

Since $\frac{\epsilon}{K_i} \sum_{k \in \Omega_K, P_i^k > 0} R_i^{(SA)k} < 1$, as long as the malicious node i is active on less than half of the channels, $K_i < \frac{K}{2} \Leftrightarrow \frac{K - 2\eta K_i}{K(1-\eta)} > 1$, the requirement is satisfied. In this case, the malicious node is guaranteed to receive $R_i < 1$, which indicates a higher price in the spectrum allocation process.

For an active malicious neighbour i that attacks in more than half of the channels $K_i > \frac{K}{2}$, we need to analyze the effect of parameter η. We can observe that the more channels i actively attacks, the lower $\frac{\epsilon}{K_i} \sum_{k \in \Omega_K, P_i^k > 0} R_i^{(SA)k}$ is. At the same time, the lower $\frac{K - 2\eta K_i}{K(1-\eta)}$ also turns out to be. In the extreme situation where the malicious nodes attack all channels, $K_i = K$. The requirement for $0 < R_i < 1$ turns to be $\frac{\epsilon}{K_i} \sum_{k \in \Omega_K, P_i^k > 0} R_i^{(SA)k} < \frac{1-2\eta}{1-\eta}$, where $\frac{1-2\eta}{1-\eta}$ is the lower bound for the system to meet the requirement.

Once the allocation decision is made, there could be many new ways of attacking the system by abusing the allocated resources. The enforcement on the spectrum usage has a wide plethora of research problems and solutions, and thus is out of the scope of this thesis. Such enforcing methods in the spectrum sharing process can be found in independent literature, such as [25, 55].

6.2.5 Reputation Update Process

Our hitherto discussion has been focusing on the comparison within a single sensing session. The calculations and comparisons all happen in one sensing session and restart in the next sensing session. If a selfish or malicious node changes its behaviour across sessions, reputation calculation in previous sensing sessions are independent. However, a realistic cognitive radio network is dynamic. The nodes, both honest and malicious, may move to different locations in different sensing sessions. Their neighbourhood can be different in different sensing sessions. In some sensing sessions, the majority of the neighbourhood may not be dominated by nodes that report correct values.

To better reflect the dynamic behaviour changes of the secondary users, we wish to design a reputation update process to consider both previous behaviour as well as the current behaviour, including both sensing participation and sensing accuracy. The more recent behaviour shall be given higher weights than the more distant behaviour. If a secondary user stops participation in some sensing sessions, its reputation shall also be reduced. This method can tolerate some misbehaviour of honest nodes upon system failures. In this case, an honest node can still gain a better price based on previous good behaviour.

We propose a reputation update process, which can reflect the behaviour changes of the secondary users:

$$R_i^T = \delta R_i^{T-1} + \begin{cases} (1-\delta)\Psi^T & \text{if } \ i \text{ participates in the sensing session } T \\ 0 & \text{if } \ i \text{ does not participate in the sensing session } T \end{cases} \tag{6.7}$$

where $\Psi^T = (\frac{\epsilon}{K_i N_i} \sum_{k \in \Omega_K, P_i^k > 0} \sum_{j \in \Omega_N, j \neq i} (2 - \frac{(m_j+n_j+1)|V_{i,j}^k - \tilde{V}_j^k|}{\sum_{l=1}^{m_j+n_j+1} |V_{l,j}^k - \tilde{V}_j^k|}) + \frac{2\eta K_i}{K})^T$, and δ is a discount factor of previous reputation values in $(0, 1)$. We can observe that $0 \leq R_i^T \leq 2$.

We can derive the value of $R_{j,i}^T$ as

$$R_i^T = \delta^{T-1}\Psi^1 + \delta^{T-2}(1-\delta)\Psi^2 + \delta^{T-3}(1-\delta)\Psi^3 + \delta(1-\delta)\Psi^{T-1} + (1-\delta)\Psi^T, \tag{6.8}$$

where any Ψ^T can be replaced by 0 if i does not participate in sensing session T.

Let us discuss the impact of the discount factor δ. It is easy to observe that $(\delta)^{T-2}(1-\delta) < (\delta)^{T-3}(1-\delta) < \cdots < \delta(1-\delta) < (1-\delta)$. So the most recent behaviour is more important than the previous ones for the sensing sessions where a secondary user is active, starting from the second sensing session. To extend this requirement to the first sensing session, we require that $\delta^{T-1} < \delta^{T-2}(1-\delta) \Leftrightarrow \delta < 0.5$. As long as $0 < \delta < 0.5$, the reputation update method in (6.7) can assign higher weights to the recent behaviour when taking the previous behaviour into account.

6.3 Improving Robustness of Reputation

Malicious nodes are interested in manipulating the reputation values to give themselves lower prices, while giving higher prices to honest nodes. Once fused with correct data, such spurious data can lead to detrimental, unfair prices. We further assign differentiated weights to the reputation values about sensing accuracy. Such *reputation-of-reputation* serves as *credibility* to help honest nodes obtain more accurate reputation values for their neighbours.

An honest node calculates the credibility of its neighbours based on their reported reputation vectors and its own reputation vector after the first round of reputation exchange in Algorithm 4. We use differentiated weight $\omega_{j,i}^{(SA)k}$ to denote the credibility of the transmitter i generated by the receiver j. Then, we can modify (6.5) to

$$R_{j,i}^{(SA)k(t+1)} = R_{j,i}^{(SA)kt} + \sum_{l=1}^{m_j+n_j} \mu\omega_{j,i}^{(SA)k}(R_{l,i}^{(SA)kt} - R_{j,i}^{(SA)kt}). \tag{6.9}$$

For requirements on $\omega_{j,i}^{(SA)k}$ to guarantee that the reputation fusion in (6.9) is better than that in (6.5), we have:

Proposition 3. Assume a node j can assign credibility $0 < \omega_{j,i}^{(SA)k} < 1$ to a neighbour that reports spurious reputation values, and $\omega_{j,i}^{(SA)k} > 1$ to a neighbour that reports correct reputation values. Then j can update the fused reputation value of a neighbour i to a higher reputation value when i reports correct sensing results, and a lower reputation value when i reports falsified sensing results, compared to the reputation fusion process without credibility $\omega_{j,i}^{(SA)k}$.

Proof. Let s_i be the number of i's neighbours who transmit spurious reputation, and c_i be number of other neighbours. For an honest node j, we denote the credibility of a neighbour i that reports a correct reputation with $\omega_{j,i_C}^{(SA)k}$, and the credibility of a node i that reports a spurious reputation with $\omega_{j,i_S}^{(SA)k}$. Comparing the two reputation update methods (6.5) and (6.9), we have $R_{j,i}^{(SA)k(t+1)} = R_{j,i}^{(SA)kt} + \mu[\sum_{i=1}^{s_j} \omega_{j,i_S}^{(SA)k}(R_{l,i}^{(SA)kt} - R_{j,i}^{(SA)kt}) +$

$\sum_{i=s_j+1}^{s_j+c_j}\omega_{j,i_C}^{(SA)k}(R_{l,i}^{(SA)kt}-R_{j,i}^{(SA)kt})]$ and $R_{j,i}^{(SA)k(t+1)}=R_{j,i}^{(SA)kt}+\mu[\sum_{i=1}^{s_j}(R_{l,i}^{(SA)kt}-R_{j,i}^{(SA)kt})+\sum_{i=s_j+1}^{s_j+c_j}(R_{l,i}^{(SA)kt}-R_{j,i}^{(SA)kt})]$. Therefore, the difference between these two methods is:

$$\mu[\sum_{i=1}^{s_j}(\omega_{j,i_S}^{(SA)k}-1)(R_{l,i}^{(SA)kt}-R_{j,i}^{(SA)kt})+\sum_{i=s_j+1}^{s_j+c_j}(\omega_{j,i_C}^{(SA)k}-1)(R_{l,i}^{(SA)kt}-R_{j,i}^{(SA)kt})]. \tag{6.10}$$

We now examine the two scenarios, when an honest node j generates the reputation of a neighbour (i) correctly, or (ii) incorrectly. In case (ii), the effect is the same as a spurious reputation value. In case (i), $R_{j,i}^{(SA)kt}\approx R_{l,i}^{(SA)kt}$ for a neighbour l that also generate a correct reputation value, then the difference between the two methods is approximately $\mu\sum_{i=1}^{s_j}(\omega_{j,i_S}^{(SA)k}-1)(R_{l,i}^{(SA)kt}-R_{j,i}^{(SA)kt})$. While i reports a correct sensed value, we have $R_{l,i}^{(SA)kt}<R_{j,i}^{(SA)kt}$ for a neighbour l that reports a spurious reputation value. As long as $\sum_{i=1}^{s_j}(\omega_{j,i_S}^{(SA)k}-1)<0$, (6.9) can help j obtain a higher converged reputation for i than (6.5). While node i reports a falsified sensed value, $R_{l,i}^{(SA)kt}>R_{j,i}^{(SA)kt}$ for a neighbour l that reports a spurious reputation value and so as long as $\sum_{i=1}^{s_j}(\omega_{j,i_S}^{(SA)k}-1)<0$, (6.9) can help j obtain a lower converged reputation for i than (6.5). Thus the first requirement for credibility is that $\sum_{i=1}^{s_j}(\omega_{j,i_S}^{(SA)k}-1)<0$ for a neighbour l reporting incorrectly.

In case (ii), $R_{j,i}^{(SA)kt}\approx R_{l,i}^{(SA)kt}$ for a neighbour l that also generates a spurious reputation value, then the difference between the two methods is approximately $\mu\sum_{i=1}^{s_j}(\omega_{j,i_C}^{(SA)k}-1)(R_{l,i}^{(SA)kt}-R_{j,i}^{(SA)kt})$. While i reports incorrectly, we have $R_{l,i}^{(SA)kt}<R_{j,i}^{(SA)kt}$ for a neighbour l that reports a correct reputation value. As long as $\sum_{i=1}^{s_j}(\omega_{j,i_C}^{(SA)k}-1)>0$, (6.9) can help j obtain a higher converged reputation for i than (6.5). While i reports a correct sensed value, $R_{l,i}^{(SA)kt}<R_{j,i}^{(SA)kt}$ for a neighbour i that reports a correct reputation value and so as long as $\sum_{i=1}^{s_j}(\omega_{j,i_C}^{(SA)k}-1)<0$, (6.9) can help j obtain a lower converged reputation for i than (6.5). Thus the second requirement for credibility is that $\sum_{i=1}^{s_j}(\omega_{j,i_C}^{(SA)k}-1)>0$ for a neighbour l reporting a correct reputation value. □

To generate the credibility $\omega_{j,i}^{(SA)k}$ that can meet the two requirements, we propose the method of:

$$\omega_{j,i}^{(SA)k} = 2 - \frac{|R_{j,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)kt}|}{\frac{\sum_{l=1}^{s_j+c_j} |R_{l,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)kt}|}{s_j+c_j}} = 2 - \frac{(s_j + c_j)|R_{j,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)t}|}{\sum_{l=1}^{s_j+c_j} |R_{l,i}^{(SA)t} - \tilde{R}_{j,i}^{(SA)t}|} \tag{6.11}$$

where $\tilde{R}_{j,k}^{(SA)kt} = \frac{\sum_{l=1}^{s_j+c_j} R_{j,i}^{(SA)kt}}{s_j+c_j}$ is the average reputation value of i from neighbours of j. We have $0 \leq \omega_{j,i}^{(SA)k} \leq 2$.

The rationale of this method lies in the observation on the distances to the average reputation value. As long as there are more neighbours that report correct reputation values for i, the distance from the reputation value of a node that reports correctly to the average reputation value will be smaller than the average distance to the average reputation value, and *vice versa*. That leads to the following theorem:

Theorem 3. The credibility-generating method in (6.11) enables honest nodes to assign $0 < \omega_{j,i}^{(SA)k} < 1$ for neighbours reporting spurious reputation, $\omega_{j,i}^{(SA)k} > 1$ for neighbours reporting correct reputation, for the reputation fusion method in (6.9). Therefore, (6.9) and (6.11) can help honest nodes obtain higher reputation values for other honest nodes, lower reputation values for malicious nodes, given the condition that more neighbours report correct reputation values. This improvement of reputation robustness can assign higher prices to the malicious nodes, and lower prices to honest nodes in the spectrum allocation process.

Proof. For a neighbour that reports spurious reputation values, the distance to the average reputation value is above average: $|R_{j,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)kt}| > \frac{\sum_{l=1}^{s_j+c_j} |R_{l,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)kt}|}{s_j+c_j}$. Since both $s_j + c_j > 0$ and $\sum_{l=1}^{s_j+c_j} |R_{l,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)kt}| > 0$, we can have $\frac{(s_j+c_j)|R_{j,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)t}|}{\sum_{l=1}^{s_j+c_j} |R_{l,i}^{(SA)t} - \tilde{R}_{j,i}^{(SA)t}|} > 1$, which is equivalent to $2 - \frac{(s_j+c_j)|R_{j,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)t}|}{\sum_{l=1}^{s_j+c_j} |R_{l,i}^{(SA)t} - \tilde{R}_{j,i}^{(SA)t}|} < 1$. According to (6.11), we have $0 < \omega_{j,i_S}^{(SA)k} < 1$.

For a neighbour that reports correct reputation values, the distance to the average reputation value is smaller than the average distance from the average reputation value: $|R_{j,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)kt}| < \frac{\sum_{l=1}^{s_j+c_j} |R_{l,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)kt}|}{s_j+c_j}$. Since both $s_j + c_j > 0$ and $\sum_{l=1}^{s_j+c_j} |R_{l,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)kt}| > 0$, we can have $\frac{(s_j+c_j)|R_{j,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)t}|}{\sum_{l=1}^{s_j+c_j} |R_{l,i}^{(SA)t} - \tilde{R}_{j,i}^{(SA)t}|} < 1$, which is equivalent to $2 - \frac{(s_j+c_j)|R_{j,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)t}|}{\sum_{l=1}^{s_j+c_j} |R_{l,i}^{(SA)t} - \tilde{R}_{j,i}^{(SA)t}|} > 1$.

According to (6.11), we can have $\omega_{j,i_C}^{(SA)k} > 1$.

Combining these two cases with the requirements on credibility, we can verify the validity of the theorem. □

6.4 Performance Evaluation

6.4.1 Simulation Objective and Outline

We simulate the system performance in *Matlab*, studying: (1) assigning lower prices to honest but selfish nodes, when they are incentivized to participate in more channels; (2) assigning higher prices to malicious nodes when it reports falsified sensing results; (3) improving the robustness of reputation by reducing the effect of spurious reputation values.

In our simulations, the SNR gap β is 0.3. Each secondary user has the same capacity to communicate with other secondary users in its proximity. The noise is set as $M_i^k = -80dBm, \forall i \in \Omega_N, \forall k \in \Omega_K$. The primary users transmit with the probability $\alpha = 0.5$ on all channels.

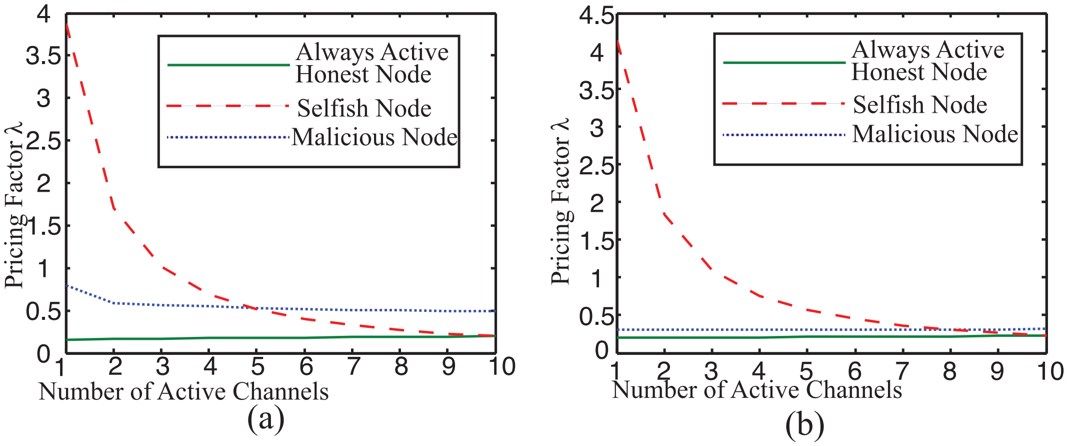
We simulate a network of 10 secondary users, to observe: (1), the pricing factor values generated from both sensing accuracy and sensing participation; (2), the reputation fusion process under attacks from malicious nodes reporting spurious reputation values.

We examine the extreme situation where malicious nodes attack on all channels, reporting falsified sensed values in the cooperative sensing process and spurious reputation values in the reputation update process. The honest but selfish secondary users participate in a subset of 10 different channels, reporting correctly sensed values in the cooperative sensing process and correct reputation values in the reputation update process.

We now present simulation results for verifying the efficacy of the proposed incentive mechanisms.

6.4.2 Pricing Factor

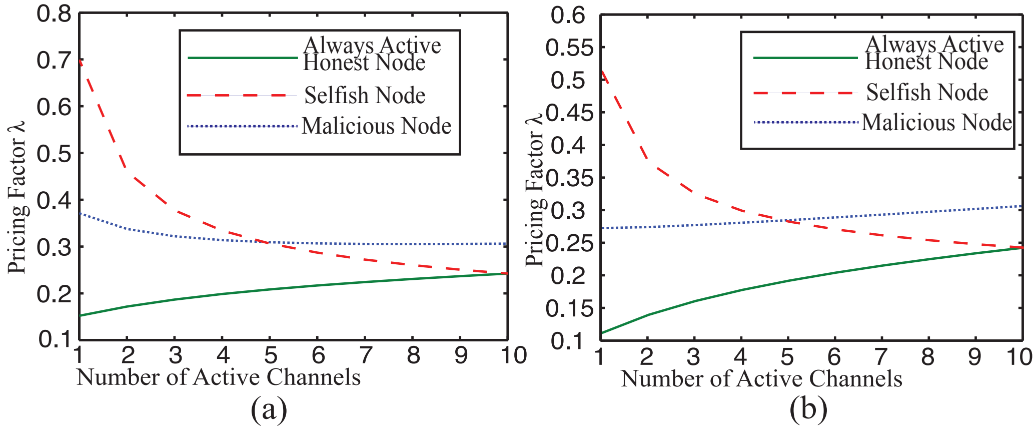
We first simulate the pricing factor for different kinds of secondary users in different situations. In Figure 6.2, 6.3, 6.4, and 6.5, the x-axis indicates the number of channels a selfish node participates in, the y-axis is the pricing factor for an honest node, a malicious node, or a selfish node. We use the tuple {# of always active nodes, # of selfish nodes, # of malicious nodes, ϵ, η} to denote the different parameters.



(a)

(b)

Figure 6.2: Pricing Factors for an Always Active Node, a Selfish Node and a Malicious Node. Parameters: (a) {6, 1, 3, 0.5, 0.5}, (b) {5, 1, 4, 0.5, 0.5}.



(a)

(b)

Figure 6.3: Pricing Factors for an Always Active Node, a Selfish Node and a Malicious Node. Parameters: (a) {4, 3, 3, 0.5, 0.5}, (b) {2, 5, 3, 0.5, 0.5}.

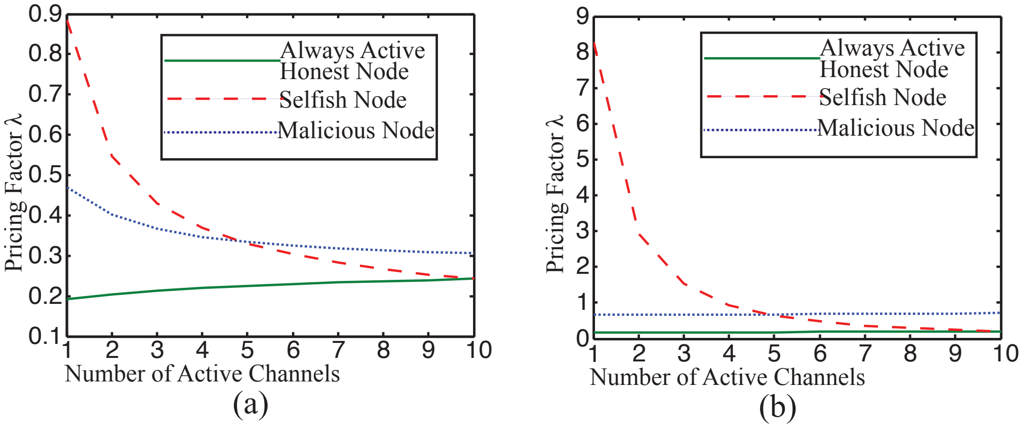


Figure 6.4: Pricing Factors for an Always Active Node, a Selfish Node and a Malicious Node. Parameters: (a) {6, 1, 3, 0.9, 0.1}, (b) {6, 1, 3, 0.1, 0.9}.

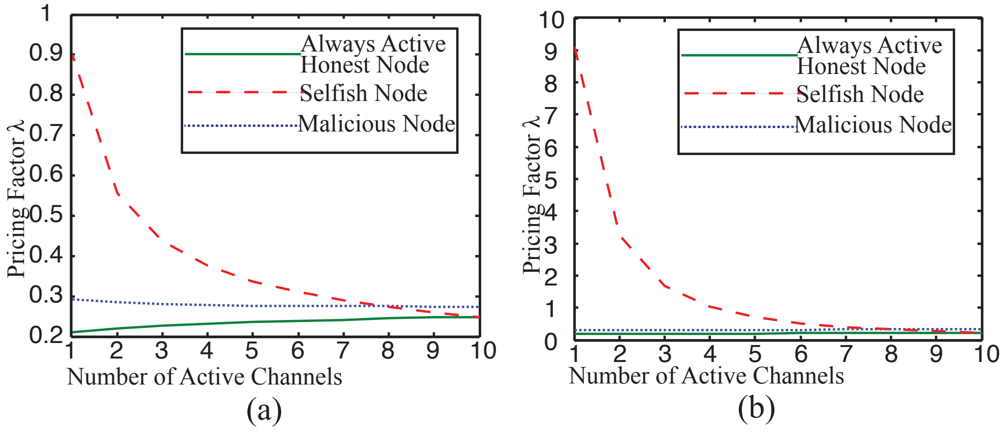


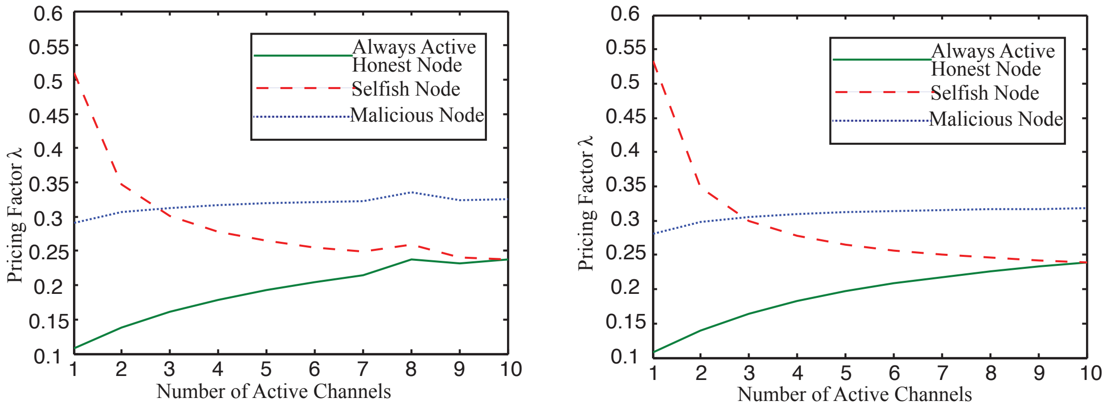
Figure 6.5: Pricing Factors for an Always Active Node, a Selfish Node and a Malicious Node. Parameters: (a) {5, 1, 4, 0.9, 0.1}, (b) {5, 1, 4, 0.1, 0.9}.

We can observe that the always active nodes have lower pricing factors compared to the malicious nodes. As the number of active channels increases, the pricing factors of the selfish nodes are eventually lowered to the same level of an always active honest node. The more active channels the selfish nodes participate in, the lower prices they can obtain. Figure 6.2 depicts scenarios with different numbers of malicious nodes. Since malicious nodes are all actively spreading falsified sensing results on all the channels, the selfish node needs to participate in at least five channels when there are three malicious nodes, and eight channels when there are four malicious nodes, to obtain a lower price than the malicious nodes.

As the number of malicious nodes increases, the differences between the pricing factors of an always active honest node and a malicious node shrink. Figures 6.2 and 6.3 depict the scenarios with different numbers of selfish nodes. As the number increases, the pricing factor for a selfish node decreases. This is because the pricing factor depends on the comparable reputation values of all the nodes in the network. If other nodes have lower reputation values, the pricing factor for the selfish nodes can increase. Figures 6.2, 6.4 and 6.5 depict the scenarios with different selection of parameters ϵ and η. We can observe that the higher are the value η is, the higher differences between the selfish node and an always active honest node. The reason is that the higher η amplifies the role of sensing participation in the pricing factor. In this case, the secondary users can be incentivized to participate on more channels. However, the importance of sensing accuracy is downplayed. This is the tradeoff between the two parameters ϵ and η. *These observations indicate that the system can offer the selfish but honest secondary users strong incentives to participate more actively into the distributed cooperative sensing process to obtain lower prices in the spectrum allocation process.* The system can also assign higher prices to malicious nodes who attack by reporting falsified sensed results.

6.4.3 Reputation Update Process

Figures 6.6 and 6.7 depict the pricing factors when the secondary users update their reputation values as (6.7). The other parameters are the same as Figure 6.3 (b): {4, 3, 3, 0.5, 0.5}. We can observe that the higher δ is, the lower are the prices a selfish node or a malicious node has. This is due to the tolerance of their previous misbehaviour. Compared to Figure 6.3(b), we can also observe that the selfish nodes can obtain better prices than the malicious nodes faster.



(a)

(b)

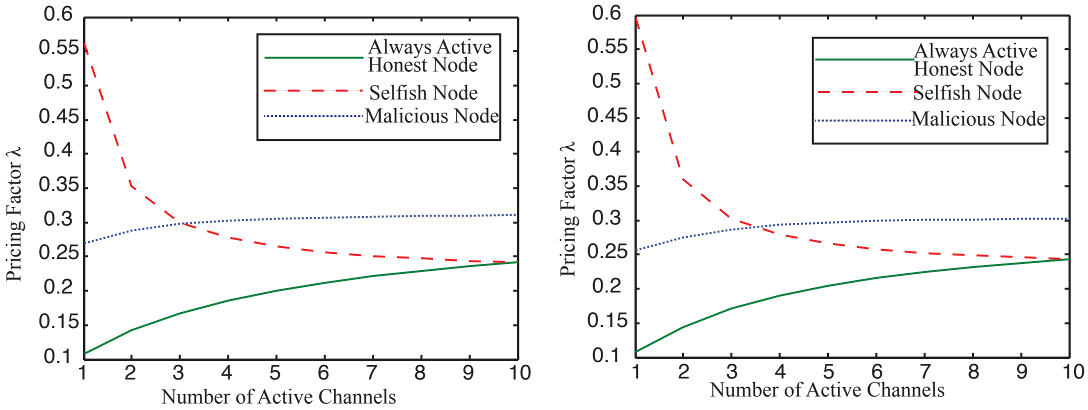
Figure 6.6: Pricing Factors for an Always Active Node, a Selfish Node and a Malicious Node when the Reputation Values are Updated as (6.7): (a) $\delta = 0.1$, (b) $\delta = 0.2$.

6.4.4 Credibility

Figure 6.8 depicts the differences credibility ω brings to the system performance for an honest node and a malicious node. For an honest node, the malicious nodes report the lowest reputation 0. With the help of credibility ω, the converged reputation value $R^{(SA)}$ of another honest node for the victim honest node is approximately 0.3 higher than the scenario without credibility. For a malicious node, the other malicious nodes report extremely high reputation values. With the help of credibility ω, the converged reputation value $R^{(SA)}$ of an honest node for the malicious node is approximately 0.4 lower than the scenario without credibility. These observations indicate that the system can improve the robustness of reputation by reducing the effect of spurious reputation values.

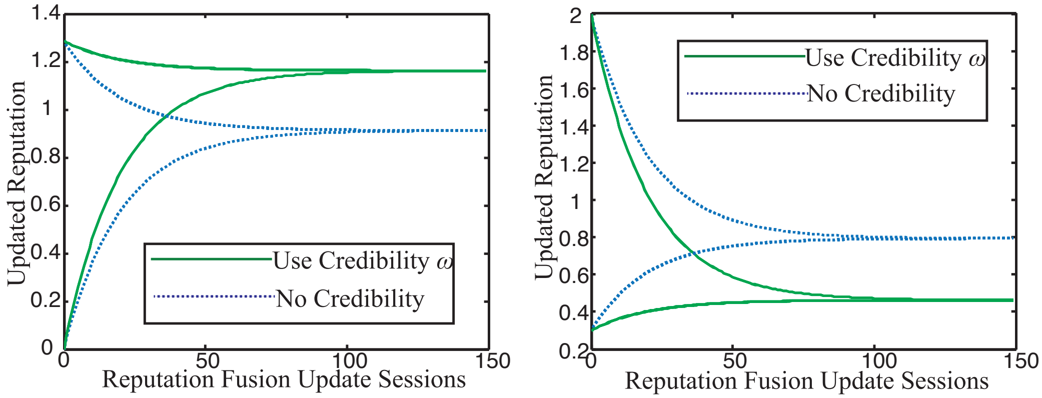
6.5 Concluding Remarks

In this Chapter, we proposed the first fully distributed scheme to incentivize cooperative sensing in CRNs. In our system, we assume that a single identity system exists among all the secondary users. We also assume that all the secondary users use an out-of-band communication system to exchange control messages. In our adversary model, we assume



(a) (b)

Figure 6.7: Pricing Factors for an Always Active Node, a Selfish Node and a Malicious Node when the Reputation Values are Updated as (6.7): (a) $\delta = 0.3$, (b) $\delta = 0.4$.



(a) (b)

Figure 6.8: Reputation Fusion Process. The Reputation Fusion for the $R^{(SA)}$ of (a) An Honest Node, (b) A Malicious Node.

that the malicious users attack in the same manner during a sensing session without collusion.

In our simulation process, we only implemented the system in a small scale. A future direction to extend this work can be a thorough experimental study in a real CRN, with different kinds of devices as primary and secondary users. During the experimental study, the parameters about SRN gap, the channel gains, and the noise floor depend on the communication media; the probability of primary user transmitting depends on the nature of the primary users; the selection of ϵ and η depends on whether the secondary users want to give more incentives to sensing participation, or sensing accuracy.

Another future direction to extend this work can be a study on more sophisticated malicious behaviours, such as

1. The malicious users may not attack in the same manner during an attack. For example, some of the malicious users may attack the cooperative sensing process by reporting falsified sensing reports, while the other malicious users attack the reputation system by reporting spurious reputation values.

2. The malicious users can collude to coordinate how to attack the system rotationally, so that their reputation values are kept above a certain level to avoid the detection from the honest secondary users.

3. The malicious users can attack the whole distributed spectrum sensing and allocation process together, including the work presented in Chapter 5 and Chapter 7.

4. The malicious users can implement other security attacks to a CRN, such as primary user emulation attacks and jamming attacks into the control channels, as described in Section 3.4.

Chapter 7

VERIFYING VCG SPECTRUM AUCTIONS

When primary users are also included into the spectrum allocation process, spectrum auctions are a natural solution. To secure the VCG spectrum auctions, this thesis introduces a method to detect the misbehaviour of the auctioneer during the spectrum auction process. Our design goal is to enable the bidders to verify the correctness of the auction, when the auctioneer is potentially malicious. For the winner determination phase, the proposed method shall be able to verify whether the winning independent set has the highest total valuation among all independent sets of bidders, in the interference graph. For the pricing phase, the proposed method can verify whether the price for a winner equals the opportunity cost its presence introduces to other bidders. The verification scheme shall be distributed among the secondary users without the need of a central authority. The verification process shall also have the privacy-preserving property. When protecting the integrity of the VCG auctions, we shall not make bidder privacy significantly worse than the case of no verification. In particular, individual bids shall not be revealed to other bidders whenever possible.

The glossary of notations in this Chapter is listed as Table 7.1

Symbol	Description
N_{MIS}	Number of Maximal Independent Sets
b_i	Bid of Bidder i
v_i	Valuation of Bidder i
p_i	Price Charged to Bidder i
s_W	Winning Independent Set
N_w	Number of Winners in a Winning Independent Set
N_s	Number of Bidders in an Independent Set
$x_1, x_2, \ldots$	Winners and Their Bids
$y_1, y_2, \ldots$	Verifiers and Their Bids
N_B^M	Number of Random Number Groups
$r(i)$	Random Number Generated by i

Table 7.1: Glossary of Notations in Chapter 7.1

7.1 Verifying Winner Determination

In order to discover all possible misbehaviour of the auctioneer, the set of bidders, including both winning and losing ones, need to collaborate in the auction verification process. In the proposed verification mechanism, they jointly conduct maximal independent set enumeration and a series of secure multi-party computation tasks.

7.1.1 Verification Algorithm

A maximal independent set of a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is a subset $\mathcal{V}' \subseteq \mathcal{V}$ of the vertices such that no two vertices in $\mathcal{V}'$ are connected by an edge in $\mathcal{E}$, and such that each vertex in $\mathcal{V} - \mathcal{V}'$ is connected by an edge to some vertex in $\mathcal{V}'$ [46]. In the auction process, since the conflict graph is public, the bidders and the auctioneer then check the conflict graph and enumerate the maximal independent sets [46]. Let N_{MIS} be the number of maximal independent sets in the conflict graph. Considering only maximal independent sets instead of all possible independent sets greatly reduces the computational complexity of the verification process, as later illustrated in Section 7.3.

For N_b bidders, the number of maximal independent sets N_{MIS} falls into $[N_b, 2^{N_b} - 1]$. One of them is declared as the winning set in the winner determination phase. The other $N_{MIS} - 1$ are potentially the verifiers. We use Secure Multiparty Computation as a black-box to verify the winner determination of a VCG auction. SMC enables different parties to compute a function of their private inputs without revealing information beyond just the output of the function. The computation is performed by the parties jointly, without a trusted authority. The input of the verification is the individual bids of the bidders. The output is a binary value indicating whether the winner determination is truthful. A bidder is convinced that the outcome is truthful if it discovers that the declared set does dominate other independent sets in total bids: $\forall s \backslash s_W, \sum_{i=1}^{N_w} v_i - \sum_{j=1}^{N_{MIS}} v_j > 0$. The bidders will not know the addition result of their SMC. They only know whether the summation is larger than, equal to, or smaller than 0. The bidders cannot learn more than the binary output, in particular they cannot learn other bidders' valuations through multiple verification additions.

We denote the algorithm of the winner determination verification as Algorithm 5.

Algorithm 5 Verify Winner Determination (Input: Bids of the Bidders. Output: Whether the Winner Determination is Correct or Not

```
while  A bidder $i$ is a winner of a VCG auction do
    $i$ supplies its bid $v_i$ into the SMC
end while
while  A bidder $j$ is not a winner of a VCG auction do
    $j$ supplies its bid $v_j$ into the SMC
end while
The SMC outputs 1, if $\sum_{i=1}^{N_w} v_i - \sum_{j=1}^{N_s} v_j \geq 0$, outputs 0 if $\sum_{i=1}^{N_w} v_i - \sum_{j=1}^{N_s} v_j < 0$
```

Each losing maximal independent set can verify the winner determination individually. If one of them detects that the verification result is 0, indicating identified misbehaviour of the auctioneer, bidders in this maximal independent set broadcast the result to other bidders, marking the auction fraudulent and the auctioneer misbehaving. The further steps after detection are orthogonal to the detection mechanism, and are not within the scope of this paper.

7.1.2 Information Leakage

During the verification process, a curious bidder may belong to the winner group, a verifier group, or both. We characterize the different scenarios based on the roles of a curious bidder and the number of bidders in either the winner set or the verifier set, as illustrated in Table 7.2. Note that if a curious bidder belongs to both the winners and the verifiers, then both groups must have two or more bidders. During the verification process, inequality may arise due to comparisons between the winner set and verification sets. A verifier participating in a number of such comparisons may attempt to learn information about other verifiers. We analyze what information may be leaked in the worst case scenario.

In the seven scenarios, we denote the winners and their bids as $x_1, x_2, \ldots,$ the verifiers

Role of A Curious Bidder	Scenario
Winner Only	One Winner (a)
	Two Winners (b)
	Three or More Winners (c)
Verifier Only	One Verifier (d)
	Two or More Verifiers (e)
Winner and Verifier	Two Winners (f)
	Three or More Winners (g)

Table 7.2: Different Scenarios During the Winner Determination Verification Process

and their bids as $y_1, y_2, \ldots$:

a: As the only winner, x_1 is curious to learn more about the verifiers. If there is only one winner and one verifier, then x_1 learns that $x_1 > y_1$. If $x_1 = 2$, x_1 learns $y_1 = 1$. For the case of two verifiers, if x_1 learns that $x_1 > y_1 + y_2$, and $x_1 = 3$, then x_1 learns that $y_1 = 1$ and $y_2 = 1$ because the bids are positive integers. In general, if the number of verifiers $N_s = x_1 - 1$, x_1 learns that all the verifiers have bid 1.

b: x_1 and x_2 are the two winners. If there is only one verifier in a maximal independent set, then x_1 can learn $x_1 + x_2 < y_1 \Rightarrow x_2 < y_1$. x_2 can also learn $x_1 < y_1$. However, $x_1 + x_2 < y_1$ can only happen once as this inequality will stop the comparisons by detecting the misbehaviour of the auctioneer. If another bidder x_2 exists in both winners and verifiers, such as $x_1 + x_2 > x_2 + y_1$, then x_1 can learn $x_1 > y_1$. x_1 learns an upper bound of y_1. If $x_1 = 2$, then x_1 learns $y_1 = 1$ because the bids are positive integers. If $x_1 + x_2 < x_2 + y_1$, x_1 can also learn y_1's lower bound $x_1 < y_1$. After many comparisons, x_1 may learn $x_1 > y_1, x_1 > y_2, x_1 > y_3 \ldots$. However, x_1 cannot learn the sorted order of $y_1, y_2, y_3, \ldots$.

c: if $x_1 + x_2 + x_3 + \cdots < y_1$, x_1 learns that $x_2 < y_1, x_3 < y_1, \ldots$. If other bidders coexist in both winners and verifiers, such as $x_1 + x_2 + x_3 > x_2 + x_3 + y_1$, then x_1 can learn $x_1 > y_1$. x_1 learns an upper bound of y_1. Again, after many comparisons, x_1 may learn $x_1 > y_1, x_1 > y_2, x_1 > y_3 \ldots$, but not the sorted order of $y_1, y_2, y_3, \ldots$.

d: As the only verifier, y_1 is curious to learn about the winners. If there is only one winner and one verifier, then y_1 learns that $x_1 > y_1$. In the case of two winners, if y_1 learns that $x_1 + x_2 < y_1$, and $y_1 = 3$, then y_1 learns that $x_1 = 1$ and $x_2 = 1$. In general, if the number of winners $N_w = y_1 - 1$, y_1 learns that all the winners have bid 1.

e: y_1 and y_2 are the two verifiers. If there is only one winner in the winning independent set, then y_1 can learn $x_1 > y_1 + y_2 \Rightarrow x_1 > y_2$. y_2 can also learn $x_1 > y_1$. After many comparisons, a curious bidder can learn the relations of other bids, but not the sorted order of $y_1, y_2, y_3, \ldots$. If other bidders y_2, y_3 exists in both winners and verifiers, such as $x_1 + x_2 + y_2 + y_3 < y_1 + y_2 + y_3$, then y_1 can learn $x_1 + x_2 < y_1$. If $y_1 = 3$, then y_1 learns $x_1 = 1$ and $x_2 = 1$ because the bids are positive integers. In general, if the other bidders are exactly the same except for the verifier and the number of other winners $N'_w = y_1 - 1$, the verifier can learn the bids of the winners.

f: In this scenario, $x_1 + x_2 > x_1 + y_1$ can lead to the case that x_1 learns $x_2 > y_1$. Similarly, x_1 can learn the relation among other bids, but not the complete order. If $x_1 + x_2 < x_1 + y_2$, x_1 can further learn that $x_2 < y_2$. Then x_1 learns $y_1 < x_2 < y_2$. The auction is detected as incorrect, so the smaller-than relation between the winner and a verifier happens only once.

g: $x_1 + x_2 + x_3 > x_1 + y_1 + x_3$ can lead to the case that x_1 learns $x_2 > y_1$. Again, x_1 can learn the relations of other bids, but not the entire order. If $x_1 + x_2 + x_3 < x_1 + y_2 + x_3$, x_1 can further learn that $x_2 < y_2$. Then x_1 learns that $y_1 < x_2 < y_2$. The auction is detected as incorrect, so the less-than relation of the winner compared to a verifier only exists once. In another case, $x_1 + x_2 + x_3 < x_1 + y_1$ can result that x_1 learns $x_2 + x_3 < y_1 \Rightarrow x_2 < y_1, x_3 < y_1$.

In cases b and c, a bidder may learn an upper bound or a lower bound of some bids. We now discuss whether it is possible for a bidder to learn both. Assume x_1 and x_2 are the two verifiers coexisting in many maximal independent sets. We want to know whether it is possible for x_1 to restrict the range of x_2, such as $F_2(x_1) < x_2 < F_1(x_1)$, where F_1 and F_2 are two functions known to x_1.

Proposition 4. *A curious bidder can learn an upper bound or a lower bound of some bids, but never both, through the inequalities revealed through different comparisons.*

Proof. If x_1 and x_2 both belong to the sets of verifiers during many comparisons, x_1 can learn that $x_1+x_2+V_1 > V_2$ and $x_1+x_2+V_3 < V_2$ where V_1, V_2 and V_3 are the other verifiers' inputs. If x_1 can learn $V_2 - V_1 - x_1 < x_2 < V_2 - V_3 - x_1$, x_1 must have the knowledge of V_1, V_2 and V_3. To learn V_1, V_2 and V_3, x_1 must collude with other verifiers to learn the inputs from other verifiers. So unless x_1 has collusion with both the winners and other verifiers, x_1 cannot learn x_2 by restricting both the upper bound and lower bound of x_2.

If x_1 belongs to both winners and verifiers during many comparisons, x_1 can also learn that $x_2+V_1 > V_2$ and $x_2+V_3 < V_2$. In this case, b can learn $V_2 - V_1 < x_2 < V_2 - V_3$. Unless x_1 learns V_1, V_2 and V_3 through collusion, x_1 cannot learn both the upper bound and lower bound of x_2. □

The above discussion on the verification correctness and information leakage leads to Theorem 4.

Theorem 4. *Algorithm 5 to verify winner determination is*

1. *Correct: It can verify whether the winner determination is correctly implemented by the auctioneer.*
2. *Privacy-Preserving: It protects the privacy of the bidders by concealing individual bids, unless in extreme cases where the bids are very small or the number of winners or verifiers is very specific (as Section 7.1.2* a *and* d*). After learning the relations of the total valuations between the winner and the other maximal independent sets, a bidder may partially learn: (a) the relations between a winner and a verifier (as Section 7.1.2* b*,* c*,* f *and* g*); (b) the upper or lower bounds of another bidder (as Section 7.1.2* b *and* c*), but not both.*

Proof. For verification correctness, if $\sum_{i=1}^{N_w} v_i - \sum_{j=1}^{N_s} v_j \geq 0$ and the auctioneer publishes the winning independent set as s_W, then the auction is verified as correct. Otherwise, the misbehaviour of the auctioneer is detected.

For privacy, the only system outputs in Algorithm 5 are the relations between the two groups of inputs. Learning the relations of the total valuations between the winner and all other maximal independent sets is necessary to convince all verifiers that the auction is correct. As Section 7.1.2 b, c, f and g, a curious bidder may learn relations of a winner (or verifier) compared to some verifiers (or winners), but not the sorted order. As Proposition 4, a curious bidder may learn the upper bound or lower bound of some bids, but not both.

Partially learning the relations of other bids, as well as the upper or lower bounds of other bids does not necessarily lead to information leaking on the individual bids. Bid leakage happens only when $N_s = x_1 - 1$, $N_w = y_1 - 1$. Those scenarios represent a limitation of the verification scheme. □

7.1.3 Reducing Comparisons

If the winners all participate in the verification process individually, each winner will have to supply its valuation as the input to a secure multiparty comparison N_{MIS} times. We propose another method for them to reveal some information that is related to their total valuation only once to save the computation resources. Intuitively, we can design a method to collect the inputs from the winners as their total valuation. If the winners collectively publish their total valuation through another secure multiparty computation $f(TW) = \sum_{i=1}^{N_w} v_i$, then the other bidders can accept the total valuation of the winners as a single input to the verification. This method is denoted as Algorithm 6.

In this case, the winners only participate in the secure comparison once. Since we assume that the bidders are curious, they can still learn extra information as in Section 7.1.2. We use Table 7.2 to analyze the extra information leakage other than those of Section 7.1.2:

a: Since x_1 is the only winner, if it publishes its valuation, then all other verifiers can learn its bid.

b: In this scenario, x_1 and x_2 are the two winners. If they publish their total valuation, then they will learn each other's bid. If there is only one verifier y_1, then y_1 can learn x_1+x_2.

Algorithm 6 Verify Winner Determination with Reduced Comparisons of Winners (Input: Bids of the Bidders. Output: Whether the Winner Determination is Correct or Not

```
while A bidder $i$ is a winner of a VCG auction do
    $i$ supplies its bid $v_i$ into a secure multiparty addition
end while
The winners publish the secure addition result $f(TW) = \sum_{i=1}^{N_w} v_i$
while A bidder $j$ is not a winner of a VCG auction do
    $j$ supplies its bid $v_j$ into the secure multiparty computation
end while
The secure multiparty computation outputs 1, if $f(TW) - \sum_{j=1}^{N_s} v_j \geq 0$, outputs 0 if
    $f(TW) - \sum_{j=1}^{N_s} v_j < 0$
```

c: In this scenario, x_1, x_2 and x_3 are the three winners. If they publish their total valuation, then they will learn the total valuation of the other two.

d: Since y_1 is the only verifier, it can learn the total valuation of the winners. Note that this verifier cannot belong to any other maximal independent set based on the definition of maximal independent sets.

e: If there are only two verifiers y_1 and y_2, one of them can learn the upper bound or the lower bound by learning $y_1 + y_2 < \sum x_i$ or $y_1 + y_2 > \sum x_i$. Since the winners publish their total valuation $\sum x_i$, y_1 can learn that $y_2 < \sum x_i - y_1$ or $y_2 > \sum x_i - y_1$.

f: In this scenario, x_1 can learn the bid of x_2 if x_1 learns the total valuation $x_1 + x_2$. If $x_1 + x_2 > x_1 + y_1$, x_1 learns the upper bound of y_1. If $x_2 = 2$, x_1 learns $y_1 = 1$. x_1 can also learn the upper bound of y_1.

g: In this scenario, x_1 can learn the total valuation of other winners, such as $x_2 + x_3$ if x_1 learns the total valuation $x_1 + x_2 + x_3$. $x_1 + x_2 + x_3 > x_1 + y_1$ can result that x_1 learns upper bound of y_1: $x_2 + x_3 > y_1$. If $x_2 = 2$, x_1 learns $y_1 = 1$. x_1 can also learn the upper bound of y_1.

To summarize, when the winners publish their total valuation, the extra information that may be leaked other than those discussed in Section 7.1.2 include:

1. The bid of the single winner.

2. The total valuation of other winners. If there are only two winners, the bid of the other winner.

3. Extra information leakage about the upper or the lower bounds of another bidder.

Knowing the total valuation of other winners for a group of three or more winners does not reveal the individual bids of other winners. However, learning the total valuation of other winners can result in the leakage of the bid of the other verifier if a winner happens to be one of the two verifiers. So our goal is to design a verification scheme where the winners still publish some information only once to save the computation cost, and the total valuation of the winners, including the case of only one or two winners, is protected.

7.1.4 Privacy-Oriented Comparison

While publishing total valuation of the winners can reduce their computation cost, this method will incur extra information leakage, especially when there is only one or two winners in the winning independent set. We propose a privacy-oriented comparison scheme where the winners, no matter how many of them, can publish some information to the other maximal independent sets once without revealing their individual valuations.

After the enumeration of the maximal independent sets, the number of bidders in different maximal independent sets is public. We denote the maximum number of bidders in a maximal independent set at N_B^M. Then each winner will generate N_B^M different combinations of random numbers, the sum of each combination is equal to a random number it holds. An intuitive way to generate the shares is to generate one share per verifier per maximal independent set. However, this method requires a winner to generate a large number of shares. To reduce the computation overhead, a winner i can generate a random number $r(i)$ and generate N_B^M groups of random numbers:

$$r(i) = \begin{cases} r(i)_1^1 \\ r(i)_2^1 + r(i)_2^2 \\ r(i)_3^1 + r(i)_3^2 + r(i)_3^3 \\ \dots \\ r(i)_{N_B^M}^1 + r(i)_{N_B^M}^2 + \dots + r(i)_{N_B^M}^{N_B^M} \end{cases} \tag{7.1}$$

Each group responds to a subset of all the losing maximal independent sets with the same number of bidders. For two different losing maximal independent sets with the same number of bidders, the generated random numbers can be reused to save computation and communication cost. Each winner only calculates one group of shares for all the maximal independent sets with the same size. Each verifier only receives one share for all the maximal independent sets of the same size. The maximum number of shares a verifier holds is M_B rather than 2^{M_B}. To make sure a verifier only receives one version of a share in the groups of bidders with the same size (number of bidders), each winner i first checks whether it has shared $r(i)$ with a verifier j for $r(j)_2^1, r(j)_3^1, r(j)_4^2, \dots$. If some of the verifiers in a maximal independent set already received their share from the other maximal independent sets with the same number of bidders, the other bidders' share will be generated from the leftover of $r(i)$.

We now study whether it is always possible for the groups of bidders with the same size to share the same group of random shares. We present the result in Theorem 5.

Theorem 5. *It is always possible to assign only one group of shares to the groups of bidders with the same size.*

Proof. We assume any two maximal independent sets have the same number of bidders: $x_1, x_2, \dots, x_{n-1}, x_n$ and $y_1, y_2, \dots, y_{n-1}, y_n$. We sort the two sets, so the elements in the two sets that share the same bidders are $x_i = y_i, \forall i \in [1, l)$. None of the other elements in $x_l, \dots, x_n$ and $y_l, \dots, y_n$ can be connected to the duplicate elements. For the other elements in the two sets, any element in $x_l, \ldots, x_n$ has to be connected to at least one of $y_l, \ldots, y_n$, otherwise this element can be added to $y_1, y_2, \ldots, y_n$ as a maximal independent set, contradicting the fact that $y_1, y_2, \ldots, y_n$ is a maximal independent set. For the same reason, any element in $y_l, \ldots, y_n$ has to be connected to at least one of $x_l, \ldots, x_n$.

The connections between elements of the two groups $x_l, \ldots, x_n$ and $y_l, \ldots, y_n$ are at least $n - l$ pairwise connections that connect all the elements in the two groups, or these $n - l$ pairwise connections plus some other connections between the two groups. Otherwise, if there exists an element in a group that does not connect to any element in the other group, this element can be added to the other group to invalidate its definition of maximal independent set. So we can at least find $n-l$ pairwise connections that cover all the elements of $x_l, \ldots, x_n$ and $y_l, \ldots, y_n$, and assign the same share for the two connected elements. Since the two connected elements cannot coexist in the same maximal independent sets, the same share cannot coexist in the same secret sharing $r(i)^1_n, r(i)^2_n, \ldots, r(i)^n_n$.

Since l can be any value that is $0 \leq l \leq n$, the above analysis applies to all possibilities of the number of duplicate elements. For more than two maximal independent sets, $x_1, x_2, \ldots, x_n; y_1, y_2, \ldots, y_n; \ldots; z_1, z_2, \ldots, z_n$, and each of them share the same l duplicates, all the other elements can be connected by at least $n - l$ connections that connect one element per maximal independent set. As long as we assign the same share for a connection that connects one element per maximal independent set, it is always possible to assign the same group of shares to the maximal independent sets. □

After sharing the random number combinations, a winner i publishes the sum of its valuation v_i and its random number $r(i)$ to other winners. Then they each calculate the sum of all the $v_i + r(i)$ as the input to the SMC as Algorithm 7.

We also use Table 7.2 to analyze the extra information leakage other than those of Section 7.1.2:

a: If there is only one winner and one verifier, the bid of the winner is leaked to the verifier.

Algorithm 7 Verify Winner Determination with Privacy-Oriented Comparison (Input: Bids of the Bidders. Output: Whether the Winner Determination is Correct or Not

```
while  A bidder $i$ is a winner of a VCG auction do
    $i$ generates a random value $r(i)$
    $i$ supplies $v_i + r(i)$ into a secure multiparty addition
    $i$ calculates $r(i)_1^1, r(i)_2^1, r(i)_2^2, \ldots, r(i)_{N_B^M}^1 + r(i)_{N_B^M}^2 + \cdots + r(i)_{N_B^M}^{N_B^M}$ as random shares for $r(i)$
end while
The winners publish the secure addition result $f(TW') = \sum_{i=1}^{N_w}(v_i + r(i))$
while  A bidder $j$ is not a winner of a VCG auction do
    while  A bidder $i$ is a winner of a VCG auction do
        $i$ supplies $r(i)_n^j$, part of $r(i)$ to $j$ according to the size of the maximal independent set $n$ and (7.1)
    end while
    $j$ supplies its bid $v_j$ plus its share into a SMC
end while
The SMC outputs 1, if $f(TW') - \sum_{j=1}^{N_s}(v_j + r(i)_n^j) \geq 0$, outputs 0 if $f(TW') - \sum_{j=1}^{N_s}(v_j + r(i)_n^j) < 0$
```

If there is only one winner x_1 and two verifiers y_1 and y_2. x_1 shares $r(x_1)_2^1$ with y_1, and $r(x_1)_2^2$ with y_2. Then x_1 supplies $x_1 + r(x_1)$, y_1 supplies $y_1 + r(x_1)_2^1$, e supplies $y_2 + r(x_1)_2^2$ as the inputs for the secure comparison. If $x_1 + r(x_1) - (y_1 + r(x_1)_2^1) - (y_2 + r(x_1)_2^1) \geq 0 \Leftrightarrow x_1 - y_1 - y_2 \geq 0$, the winner determination is verified, and *vice versa*. x_1 is not leaked to y_1 or y_2.

b: There are two winners x_1 and x_2 and only one verifier y_1. y_1 receives shares $r(x_1)_1^1 = r(x_1)$ from x_1 and $r(x_2)$ from x_2. In this case, x_1 and x_2 each only knows $x_1 + x_2 + r(x_1) + r(x_2)$. x_1 and x_2 cannot learn each other's bids. y_1 can learn $x_1 + x_2$. Unless there is a collusion between x_1 (or x_2) and y_1, x_2 (or x_1) is protected.

c: x_1, x_2 and x_3 as the three winners, can only learn $x_1 + x_2 + x_3 + r(x_1) + r(x_2) + r(x_3)$, rather than the total valuation of other winners.

d: Since y_1 is the only verifier, it can learn the total valuation of the winners. Note that this verifier cannot belong to any other maximal independent set based on the definition of maximal independent sets.

e: No extra information about the bid is leaked other than those discussed in Section 7.1.2 e.

f: In this scenario, since x_1 cannot learn the bid of x_2 because x_1 does not know the total valuation $x_1 + x_2$, so x_1 cannot learn the upper bound or the upper bound of y_1.

g: In this scenario, since x_1 cannot learn the total valuation of other winners, such as $x_2 + x_3$ because x_1 does not know the total valuation $x_1 + x_2 + x_3$, so x_1 cannot learn the upper bound or the lower bound of y_1.

The above discussions on the information leakage leads to Theorem 6.

Theorem 6. *Using random numbers from the winners can achieve almost the same level of privacy protection as in the case of full winner participation, while reducing the computation cost. The only exception is the scenario where there is only one winner and one verifier.*

Proof. The extra information leakage discussed in Section 7.1.3 can be prevented by introducing the random share method. The bid of the single winner can be protected for two or more verifiers as discussed in Section 7.1.4 a. If there are only two winners, the bid of the other winner is also protected as discussed in Section 7.1.4 b. The extra upper or lower bounds are also unknown to a curious bidder as discussed in Section 7.1.4 f and Section 7.1.4 g. □

7.2 Verifying Prices

In the pricing phase, each winner in the winning independent set has its price calculated as the difference between the total valuation of the winning independent set and the total valuation of another winning independent set when the winner is absent from the auction. We assume that there are N_W bidders in the winning independent set for the original auction. The maximal independent sets without the winner being removed do not change in the pricing verification process. For those maximal independent sets that previously have the winner, removing the winner results in an independent set that may or may not be still maximal — and that will be checked during the verification. The remaining elements in a independent set without a winner may belong to other maximal independent sets. Hereby, after removing a winner from all the maximal independent sets it belongs to, we shall check whether the remaining elements compose a maximal independent set first.

7.2.1 Verification Algorithm

Recall that the goal is to verify whether the price p_a for a winner a is equal to the damage caused to other bidders by the winner's presence. For all the $\sum_{i=1}^{N_w} v_i - \sum_{j=1}^{N_a} v_j - p_a$, there should be only one that equals 0, and all others shall be larger than 0.

Theorem 7. *The method of checking whether $\sum_{i=1}^{N_w} v_i - \sum_{j=1}^{N_a} v_j - p_a = 0$ exists for only one, and all other comparisons are $\sum_{i=1}^{N_w} v_i - \sum_{j=1}^{N_a} v_j - p_a > 0$, can verify whether the pricing is correctly implemented by the auctioneer.*

Proof. By definition of VCG prices, $\sum_{i=1}^{N_w} v_i - \sum_{j=1}^{N_a} v_j - p_a = 0$ only exists for the highest maximal independent set N_a. For all other maximal independent sets without a, $\sum_{j=1}^{N_a} v_j + p_a < \sum_{i=1}^{N_w} v_i$.

If the auctioneer charges the winner a higher price, there will be an instance of $\sum_{j=1}^{N_a} v_j + p_a > \sum_{i=1}^{N_w} v_i$. If the auctioneer colludes with a winner by charging a lower price, all the maximal independent sets without a will have $\sum_{j=1}^{N_a} v_j + p_a < \sum_{i=1}^{N_w} v_i$. Therefore, the auctioneer has to charge the price correctly following the requirement of VCG auctions. Otherwise, the one equal, all others less relations will not hold. □

Each maximal independent set shall expect the result to be greater-than, with one exception of equality. Once a maximal independent set observes equality, the bidders in this set shall broadcast to all the other bidders. If more than one maximal independent set broadcast equality, the pricing is declared as fraudulent and the verification process terminates. If a less-than inequality is detected, the verification similarly terminates.

We propose two methods for pricing verification. One aims to protect the privacy of the bidders in the best capacity. The other is more computationally efficient by reusing intermediate computation.

7.2.2 Privacy-Oriented Comparison

Algorithm 8 Privacy-Oriented Pricing Verification (Input: Bids of the Bidders, Price of a Winner p_a. Output: Whether p_a is Correct or Not

```
while A bidder $i$ is a winner of a VCG auction do
    $i$ generates a random value $r(i)$
    $i$ supplies $v_i + r(i)$ into a secure multiparty addition
    $i$ calculates $r(i)^1_1, r(i)^1_2, r(i)^2_2, \ldots, r(i)^1_{N_B^M} + r(i)^2_{N_B^M} + \cdots + r(i)^{N_B^M}_{N_B^M}$ as random shares for $r(i)$
end while
The winners publish the secure addition result $f(TW') = \sum_{i=1}^{N_w}(v_i + r(i))$
while A bidder $j$ is the winner $a$, or it belongs to a maximal independent set when a winner $a$ is removed do
    if The bidder is the winner $a$ then
        $a$ sets $v_a = p_a$
    end if
    while A bidder $i$ is a winner of a VCG auction do
        $i$ supplies $r(i)^j_n$, part of $r(i)$ to $j$ or $a$ according to the size of the maximal independent set $n$ and (7.2)
    end while
    $j$ supplies its bid $v_j$ plus its share into a SMC
end while
The SMC outputs $f(TW') - \sum_{j=1}^{N_a}(v_j + r(i)^j_n)$
The pricing is correct, iff. $\forall f(TW') - \sum_{j=1}^{N_a}(v_j + r(i)^j_n)$, one of them is equal to 0, all other are greater than 0; otherwise the pricing is incorrect
```

The first comparison method, in Algorithm 8, focuses on privacy protection. Prices charged to the winners are only known to themselves. We can use the similar method with SMC, except that a winner a with price p_a also acts as a verifier with input p_a to a SMC after the removal of a. In this case, a holds p_a as well as $v_a + r(a)$. For each $r(a)$, the number of random numbers that can add up to $r(a)$ will be the length of the maximal independent sets plus one:

$$r(a) = \begin{cases} r(a)^1_2 + r(a)^2_2 \\ r(a)^1_3 + r(a)^2_3 + r(a)^3_3 \\ \cdots \\ r(a)^1_{N^{M'_B}+1} + r(a)^2_{N^{M'_B}+1} + \cdots + r(a)^{N^{M'_B}+1}_{N^{M'_B}+1} \end{cases} \tag{7.2}$$

We denote the algorithm of the privacy-focused pricing verification as Algorithm 8.

For the extra information leakage, we discuss the scenarios where the curious bidder belongs to a highest maximal independent set when a winner is removed. In these scenarios, a bidder may learn extra information by learning the equation.

Role of A Curious Bidder	Scenario
Only in a Maximal Independent Set	One Winner (h)
Both in the Winner Set and in a Maximal Independent Set	Two Winners (i)
	Three or More Winners (j)

Table 7.3: Different Scenarios During the Pricing Verification Process

h: There is only one winner x_1. For all the maximal independent sets without x_1, the highest one is also a single bidder y_1. In this case, x_1 supplies $x_1 + r(x_1)$ as the input from the winners. y_1 learns $r(x_1)^1_2$ and $x_1 + r(x_1)$. It still cannot learn x_1 without knowing p_1.

i: For two winners x_1 and x_2, the removal of x_1 will bring x_2 as the only member of the maximal independent set after the removal of x_1. Then the desired verification result is $x_1 + x_2 = x_2 + p_1$. The verification process is as follows. x_1 supplies $r(x_1)^1_2$ to x_2 and keeps $r(x_1)^2_2$ to itself. x_2 supplies $r(x_2)^2_2$ to x_1 acting as the verifier, and keeps $r(x_2)^1_2$ to itself. Then x_1 and x_2 calculates $x_1 + x_2 + r(x_1) + r(x_2)$ as the input from the winners. x_2 acts as a verifier by supplying $x_2 + r(x_1)^1_2 + r(x_2)^1_2$. x_1 also acts as a verifier by supplying $p_1 + r(x_1)^2_2 + r(x_2)^2_2$. If $x_1 + x_2 + r(x_1) + r(x_2) = x_2 + r(x_1)^1_2 + r(x_2)^1_2 + p_1 + r(x_1)^2_2 + r(x_2)^2_2$, x_2 is verified as the highest maximal independent set among all the maximal independent sets without x_1. During this process, x_2 learns $x_1 + r(x_1)$ and $r(x_1)^1_2$. However, it cannot learn x_1 without knowing p_1. x_1 also learns $x_2 + r(x_2)$ and $r(x_2)^2_2$, but cannot learn x_2.

j: For three winners x_1, x_2 and x_3, the removal of x_1 will bring x_2 and x_3 as the members of the maximal independent set after the removal of x_1. Then the desired verification result is $x_1 + x_2 + x_3 = x_2 + x_3 + p_1$. The verification process is as follows. x_1 supplies $r(x_1)^1_3$ to x_2, $r(x_1)^2_3$ to x_3, and keeps $r(x_1)^3_3$ to itself. x_2 supplies $r(x_2)^3_3$ to x_1 acting as the verifier, $r(x_2)^2_3$ to x_3, and keeps $r(x_2)^1_3$ to itself. x_3 supplies $r(x_3)^3_3$ to x_1 acting as the verifier, $r(x_3)^1_3$ to x_2, and keeps $r(x_3)^2_3$ to itself. Then x_1, x_2 and x_3 calculate $x_1+x_2+x_3+r(x_1)+r(x_2)+r(x_3)$ as the input from the winners. x_2 acts as a verifier by supplying $x_2 + r(x_1)^1_3 + r(x_2)^1_3 + r(x_3)^1_3$. x_3 acts as a verifier by supplying $x_3 + r(x_1)^2_3 + r(x_2)^2_3 + r(x_3)^2_3$. x_1 also acts as a verifier by supplying $p_1 + r(x_1)^3_3 + r(x_2)^3_3 + r(x_3)^3_3$. If $x_1 + x_2 + x_3 + r(x_1) + r(x_2) + r(x_3) = x_2+r(x_1)^1_3+r(x_2)^1_3+r(x_3)^1_3+x_3+r(x_1)^2_3+r(x_2)^2_3+r(x_3)^2_3+p_1+r(x_1)^3_3+r(x_2)^3_3+r(x_3)^3_3$, x_2+x_3 is verified as the highest maximal independent set among all the maximal independent sets without x_1. During this process, x_2 learns $x_1+x_2+x_3+r(x_1)+r(x_2)+r(x_3)$ and $r(x_1)^1_3, r(x_3)^1_3$. However, it cannot learn x_1 or x_3. x_3 learns $x_1 + x_2 + x_3 + r(x_1) + r(x_2) + r(x_3)$ and $r(x_1)^2_3, r(x_2)^2_3$. However, it cannot learn x_1 or x_2. x_1 learns $x_1+x_2+x_3+r(x_1)+r(x_2)+r(x_3)$ and $r(x_2)^3_3, r(x_3)^3_3$. However, it cannot learn x_2 or x_3.

In summary, as long as the price is kept private, the bidders cannot learn the bids of other bidders by taking advantage of the equation where the total valuation of the winners equals to the total valuation of maximum independent set after the removal of the winner plus the price.

7.2.3 Efficiency-Oriented Comparison

The second comparison method focuses on computational efficiency. We note that the maximal independent set based comparisons in price verification may contain a substantial level of redundancy. If we assume that the prices charged to the winners are public, then we can enable the bidders to reuse previously computed comparison results. We can further even combine price verification and winner verification to improve system efficiency.

Recall that the auctioneer is verified as correct if and only if $\sum_{i=1}^{N_w} v_i - \sum_{j=1}^{N_a} v_j - p_a = 0$ exists for only one, and all other comparisons are $\sum_{i=1}^{N_w} v_i - \sum_{j=1}^{N_a} v_j - p_a > 0$. In the privacy-oriented comparison where the price p_a is kept secret, the winner a puts its price p_a into the same group of verifiers, aiming to compare $\sum_{i=1}^{N_w} v_i$ and $\sum_{j=1}^{N_a} v_j - p_a = 0$. If p_a is public, a can output $\sum_{i=1}^{N_w} v_i - p_a$ with the random numbers to compare with $\sum_{j=1}^{N_a} v_j$. We denote the algorithm of the efficiency-oriented pricing verification as Algorithm 9.

Algorithm 9 Efficiency-Oriented Pricing Verification (Input: Bids of the Bidders, Price of a Winner p_a. Output: Whether p_a is Correct or Not

```
while A bidder $i$ is a winner of a VCG auction do
    $i$ generates a random value $r(i)$
    $i$ supplies $v_i + r(i)$ into a secure multiparty addition
    $i$ calculates $r(i)^1_1, r(i)^1_2, r(i)^2_2, \ldots, r(i)^1_{N_B^M} + r(i)^2_{N_B^M} + \cdots + r(i)^{N_B^M}_{N_B^M}$ as random shares for $r(i)$
end while
The winners publish the secure addition result $f(TW') = \sum_{i=1}^{N_w}(v_i + r(i))$ and their prices $p_a, \ldots$
while A bidder $j$ belongs to a maximal independent set when a winner $a$ is removed do
    while A bidder $i$ is a winner of a VCG auction do
        $i$ supplies $r(i)^j_n$, part of $r(i)$ to $j$ according to the size of the maximal independent set $n$ and (7.1)
    end while
    $j$ supplies its bid $v_j$ plus its share into a SMC
end while
The SMC outputs $f(TW') - \sum_{j=1}^{N_a}(v_j) - p_a$
The pricing is correct, iff. $\forall f(TW') - \sum_{j=1}^{N_a}(v_j) - p_a$, one of them is equal to 0, all other are greater than 0; otherwise the pricing is incorrect
```

The system efficiency is improved along two directions:

1. For two prices $p_a > p_b$, when the maximal independent set after the removal of b is the same as that after removing a, if the total valuation of the winners $\sum_{i=1}^{N_w} v_i$ subtracting the price p_a is greater than the total valuations of the maximal independent set after removal of a, then the total valuation of the winners subtracting the price p_b must also be greater than $\sum_{j=1}^{N_a} v_j$.

2. If the total valuation of the winners $\sum_{i=1}^{N_w} v_i$ subtracting the price p_a is at least the total valuations of the maximal independent set after removal of a, then

due to $p_a > 0$, we have $\sum_{i=1}^{N_w} v_i > \sum_{j=1}^{N_a} v_j$.

The first observation can be used when a maximal independent set exists in both the verification process for the prices of a and b. This relation can be extended to all prices charged to the winners. The winners first sort their prices and then each maximal independent set can only compare with the highest price first. If the relation is less-than, the auction is detected as incorrect. If the relation is equal-to or greater-than, the same maximal independent set does not need to compare with other prices.

The second observation can be used to combine the two verification processes for winner determination and pricing together. Some maximal independent sets do not contain the winners and they remain the same in the two processes. With the verification of pricing coming first, the bidders first compare the total valuation subtracting the price first. If $\sum_{i=1}^{N_w} v_i - p_a < \sum_{j=1}^{N_a} v_j$, the auction is detected as incorrect. If $\sum_{i=1}^{N_w} v_i - p_a = \sum_{j=1}^{N_a} v_j$ or $\sum_{i=1}^{N_w} v_i - p_a > \sum_{j=1}^{N_a} v_j$, the bidders can also learn that $\sum_{i=1}^{N_w} v_i > \sum_{j=1}^{N_a} v_j$, which is needed for the winner determination verification process.

This comparison method can improve the system efficiency by reducing the number of comparisons. However, by publishing the prices charged to the winners, individual bids may be leaked in the two scenarios Section 7.2.2 h and Section 7.2.2 i discussed above. There is an inherent trade-off between privacy protection and computational efficiency. If the winners are not willing to share their prices and there are some maximal independent sets with only one or two bidders, the efficiency-oriented method is not applicable.

7.3 Sufficiency of Only Using Maximal Independent Sets

Since all the bids are positive integers, the total valuation of a maximal independent set is greater than any subset of it. For the verification of pricing, if the total valuation of the winners is greater than the total valuation of every maximal independent set, then it is greater than the total valuation of any independent set. Hence we have the Corollary 1.

Corollary 1. *The verification process can verify the results of winner determination and pricing with only maximal independent sets, without comparing with other independent sets*

7.4 Incentive for the Bidders

In our proposed methods for verifying winner determination and pricing, different bidders have different incentives. In the winner determination verification process, all losing bidders have a natural incentive to verify the correctness of the auction, for which they need assistance from the winners. The winners can be very active in the verification process by supplying their individual bids for every comparison (as Section 7.1.1), or be less active by supplying the total valuation as well as the random numbers, and provide the secret shares for the verifiers in maximal independent sets of different lengths (Section 7.1.4). In the latter case, the winners only supply their input to the verification process once.

In the pricing verification process, winners have a natural incentive to verify whether the prices charged to them are correct, for which they need assistance from losing bidders. The losing bidders are expected to participate in all the comparisons with their maximal independent sets. To improve efficiency, they can reduce the number of comparisons if they know the prices charged to the winners (Section 7.2.3). The comparisons can also be implemented before the verification of winner determination to reduce the overhead (Section 7.2.3).

Winning and losing bidders in the VCG spectrum auctions are therefore motivated to enter such a mutually benefiting cooperation, by participating both verification phases.

During the two phases of verification for VCG auctions, the winners and the verifiers need to help each other to achieve their verification goals. These mutual interest can be an incentive for all the bidders no matter whether they are the winners or not. In addition, the verification processes aim to detect whether the auction is correctly implemented by the auctioneer or not. Once an auctioneer is detected as faulty, it will not be trusted in the future auctions. Thus, the common goal of identifying the misbehaviour of the auctioneer is another incentive for the bidders.

7.5 Performance Evaluation

7.5.1 Efficiency Evaluation

We implement the verification methods for winner determination and pricing in FairplayMP [10]. FairplayMP is the first framework that allows to implement generic SMC in a high level language. Since the run time has linear dependency on the size of the circuit, we only evaluate the relations between the size of circuit and the number of inputs. Figure 7.1 illustrates the relations in the winner determination and pricing verifications. We can observe that the run time has linear dependency on the number of inputs in the SMC, in verification methods for both winner determination and pricing phases; the pricing verification costs more resources than the winner determination verification.

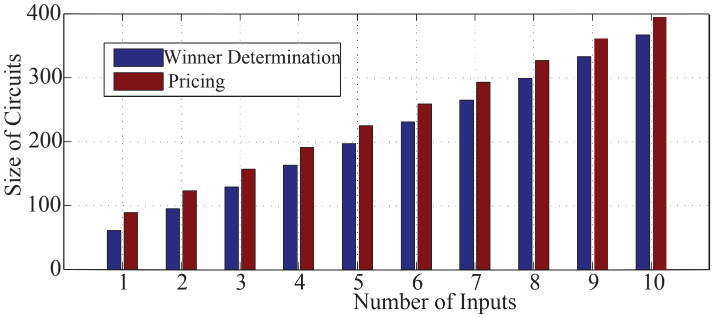


Figure 7.1: Relations between the Size of Circuits and the Number of Inputs.

7.5.2 Reducing Number of Comparisons in Winner Determination Verification

In Section 7.1, we proposed two methods of comparing the total valuation of a winning independent set with other maximal independent sets: one with the winners participating in all the comparisons (as in Section 7.1.1), the other with the winners publishing their total valuation with random numbers (as in Section 7.1.4). Now we want to observe how many comparisons can be saved when the winners only participate in a secure addition once to calculate their total valuation with random numbers. Figure 7.2 illustrates the relations between the number of bidders and the number of comparisons in simulation results in a random graph.

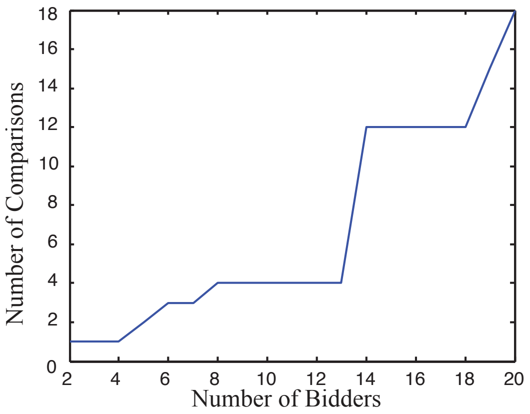


Figure 7.2: Relations between the Number of bidders and the Number of Comparisons in a Random Graph.

The method to verify winner determination in Section 7.1.4, where the winners publish their total valuation with random numbers, can reduce the number of secure comparisons, compared to the method in Section 7.1.1 where the winners participate in all the comparisons.

7.5.3 Reducing Number of Shares in Secret Sharing

In Section 7.1.4, we introduced a privacy-oriented comparison with secret sharing of random numbers generated by the winners. In contrast to the intuitive way of generating one share per verifier per maximal independent set, we proposed the secret sharing method as in (7.1). We simulate the enumeration of maximal independent sets and the sharing of random numbers on conflict graphs with different number of verifiers. Figure 7.3 illustrates the comparisons of these two methods.

Our proposed secret sharing methods as in (7.1) can significantly reduce the number of shares generated for the verifiers. The more verifiers, the better efficiency improvement.

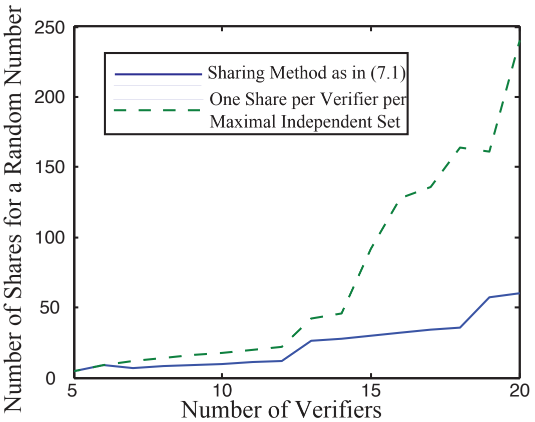


Figure 7.3: Comparison of Two Secret Sharing Methods.

7.5.4 Reducing Number of Comparisons in Pricing Verification

In Section 7.2.3, we introduced an efficiency-oriented method to reduce the comparisons during the verification process. Figure 7.4 illustrates the number of comparisons with (1) no improvement of efficiency; (2) efficiency improvement based on observation 1; (3) efficiency improvement based on observation 2; and (4) efficiency improvement based on both. For the winners, the two observations in Section 7.2.3 can be applied to reduce the number of comparisons.

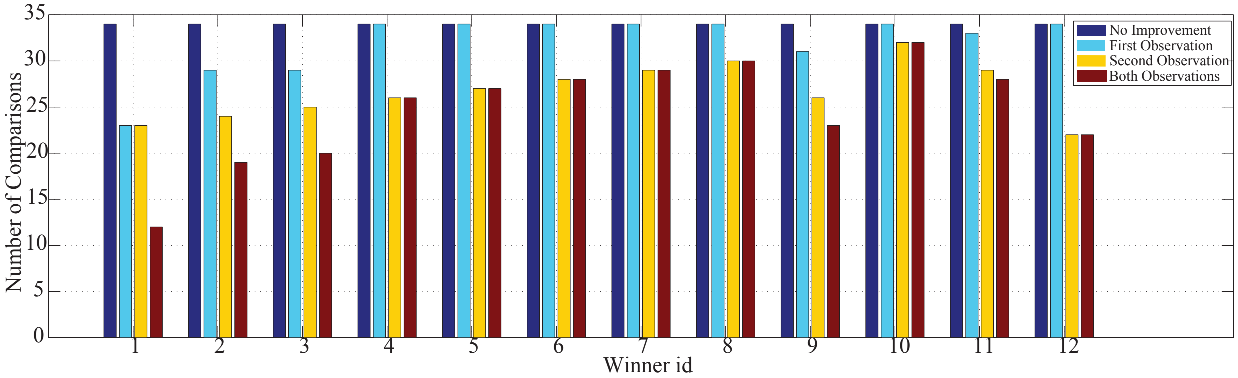


Figure 7.4: Number of Comparisons in Pricing Verification.

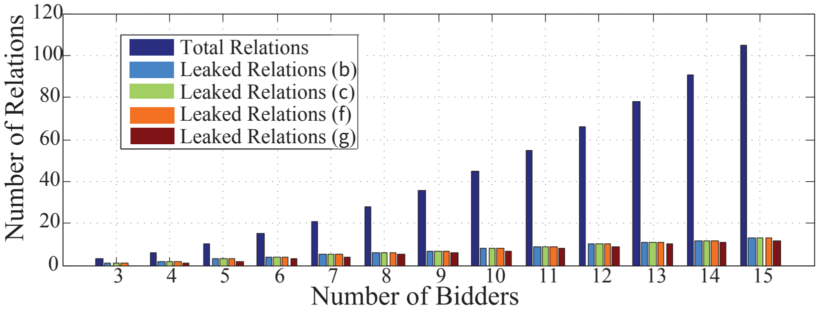


Figure 7.5: Number of Leaked Relations During Comparisons.

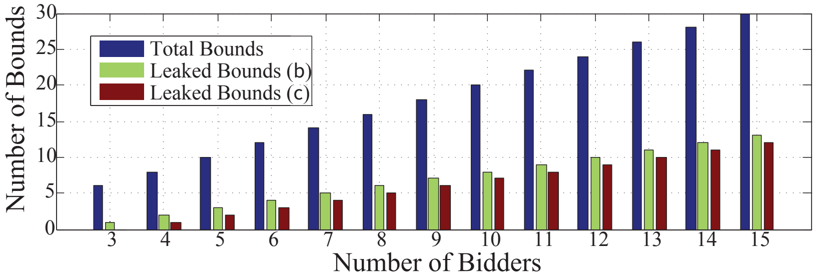


Figure 7.6: Number of Leaked Bounds During Comparisons.

7.5.5 Information Leakage Evaluation

In Section 7.1.2, we discussed information leakage after a bidder learns the results of many comparisons. We simulate the number of relations and bounds (upper or lower) leaked during the verification process as in Figure 7.5 and Figure 7.6.

The comparisons to verify winner determination as in Section 7.1.1 can only partially leak the relations between bidders, as well as the upper or lower bounds of other bidders. As the number of bidders increases, the probabilities of the relations and bounds to be leaked will decrease.

7.6 Concluding Remarks

In this Chapter, we proposed the first fully distributed scheme to verify whether a VCG spectrum auction is correctly implemented by the auctioneer or not, without modifying the auction itself. In our system, we assume that a single identity system exists among all the secondary users. We also assume that all the secondary users use an out-of-band communication system to exchange control messages. In our adversary model, we assume that the secondary users themselves are honest by reporting truthful values. We also assume that there is no collusion between the auctioneer and the secondary users.

In our simulation process, we only implemented the system in a small scale. A future direction to extend this work can be a thorough experimental study in a real spectrum auction process, with different kinds of secondary users as bidders. Another future direction to extend this work can be a study on the verification methods for double spectrum auctions, where multiple primary users simultaneously submit their ask prices when the secondary users submit their bids to the auctioneer.

Another future direction to extend this work can be a study on more sophisticated malicious behaviours, such as

1. The malicious auctioneer may collude with some secondary users whose bids are low, aiming to get some side payments from the falsified winners. This is the limit of explicit manipulation. In this scenario, the inputs from the secondary users into a SMC may not be trustworthy. Extra security mechanisms are required to verify the auction results, including both winners and prices.

2. The malicious users can attack the whole distributed spectrum sensing and allocation process together, including the work presented in Chapter 5 and Chapter 6.

3. The malicious users can implement other security attacks to a CRN, such as primary user emulation attacks and jamming attacks into the control channels, as described in Section 3.4.

Chapter 8

CONCLUSION AND FUTURE DIRECTIONS

In this chapter, we conclude the thesis by summarizing the contributions made, and directions for future research.

8.1 Summary of the Thesis

We can summarize the contributions of this thesis as follows.

1. We studied SSDF attacks in CRNs, and proposed the first fully distributed security scheme *ReDiSen* to countermeasure SSDF attacks in cooperative sensing. Using well-designed reputation systems in the value update algorithms, *ReDiSen* can effectively improve the cooperative sensing performance in dynamic yet adversarial environments, despite the removal of the fusion centre. We proposed two methods of assigning reputation on value differences and received values. Theoretical analysis and simulation results both indicate that reputation can help honest nodes obtain higher cooperative sensing results when the primary user is transmitting, and lower cooperative sensing results when the primary user is not transmitting, as long as the majority of neighbours report correctly sensed values. The method of assigning reputation to received values is less effective compared to the method of assigning reputation to value differences since the improvements are less significant. The method of assigning reputation to received values can help honest nodes converge to consensus faster.

2. We proposed to use reputation as a pricing factor in the spectrum allocation process to incentivize cooperative sensing in distributed CRNs. The repu-

tation values are generated from both sensing accuracy and sensing participation. Both theoretical analysis and simulation results indicate that this method can incentivize secondary users to participate in more channels and report more accurate sensing results, in order to obtain lower prices in the spectrum allocation process. To countermeasure attacks in the reputation fusion process, where malicious nodes report spurious reputation values, we proposed a method with the help of other honest neighbours. Our methods, from cooperative spectrum sensing to reputation fusion then to spectrum allocation, are entirely distributed without a central authority, and are thus more applicable to distributed CRNs.

3. We proposed the first verification scheme for VCG spectrum auctions in cognitive radio networks. When the auctioneer misbehaves, our scheme can protect the integrity of VCG auctions by verifying the correctness of the auctioneer in the winner determination and pricing processes. Our method protects the privacy of individual bidders. Our method does not bring any new computation or communication to the auction itself. The optional verification and introducing no third party enable our verification scheme to be more applicable in the cognitive radio networks.

8.2 Limitations and Future Directions

This thesis has some limitations, such as

1. Our simulation is in a small scale, without an experimental study in a real CRN, with different kinds of devices as primary and secondary users.

2. In our adversary model, we assume that the malicious users attack in the same manner during a sensing session without collusion. Malicious users can im-

plement more sophisticated attacks. They can coordinate how to attack the system in a colluded manner, aiming to reduce the probabilities of being detected. They can attack the whole distributed spectrum sensing and allocation process together, including the work presented in Chapter 5, Chapter 6, and Chapter 7. They can also implement other security attacks to a CRN, such as primary user emulation attacks, as described in Section 3.4.

3. We assume that all the secondary users use an out-of-band communication system to exchange control messages, without considering potential jamming attacks into common control channels.

Below we list some of the possible future works.

1. A future direction to extend this work can be a thorough experimental study in a real CRN. The recommended parameters during the experiment process are presented in Section 5.5 and Section 6.5.

2. Another future direction is to explore how to achieve the security goals during the spectrum sensing and spectrum allocation process, when the malicious users attack in a sophisticated manner.

3. The cooperative sensing performance can be further improved, by enabling nodes to use second-hand reputation information from trustworthy neighbours about the nodes in the network that they have not interacted with. Such second-hand information needs to pass a deviation test in the reputation system. We also plan to explore other possible applications for reputation information in a computer communication system.

4. To improve system performance, we may use other information to help with the reputation update process. Even within a single neighbourhood, the distance

between two honest nodes may differ significantly. A node closer to the primary user has a higher sensed value compared with a node that is farther away from the primary user. These two nodes have a high chance to judge each other as malicious. In this case, the distance between two honest secondary users may be taken into the process of generating reputation. The farther away a neighbour is, the higher is the difference the two nodes may have on the sensed values. The success of this approach relies on the accuracy and overhead of the localization algorithm between secondary users.

5. VCG auctions have many extensions, such as double spectrum auctions where multiple primary users also submit their ask prices, to achieve other desired goals. Extending the verification methods to reflect other new auction mechanisms is another future direction.

Bibliography

[1] M. Abdelhakim, J. Ren, and T. Li, Reliable Cooperative Sensing in Cognitive Networks, *Proceedings of the 7th International Conference on Wireless Algorithms, Systems, and Applications (WASA)*, vol. 7405, pp.206-217, August 2012.

[2] I. F. Akyildiz, W-Y, Lee, M. C. Vuran, S. Mohanty, NeXt Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A Survey, *Computer Networks*, vol. 50, no. 13, pp. 2127-2159, September 2006.

[3] 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, July 2009.

[4] I. F. Akyildiz, B. F. Lo, and R.Balakrishnan, Cooperative Spectrum Sensing in Cognitive Radio Networks: A survey, *Physical Communication* vol. 4, no. 1, pp. 40-62, March 2011.

[5] S. Angel, and M. Walfish, Verifiable Auctions for Online Ad Exchanges, *Proceedings of the 2013 Annual conference of the ACM Special Interest Group on Data Communication (SIGCOMM 2013)*, pp. 195-206, August 2013.

[6] I. Atzeni, L. G. Ordóñez, G. Scutari, D. P. Palomar, and J. R. Fonollosa, Noncooperative and Cooperative Optimization of Distributed Energy Generation and Storage in the Demand-Side of the Smart Grid, *IEEE Transactions on Signal Processing*, vol. 61, no. 110, pp. 2454-2472, May 2013.

[7] G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Godor, and M. Street, Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead, *IEEE Communications Surveys and Tutorials*, vol. 14, no. 2, pp. 355-379, Second Quarter 2012.

[8] O. Bamasak, and N. Zhang, A Distributed Reputation Management Scheme for Mobile Agent-based E-commerce Applications, *Proceedings of the 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE2005)*, pp. 270-275, March 2005.

[9] D. Beaver, S. Micali, and P. Rogaway. The Round Complexity of Secure Protocols. *Proceedings of the 22nd Symposium on the Theory of Computing (STOC 1990)*, pp. 503-513, May 1990.

[10] A. Ben-David, N. Nisan, and B. Pinkas, FairplayMP - A System for Secure Multi-Party Computation, *Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS 2008)*, pp. 17-21, October 2008.

[11] M. Ben-Or, S. Goldwasser, and A. Widgerson, Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation, *Proceedings of the 20th Symposium on the Theory of Computing (STOC 1988)*, pp. 1-10, May 1988.

[12] K. Bian, and J. -M. Park, Security Vulnerabilities in IEEE 802.22, *Proceedings of the 4th Annual International Conference on Wireless Internet (WICON)*, pp. 1-9, October 2008.

[13] K. Bian, J. -M. Park, and R. Chen, A Quorum-based Framework for Establishing Control Channels in Dynamic Spectrum Access Networks , *Proceedings of the 15th ACM International Conference on Mobile Computing and Networking (MobiCom)*, pp. 25-36, September 2009.

[14] S. Buchegger and J. -Y. L. Boudec. Self-Policing Mobile Ad-Hoc Networks by Reputation Systems. *IEEE Communications Magazine*, vol. 43, no. 7, pp. 101-107, July 2005.

[15] J. M. Byskov. Enumerating Maximal Independent Sets with Applications to Graph Colouring, *Operations Research Letters*, vol. 32, no. 6, pp. 547-556, November 2004.

[16] L. Cao, and H. Zheng, Distributed Rule-Regulated Spectrum Sharing, *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 130-145, January 2008.

[17] C-Y. Chen, Y-H Chou, H-C Chao, and C-H Lo, Secure Centralized Spectrum Sensing for Cognitive Radio Networks, *Wireless Networks*, vol. 18, no. 6, pp. 667-677, August 2012.

[18] K-C. Chen, and R. Prasad, Cognitive Radio Networks, Wiley, 2009.

[19] R. Chen, J. -M. Park, and K. Bian, Robust Distributed Spectrum Sensing in Cognitive Radio Networks, *Proceedings of the 27th Annual IEEE International Conference on Computer Communications (INFOCOM 2008)*, pp. 31-35, April 2008.

[20] R. Chen, J-M. J. Park, and K. Bian, Robustness Against Byzantine Failures in Distributed Spectrum Sensing, *Computer Communications*, vol. 35, no. 17, pp. 2115-2124, October 2012.

[21] Z. Chen, L. Huang, L. Li, W. Yang, H. Miao, M. Tian, and F. Wang, PS-TRUST: Provably Secure Solution for Truthful Double Spectrum Auctions, *Proceedings of the 33rd Annual IEEE International Conference on Computer Communications (INFOCOM 2014)*, April 2014.

[22] E. Clarke, Multipart Pricing of Public Goods, *Public Choice*, vol. 11, no. 1, pp. 17-33, September 1971.

[23] L. E. Doyle, Essentials of Cognitive Radio, Cambridge University Press, 2009.

[24] A. A. El-Sherif, and K. J. R. Liu, Joint Design of Spectrum Sensing and Channel Access in Cognitive Radio Networks, *IEEE Transactions on Wireless Communications*, vol. 10, no. 6, pp.1743-1753, June 2011.

[25] R. Etkin, A. Parekh, and D. Tse, Spectrum Sharing for Unlicensed Bands, *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 3, pp. 517-528, April 2007

[26] F. Farmani, M.A. Jannat-Abad, and R. Berangi, Detection of SSDF Attack Using SVDD Algorithm in Cognitive Radio Networks, *Proceedings of the 3rd International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN2011)*, pp. 201-204, July 2011.

[27] O. Fatemieh, A. Farhadi, R. Chandra, and C. A. Gunter, Using Classification to Protect the Integrity of Spectrum Measurements in White Space Networks, *Proceedings of the 18th Annual Network and Distributed System Security Symposium (NDSS)*, pp. 1-12, February 2011.

[28] S. Forbes, Wireless Spectrum: Washington Is Clueless, *Forbes Magazine*, March 14, 2011.

[29] A. G. Fragkiadakis, E.Z. Tragos, and I. G. Askoxylakis, A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks, *IEEECommunications Surveys and Tutorials*, vol. 15, no. 1, pp. 428-445, First Quarter 2013.

[30] R. Gennaro, J. Katz, H. Krawczyk, and T. Rabin, Secure Network Coding Over the Integers, *Proceedings of the 13th International Conference on Practice and Theory in Public Key Cryptography (PKC 2010)*, vol. 6056, pp. 142-160, May 2010.

[31] A. Ghasemi, and E. S. Sousa, Collaborative Spectrum Sensing for Opportunistic Access in Fading Environment, *Proceedings of the First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2005)*, pp. 131-136, November 2005.

[32] A. Goldsmith, Wireless Communications, Cambridge University Press, pp.27-56, 2005.

[33] T. Groves, Incentives in Teams, *Econometrica: Journal of the Econometric Society*, vol. 41, no. 4, pp. 617-631, July 1973.

[34] A. Gopinathan, and Z. Li, Strategyproof Wireless Spectrum Auctions with Interference, *Proceedings of IEEE Global Communications Conference (GLOBECOM 2010)*, pp.1-5, December 2010.

[35] A. Gopinathan, and Z. Li, A Prior-Free Revenue Maximizing Auction for Secondary Spectrum Access, *Proceedings of the 30th Annual IEEE International Conference on Computer Communications (INFOCOM 2011)*, pp. 86-90, April 2011.

[36] A. Gopinathan, Z. Li, and C. Wu, Strategyproof Auctions for Balancing Social Welfare and Fairness in Secondary Spectrum Markets, *Proceedings of the 30th Annual IEEE International Conference on Computer Communications (INFOCOM 2011)*, pp. 3020-3028, April 2011.

[37] Y. Han, Q. Chen, and J-X. Wang, An Enhanced D-S Theory Cooperative Spectrum Sensing Algorithm against SSDF Attack, *Proceedings of 2012 IEEE 75th Vehicular Technology Conference (VTC Spring)*, pp. 1-5, May 2012.

[38] Z. Han, D. Noyato, W. Saad, T. Başar, and A. Hjørungnes, Game Theory in Wireless and Communication Networks, Theory, Models, and Applications, Cambridge University Press, 2011.

[39] H. Huang, Y. Sun, X-Y. Li, Z. Chen, W. Yang, H. Xu, Near-optimal Truthful Spectrum Auction Mechanisms with Spatial and Temporal Reuse in Wireless Networks, *Proceedings of the fourteenth ACM international symposium on Mobile ad hoc networking and computing (MobiHoc2013)*, pp. 237-240, July 2013.

[40] J. Huang, R. A. Berry, and M. L. Honig, Auction-based Spectrum Sharing, *ACM / Springer Mobile Networks and Applications (MONET) Journal*, vol. 11, no. 3, pp. 405-418, June 2006.

[41] Q. Huang, Y. Tao, and F. Wu, SPRING: A Strategy-Proof and Privacy Preserving

Spectrum Auction Mechanism, *Proceedings of the 32nd Annual IEEE International Conference on Computer Communications (INFOCOM 2013)*, pp. 827-835, April 2013.

[42] C. S. Hyder, B. Grebur, and L. Xiao, Defense against Spectrum Sensing Data Falsification Attacks in Cognitive Radio Networks, *Security and Privacy in Communication Networks*, vol. 96, pp. 154-171, September 2012.

[43] Industry Canada, Canadian Table of Frequency Allocations, http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/h_sf01678.html. Retrieved May 2014.

[44] J. Jia, Q. Zhang, Q. Zhang, and M. Liu, Revenue Generation for Truthful Spectrum Auction in Dynamic Spectrum Access, *Proceedings of the 10th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2009)*, pp. 3-12, May 2009.

[45] T. Jiang, H. Wang, and A. Athanasios, QoE-Driven Channel Allocation Schemes for Multimedia Transmission of Priority-Based Secondary Users over Cognitive Radio Networks, *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 7, pp. 1215-1224, August 2012.

[46] D. Johnson, M. Yannakakis, and C. H. Papadimitriou, On Generating All Maximal Independent Sets, *Information Processing Letters*, vol. 27, no. 3, pp. 119-123, March 1988.

[47] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, Secure Cooperative Sensing Techniques for Cognitive Radio Systems, *Proceedings of the IEEE International Conference on Communications (ICC 2008)*, pp. 3406-3410, May 2008.

[48] P. Kaligineedi, M. Khabbazian, and V. Bhargava, Malicious User Detection in a Cognitive Radio Cooperative Sensing System, *IEEE Transactions on Wireless Communications* vol. 9, no. 8, pp. 2488-2497, August 2010.

[49] P. Kasaki, M. Koivisto, and J. Nederlof, Homomorphic Hashing for Sparse Coefficient Extraction, *Proceedings of the 7th International Symposium on Parameterized and Exact Computation (IPEC 2012)*, pp.147-158, September 2012.

[50] M. Kinateder, and K. Rothermel, Architecture and Algorithms for a Distributed Reputation System, *Proceedings of the First International Conference on Trust Management (iTrust 2003)*, pp. 1-16, May 2003.

[51] Y. R. Kondareddy, P. Agrawal, and K. Sivalingam, Cognitive Radio Network Setup without a Common Control Channel , *Proceedings of IEEE Military Communications Conference (MILCOM)*, pp. 1-6, November 2008.

[52] V. Krishnamurthy, M. Maskery, and G. Yin, Decentralized Adaptive Filtering Algorithms for Sensor Activation in An Unattended Ground Sensor Network, *IEEE Transactions on Signal Processing*, vol. 56, no. 12, pp. 6086-6101, December 2008.

[53] M. N. Krohn, M. J. Freeman, and D. Mazières, On-the-fly Verification of Rateless Erasure Codes for Efficient Content Distribution, *Proceedings of the 2004 IEEE Symposium on Security and Privacy*, pp. 226-240, May 2004.

[54] L. Lazos, S. Liu, and M. Krunz, Mitigating Control-Channel Jamming Attacks in Multichannel Ad Hoc Networks. *Proceedings of the 2nd ACM Conference on Wireless Security (Wisec2009)*, pp. 169-180, March 2009.

[55] W. Lehr, and J. Crowcroft, Managing Shared Access to A Spectrum Commons, *Proceedings of the First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2005)*, pp. 420-444, Nov. 2005.

[56] H. Li, and Z. Han, Catch Me if You Can: An Abnormality Detection Approach for Collaborative Spectrum Sensing in Cognitive Radio Networks, *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3554-3565, November 2010.

[57] H. Li, and Z. Han, Dogfight in Spectrum: Combating Primary User Emulation Attacks in Cognitive Radio Systems, Part I: Known Channel Statistics. *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3566-3577, November 2010.

[58] S. Li, H. Zhu, Z. Gao, X. Guan, and K. Xing, YouSense: Mitigating Entropy Selfishness in Distributed Collaborative Spectrum Sensing, *Proceedings of the 32nd IEEE International Conference on Computer Communications (INFOCOM 2013)*, pp. 2635-2643, April 2013.

[59] Z. Li, F. R. Yu, and M. Huang, A Distributed Consensus-Based Cooperative Spectrum-Sensing Scheme in Cognitive Radios, *IEEE Transactions on Vehicular Technology*, vol. 59, no. 1, pp. 383-393, January 2010.

[60] Z. Li, and G. Gong, Data Aggregation Integrity Based on Homomorphic Primitives in Sensor Networks, *Proceedings of the 9th International Conference on Ad Hoc Networks and Wireless (ADHOC-NOW 2010)*, pp. 149-162, August 2010.

[61] Q. Liang, S. Han, F. Yang, G. Sun, and X. Wang, A Distributed-Centralized Scheme for Short- and Long- Term Spectrum Sharing with a Random Leader in Cognitive Radio Networks, *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 11, pp. 2274-2284, December 2012.

[62] K. J. Lin, H. Lu, T. Yu and C.Tai, A Reputation and Trust Management Broker Framework for Web Applications. *Proceedings of the 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE 2005)*, pp. 262-269, March 2005.

[63] Y. Liu, P. Ning, and H. Dai, Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures, *Proceedings of 2010 IEEE Symposium on Security and Privacy (S&P)*, pp. 286-301, May 2010.

[64] B. F. Lo, I. F. Akyildiz, andA. M. Al-Dhelaan, Efficient Recovery Control Channel Design in Cognitive Radio Ad Hoc Networks, *IEEE Transactions on Vehicular Technology*, vol. 59, no. 9, pp. 4513-4526, November 2010.

[65] B. F. Lo, A survey of Common Control Channel Design in Cognitive Radio Networks, *Physical Communication*, vol. 4, no. 1, pp. 26-39, March 2011.

[66] M. López-Benítez, Cognitive Radio, Heterogeneous Cellular Networks, Ed. X. Chu, D. Lopez-Perez, Y. Yang, and F. Gunnarsson, Cambridge University Press, 2013.

[67] D. Malkhi, N. Nisan, B. Pinkas, and Y. Sella, Fairplay - A Secure Two-Party Computation System, *Proceedings of the 13th Conference on USENIX Security Symposium (SSYM 2004)*, pp. 287-302, August 2004.

[68] P. Marshall, Quantitative Analysis of Cognitive Radio and Network Performance, Artech House Press, 2010.

[69] A. W. Min, K. G. Shin, and X. Hu, Attack-Tolerant Distributed Sensing for Dynamic Spectrum Access Networks, *Proceedings of the 17th IEEE International Conference on Network Protocols (ICNP)*, pp. 294-303, October 2009.

[70] A. W. Min, K. H. Kim, and K. G. Shin, Robust Cooperative Sensing via State Estimation in Cognitive Radio Networks, *Proceedings of the 4th IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pp. 185-196, May 2011.

[71] S. M. Mishra, A. Sahai, and R. W. Brodersen, Cooperative sensing among Cognitive Radios, *Proceedings of the 2006 IEEE International Conference on Communications (ICC)*, pp. 1658-1663, June 2006.

[72] J. Mitola, Software Radio Architecture, Wiley-Interscience, 2000.

[73] J. Mitola, Cognitive radio: An Integrated Agent Architecture for Software Defined Radio, Ph.D. dissertation, Royal Institute of Technology (KTH), Stockholm, Sweden, May 2000.

[74] J. Mitola, Cognitive Radio Architecture, Wiley-Interscience, 2006.

[75] A. N. Mody, and G. Chouinard, IEEE 802.22 Wireless Regional Area Networks - Enabling Rural Broadband Wireless Access Using Cognitive Radio Technology, doc.: IEEE 802.22-10/0073r03, June 2010.

[76] A. Mukherjee, Diffusion of Cooperative Behavior in Decentralized Cognitive Radio Networks with Selfish Spectrum Sensors, *IEEE Journal of Selected Topics in Signal Processing*, vol. 7, no. 2, pp. 175-183, April 2013.

[77] J. Mundinger, and J. Le Boudec, Analysis of a Reputation System for Mobile Ad Hoc Networks with Liars, *Performance Evaluation*, vol. 65, no. 3-4, pp. 212-226, March 2008.

[78] J. W. Mwangoka, K. B. Letaief, and Z. Cao, Joint Power Control and Spectrum Allocation for Cognitive Radio Networks via Pricing, *Physical Communication* vol. 2, no. 1-2, pp.103-115, March - June 2009.

[79] J. Newsome, E. Shi, D. Song, and A. Perrig, The Sybil Attack in Sensor Networks: Analysis & Defenses, *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks (IPSN 2004)*, pp. 259 - 268, April 2004.

[80] R. Olfati-Saber, J. A. Fax, and R. M. Murray, Consensus and Cooperation in Networked Multi-Agent Systems, *Proceedings of the IEEE*, vol. 95, no. 1, pp. 215-233, January 2007.

[81] P. Obreiter, A Case for Evidence-Aware Distributed Reputation Systems: Overcoming the Limitations of Plausibility Considerations, *Proceedings of the 2nd International Conference on Trust Management (iTrust 2004)*, pp. 33-47, March 2004.

[82] M. Pan, J. Sun, and Y. Fang, Purging the Back-Room Dealing: Secure Spectrum Auction Leveraging Paillier Cryptosystem, *IEEE Journal on Selected Areas in Communications*, vol 29, no. 4, pp. 866-876, April 2011.

[83] S. Parvina, F. K. Hussain, O. K. Hussain, S. Han, B. Tian, and E. Chang, Cognitive radio network security: A survey, *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 1691-1708, November 2012.

[84] 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 Transactions on Signal Processing*, vol. 59, no. 2, pp. 774-786, February 2011.

[85] J. Redi, R. Ramanathan, The DARPA WNaN Network Architecture, *Proceedings of the 2011 Military Communications Conference*, pp. 2258-2263, November 2011.

[86] T. Roosta, M. Meingast, S. Sastry, Distributed Reputation System for Tracking Applications in Sensor Networks, *Proceedings of the 3rd Annual International Conference on Mobile and Ubiquitous Systems* pp. 1-8, July 2006.

[87] G. Safdar, and M. O'Neill, Common control channel security framework for cognitive radio networks. *Proceedings of the 69th IEEE Vehicular Technology Conference (VTC Spring 2009)*, pp. 1-5, April 2009.

[88] A. Sahai, N. Hoven, and R. Tandra, Some Fundamental Limits on Cognitive Radio, *Proceedings of the 42nd Annual Allerton Conference on Communication, Control and Computing*, October 2004.

[89] D. A. Schmidt, C. Shi, R. A. Berry, M. L. Honig, and W. Utschick, Distributed Resource Allocation Schemes, *IEEE Signal Processing Magazine*, vol. 26, no. 5, pp.53-63, September 2009.

[90] S. S. D. Selvi, S. S. Vivek, and C. P. Rangan, Cryptanalysis of Certificateless Signcryption Schemes and an Efficient Construction without Pairing, *Information Security and Cryptology*, vol.6151, pp. 75-92, December 2009.

[91] Shared Spectrum Company, General Survey of Radio Frequency Bands - 30 MHz to 3 GHz, http://www.sharedspectrum.com/papers/spectrum-reports. Retrieved March 2014.

[92] H, -P, Shiang, and M. van der Schaar, Distributed Resource Management in Multihop Cognitive Radio Networks for Delay Sensitive Transmission, *IEEE Transactions on Vehicular Technology*, vol. 58, no. 2, pp. 941-953, February 2009.

[93] C. Song, and Q. Zhang, Achieving Cooperative Spectrum Sensing in Wireless Cognitive Radio Networks, *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 13, no. 2, pp. 14-25, April 2009.

[94] Y. Song, and J. Xie, Performance Analysis of Spectrum Handoff for Cognitive Radio Ad Hoc Networks without common control channel under Homogeneous Primary Traffic. Proceedings of the 30th Annual IEEE International Conference on Computer Communications (INFOCOM 2011), pp. 3011-3019, April 2011.

[95] W. Song, and V. V. Phoha, Neural Network-Based Reputation Model in a Distributed System, *Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE2004)*, pp. 321-324, July 2004.

[96] A. Srinivasan, J. Teitelbaum, and J. Wu, DRBTS: Distributed Reputation-based Beacon Trust System, *Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC2006)*, pp. 277-283, September 2006.

[97] Y. Tachwali, B. F. Lo, I. F. Akyildiz, and R. Agustí, Multiuser Resource Allocation Optimization Using Bandwidth-Power Product in Cognitive Radio Networks, *IEEE Journal*

on Selected Areas in Communications, vol. 31, no. 3, pp. 451-463, March 2013.

[98] P. Tague, M. Li, and R. Poovendran, Mitigation of Control Channel Jamming under Node Capture Attacks. *IEEE Transactions on Mobile Computing*, vol. 8, no. 9, pp. 1221-1234, September 2009.

[99] D. Talbot, The Spectrum Crunch that Wasn't, *MIT Technology Review*, vol. 116, no. 1, pp. 80-81, January 2013.

[100] L. T. Tan, and L. B. Le, Channel Assignment with Access Contention Resolution for Cognitive Radio Networks, *IEEE Transactions on Vehicular Technology*, vol. 61, no. 6, pp. 2808-2823, July 2012.

[101] H. Tang, Some Physical Layer Issues of Wide-Band Cognitive Radio System, *Proceedings of the First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2005)*, pp. 151-159, November 2005.

[102] P. Tague, M. Li, and R. Poovendran, Mitigation of Control Channel Jamming under Node Capture Attacks, *IEEE Transactions on Mobile Computing*, vol.8, no.9, pp. 1221-1234, September 2009.

[103] W. Vickery, Counterspeculation, Auctions, and Competitive Sealed Tenders, *Journal of Finance*, vol. 16, no. 1, pp. 8-37, March 1961.

[104] B. Wang, K. Liu, and T. Clancy, Evolutionary Cooperative Spectrum Sensing Game: How to Collaborate? *IEEE Transactions on Communications*, vol. 58, no. 3, pp. 890-900, March 2010.

[105] F. Wang, M, Krunz, and S. Cui, Price-Based Spectrum Management in Cognitive Radio Networks, *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, no. 1, pp. 74-87, February 2008.

[106] H. Wang, L. Lightfoot, and T. Li, On PHY-layer security of cognitive radio: Collaborative sensing under malicious attacks, *Proceedings of the 44th Annual Conference on Information Sciences and Systems (CISS)*, pp. 1-6, March 2010.

[107] J. Wang, M. S. Song, S. Santhiveeran, K. Lim, G. Ko, K. Kim, S. H. Hwang, M. Ghosh, V. Gaddam, and K. Challapali. First Cognitive Radio Networking Standard for Personal/Portable Devices in TV White Spaces, *Proceedings of the 6th IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2010)*, pp. 1-12, April 2010.

[108] S. Wang, Z, -H. Zhou, M. Ge, and C. Wang, Resource Allocation for Heterogeneous Cognitive Radio Networks with Imperfect Spectrum Sensing, *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 3, pp. 464-475, March 2013.

[109] W. Wang, H. Li, Y. Sun, and Z. Han, CatchIt: Detect Malicious Nodes in Collaborative Spectrum Sensing, *Proceedings of 2009 IEEE Global Telecommunications Conference (GLOBECOM)*, pp. 1-6, December 2009.

[110] W. Wang, H. Li, Y. Sun, and Z. Han, Attack-Proof Cooperative Spectrum Sensing in Cognitive Radio Networks, *ACM Transactions on Interactive Intelligent Systems*, vol. 4, no.6, pp. 1042-1062, June 2010.

[111] J. Wei, and X. Zhang, Two-Tier Optimal-Cooperation Based Secure Distributed Spectrum Sensing for Wireless Cognitive Radio Networks, *Proceedings of the IEEE INFOCOM Workshop on Cognitive Wireless Communications and Networking*, pp. 1-6, March 2010.

[112] F. Wu, and N. Vaidya, A Strategy-Proof Radio Spectrum Auction Mechanism in Noncooperative Wireless Networks, *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 885-894, May 2013.

[113] Y. Wu, B. Wang, K. J. R. Liu, and T. C. Clancy, A Multi-Winner Cognitive Radio

Spectrum Auction Framework with Collusion-Resistant Mechanisms, *Proceedings of the 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2008)*, pp. 1-9, October 2008.

[114] A. M. Wyglinski, M. Nekovee, and Y. T. Hou, Cognitive Radio Communications and Networks, Elsevier, 2010.

[115] R. Xie, F. R. Yu, and H. Ji, Dynamic Resource Allocation for Heterogeneous Services in Cognitive Radio Networks with Imperfect Channel Sensing. *IEEE Transactions on Vehicular Technology*, vol. 61, no. 2, pp. 770-780, February 2012.

[116] R. Xie, F. R. Yu, H. Ji, and Y. Li, Energy-Efficient Resource Allocation for Heterogeneous Cognitive Radio Networks with Femtocells. *IEEE Transactions on Wireless Communications*, vol. 11, no. 11, pp. 3910-3920, November 2012.

[117] S. Yadav, and M. J. Nene, RSS Based Detection and Expulsion of Malicious Users from Cooperative Sensing in Cognitive Radios, *Proceedings of the 3rd IEEE International Advance Computing Conference (IACC 2013)*, pp. 181-184, February 2013.

[118] Q. Yan, M. Li, T. Jiang, W. Lou, and Y. T. Hou, Vulnerability and Protection for Distributed Consensus-based Spectrum Sensing in Cognitive Radio Networks, *Proceedings of the 31st Annual IEEE International Conference on Computer Communications (INFOCOM 2012)*, pp. 900-908, March 2012.

[119] G. Yin, D. Shi, H. Wang, and M. Guo, RepCom: Towards Reputation Composition over Peer-to-Peer Communities, *Proceedings of 2009 International Conference on Computational Science and Engineering (CSE)*, pp. 765-771, August 2009.

[120] B. Yu, and M. P. Singh, An Evidential Model of Distributed Reputation Management. *Proceedings of the First International Joint Conference on Autonomous Agents and Multi-Agent Systems*, pp. 294-301, July 2002.

[121] B. Yu, and M. P. Singh, Distributed reputation management for electronic commerce, *Computational Intelligence*, vol. 18, no. 4, pp. 535-549, November 2002.

[122] T. Zhang, Z. Li, and R. Safavi-Naini, Incentivize Cooperative Sensing in Distributed Cognitive Radio Networks with Reputation-based Pricing, in the *Proceedings of 33rd IEEE International Conference on Computer Communications (INFOCOM 2014)*, April 2014.

[123] T. Zhang, R. Safavi-Naini, and Z. Li, ReDiSen: Reputation-based Secure Cooperative Sensing in Distributed Cognitive Radio Networks, *Proceedings of 2013 IEEE International Conference on Communications (ICC)*, pp. 1194-1198, June 2013.

[124] Q. Zhao, L. Tong, and A. Swami, Decentralized Cognitive MAC for Dynamic Spectrum Assess, *Proceedings of the First IEEE Symposium on New Frontiers in Dynamic Spectrum (DySPAN2005)*,pp. 224-232, November 2005.

[125] M. Zhou, J. Shen, H. Chen, and L. Xie, A Cooperative Spectrum Sensing Scheme based on the Bayesian Reputation Model in Cognitive Radio Networks, *Proceedings of 2013 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 614-619, April 2013.

[126] X. Zhou, S. Gandhi, S. Suri, and H. Zheng, eBay in the Sky: Strategy-Proof Wireless Spectrum Auctions, *Proceedings of the 14th Annual International Conference on Mobile Computing and Networking (MobiCom 2008)*, pp. 2-13, September 2008.

[127] X. Zhou, and H. Zheng, TRUST: A General Framework for Truthful Double Spectrum Auctions, *Proceedings of the 28th Annual IEEE International Conference on Computer Communications (INFOCOM 2009)*, pp. 999-1007, April 2009.

[128] Y. Zhu, B. Li, and Z. Li, Truthful Spectrum Auction Design for Secondary Networks,

Proceedings of the 31st Annual IEEE International Conference on Computer Communications (INFOCOM 2012), pp. 873-881, March 2012.

[129] Y. Zhu, B. Li, and Z. Li, Designing Two-Dimensional Spectrum Auctions for Mobile Secondary Users, *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 3, pp. 604-613, March 2013.

[130] Y. Zhu, B. Li, and Z. Li, Core-Selecting Combinatorial Auction Design for Secondary Spectrum Markets, *Proceedings of the 32nd Annual IEEE International Conference on Computer Communications (INFOCOM 2013)*, pp. 1986-1994, April 2013.