Distributed Consensus-Based Cooperative Spectrum Sensing in Cognitive Radio Ad Hoc Networks

by

Zhiqiang Li

A thesis submitted to the

Faculty of Graduate Studies and Research

in partial fulfillment of the requirements for the degree of

Master of Applied Science in Electrical and Computer Engineering

Ottawa-Carleton Institute for Electrical and Computer Engineering

Department of Systems and Computer Engineering

Carleton University

Ottawa, Ontario

November, 2009

Your file Votre référence
ISBN: 978-0-494-63209-3
Our file Notre référence
ISBN: 978-0-494-63209-3

The undersigned hereby recommends to the

Faculty of Graduate Studies and Research

acceptance of the thesis

Distributed Consensus-Based Cooperative Spectrum Sensing in Cognitive Radio Ad Hoc Networks

submitted by

Zhiqiang Li, M.Eng., B.Eng.

in partial fulfillment of the requirements for the degree of

Master of Applied Science in Electrical and Computer Engineering

---

Professor Fei Richard Yu, Thesis Supervisor

Chairperson,
Department of Systems and Computer Engineering

Ottawa-Carleton Institute for Electrical and Computer Engineering

Department of Systems and Computer Engineering

Carleton University

November, 2009

Abstract

In cognitive radio (CR) mobile ad hoc networks (MANETs), secondary users can cooperatively sense the spectrum to detect the presence of primary users. In this thesis, we propose a fully distributed and scalable cooperative spectrum sensing scheme based on recent advances in consensus algorithms. In the proposed scheme, the secondary users can maintain coordination based on only local information exchange without a centralized common receiver. We use the consensus of secondary users to make the final decision. The proposed scheme is essentially based on recent advances in consensus algorithms that have taken inspiration from complex natural phenomena including flocking of birds, schooling of fish, swarming of ants and honeybees. In addition, we consider the security issues such as spectrum sensing data falsification (SSDF) attacks in CR MANETs. In SSDF attacks, intruders send false local spectrum sensing results in cooperative spectrum sensing, which will cause wrong spectrum sensing decisions by cognitive radios. To counter SSDF attacks in cognitive radio MANETs, we further make little modification on the proposed consensus-based scheme. Simulation results show that the proposed consensus scheme can have significant lower missing detection probabilities and false alarm probabilities in cognitive radio MANETs. It is also demonstrated that the proposed scheme not only has proven sensitivity in detecting the primary user's presence, but also has robustness in choosing a desirable decision threshold.

Acknowledgments

I would like to thank the invaluable supervision and support of my supervisor Professor Fei Richard Yu during the development of this work. Professor Yu offered great guidance during my study. He also helped me in every way possible to achieve success. I would like also to express my deep gratitude to Professor Minyi Huang for his guidance throughout the research.

To my family, for their constant support and love through the course of my studies.

To my friends Fei Wang, Pengbo Si and Junwu Zhu, for their consistent support and encouragement helped me to overcome difficulties.

Table of Contents

List of Figures

List of Abbreviations

AWGN	Additive While Gaussian Noise
BPF	Band Pass Filter
CA	Certificate Authority
CDMA	Code Division Multiple Access
CR	Cognitive Radio
DARPA	Defence Advance Research Projects Agency
dB	Decibel
DCCSS	Distributed Consensus-based Cooperative Spectrum Sensing
DCSS	Distributed Cooperative Spectrum Sensing
FCC	Federal Communication Commission
IBE	Identity Based Encryption
IE	Incumbent Emulation
IMT	International Mobile Telecommunications
LQ	Linear-Quadratic
MAC	Medium Access Control
MANET	Mobile Ad-hoc NETwork
MIMO	Multiple Input and Multiple Output
OFDM	Orthogonal Frequency Division Multiplexing
PDAs	Personal Digital Assistants
PK	Private Key
PKI	Public Key Infrastructure
PKG	Private Key Generator

POMDP	Partially Observed Markov Decision Process
RF	Radio Frequency
SMa	Spectrum Management
SMo	Spectrum Mobility
SNR	Signal to Noise Ratio
SS	Spectrum Sensing
SSDF	Spectrum Sensing Data Falsification
SSh	Spectrum Sharing
TA	Trusted Authority

List of Symbols

$\boldsymbol{A}$	The Adjacency Matrix
$\mathcal{E}$	The Set of Edges in the Graph $\boldsymbol{G}$
$\boldsymbol{G}$	A Graph
rank($\boldsymbol{G}$)	The Rank of the Graph $\boldsymbol{G}$
$\boldsymbol{L} = (l_{ij})_{n \times n}$	The Laplacian of the Graph $\boldsymbol{G}$
$\mathcal{N}_i = \{j \mid (j,i) \in \mathcal{E}\} \subset \mathcal{N}$	The Neighbors of Node i
$\lvert\mathcal{N}_i\rvert$	The Number of Elements in $\mathcal{N}_i$
$\boldsymbol{P} = \boldsymbol{I} - \epsilon \boldsymbol{L}$	The Matrix That Equals to Unit Matrix Minus the Laplacian
P_d	The Probability of Detection
P_f	The Probability of False Alarm
P_m	The Probability of Missing Detection
T	The Period during Which the Signal Goes through Input Band Pass Filter
W	The Bandwidth of Interest of Input Band Pass Filter
Y	The Output of the Integrator in an Input Band Pass Filter
Y_i	Local Measurement of the Sensing Channel from the Primary User to Secondary User i
Δ	The Maximum Degree of the Graph $\boldsymbol{G}$
$O(e^{-\delta t})$	The Order of Complexity with the Exponent $\delta > 0$
d_i	The Degree of Node i
f_s	The Center Frequency of Input Band Pass Filter

h	The Amplitude Gain of the Sensing Channel
i	Secondary User or Node i
(i, j)	The Bidirectional Edge from Node/User i to j
k	The Number of Time Instant or Iteration Step
$m = TW$	The Time-bandwidth Product in an Input Band Pass Filter
$n(t)$	The Additive White Gaussian Noise
p	The probability
$s(t)$	The Primary User's Transmitted Signal
x^*	The Converged Common Value
$x_i(k)$	Local State Variable of Secondary User i in Iteration Step k
$x(t)$	The Signal Received by the Secondary User at time t
γ	SNR
$\overline{\gamma}$	The Average SNR
λ	The Eigenvalue of the Laplacian
χ^2_{2TW}	Random Quantities with Central Chi-square Distributions
$\chi^2_{2TW}(2\gamma)$	Random Quantities with Non-central Chi-square Distributions

Chapter 1

Introduction

1.1 Research Overview

Recently, there has been tremendous interest in the field of cognitive radio (CR), which has been introduced in [1]. CR is an enabling technology that allows unlicensed (secondary) users to operate in the licensed spectrum bands. This can help to overcome the lack of available spectrum in wireless communications, and achieve significant improvements over services offered by current wireless networks. It is designed to sense the changes in its surroundings, thus learns from its environment and performs functions that best serve its users. A very crucial feature of CR networks is to allow users to operate in licensed bands without a license [2]. To achieve this goal, spectrum sensing is an indispensable part in cognitive radio.

There are three fundamental requirements for spectrum sensing. In the first place, the unlicensed (secondary) users can use the licensed spectrum as long as the licensed (primary) user is absent at some particular time slot and some specific geographic location. However, when the primary user comes back into operation, the secondary users should vacate the spectrum instantly to avoid interference with the primary

user. Hence, a first requirement of cognitive radio is that continuous spectrum sensing is needed to monitor the existence of the primary user. Also, since cognitive radios are considered as lower priority and they are secondary users of the spectrum allocated to a primary user, the second fundamental requirement is to avoid the interference to potential primary users in their vicinity [3]. Furthermore, primary user networks have no requirement to change their infrastructure for spectrum sharing with cognitive radios. Therefore, the third requirement is for secondary users to be able to independently detect the presence of primary users.

Taking those three requirements into consideration, spectrum sensing can be conducted non-cooperatively (individually), in which each secondary user conducts radio detection and makes decision by itself. However, the sensing performance for one cognitive user will be degraded when the sensing channel experiences fading and shadowing [4]. In order to improve spectrum sensing, several authors have recently proposed collaboration among secondary users [3, 5–7], which means a group of secondary users perform spectrum sensing by collaboration. Collaboration can be proved to enhance secondary spectrum access significantly [5].

1.2 Thesis Motivation

Our research is focused on distributed cooperative spectrum sensing (DCSS) in cognitive radio, and more precisely, the distributed cooperative schemes of spectrum sensing in a Mobile Ad-hoc NETworks (MANETs). In addition, since security issues are crucial in such MANET networks, they are also considered as an indispensable part of our research focus.

In the first place, at present, distributed cooperative detection problems are discussed in [6, 8–10]. In a typical wireless distributed detection problem, each sensor or secondary user individually forms its own discrete messages based on its local

measurement and then reports to a fusion center via wireless reporting channels. In certain models [10], however, there is in general no direct communication among the sensors. A sensor may indirectly obtain information about other sensors, but this is achieved by feedback from a common fusion center. Nevertheless, a centralized fusion center may not be available in some CR-based MANETs. Moreover, as indicated in [11], gathering the entire received data at one place may be very difficult under practical communication constraints. In addition, authors of [4] study the reporting channels between the cognitive users and the common receiver. The results show that there are limitations for the performance of cooperation when the reporting channels to the common receiver are under deep fading.

In the second place, although some security work has been done in CR technologies, the area of security in MANETs with CRs has received relatively little attention. Unlike wired networks, MANETs are inherently insecure because of the lack of any central authority. Certainly, threats to non-cognitive wireless networks in general are still of interest in the CR paradigm. However, some distinct characteristics of CRs introduce new non-trivial security risks to MANETs with CRs. For example, locally-collected and exchanged spectrum sensing information is used to construct a perceived environment that will impact CR behavior. This opens opportunities to malicious attackers. Two known security threats in CRs are Incumbent Emulation (IE) and Spectrum Sensing Data Falsification (SSDF). In an IE attack, intruders emulate signals with the characteristics of incumbent primary users to fool other secondary users. IE attacks can severely interfere with the spectrum sensing process and significantly reduce the channel resources available to authentic secondary users. A transmitter verification scheme is proposed in [12] to identify such IE attacks. In an SSDF attack, intruders send false local spectrum sensing results in cooperative spectrum sensing, which will result in suspect spectrum sensing decisions by CRs. Authors in [13] make

fine attempts by suggesting several approaches to counter SSDF attacks. However, no further development is reported.

1.3 Thesis Contributions and Accepted Papers

Based on recent advances in consensus algorithms [14], we propose a new scheme in distributed cooperative spectrum sensing called distributed consensus-based cooperative spectrum sensing (DCCSS). In addition, we make some modification on our consensus-based cooperative spectrum sensing scheme to counter SSDF attacks in MANETs with CRs.

The main contributions of this thesis include:

- We propose a consensus-based spectrum sensing scheme, which is a fully distributed and scalable scheme. Unlike many existing schemes, there is no need for a common receiver to do data fusion and to reach the final decision. Since it is rare to have a centralized node in MANETs, in the proposed scheme, a secondary user needs only to setup local interactions without centralized information exchange.

- Unlike most decision rules, such as OR-rule or n-out-of-N, adopted in existing spectrum sensing schemes, we use consensus from secondary users. The proposed scheme has self-configuration and self-maintenance capabilities, and is robust against SSDF attacks by using consensus to differentiate the trustworthiness of the local spectrum sensing reports received from each sensing terminal.

- Since the CR paradigm imposes human-like characteristics (e.g., learning, adaptation and cooperation) in wireless networks, the bio-inspired consensus algorithm used in this thesis can provide some insight into the design of future

MANETs with CRs.

Extensive simulation results illustrate the effectiveness of the proposed scheme. It is shown that the proposed scheme can have both lower missing detection probability and lower false alarm probability compared to the existing schemes. In addition, it is able to make better detection when secondary users undergo worse fading (lower average SNR). Also, with the help of this scheme, a fixed threshold is feasible, which can take active effect in different fading channels. Last but not the least, it is shown that the proposed schemes have significant improvement in identifying and preventing SSDF attacks.

The following papers have been accepted/published based on this work.

- Zhiqiang Li, F.R. Yu and M. Huang, "A Distributed Consensus-Based Cooperative Spectrum Sensing in Cognitive Radios", to appear in *IEEE Trans. Vehicular Technology*, 2010.

- Zhiqiang Li, F.R. Yu and M. Huang, "A Cooperative Spectrum Sensing Consensus Scheme in Cognitive Radios", in *Proc. IEEE INFOCOM'09 Mini Conference*, Rio de Janeiro, Brazil, Apr. 2009.

- Zhiqiang Li, F.R. Yu and M. Huang, "Distributed Spectrum Sensing in Cognitive Radio Networks", in *Proc. IEEE WCNC'09*, Budapest, Hungary, Apr. 2009.

- F.R. Yu, H. Tang, M. Huang, Zhiqiang Li and P.C. Mason, "Defense against Spectrum Sensing Data Falsification Attacks in Mobile Ad Hoc Networks with Cognitive Radios", in *Proc. IEEE Milcom'09*, Boston, MA, USA, Oct. 2009.

1.4 Thesis Organization

The rest of the thesis is organized as follows. Chapter 2 describes the research background of this thesis, which includes spectrum sensing in cognitive radios, cooperative spectrum sensing, centralized/distributed cooperative spectrum sensing, security issues in CRs MANETs etc. Chapter 3 presents system models, spectrum sensing models, graph theories and consensus notions. In Chapter 4, the distributed consensus-based cooperative spectrum sensing scheme is proposed based on fixed graphs without considering SSDF attacks. Going further, the distributed consensus-based cooperative spectrum sensing scheme based on random graphs is described in Chapter 5, which does not consider SSDF attacks, either. In Chapter 6, a modified consensus-based scheme is presented to counter SSDF attacks. In Chapter 7, the simulation results and discussions are presented. Finally, we conclude this thesis in Chapter 8, together with research areas for future work.

Chapter 2

Research Background

This chapter covers the topics regarding the research background. They include the introduction of cognitive radio, functionalities of cognitive radio, differences of individual spectrum sensing and cooperative spectrum sensing, followed by the introduction of centralized distributed cooperative spectrum sensing and distributed consensus-based cooperative spectrum-sensing. The second part of this chapter introduces MANETs and its security constraints.

2.1 Introduction of Spectrum Sensing in Cognitive Radio

The idea of cognitive radio is first presented officially in an article by Joseph Mitola and Gerald Q. Maguire, Jr. [15]. It is a novel approach in wireless communications that Mitola later describe in his PhD dissertation as:

"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 communications needs as a function of use context, and to provide radio resources and wireless services most

appropriate to those needs."

It is thought of as an ideal goal towards which a software-defined radio platform should evolve: a fully reconfigurable wireless black-box that automatically changes its communication variables in response to network and user demands.

The above citation originates from the following fact. The growing number of wireless standards is occupying more and more naturally limited frequency bandwidth for exclusive use as licensed bands. However, large part of licensed bands are unused for what concerns a large amount of both time and space: even if a particular range of frequencies is reserved for a standard, at a particular time and at a particular location it could be found free. The Federal Communication Commission (FCC) estimates that the variation of use of licensed spectrum ranges from 15% to 85%, whereas according to Defence Advance Research Projects Agency (DARPA) only 2% of the spectrum is in use in US at any given moment. It is then clear that the solution to these problems can be found dynamically looking at spectrum as a function of time and space.

With the high demand of bit transmission rate for 4G or IMT-advanced high-speed wireless applications, there are several approaches to increase the system capacity as stated in the following equation:

$$C = n \cdot B \cdot log_2(1 + SNR) \tag{2.1}$$

Where C is system capacity, n is number of channels, B is system bandwidth, and SNR is signal to noise radio.

The first approach is using MIMO to increase n, so that capacity may have a gain proportionally. The second approach is trying to increase SNR. The third one is focusing on the bandwidth. Cognitive radio is among the third category, and thrives to fully utilize the frequency.

2.1.1 Functionalities of Cognitive Radios

The main functionalities of cognitive radios are [16]:

- **Spectrum Sensing (SS)**: detecting the unused spectrum and sharing it without harmful interference with other users, it is an important requirement of the cognitive Radio network to sense spectrum holes, detecting primary users is the most efficient way to detect spectrum holes. Spectrum sensing techniques can be classified into three categories:
  - Transmitter detection: cognitive radios must have the capability to determine if a signal from a primary transmitter is locally present in a certain spectrum, there are several approaches proposed:
    * Matched filter detection
    * Energy detection
    * Cyclostationary feature detection
  - Cooperative detection: multiple cognitive radio users are incorporated for primary user detection.
  - Interference based detection.
- **Spectrum Management (SMa)**: Capturing the best available spectrum to meet user communication requirements. Cognitive radios should decide on the best spectrum band to meet the quality of service requirements over all available spectrum bands, therefore spectrum management functions are required for cognitive radios, these management functions can be classified as: spectrum analysis and spectrum decision.
- **Spectrum Mobility (SMo)**: is defined as the process when a cognitive radio user exchanges its frequency of operation. Cognitive radio networks target to

use the spectrum in a dynamic manner by allowing the radio terminals to operate in the best available frequency band, maintaining seamless communication requirements during the transition to better spectrum.

- **Spectrum Sharing (SSh)**: providing the fair spectrum scheduling method, which is one of the major challenges in open spectrum usage is the spectrum sharing. It can be regarded to be similar to generic media access control MAC problems in existing systems.

2.1.2 Individual and Cooperative Spectrum Sensing

Spectrum sensing can be conducted either non-cooperatively (individually), in which each secondary user conducts radio detection and makes decision by itself, or cooperatively, in which a group of secondary users perform spectrum sensing by collaboration. No matter in which way, the common topology of such a cognitive radio network can be depicted as in Figure 2.1. Individual spectrum sensing is conducted by secondary users on its own, and each user has a local observation and a local decision accordingly. Thus, in Figure 2.1, each secondary user performs the spectrum sensing locally and no communication is between one another, nor is the common receiver (fusion center). In such a condition, cognitive radio sensitivity can only be improved [6] by enhancing radio RF front-end sensitivity, exploiting digital signal processing gain for specific primary user signal, and network cooperation where users share their spectrum sensing measurements. However, if the sensing channels are facing deep fading or shadowing, then affected individuals will not be able to detect the presence of the primary user, which leads to missing detection failure.

In order to improve the performance of spectrum sensing, several authors have recently proposed cooperation among secondary users [2,4,5,17]. Cooperative spectrum

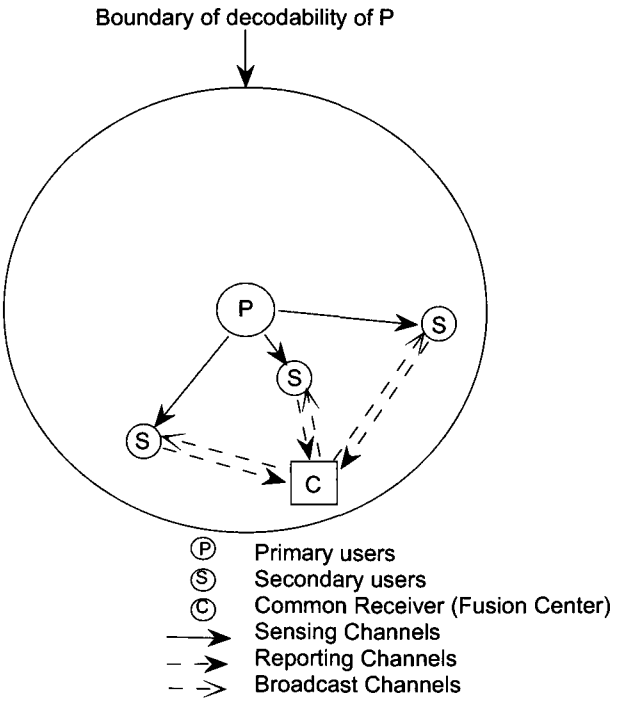


Figure 2.1: A typical cognitive radio network

sensing has been proposed to exploit multi-user diversity in sensing process. It is usually performed in three successive stages: sensing, reporting and broadcasting. In the sensing stage, every cognitive user performs spectrum sensing individually. This can be shown as in Figure 2.1, where secondary users try to collect the signal of interest through sensing channels. In the reporting stage, all the local sensing observations are reported to a common receiver via reporting channels (see Figure 2.1) and the latter will make a final decision on the absence or the presence of the primary user. Finally, the final decision is broadcasted via broadcast channels to all the secondary users concerned, which include not only the ones involved into the sensing stage, but also those that do not have sensing capabilities but want to participate into the spectrum sharing stage.

There are several advantages offered by cooperative spectrum sensing over the

non-cooperative ones [5, 11, 18–24]. If a secondary user is in the condition of deep shadowing and fading, it is very difficult for a secondary user to distinguish a white space from a deep shadowing effect. Therefore, a non-cooperative spectrum sensing algorithm may not work well in this case, and a cooperative scheme can solve the problem by sharing the spectrum sensing information among secondary users. Moreover, because of the hidden terminal problem, it is very challenging for single cognitive radio sensitivity to outperform the primary user receiver by a large margin in order to detect the presence of primary users. For this reason, if secondary users spread out in the spatial distance, and any one of them detects the presence of primary users, then the whole group can gain benefit by collaboration.

Authors of [5] quantify the performance of spectrum sensing in fading environments and study the effect of cooperation. The simulation results in [5] indicate that significant performance enhancements can be achieved through cooperation. Authors of [18] study the possibility to forward the signal with higher SNR to the one on the boundary of decidability region of the primary user. The performance is evaluated under correlated shadowing and user compromise in [11]. When the exchange of observations from all secondary users to the common receiver is not applicable, authors of [19] show that it is still worth doing by cooperating a certain number of users with relatively higher SNR. Moreover, in [20], a linear-quadratic (LQ) fusion strategy is designed with the consideration of the correlation between the nodes. In order to further reduce the computational complexity, authors of [21] propose a heuristic approach so as to develop an optimal linear framework during cooperation. Sensing-throughput tradeoff is analyzed in [22] for both multiple mini-slots and multiple secondary users cooperative sensing.

2.1.3 Centralized Cooperative Spectrum Sensing

Although some research activities have been conducted in cooperative spectrum sensing, most of them use a common receiver (fusion center) to do data fusion for the final decision whether or not the primary user is present. However, a common receiver may not be available in some CR-based networks, such as mobile ad hoc networks (MANETs). Moreover, as indicated in [11], gathering the entire received data at one place may be very difficult under practical communication constraints. In addition, authors of [4] study the reporting channels between the cognitive users and the common receiver. The results show that there are limitations for the performance of cooperation when the reporting channels to the common receiver are under deep fading. In summary, the use of a centralized fusion center in MANETs may have the following problems (see Figure 2.1):

- Every secondary user needs to join/establish the connection with the common receiver, which requires a network protocol to implement.
- Some secondary users need a kind of relay routes to reach the common receiver if they are far away from the latter.
- Communication errors or packet drops can affect the performance of such a network if more users have worse reporting channels (e.g. Rayleigh Fading) to reach the common receiver.
- There should be a reliable wireless broadcast channel for the common receiver to inform each of every user once there is a decision made.
- The current centralized network does not fit for the average calculation of all the estimated sensing energy levels, because it requires the common receiver to correctly receive all the local estimated sensing results. Otherwise, the decision precision can not be guaranteed.

2.2 CR-based Mobile Ad hoc Networks

Before presenting the proposed scheme, it is worth noting the particular requirements and restraints about cognitive radio mobile Ad hoc networks. In recent years, MANETs have become a popular subject because of their self-configuration and self-organization capabilities. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Wireless nodes can establish a dynamic network without the need of a fixed infrastructure. A node can function both as a network router for routing packets from the other nodes and as a network host for transmitting and receiving data. MANETs are particular useful when a reliable fixed or mobile infrastructure is not available. Instant conferences between notebook PC users, military applications, emergency operations, and other secure-sensitive operations are important applications of MANETs due to their quick and easy deployment.

2.2.1 Self-organization of MANETs

Due to the complete lack of centralized control, MANETs nodes cooperate with each other to achieve a common goal. The major activities involved in self-organization are neighbor discovery, topology organization, and topology reorganization. Through periodically transmitting beacon packets, or promiscuous snooping on the channels, the activities of neighbors can be acquired. Each node in MANETs maintains the topology of the network by gathering the local or entire network information. MANETs need to update the topology information whenever the networks change such as participation of new node, failure of node and links, etc. Therefore, self-organization is a continuous process that has to adapt to a variety of changes or failures.

2.2.2 Security and Constraints in MANETs

The security in MANETs is very important especially in military environments. Unlike the wired networks, MANETs are inherently insecure because of the lack of any central authority and shared wireless medium. The major security threats that exist in ad hoc wireless networks are as follows: denial of service, resource consumption, host impersonation, information disclosure, and interference. The unique characteristics of MANETs present some new challenges to security design [25].

- Shared wireless broadcast radio: A node can receive and transmit data from and to all the nodes within its direct transmission range.
- Insecure operation environment: MANETs may operate in hostile environments, especially for the tactical MANETs. Nodes frequently move in and out of hostile enemy territory. The chances of node capture are high in such environments, which requires re-authentication.
- Lack of central coordination: There is no centralized network management functionality in MANETs. The existing security solutions for wired networks cannot be applied directly to the MANETs domain.
- Lack of association: Because of the dynamic characteristic of MANETs, it is difficult to find a proper authentication mechanism to use for associating nodes with a network.
- Limited resource availability: Bandwidth, battery power, and computational power are scarce in MANETs.

In tactical MANETs, there are some extra requirements for security design. Since MANETs need to transmit some critical information, security is paramount important. For instance, when CRs are combined with MANETs, there are more security

issues in the aspect of cooperative spectrum sensing. If one or more sensing nodes are compromised, intruders will send false local spectrum sensing results in cooperative spectrum sensing, and it will result in wrong spectrum sensing decisions by CRs in MANETs. Due to the fact that some distinct characteristics of CRs introduce new non-trivial security risks to MANETs with CRs, we have to find a more effective method to counter such attacks.

2.3 Distributed Consensus-based Cooperative Spectrum Sensing Scheme

In this work, we will present a distributed consensus-based cooperative spectrum sensing scheme without using a common receiver. Our scheme is based on recent advances in consensus algorithms [14], or more precisely, bio-inspired mechanisms, which have become important approaches to handle complex communication networks [26–28]. An important motivational background of this area is initially related to the study of complex natural phenomena including flocking of birds, schooling of fish, swarming of ants and honeybees, among others (see the survey [29]). The investigation of such biological systems has generated fundamental insights into understanding the relation between group decision making at the higher level and the individual animals' communication at the lower level [30–34], and in fact consensus seeking in animal colonies is vital for group survival [34]. Such collective animal behavior has motivated many effective yet simple control algorithms for the coordination of multi-agent systems in engineering. Recently, consensus problems have played a crucial role in spacial distributed control models [14, 35], wireless sensor networks [36], and stochastic seeking with noise measurement [37]. Since these algorithms are usually constructed based

on local communication of neighboring agents, they have low implementation complexity and good robustness, and the overall system may still function when local failure occurs. Also, concerning security issues in CRs-based spectrum sensing models in MANETs, the second basic requirement is for the secondary users to collectively filter out the falsified data inserted by SSDF attacks and make the correct decision about the presence of primary users, which can be viewed as a typical multi-agent coordination situation. To achieve more secure results, we incorporate the modified scheme with an authentication scheme using identity (ID)-based cryptography [38] with threshold secret sharing to further improve the security of MANETs with CRs. Compared to traditional public key infrastructure (PKI) approaches, ID-based approaches can reduce the computational complexity of the encryption and decryption operations [39].

The main highlights of this scheme are as follows.

- It is a fully distributed and scalable scheme. Unlike the existing schemes, there is no need for a common receiver to do the data fusion for the final decision. A secondary user only needs to set up neighborhood with those users having desired channel characteristics, such as Line of Sight ones, or even with probabilistic link failures.

- Unlike most decision rules, such as OR-rule or 1-out-of-N, adopted in the existing schemes, we use the consensus of secondary users to make the final decision. Therefore, the proposed scheme can leverage the detection results among users in a severe wireless fading networks.

- The proposed spectrum sensing scheme uses a consensus algorithm to cope with two underlying network models, one with *fixed* bidirectional graphs and one with *random* graphs.

Our consensus-based approach is different from those used in distributed/decentralized detection problems [8–10, 40]. In a typical distributed detection problem [8, 9, 40], each sensor individually forms its own discrete messages based on its local measurement and then reports to a fusion center, and there is in general no direct communication among the sensors. In certain models [10], a sensor may indirectly obtain information about other sensors, but this is achieved by feedback from a common fusion center.

Chapter 3

Secondary Users Network Modeling

This chapter is organized in the following order. First, a network topology in distributed consensus-based cooperative spectrum sensing is presented. Then, the local spectrum sensing model is discussed in details. At last, the network model and consensus notions are presented.

3.1 Network Topology in Distributed Consensus-based Cooperative Spectrum Sensing

As shown in Figure 3.1, no common receiver is necessary compared with Figure 2.1, and secondary users are communicating with each other via communication channels that are in good radio coverage of each of secondary users. Secondary users that are far away from each other do not have direct communication channels due to poor radio signal quality.

There are two stages in the proposed cognitive radio consensus schemes. In the first stage, secondary users use a spectrum sensing model to make measurements about primary users at the beginning of detection. This is done via sensing channels in Figure 3.1. We denote the local measurement of user i as Y_i. In the second stage,

secondary users establish communication links with their own neighbors to locally exchange information among them, and then calculate the obtained data so as to make a local decision whether primary users are around. The above process in the second stage is done iteratively. At the initial time instant $k = 0$, each user i sets $x_i(0) = Y_i$ as the initial value of the local state variable. Next, at time $k = 0, 1, 2, \cdots$, according to the real-time network topology (or local wireless neighborhood), users mutually transmit and receive their states and then use local computation rules to generate updated states $x_i(k+1)$. Those iterations are done repeatedly until all the individual states $x_i(k)$ converge toward a common value x^*.

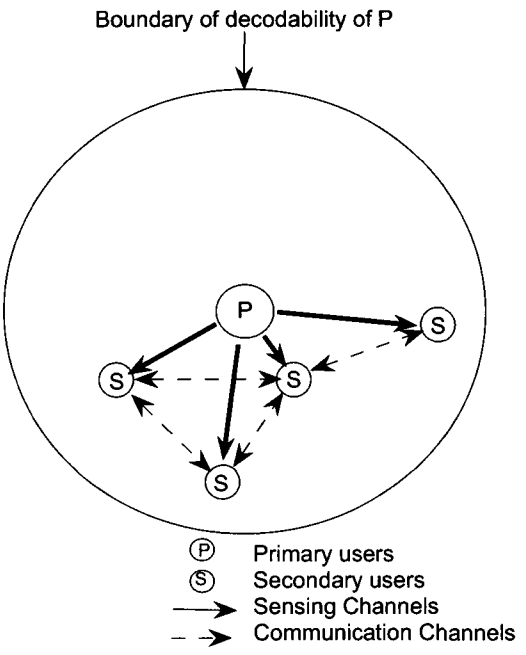


Figure 3.1: A prototype topology of distributed consensus-based cooperative spectrum sensing

Before we introduce the detailed algorithms used in our consensus scheme, the common spectrum sensing model used in the first stage and the network model used in the second stage are to be presented, followed by the formal definition of the spectrum sensing consensus scheme.

3.2 The Spectrum Sensing Model

In the first stage, secondary users make measurements about primary users at the beginning of each time slot. Three kinds of methods are widely used for spectrum sensing [6]: matched filter, energy detector and cyclostationary feature detector.

- **Matched Filter**

The optimal way for any signal detection is a matched filter [41], since it maximizes received signal-to-noise ratio. However, a matched filter effectively requires demodulation of a primary user signal. This means that cognitive radio has a priori knowledge of primary user signal at both PHY and MAC layers, e.g. modulation type and order, pulse shaping, packet format. Such information might be pre-stored in CR memory, but the cumbersome part is that for demodulation it has to achieve coherency with primary user signal by performing timing and carrier synchronization, even channel equalization. This is still possible since most primary users have pilots, preambles, synchronization words or spreading codes that can be used for coherent detection. For examples: TV signal has narrowband pilot for audio and video carriers; CDMA systems have dedicated spreading codes for pilot and synchronization channels; OFDM packets have preambles for packet acquisition. The main advantage of matched filter is that due to coherency it requires less time to achieve high processing gain [42]. However, a significant drawback of a matched filter is that a cognitive radio would need a dedicated receiver for every primary user class.

- **Energy Detector**

  One approach to simplify matched filtering approach is to perform non-coherent detection through energy detection. This sub-optimal technique has been extensively used in radiometry. There are several drawbacks of energy detectors that might diminish their simplicity in implementation. First, a threshold used for primary user detection is highly susceptible to unknown or changing noise levels. Even if the threshold would be set adaptively, presence of any in-band interference would confuse the energy detector. Furthermore, in frequency selective fading it is not clear how to set the threshold with respect to channel notches. Second, energy detector does not differentiate between modulated signals, noise

and interference. Since, it cannot recognize the interference, it cannot benefit from adaptive signal processing for canceling the interferer. Furthermore, spectrum policy for using the band is constrained only to primary users, so a cognitive user should treat noise and other secondary users differently. Lastly, an energy detector does not work for spread spectrum signals: direct sequence and frequency hopping signals, for which more sophisticated signal processing algorithms need to be devised. In general, we could increase detector robustness by looking into a primary signal footprint such as modulation type, data rate, or other signal feature.

- **Cyclostationary Feature Detection**

  Modulated signals are in general coupled with sine wave carriers, pulse trains, repeating spreading, hoping sequences, or cyclic prefixes which result in built-in periodicity. Even though the data is a stationary random process, these modulated signals are characterized as cyclostationary, since their statistics, mean and autocorrelation, exhibit periodicity. This periodicity is typically introduced intentionally in the signal format so that a receiver can exploit it for: parameter estimation such as carrier phase, pulse timing, or direction of arrival. This can then be used for detection of a random signal with a particular modulation type in a background of noise and other modulated signals.

In summary, Matched filter is optimal theoretically, but it needs the prior knowledge of the primary system, which means higher complexity and cost to develop adaptive sensing circuits for different primary wireless systems. Energy detection is suboptimal, but it is simple to implement and does not have too much requirement on the position of primary users. Cyclostationary feature detection can detect the signals with very low SNR, but it still requires some prior knowledge of the primary user [4].

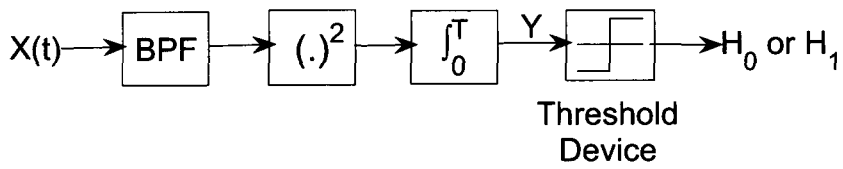


Figure 3.2: Block diagram of an energy detector.

In this thesis, we consider the modeling scenario where the prior knowledge of the primary user is unknown. For implementation simplicity, an energy detection spectrum sensing method [5] is used. Figure 3.2 shows the block-diagram of an energy detector. The input band pass filter (BPF) selects the center frequency f_s and the bandwidth of interest W. This filter is followed by a squaring device and subsequently an integrator over a period of T. The output Y of the integrator is the received energy at the secondary user and its distribution depends on whether the primary user signal is present or not. The goal of spectrum sensing is to decide between the following two hypotheses,

$$x(t) = \begin{cases} n(t), & H_0 \\ h \cdot s(t) + n(t), & H_1 \end{cases} \tag{3.1}$$

where $x(t)$ is the signal received by the secondary user, $s(t)$ is the primary user's transmitted signal, $n(t)$ is the additive white Gaussian noise (AWGN) and h is the amplitude gain of the channel. We also denote by γ the signal-to-noise ratio (SNR). The output of integrator in Figure 3.2 is Y, which serves as the decision statistic. Following the work of [43], Y has the following form,

$$Y = \begin{cases} \chi^2_{2TW}, & H_0 \\ \chi^2_{2TW}(2\gamma), & H_1 \end{cases} \tag{3.2}$$

where χ^2_{2TW} and $\chi^2_{2TW}(2\gamma)$ denote random quantities with central and non-central chi-square distributions, respectively, each with $2TW$ degrees of freedom and a non-centrality parameter of 2γ for the latter distribution. For simplicity we assume that the time-bandwidth product, TW, is an integer number, which is denoted by m.

Under Rayleigh fading, the gain h is random, and the resulting SNR γ would have an exponential distribution, so in this case the distribution of the output energy depends on the average SNR ($\overline{\gamma}$). When the primary user is absent, Y is still distributed according to χ^2_{2TW}. When the primary user is present, Y may be denoted as the sum of two independent random variables [44], [45]:

$$Y = Y_\chi + Y_e, \qquad H_1, \tag{3.3}$$

where the distribution of Y_χ is χ^2_{2TW-2} and Y_e has an exponential distribution with parameter $2(\overline{\gamma}+1)$.

As a summary, after T seconds, each secondary user i detects the energy and gets the measurement $Y_i \in \mathbb{R}^+$.

3.3 The Network Model and Consensus Notions

In the second stage, secondary users establish communication links with its neighbors to locally exchange information among them. In our scheme, the network formed by the secondary users can be described by a standard graph model. For simplicity, this can be represented by an undirected graph (to be simply called a graph) $\boldsymbol{G} = (\mathcal{N}, \mathcal{E})$ [46] consisting of a set of nodes $\{i = 1, 2, \cdots, n\}$ and a set of edges $\mathcal{E} \subset \mathcal{N} \times \mathcal{N}$. Denote each edge as an unordered pair (i, j). Thus, if two secondary users are connected by an edge, it means they can mutually exchange information. A path in $\boldsymbol{G}$ consists of a sequence of nodes $i_1, i_2, \cdots, i_l$, $l \geq 2$, such that $(i_m, i_{m+1}) \in \mathcal{E}$ for all $1 \leq m \leq l-1$.

The graph $\boldsymbol{G}$ is connected if any two distinct nodes in $\boldsymbol{G}$ are connected by a path. For convenience of exposition, we often refer node i as secondary user i. The two names, secondary user and node, will be used interchangeably. The secondary user j (resp., node j) is a neighbor of user i (resp., node i) if $(j,i) \in \mathcal{E}$, where $j \neq i$. Denote the neighbors of node i by $\mathcal{N}_i = \{j|(j,i) \in \mathcal{E}\} \subset \mathcal{N}$. The number of elements in $\mathcal{N}_i$ is denoted by $|\mathcal{N}_i|$ and called the degree of node i.

Throughout this thesis, the analysis is for undirected graphs, because we only deal with good duplex wireless links by which two adjacent nodes can establish communication (being connected) with each other. That is, the graph $\boldsymbol{G}$ is connected, and the information exchange between two neighboring nodes is bidirectional.

The Laplacian of the graph $\boldsymbol{G}$ is defined as $\boldsymbol{L} = (l_{ij})_{n\times n}$, where

$$l_{ij} = \begin{cases} |\mathcal{N}_i|, & \text{if } j = i \\ -1, & \text{if } j \in \mathcal{N}_i \\ 0, & \text{otherwise} \end{cases} \tag{3.4}$$

The matrix $\boldsymbol{L}$ defined by (3.4) is positive semi-definite. Further, if $\boldsymbol{G}$ is a connected undirected graph, then $\text{rank}(\boldsymbol{G}) = n - 1$ (see, e.g., [29]).

Since the cooperative spectrum sensing problem is viewed as a consensus problem where the users locally exchange information regarding their individual detection outcomes before reaching an agreement, we give the formal mathematical definition of consensus as follows.

The underlying network turns out to consist of secondary users reaching a consensus via local communication with their neighbors on a graph $\boldsymbol{G} = (\mathcal{N}, \mathcal{E})$.

For the n secondary users distributed according to the graph model $\boldsymbol{G}$, we assign them a set of state variables x_i, $i \in \mathcal{N}$. Each x_i will be called a consensus variable,

and in the cooperative spectrum sensing context, it is essentially used by node i for its estimate of the energy detection. By reaching consensus, we mean the individual states x_i asymptotically converge to a common value x^*, i.e.,

$$x_i(k) \to x^* \quad \text{as } k \to \infty, \tag{3.5}$$

for each $i \in \mathcal{N}$, where k is the discrete time, $k = 0, 1, 2, \cdots$, and $x_i(k)$ is updated based on the previous states of node i and its neighbors.

The special cases with $x^* = \text{Ave}(x) = (1/n)\sum_{i=1}^{n} x_i(0)$, $x^* = \max_{i=1}^{n} x_i(0)$ and $x^* = \min_{i=1}^{n} x_i(0)$ are called average-consensus, max-consensus, and min-consensus, respectively. It is worth mentioning that the existing spectrum sensing algorithm with the OR-rule can be viewed as a form of max-consensus. This thesis is intended to propose a cooperative spectrum sensing scheme in the framework of average-consensus.

Chapter 4

Distributed Consensus-based Cooperative Spectrum Sensing in Fixed Graphs

In this chapter, let us assume the secondary users have established duplex wireless connections with their desired neighbors, and the connections remain working until the consensus is reached. This kind of topology is called as a fixed graph. Based on this assumption, we are going to propose the spectrum sensing consensus algorithm as follows.

4.1 The Consensus Algorithm

We denote for user i, its measurement Y_i at time $k = 0$ by $x_i(0) = Y_i \in \mathbb{R}^+$. The state update of the consensus variable for each secondary user occurs at discrete time $k = 0, 1, 2, \cdots$, which is associated with a given sampling period. From $k = 0, 1, 2, \cdots$, the iterative form of the consensus algorithm can be stated as follows [29]:

$$x_i(k+1) = x_i(k) + \epsilon \sum_{j \in \mathcal{N}_i} (x_j(k) - x_i(k)), \tag{4.1}$$

where

$$0 < \epsilon < (\max_i |\mathcal{N}_i|)^{-1} \triangleq 1/\Delta. \tag{4.2}$$

The number Δ is called the maximum degree of the network.

This algorithm can be written in the vector form:

$$\boldsymbol{x}(k+1) = \boldsymbol{P}\boldsymbol{x}(k), \tag{4.3}$$

where $\boldsymbol{P} = \boldsymbol{I} - \epsilon \boldsymbol{L}$. Notice that the upper bound in (4.2) for ϵ ensures that $\boldsymbol{P}$ is a stochastic matrix, and in fact one can further show that $\boldsymbol{P}$ is ergodic when $\boldsymbol{G}$ is connected[1]. Since $\boldsymbol{G}$ is an undirected graph, all row sums and column sums of $\boldsymbol{L}$ are equal to zero. Hence $\boldsymbol{P}$ is a doubly stochastic matrix (i.e.,$\boldsymbol{P}$ is a nonnegative matrix and all of its row sums and column sums are equal to one).

We also point out that (4.3) uses only a particular construction of the coefficient matrix for the consensus algorithm, which is based on the graph Laplacian $\boldsymbol{L}$. As long as each node has the prior knowledge of an upper bound of the maximum degree Δ of the network, the iteration may be implemented and there is no necessity for neighboring nodes to exchange information regarding the network structure. Also, it is possible to construct $\boldsymbol{P}$ in other forms. An alternative choice of $\boldsymbol{P}$ may be based

[1]For some network topologies, it is possible to have an ergodic matrix $P = I - \epsilon L$ when $\epsilon = 1/\Delta$. For instance, if ϵ is taken as $1/\Delta$ and meanwhile it is ensured that P has at least one positive diagonal entry, then it can be shown that P is an ergodic stochastic matrix.

on the so called Metropolis weights [36] by taking

$$\tilde{p}_{ij} = \begin{cases} \frac{1}{1+\max\{d_i,d_j\}} & \text{if } (j,i) \in \mathcal{E}, \\ 1 - \sum_{j \in \mathcal{N}_i} \tilde{p}_{ij} & \text{if } i = j, \\ 0 & \text{otherwise,} \end{cases}$$

where $d_i = |\mathcal{N}_i|$ is the degree of node i. If $\boldsymbol{G}$ is a connected graph and we define $\widetilde{\boldsymbol{P}} = (\tilde{p}_{ij})_{n \times n}$, then $\widetilde{\boldsymbol{P}}$ is an ergodic doubly stochastic matrix. When $\widetilde{\boldsymbol{P}}$ is used in (4.3) in place of $\boldsymbol{P}$, the state average will still be preserved as an invariant during the iterations and our convergence analysis below is still valid. Notice that when $\widetilde{\boldsymbol{P}}$ is used in the consensus algorithm, it is only required that any two neighboring nodes report to each other their degrees, and the knowledge of the maximum degree of the network is no longer needed.

We cite a theorem concerning the convergence property of the consensus algorithm.

Theorem 4.1 *(see, e.g., [29]) Consider a network of secondary users,*

$$x_i(k+1) = x_i(k) + u_i(k), \tag{4.4}$$

with topology $\boldsymbol{G}$ applying the distributed consensus algorithm (4.1), where $u_i(k) = \epsilon \sum_{j \in \mathcal{N}_i} (x_j(k) - x_i(k))$, $0 < \epsilon < 1/\Delta$, and Δ is the maximum degree of the network. Let $\boldsymbol{G}$ be a connected undirected graph. Then

1. *A consensus is asymptotically reached for all initial states;*
2. *$\boldsymbol{P}$ is doubly stochastic, and an average-consensus is asymptotically reached with the limit $x^* = (1/n) \sum_{i=1}^{n} x_i(0)$ for the individual states.* ■

According to Theorem 4.1, if we choose ϵ such that $0 < \epsilon < 1/\Delta$, then an average-consensus is ensured and the final common value $x^* = (1/n)\sum_{i=1}^{n} x_i(0)$ will be the average of the initial vector $\boldsymbol{x(0)}$, or equivalently, the average of $\boldsymbol{Y^T} = \{Y_1, Y_2, \cdots, Y_n\}$, which has been obtained during the energy detection stage.

Finally, by comparing the average consensus result x^* with a pre-defined threshold λ based on Figure 3.2, every secondary user i gets the final data fusion locally:

$$\textit{Decision } \boldsymbol{H} = \begin{cases} 1, & x^* > \lambda \\ 0, & \text{otherwise.} \end{cases} \tag{4.5}$$

4.2 Performance of the Consensus Algorithm

It is quite apparent that the convergence rate is yet another interesting issue in evaluating the performance of the spectrum sensing consensus algorithm. This is due to the fact that secondary users must continuously detect the presence of primary users, and back up as soon as possible on recognizing such incident. From this point of view, the speed of reaching a consensus is the key in the design of the network topology as well as the analysis of the performance of a consensus algorithm for a given spectrum sensing network. For the *connected* undirected graph $\boldsymbol{G}$, the above algorithm can ensure exponential convergence rate, where the error can be parameterized in the form $O(e^{-\delta t})$ with the exponent $\delta > 0$. To have some bound estimate for the parameter δ, we first recall that $\boldsymbol{P} = \boldsymbol{I} - \epsilon \boldsymbol{L}$. Since L is a positive semi-definite matrix, denote its n eigenvalues by

$$0 = \lambda_1 < \lambda_2 \leq \cdots \leq \lambda_n. \tag{4.6}$$

Here $\lambda_2 > 0$ since the undirected graph $\mathbf{G}$ is *connected* which ensures that the rank of $\boldsymbol{L}$ is equal to $n-1$ ([47]). The second smallest eigenvalue λ_2 of $\boldsymbol{L}$ is usually called the algebraic connectivity of the undirected graph $\boldsymbol{G}$. Then the second largest absolute value of the eigenvalues of $\boldsymbol{P}$ is determined as $\alpha(\epsilon) = \max\{|1-\epsilon\lambda_2|, |1-\epsilon\lambda_n|\}$, which can be verified to satisfy $\alpha(\epsilon) < 1$. By using standard results in nonnegative matrix theory (see, e.g., [48]), we can obtain an upper bound for δ. In fact, we can take δ as any value in the interval $(0, -\ln\alpha(\epsilon))$. We also remark that similar convergence rate estimates can be carried out when general weight matrices in averaging are used.

Since $\boldsymbol{P}$ has a unit eigenvalue, we see that the difference between the first two largest absolute values of the eigenvalues of $\boldsymbol{P}$ is given as $g(\epsilon) = 1 - \alpha(\epsilon)$, which is customarily called the spectral gap of $\boldsymbol{P}$. In general, the greater is $g(\epsilon)$, the greater is the upper bound $-\ln\alpha(\epsilon)$ for the exponent δ, and the faster is the convergence of the consensus algorithm. In practical implementations, it is desirable to choose a suitable value for ϵ to increase the spectral gap $g(\epsilon)$ while $\boldsymbol{P}$ is ensured to be ergodic. We will discuss the convergence rate in the simulation part of this thesis.

Chapter 5

Distributed Consensus-based Cooperative Spectrum Sensing in Random Graphs

In the previous chapter, it has been assumed that any two neighboring nodes can reliably exchange data at all times. Hence the network topology remains unchanged during the overall time period of interest. This kind of network modeling may not be accurate in certain situations. For example, fading of wireless signals can cause packet errors, which will result in wireless link failures for that period. Furthermore, even under LOS channels, moving objects between neighboring nodes may temporarily affect signal reception. For the above reasons, in this chapter, we consider a more realistic inter-node communication model with random link failures. Unlike the previous model, which is based on fixed bidirectional graphs, the new model is based on random graphs. Nevertheless, similar to the previous fixed topology scenario, for the random graph based modeling below, we still consider bidirectional links when two nodes can communicate.

5.1 Random Graph Modeling of the Network Topology

Before characterizing random connectivity of the network of all secondary users, let us first introduce a fixed undirected graph $\boldsymbol{G} = (\mathcal{N}, \mathcal{E})$ which describes the maximal set of communication links when there is no link failure. Due to the random link failures, at time k the inter-user communication is described by a subgraph of $\boldsymbol{G}$ denoted by $\boldsymbol{G}(k) = (\mathcal{N}, \mathcal{E}(k))$ where $\mathcal{E}(k) \subset \mathcal{E}$; the edge $(j, i) \in \mathcal{E}(k)$ if and only if nodes j and i can communicate at time k where $(j, i) \in \mathcal{E}$. Thus, the (undirected) graph $\boldsymbol{G}(k)$ is generated as the outcome of random link failures. Note that an edge (j, i) never appears in $\boldsymbol{G}(k)$ if it is not an edge of $\boldsymbol{G}$. The neighbor set of node i is $\mathcal{N}_i(k) = \{j|(j, i) \in \mathcal{E}(k)\}$ at time k. The number of elements in $\mathcal{N}_i(k)$ is denoted by $|\mathcal{N}_i(k)|$. At time $k \geq 0$, the adjacency matrix of $\boldsymbol{G}(k)$ is defined as $\boldsymbol{A}(k) = (\alpha_{ji}(k))_{1 \leq j,i \leq |\mathcal{N}|}$, where $\alpha_{ji}(k) = 1$ if $(j, i) \in \mathcal{E}(k)$, and $\alpha_{ji}(k) = 0$ otherwise. It is clear that the graph $\boldsymbol{G}(k)$ is completely characterized by the random matrix $\boldsymbol{A}(k)$.

Concerning the statistical properties of link failures, we assume that for all links (each associated with an edge in the graph $\boldsymbol{G}$) fail independently with the same probability $p \in (0, 1)$. For notational simplicity we use the same parameter p to model the failure probability. The generalization of the modeling and analysis to link-dependent failure probabilities is straightforward.

5.2 The Algorithm with Random Graphs

For the random link failure-prone model, the two spectrum sensing stages introduced in the previous chapter are still applicable. In the first stage, each node performs the radio detection and computes the measurements according to (3.1). During the second stage, at time k each node exchanges states information with its neighbors

and performs the corresponding computation to generate its state update $x_i(k+1)$. Let Δ be the maximum degree of the graph $\boldsymbol{G}$, and take $\epsilon \in (0, 1/\Delta)$.

The state of user $i \in \mathcal{N}$ is updated by the rule

$$x_i(k+1) = x_i(k) + \epsilon \sum_{j \in \mathcal{N}_i(k)} [x_j(k) - x_i(k)], \tag{5.1}$$

where ϵ is a pre-determined constant step size. If $\mathcal{N}_i(k) = \emptyset$ (empty set), (5.1) reduces to $x_i(k+1) = x_i(k)$.

Theorem 5.1 *Under the independent link failure assumption, the algorithm (5.1) ensures average consensus, i.e.,* $\lim_{k\to\infty} x_i(k) = (1/n)\sum_{j=1}^n x_j(0)$ *for all* $i \in \mathcal{N}$, *with probability one. If, in addition,* $E|x(0)|^2 < \infty$ *and* $x(0)$ *is independent of the sequence of adjacency matrices* $\mathbf{A}(k)$, $k = 0, 1, \cdots$, *then each* $x_i(k)$ *converges to* $(1/n)\sum_{j=1}^n x_j(0)$ *in mean square with an exponential convergence rate.*

Proof. We can write the algorithm (5.1) in the vector form

$$\boldsymbol{x}(k+1) = [\boldsymbol{I} - \epsilon \boldsymbol{L}(k)]\boldsymbol{x}(k),$$

where $\boldsymbol{L}(k)$ is the Laplacian of the graph $\boldsymbol{G}(k)$. For a vector $\boldsymbol{z} = (z_1, \cdots, z_n)^T$, denote the Euclidean norm $|\boldsymbol{z}| = (\sum_{i=1}^n z_i^2)^{1/2}$. For any given sample point, we can show that $\boldsymbol{M}(k) = \boldsymbol{I} - \epsilon \boldsymbol{L}(k)$ is a symmetric aperiodic stochastic matrix so that it has all its eigenvalues within the interval $(-1, 1]$ (see, e.g., [48]), and therefore $\boldsymbol{M}(k)$ determines a paracontracting map [36, 49] in the sense $\boldsymbol{M}(k)\boldsymbol{z} \neq \boldsymbol{z}$ if and only if $|\boldsymbol{M}(k)\boldsymbol{z}| < |\boldsymbol{z}|$. For $\boldsymbol{M}(k)$, we denote its fixed point subspace $\mathcal{H}(\boldsymbol{M}(k)) = \{\boldsymbol{z} \in \mathbb{R}^n | \boldsymbol{M}(k)\boldsymbol{z} = \boldsymbol{z}\}$.

By the assumption on the independent link failures, we see that with probability one, $\boldsymbol{G}(k) = \boldsymbol{G}$ for an infinite number of times k. Let Ω denote the underlying probability sample space. Thus, after excluding a set A_0 of zero probability, for all

$\omega \in \Omega \backslash A_0$, $\boldsymbol{G}(k) = \boldsymbol{G}$ infinitely often with the associated Laplacian being $\boldsymbol{L}(k) = \boldsymbol{L}$. Hence, for each $\omega \in \Omega \backslash A_0$, $x(k)$ converges to a point in the space $\mathcal{H}(\boldsymbol{I} - \epsilon \boldsymbol{L}) = \{z \in \mathbb{R}^n | \boldsymbol{L}z = 0\}$ when $k \to \infty$. Furthermore, $\{\boldsymbol{z} \in \mathbb{R}^n | \boldsymbol{L}\boldsymbol{z} = 0\} = \text{span}\{1_n\}$ since $\boldsymbol{G}$ is a connected undirected graph.

On the other hand, it is straightforward to check that $(1/n)\sum_{j=1}^n x_j(k)$ remains as a constant since $\boldsymbol{M}(k)$ is a doubly stochastic matrix (i.e., nonnegative matric with all row sums and column sums equal to one). Now it follows that each $x_i(k)$ converges to $(1/n)\sum_{j=1}^n x_j(0)$ with probability one, as $k \to \infty$.

We continue to analyze mean square convergence. Since $E|\boldsymbol{x}(0)|^2 < \infty$ and $\sup_{i\in\mathcal{N}, k\geq 0} |x_i(k)| \leq \max_{i\in\mathcal{N}} |x_i(0)| \leq |\boldsymbol{x}(0)|$, by the probability one convergence of $x_i(k)$, it follows from dominated convergence results in probability theory that $x_i(k)$ also converges to $(1/n)\sum_{j=1}^n x_j(0)$ in mean square.

Now, we proceed to give an estimation of the mean square convergence rate within the random network model. Denote $\text{Ave}(\boldsymbol{x}(0)) = (1/n)\sum_{j=1}^n x_j(0)$. It is straightforward to show that

$$\boldsymbol{x}(k+1) - \text{Ave}(\boldsymbol{x}(0))\mathbf{1}_n = [\boldsymbol{I} - (1/n)\mathbf{1}_n\mathbf{1}_n^T][\boldsymbol{I} - \epsilon \boldsymbol{L}(k)][\boldsymbol{x}(k) - \text{Ave}(\boldsymbol{x}(0))\mathbf{1}_n] \tag{5.2}$$

$$\equiv \boldsymbol{B}(k)[\boldsymbol{x}(k) - \text{Ave}(\boldsymbol{x}(0))1_n]. \tag{5.3}$$

In fact, for each $\omega \in \Omega$, by the eigenvalue distribution of the matrices $(1/n)\mathbf{1}_n\mathbf{1}_n^T$ and $\boldsymbol{L}(k)$, we can show that $\boldsymbol{B}^T(k)\boldsymbol{B}(k)$, and subsequently $E[\boldsymbol{B}^T(k)\boldsymbol{B}(k)]$, have n real eigenvalues on the interval $[0, 1]$. We use a contradiction argument to show that the largest eigenvalue ρ of $E[\boldsymbol{B}^T(k)\boldsymbol{B}(k)]$ is less than one. Suppose $\rho = 1$ for $E[\boldsymbol{B}^T(k)\boldsymbol{B}(k)]$; then there exists a real-valued vector $\boldsymbol{x} \neq 0$ such that

$$\boldsymbol{x}^T E[\boldsymbol{B}^T(k)\boldsymbol{B}(k)]\boldsymbol{x} = \boldsymbol{x}^T\boldsymbol{x}. \tag{5.4}$$

By the fact $\boldsymbol{x}^T[\boldsymbol{B}^T(k)\boldsymbol{B}(k)]\boldsymbol{x} \leq \boldsymbol{x}^T\boldsymbol{x}$, the equality (5.4) leads to

$$\boldsymbol{x}^T[\boldsymbol{B}^T(k)\boldsymbol{B}(k)]\boldsymbol{x} = \boldsymbol{x}^T\boldsymbol{x} \tag{5.5}$$

with probability one. On the other hand, by the link failure assumption, there exists a set $A_1 \subset \Omega$ such that $P(A_1) > 0$ and for each $\omega \in A_1$, the associated matrix value $\boldsymbol{B}(k) = \boldsymbol{I} - \epsilon\boldsymbol{L}$. Without the loss of generality, we can assume A_1 has been chosen in such a manner that for any $\omega \in A_1$, (5.5) also holds.

By noticing the fact that for any $\boldsymbol{z} \in \mathbb{R}^n$,

$$\boldsymbol{z}^T[\boldsymbol{B}^T(k)\boldsymbol{B}(k)]\boldsymbol{z} \leq \boldsymbol{z}^T(\boldsymbol{I} - \epsilon\boldsymbol{L})^2\boldsymbol{z} \leq \boldsymbol{z}^T\boldsymbol{z}, \tag{5.6}$$

we obtain from (5.5) that

$$\boldsymbol{x}^T(\boldsymbol{I} - \epsilon\boldsymbol{L})^2\boldsymbol{x} = \boldsymbol{x}^T\boldsymbol{x}. \tag{5.7}$$

Hence, (5.7) implies that $\boldsymbol{x}$ is the eigenvector of $\boldsymbol{I} - \epsilon\boldsymbol{L}$ associated with the eigenvalue 1, which further implies that $\boldsymbol{x} \in \text{span}\{\mathbf{1}_n\}$. Denote $\boldsymbol{x} = c\mathbf{1}_n$ where c is a constant. By substituting $\boldsymbol{x} = c\mathbf{1}_n$ into the left hand side of (5.5), we obtain $\boldsymbol{x}^T[\boldsymbol{B}^T(k)\boldsymbol{B}(k)]\boldsymbol{x} = 0$ for each $\omega \in \Omega$, which contradicts with (5.5) and the fact $\boldsymbol{x} \neq 0$. Hence, we conclude that the largest eigenvalue ρ of $E[\boldsymbol{B}^T(k)\boldsymbol{B}(k)]$ is in the interval $[0, 1)$.

Finally, by elementary calculation we obtain the convergence rate estimate

$$E|\boldsymbol{x}(k) - \text{Ave}(\boldsymbol{x}(0))\mathbf{1}_n|^2 \leq \rho^k E|\boldsymbol{x}(0) - \text{Ave}(\boldsymbol{x}(0))\mathbf{1}_n|^2. \tag{5.8}$$

□

In fact, we have the simplified expression:

$$\begin{aligned}\boldsymbol{B}^T(k)\boldsymbol{B}(k) &= [\boldsymbol{I} - \epsilon\boldsymbol{L}(k)][\boldsymbol{I} - (1/n)\mathbf{1}_n\mathbf{1}_n^T]^2[\boldsymbol{I} - \epsilon\boldsymbol{L}(k)] \\ &= [\boldsymbol{I} - \epsilon\boldsymbol{L}(k)][\boldsymbol{I} - (1/n)\mathbf{1}_n\mathbf{1}_n^T][\boldsymbol{I} - \epsilon\boldsymbol{L}(k)] \\ &= [\boldsymbol{I} - \epsilon\boldsymbol{L}(k)]^2 - (1/n)\mathbf{1}_n\mathbf{1}_n^T,\end{aligned}$$

and therefore, ρ is also given as the largest eigenvalue of the positive semi-definite matrix $E[\boldsymbol{I} - \epsilon\boldsymbol{L}(k)]^2 - (1/n)\mathbf{1}_n\mathbf{1}_n^T$.

Chapter 6

Counter Spectrum Sensing Data Falsification (SSDF) Attacks in Cognitive Radio Ad Hoc Networks

This chapter contains SSDF attack models, modified consensus-based spectrum sensing scheme to counter SSDF attacks and authentication using ID-based cryptography with threshold secret sharing.

6.1 SSDF Attack Models in Cooperative Spectrum Sensing

In cooperative spectrum sensing, a group of secondary users perform spectrum sensing by collaboratively exchanging locally-collected information. Malicious secondary users may take advantage of the cooperative spectrum sensing and launch SSDF attacks by sending false local spectrum sensing results to others, resulting in a wrong spectrum sensing decision. Three attack models are presented as follows.

In the first attack model, a malicious secondary user sends out a relatively high primary user energy to indicate the presence of primary users although there is no

primary user and its sensed energy is low. In this case, fusion center and other secondary users make a wrong decision that primary users are present and they will not use the spectrum. The intention of the malicious secondary user is to gain the exclusive access to the target spectrum. We call this kind of attacks as Selfish SSDF.

In the second attack model, a malicious secondary user sends out a relatively low primary user energy to indicate the absence of primary users although there are primary users and its sensed energy is high. In this case, fusion center and other secondary users make a wrong decision that there is no primary user and they will use the spectrum. The intention of the malicious secondary user is to give interference to primary users. We call this kind of attacks as Interference SSDF.

In the third attack model, a malicious secondary user sends out a random primary user energy during the process of cooperative spectrum sensing. That is, sometimes, it sends out a correct primary user energy; sometimes, it sends out a false value. The intention of the malicious secondary user is to make other secondary confused, and overall performance of fusion center is affected. We call this kind of attacks as Confusing SSDF.

As an important line of defense, an authentication scheme, such as the one to be presented in Section 6.3, can be used to protect MANETs with CRs in cooperative spectrum sensing. However, the experience in security of traditional wireless networks indicates that there are always some weak points in the system that are hard to predict, no matter what is used for authentications. Therefore, multi-level protection mechanisms are needed in wireless networks. The is especially true for MANETs with CRs, given the low physical security of mobile devices. Therefore, to mitigate these SSDF attacks, we will apply recent advances in consensus algorithms in cooperative spectrum sensing. The network model and consensus notions will be introduced in the next chapter.

6.2 Distributed Consensus-based Cooperative Spectrum Sensing Scheme to Counter SSDF attacks

Let us assume secondary users have established duplex wireless connections with its desired neighbors, and the connections remain working until the consensus is reached. So the network topology is modeled by a fixed graph. Note that the attackers are included as some nodes in the graph and they will provide falsified information to authentic secondary users. Based on this assumption, we make little modification to the proposed consensus-based spectrum sensing scheme.

1. In the first stage, all the secondary users individually sense the target spectrum band based on the spectrum sensing models, and obtain the local estimated energy level denoted by Y_i.

2. In the second stage, all the users establish the wireless communication links with its neighbors, and then begin to exchange the local updated estimated energy level from time instant $k \in \mathbb{Z}+$. This process is done in iterations. We denote for user i, its measurement Y_i at time instant $k = 0$ by $x_i(0) = Y_i \in \mathbb{R}^+$. The state update of the consensus variable for each secondary user occurs at discrete time instant $k = 0, 1, 2, \cdots$, which is associated with a given sampling period. In each time instant k, once receiving the updated estimated energy level $x_j(k)$ from neighbors, each user i first uses a selection criterion to exclude a neighbor that is more likely to be an attacker. In turn, this procedure generates a subset of neighbors whose date will be used in updating the state of user i. After the local update computation, each user i sends out its updated estimated energy level $x_i(k+1)$ to its neighbors. Then the above neighbor selection and state

updating procedure are repeated at the individual nodes until all the estimated energy levels $x_i(k)$ converge to a common value x^* within a prescribed error.

Finally, by comparing the average consensus result x^* with a pre-defined threshold λ based on Figure 3.2, every secondary user i gets the final data fusion locally (see (4.5)

Now we describe the selection rule in detail. Consider $k \geqslant 1$ and we assume $|\mathcal{N}_i| > 2$. The procedure below is applied by each authentic secondary user.

1. First, user i gets the local mean value at time instant $k-1$

$$\mu_i(k-1) = \frac{x_i(k-1) + \sum_{j \in \mathcal{N}_i} x_j(k-1)}{1 + |\mathcal{N}_i|}. \tag{6.1}$$

2. Secondly, user i identifies the neighbor with the maximum deviation from the value $\mu_i(k-1)$:

$$\hat{j} = \arg\max_{j \in \mathcal{N}_i} |x_j(k) - \mu_i(k-1)|. \tag{6.2}$$

3. Thirdly, user i forms a set $\widehat{\mathcal{N}}_i(k)$ of neighbors that are regarded as authentic users:

$$\hat{\mathcal{N}}_i(k) = \mathcal{N}_i \backslash \{\hat{j}\}. \tag{6.3}$$

When $k = 0$ or $|\mathcal{N}_i| \leqslant 2$, we set $\hat{\mathcal{N}}_i(k) = \mathcal{N}_i$. The reason why $k = 0$ is an exception is apparent.

Next, we present the consensus algorithm incorporating neighbor selection. From $k = 0, 1, 2, \cdots$, the iterative form of the consensus algorithm can be stated as follows,

which is similar to (4.1):

$$x_i(k+1) = x_i(k) + \epsilon \sum_{j \in \widehat{\mathcal{N}}_i(k)} (x_j(k) - x_i(k)), \tag{6.4}$$

where ϵ follows the rule set by (4.2).

If the basic algorithm (where $\widehat{\mathcal{N}}_i(k)$ is always set as $\mathcal{N}_i$ in (6.4); see, e.g., [29]) is applied and there are no attackers, then an average-consensus is ensured and the final common value $x^* = (\frac{1}{n}) \sum_{i=1}^{n} x_i(0)$ will be the average of the initial vector $\boldsymbol{x(0)}$, or equivalently, the average of $\boldsymbol{Y^T} = \{Y_1, Y_2, \cdots, Y_n\}$ will be obtained in the end of the previous energy detection section.

We seek the help from Theorem 4.1 concerning the convergence property of the consensus algorithm without attackers. According to Theorem 4.1, if there is no attackers and we choose ϵ such that $0 < \epsilon < \frac{1}{\Delta}$, then an average-consensus will be ensured and the final common value $x^* = (\frac{1}{n}) \sum_{i=1}^{n} x_i(0)$ will be the average of the initial vector $\boldsymbol{x(0)}$, or equivalently, the average of $\boldsymbol{Y^T} = \{Y_1, Y_2, \cdots, Y_n\}$ will be obtained in the end of the previous energy detection section. It can be further shown that the above algorithm can achieve an exponential convergence rate. In practical implementations, the exponent δ depends on the network topology and the parameter ϵ.

However, when attackers are present, the nature of the basic consensus algorithm in Theorem 4.1 is changed in that the neighborhood of each authentic user must be determined on-line according to the information it has received so that the user most likely to be an attacker is rejected. Moreover, due to the neighbor selection procedure applied by the authentic users, it is possible that secondary user A accepts secondary user B as a neighbor but the latter does not accept the former. This may result in unidirectional information exchange along certain edges of the graph $\boldsymbol{G}$. Hence, the algorithm (6.4) is essentially associated with a sequence of directed

graphs $\mathbf{G}_t = (\mathcal{N}_a, \mathcal{E}_t)$, where $\mathcal{N}_a$ corresponds to the set of authentic secondary users. In this case, since the coefficient matrix in the algorithm is in general not doubly stochastic as in Theorem 4.1, one cannot expect convergence to the average value of the initial states. Also, the convergence of the algorithm under attacks depends on the structure of the sequence of directed graphs $\boldsymbol{G}_t$. Indeed, if there is a large constant T such that for any time window $[k, k+T]$, the union $\cup_{t=k}^{k+T} \boldsymbol{G}_t$, as the directed graph formed by putting all edges of $\boldsymbol{G}_t$ together, is strongly connected, then convergence of the algorithm is guaranteed [35]; such a joint connectivity of $\boldsymbol{G}_t$ means that any two authentic secondary users can always directly or indirectly exchange information on a sufficiently long time window.

6.3 Authentication Using ID-Based Cryptography with Threshold Secret Sharing in Cognitive Radio Ad Hoc Networks

As an important line of defense, an authentication scheme based on cryptography can be used to further improve the security of MANETs with CRs. In the proposed consensus-based spectrum sensing scheme, authentication can be done when exchanging the estimated energy levels between secondary users to identify and eliminate malicious nodes.

Traditional public key infrastructure (PKI) approaches work well in wired networks. In general, PKI-based approaches require a global trusted certificate authority (CA) to provide certificates for the nodes and the certificates can be verified using the CA's public key. However, MANETs do not possess such an infrastructure. In addition, traditional PKI-based authentication and encryption mechanisms are relatively expensive in terms of generating and verifying digital signatures, which limit

their practical application to MANETs. Symmetric cryptography is more efficient due to its reduced computational complexity, in which the communicating parties share a secret key. But when used in MANETs, the problem becomes distributing the shared keys in the first place. Compared to traditional PKI, identity based (ID-based) cryptography [38] can reduce the computational complexity of the encryption and decryption operations [39]. Moreover, ID-based approaches allow public keys to be derived from entities' known identity information, thus eliminating the need for public key distribution and certificates.

6.3.1 ID-Based Cryptography

ID-based cryptography was introduced by Shamir [38], but did not become a serious subject of study until the break-through paper of Boneh and Franklin [50] in which the first efficient and provably secure Identity Based Encryption (IBE) scheme was presented. In an ID-based system, the shared key between two parties in communication is computed based on one party's private key and another party's identity, such as an email address or a telephone number etc. The node secret key can be generated from a Trusted Authority (TA), or a Private Key Generator (PKG).

In general, an IBE scheme can be defined by four algorithms [50], with functions as suggested by their names: *Setup*, (Private Key) *Extract*, *Encrypt* and *Decrypt*.

Setup: Takes as input a security parameter k_{id} and (if probabilistic) some randomness r whose length is polynomial in k_{id}. It outputs a set of public parameters that is assumed to include descriptions of the private key space SK, plaintext space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ of the scheme. Setup also outputs a master secret key. The system parameters will be publicly known, while the master key will be known only to the PKG.

Extract: Takes as input public parameters and master key along with an identifier

$ID \in \{0,1\}^*$, and produces a private key $SK_{ID} \in SK$. This algorithm may also be probabilistic.

Encrypt: Takes as input public parameters and an identifier ID along with a message $\mathcal{M}$, and outputs a ciphertext $C \in \mathcal{C}$.

Decrypt: Takes as input parameters, a private key S_{ID} and a cipher text C. It outputs either message M or a decryption failure.

The major advantage of IBE is that it requires less interaction and lower bandwidth than traditional PKI but offers greater flexibility, which makes it very suitable in MANETs [51, 52].

6.3.2 Threshold Secret Sharing

The dynamic nature and the absence of a centralized control in MANETs make key management more difficult. Recently, several key management schemes for MANETs have been proposed [39, 53]. Since safely maintaining a super server for key distribution presents an important issue in MANETs, threshold cryptography [54, 55] is used to let some or all network nodes share a network master key and collaboratively issue private keys. In [51], a partially distributed certificate authority scheme is proposed based on PKI. In a MANET with N nodes, a group of n particular nodes is capable of generating partial certificates using their shares of the certificate signing key. A valid certificate can be obtained by combining k_{id} such partial certificates, which is called (k_{id}, n)-threshold cryptography. Authors in [56] propose to use nodes' physical characteristics to choose n nodes by the network operator for secret sharing. A key management scheme is proposed in [57] using ID-based cryptography and (k_{id}, n)-threshold secret sharing. In [53], a (k_{id}, N)-threshold scheme is proposed, in which each of the N nodes in a MANET is furnished with a share of the master key. A novel construction method for ID-based public/private keys and secret-sharing parameters

are studied in [39].

6.3.3 Key Refreshing

Public/private keys of mobile nodes in MANETs need to be refreshed when the system is in low security situations, or at certain time intervals even when it is in high security situations [58]. In a key refreshing process, a node needs to obtain its new public key and corresponding private key. The way to obtain the private key with threshold cryptography is to present the identity and request private key generation service from at least k_{id} among the n nodes that hold the master key shares. However, when a node is selected for security key services, the information from this node can be picked up and monitored by the adversary. By doing cryptanalysis, the key materials in the node could be compromised. If k_{id} nodes with master key shares are compromised, the security of the whole network is breached. Then, in the key management design, the following should be answered. How should the MANET dynamically decide which k_{id} nodes among the n nodes with master key shares do the private key generation service at each time instant in order to minimize the overall threat posed to the MANET while simultaneously taking into account the cost of using these nodes.

This problem can be formulated as a partially observed Markov decision process (POMDP) multi-arm bandit system [59], which has been widely studied in operations research in the context of an infinite-horizon discounted cost stochastic control problems [60]. This problem is studied to make the optimal decision of which arm of the multi-slot gambler machine to pull each time to maximize the total reward. The object, which is the arm in the gambler machine example, has a finite set of available states and the transition probabilities between the states. At each epoch, with the tradeoff of system studying and reward collecting, k_{id} objects among n are selected

to be active to maximize the total discounted reward over the horizon. This is very similar to the node selection problem for ID-based threshold key management with intrusion detection in MANETs. We have been studying the node selection problems in MANETs with CRs.

6.3.4 Authentication using ID-based Cryptography with Threshold Secret Sharing

The keys generated above can be used for various security schemes, such as ciphering and authentication, which follow the traditional PKI-based approaches, but handshake and exchange of certificates are not necessary. Assume that a secondary user S wants to send a secondary user D an estimated energy level, such that only secondary user D can decrypt, and secondary user D can make sure that the message is really from S. S can simply sign the message using its private key, encrypt using D's identity (public key) and send it to D. When D receives this encrypted message, it decrypts it first using its private key, and then using the S' public key. If the verification process succeeds, D accepts this message as a valid one, and the consensus-based spectrum sensing update in Chapter 6 follows. If the verification process does not succeed, the message is from a malicious secondary user, and D discards this message as an invalid one.

Chapter 7

Simulation Results and Discussions

In this chapter, we first introduce simulation results of the distributed consensus-based scheme not considering malicious attacks (see Chapter 4 and Chapter 5), and then those of the proposed scheme considering malicious attacks (see Chapter 6).

7.1 Distributed Consensus-Based Cooperative Spectrum Sensing Without Malicious Attacks

This section begins with the simulation setup for the scheme introduced in Chapter 4 and Chapter 5 without considering malicious attacks. Then, some simulation results are presented and discussed to show the performance of the proposed scheme.

7.1.1 Simulation Setup

In the simulations, we assume that all secondary users are experiencing i.i.d. Rayleigh fading without spatial correlation. Each secondary user uses an energy detector. We simulate the output Y of the energy detector directly in our simulations. When the primary user is absent, Y is a random quantity with chi-square distribution. When the primary user is present, Y may be denoted as the sum of two independent random

variables [44], [45]. The parameters of Y depend on the average SNR in the Rayleigh fading (see (3.2) and (3.3)). The simulations are done in three test conditions. In the first condition, every user has the same average $SNR(\overline{\gamma})$, which is 10dB. In the second condition, each user has different average $SNR(\overline{\gamma})$ varying from 5dB to 9dB. In the third condition, each user has different average $SNR(\overline{\gamma})$ varying from 5dB to 15dB. The relevant information of primary users, such as the position, the moving direction and the moving velocity, is unknown to the secondary users.

We compare the performance of the proposed scheme with that of an existing OR-rule cooperative sensing scheme [23, 24, 61], which is better than AND-rule and MAJORITY-rule in many cases of practical interest [24, 61]. In the OR-rule cooperative sensing scheme, each secondary user makes local spectrum sensing decision, which is a binary variable - a "one" denotes the presence of a primary user, and a "zero" denotes its absence. Then, all of the local decisions are sent to a data collector to sum up all local decision values. If the sum is greater than or equal to one, a primary user is believed to be present.

In the first stage of spectrum sensing, after time synchronization, every secondary user performs energy detection with $TW = 5$ individually to get local measurement Y_i at the selected center frequency f_s and the bandwidth of interest W. To set up the initial energy vector $\boldsymbol{X}(0)$, we set $x_i(0) = Y_i$.

In the second stage, the existing method and the proposed consensus algorithm (4.1) are conducted based on fixed graph models, while the proposed consensus algorithm (5.1) is run based on random graph models. For fixed graphs, the basic requirement is to set up duplex wireless channels. In the simulations, we consider a network topology with 10 secondary users that establish a graph, $\boldsymbol{G} = \{\mathcal{N}, \mathcal{E}\}$, as shown in Figure 7.1(a). For random graphs, we use the same set of nodes as in Figure

7.1(b), but replace solid lines with dotted ones, which have probabilities of link failure of 40% (refer to Figure 7.1(b)). The links in those figures stand for bidirectional wireless links. With regard to link failure probabilities, they mean both directions will fail to work in case of link failure. We also consider a network topology with 50 nodes in the simulations, which is shown in Figure 7.2. All of the 50 nodes are located randomly. The links in the 50-node network have probabilities of failure of 40%.

7.1.2 Convergence of the Consensus Algorithm

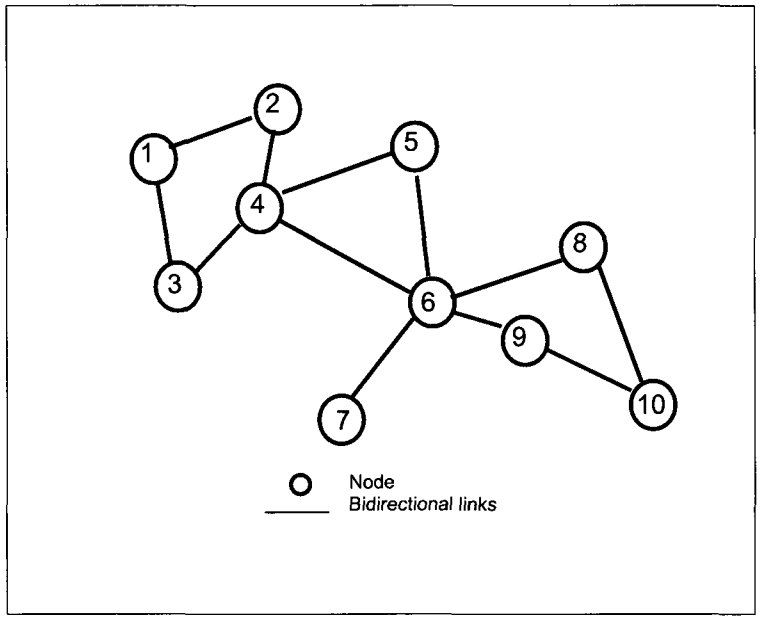
Figure 7.3(a) and Figure 7.3(b) show the estimated primary user energy in the network with a 10-node fixed graph. We can observe that, although the initially sensed energy varies greatly due to their different wireless channel conditions for different secondary nodes, a consensus will be reached after several iterations. The step size ϵ has effects on the convergence rate of the consensus algorithm. According to (4.1) and (5.1), a value should be selected for ϵ such that $0 < \epsilon < \Delta^{-1}$. Since the maximum number of neighbors of a node in Figure 7.1(a) and Figure 7.1(b) is 5, $\Delta = 5$. Then, $0 < \epsilon < 0.2$.

Here we provide some discussion about the choice of the parameter ϵ. First, given the network topology, we may construct the associated Laplacian $\boldsymbol{L}$ as a 10×10 matrix. For reasons of space, $\boldsymbol{L}$ is not displayed. The eigenvalue of $\boldsymbol{L}$ are listed as follows:

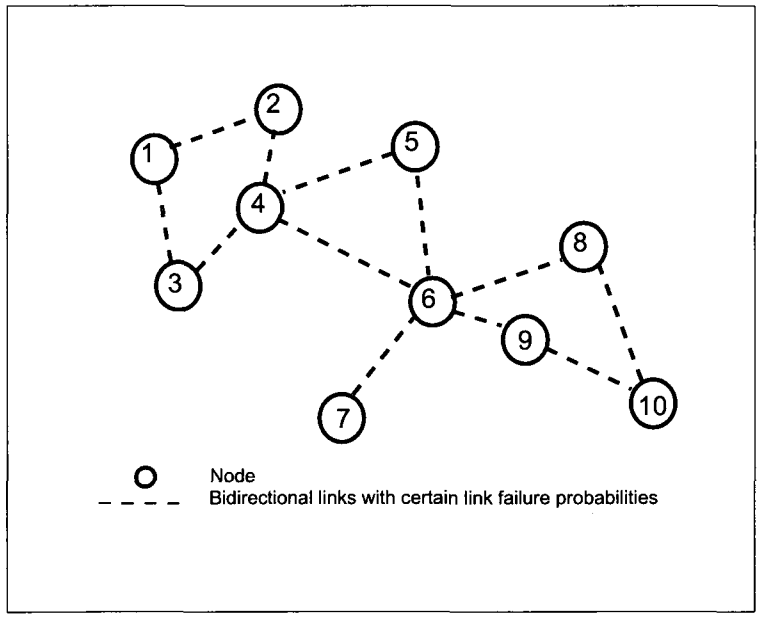
$$0,\ 0.3416,\ 0.8400,\ 1.4239,\ 2.0000,\ 2.0000,\ 3.0000,\ 3.1373,\ 4.9411,\ 6.3161. \tag{7.1}$$

On the interval $(0,\ 0.2)$, the spectral gap $g(\epsilon)$ may be shown to be

$$g(\epsilon) = 1 - 0.3416\epsilon, \tag{7.2}$$



(a) A fixed graph.



(b) A random graph.

Figure 7.1: Network topology with 10 nodes in the simulations.

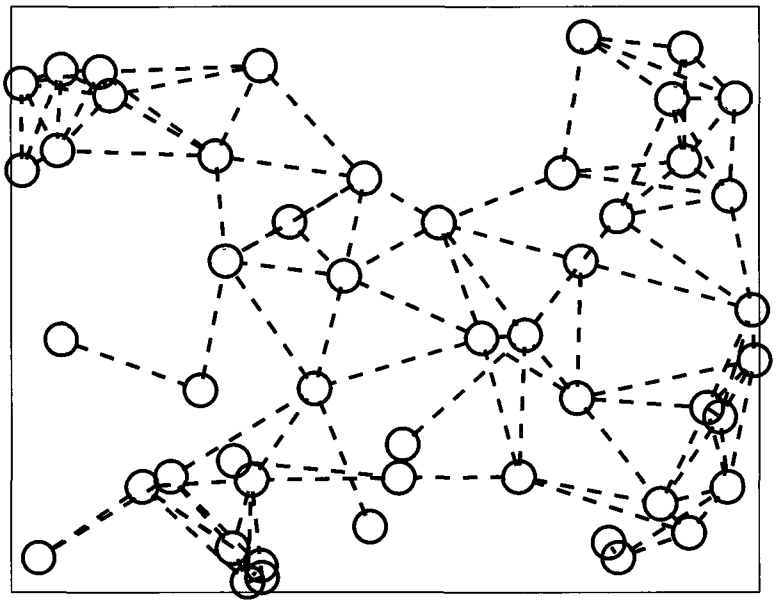


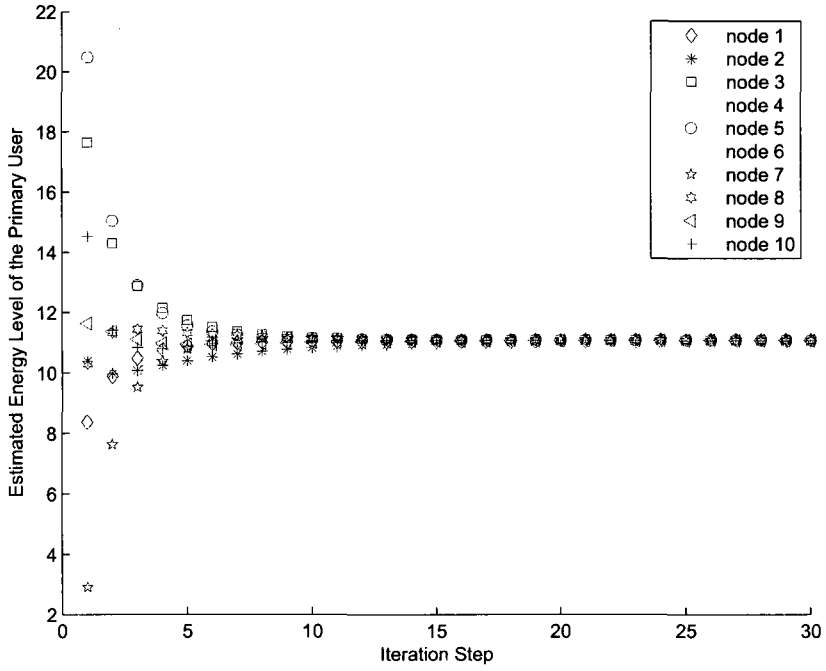
Figure 7.2: Network topology with 50 nodes in the simulations.

which monotonically decreases on (0, 0.2). We note that for this specific network topology, when $\epsilon = 0.2$, the resulting matrix $\boldsymbol{P} = I - \epsilon \boldsymbol{L}$ is ergodic. On the interval $(0, 0.2]$ the spectral gap is minimized at $\epsilon = 0.2$.

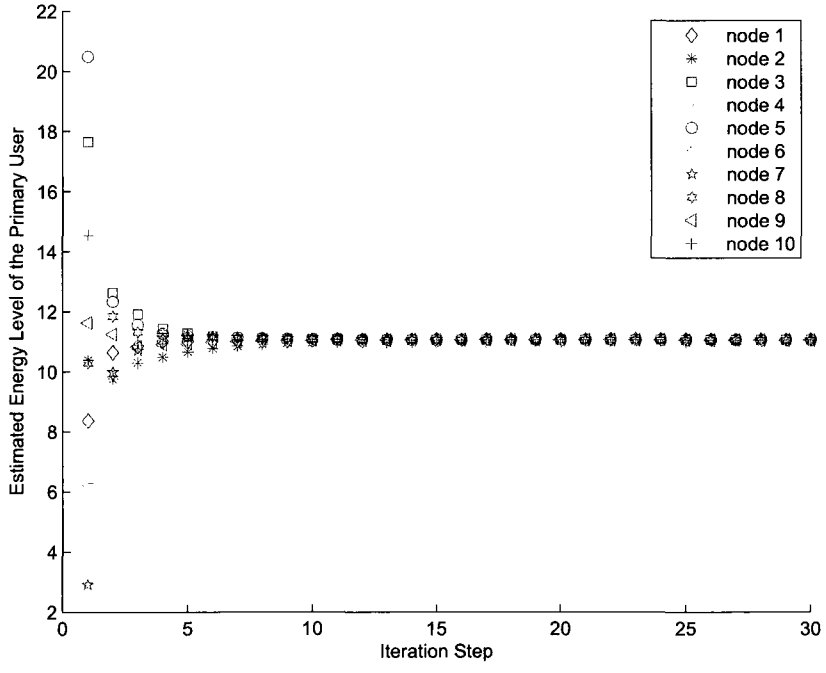
In below we select two values for ϵ, 0.1 and 0.19, in Figure 7.3(a) and Figure 7.3(b), respectively. We can see that the algorithm converges faster when $\epsilon = 0.19$ than that when $\epsilon = 0.1$, which is due to the fact that $\epsilon = 0.19$ corresponds to a larger spectral gap $g(0.19)$.

After about 5 iterations in Figure 7.3(b), the difference between the nodes is less than 1 dB, which indicates that a consensus is achieved. Figure 7.4 shows the estimated primary user energy in the network with a random graph when $\epsilon = 0.19$. Comparing Figure 7.4 with Figure 7.3(b), we can see that the algorithm converges more slowly in the random graph case due to the random link failure in the CR network. In Figure 7.4, after about 10 iterations, the difference between the nodes is less than 1 dB, which indicates that a consensus is achieved.

Figure 7.5 shows the convergence performance for the 50-node network. $\epsilon =$



(a) Fixed graph ($\epsilon = 0.1$).



(b) Fixed graph ($\epsilon = 0.19$).

Figure 7.3: Convergence of the network with a 10-node fixed graph.

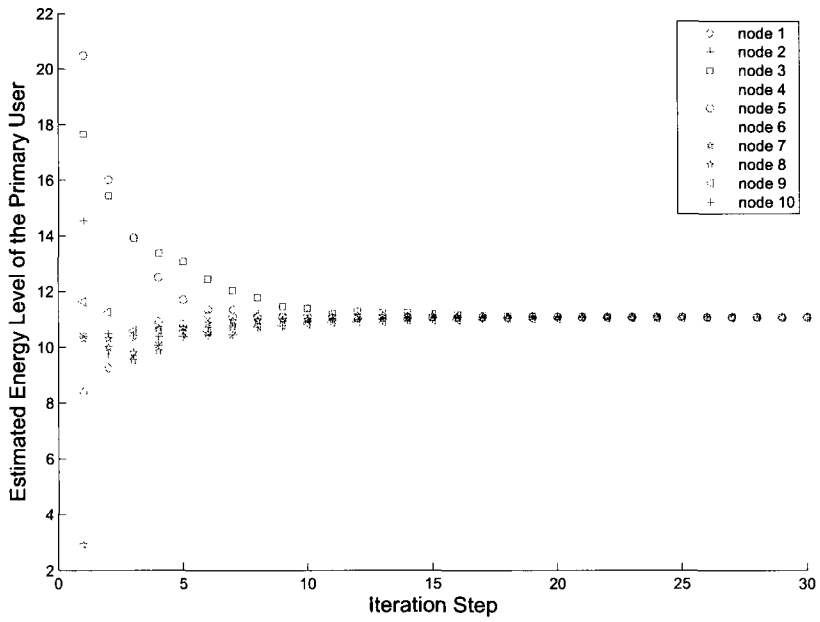


Figure 7.4: Convergence of the network with a 10-node random graph ($\epsilon = 0.19$).

0.15 is used. We can observe that the algorithm converges more slowly in the 50-node network compared to the 10-node network due to a larger number of nodes. Nevertheless, after about 30 iterations, the difference between the nodes is less than 1 dB, which indicates that a consensus is achieved.

In the rest of the simulations, we conduct the simulations in three scenarios. In scenario one, under each of the three test conditions, the simulations are conducted by using one of the existing methods and the proposed scheme, respectively. The purpose of this scenario is to evaluate the performance of the proposed scheme in terms of P_m (probability of missing detection) and P_f (probability of false alarm). In scenario two, we focus on test condition one, and try to find the best detection sensitivity for different algorithms. In scenario three, we also work on test condition one, and set a fixed detection threshold λ as stated in (4.5) to simulate the real situation in practice.

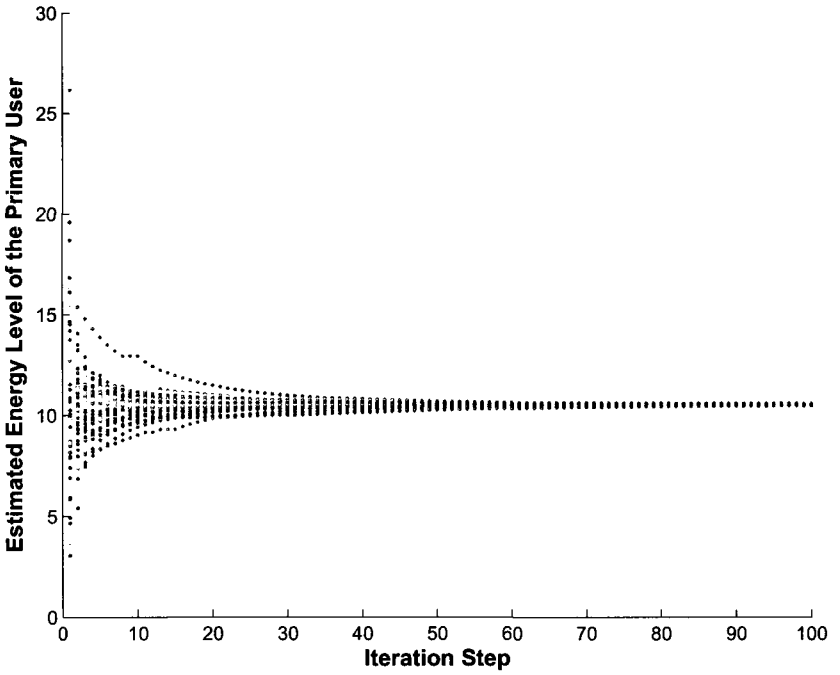


Figure 7.5: Convergence of the network with a 50-node random graph ($\epsilon = 0.15$).

7.1.3 Scenario One

We compare the performance of the proposed scheme with that of an existing OR-rule cooperative sensing scheme [23, 24, 61]. Before the comparison, let us discuss briefly the relationship between P_m (probability of missing detection)= 1 - P_d (probability of detection) and P_f (probability of false alarm). The fundamental tradeoff between P_m and P_f has different implications in the context of spectrum sensing [5]. A high P_m will result in the missing detection of primary users with high probability, which in turn increases the interference to primary users. On the other hand, a high P_f will result in low spectrum utilization since false alarms increase the number of missed opportunities (white spaces). As expected, P_f is independent of γ since under H_0 there is no primary signal.

Figure 7.6 and Figure 7.7 show P_f vs. P_m. We can see that the proposed algorithm has better performance than the existing OR-rule cooperative sensing scheme. The numbers beside the curves are the corresponding thresholds λ in dB. In Figure 7.6,

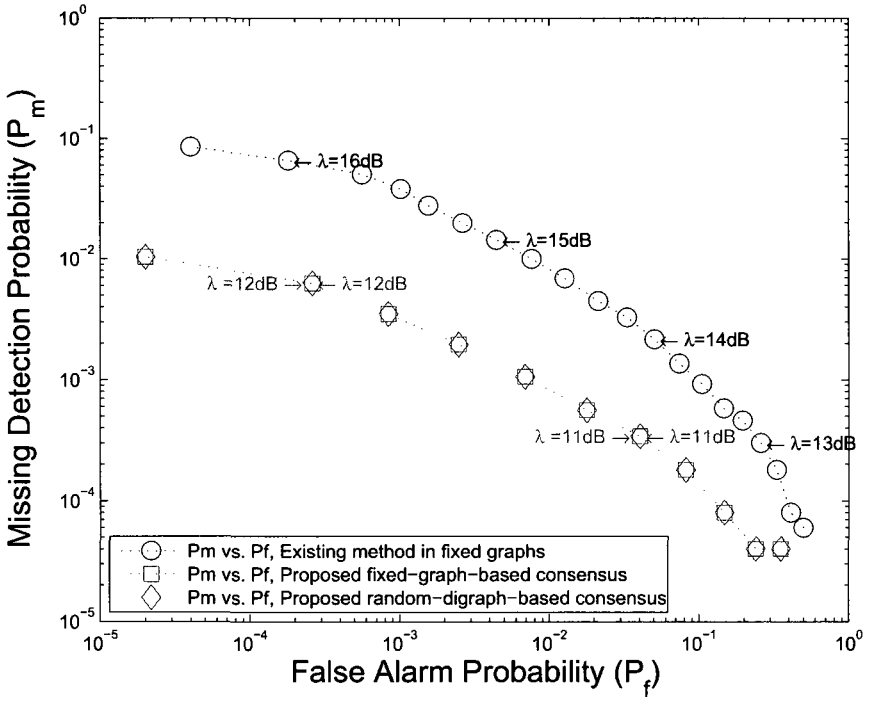


Figure 7.6: Results in simulation scenario one under test condition one: Missing detection probability (P_m) vs. false alarm probability (P_f) (Each secondary user has the same average SNR, $\overline{\gamma} = 10$dB).

where each secondary user has the same average SNR 10dB, if the threshold λ is in the range of 11.4 to 12dB, both P_f and P_m can simultaneously drop below the probability of 10^{-2} for the proposed consensus algorithm in both fixed and random graphs. Also, the results are the same between the fixed and random models. In comparison, to reach the same goal, the existing OR-rule method must set λ to be around 14.8dB, which has far worse P_m (10^{-2} vs. 10^{-3}) with regard to the same P_f level (10^{-2}).

In condition two, secondary users undergo different average SNR varying from 5dB to 9dB. In condition three, secondary users undergo different average SNR varying from 5dB to 15dB. The similar results are demonstrated in Figure 7.7 and Figure 7.8 for condition two and three, respectively.

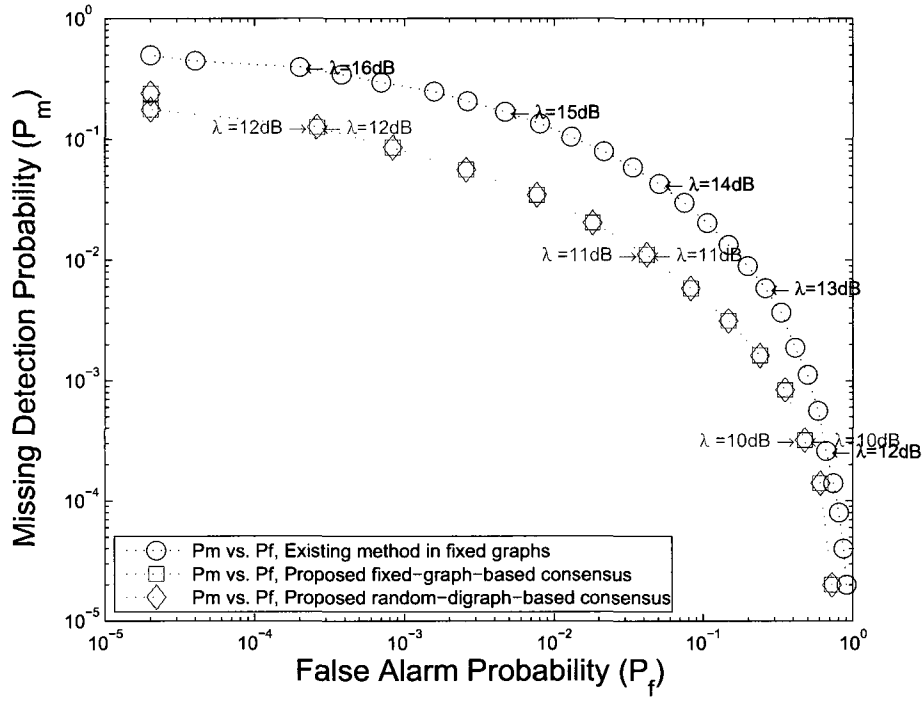


Figure 7.7: Results in simulation scenario one under test condition two: Missing detection probability (P_m) vs. false alarm probability (P_f) (Each secondary user has different average SNR varying from 5dB to 9dB).

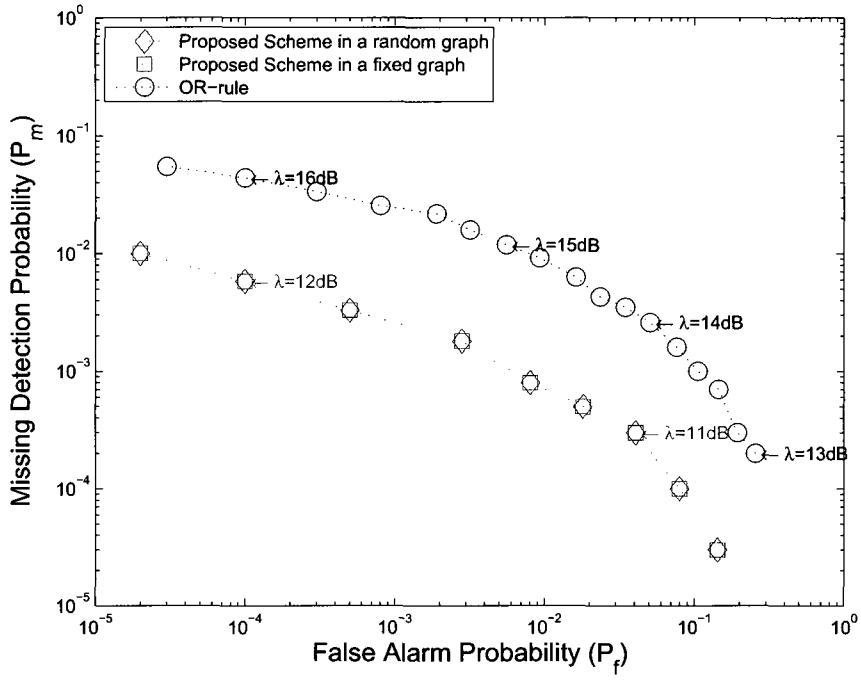


Figure 7.8: Results in simulation scenario one under test condition three: Missing detection probability (P_m) vs. false alarm probability (P_f) (Each secondary user has different average SNR varying from 5dB to 15dB).

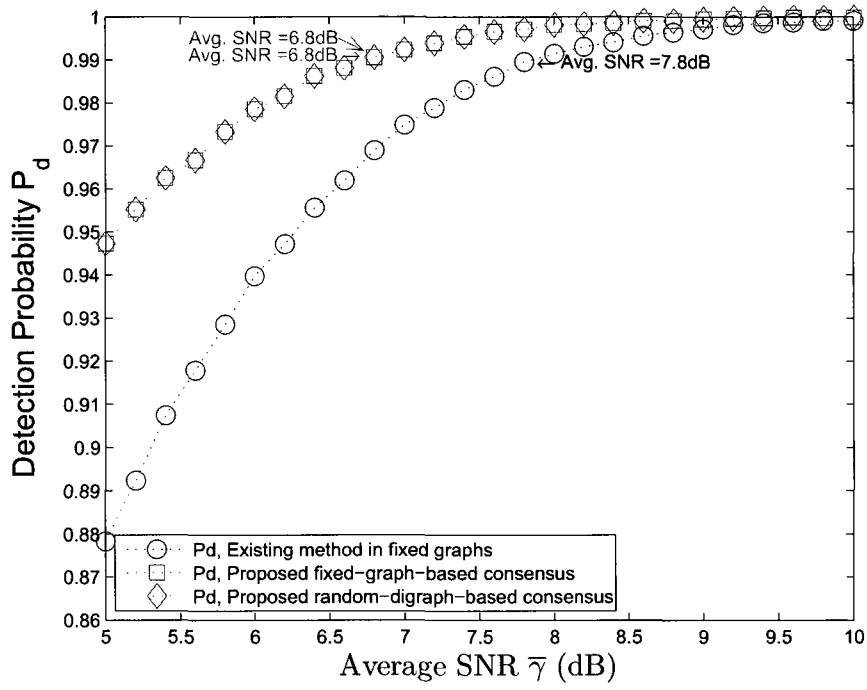


Figure 7.9: Simulation results in scenario two: detection probability (P_d) vs. average SNR ($\bar{\gamma}$) ($P_f = 10^{-1}$, $TW = 5$).

7.1.4 Scenario Two

Next, we examine the performance of detection probabilities P_d to find out the sensitivity in detecting the primary user's presence. Figure 7.9 shows P_d (detection probability $= 1 - P_m$) vs. average SNR ($\bar{\gamma}$) of secondary users. Condition one is used in this scenario, and the simulation is performed when the average SNR varies from 5dB to 10dB for all the nodes. The decision threshold, λ, is chosen so as to keep $P_f = 10^{-1}$. Time-bandwidth product, TW, is set to be 5, which is the same as before. From Figure 7.9, we see that the proposed scheme can have a significant improvement in terms of the required average SNR for detection. In particular, if the probability of detection is expected to be kept above 0.99 (or $P_m < 10^{-2}$), the existing spectrum sensing scheme requires $\bar{\gamma} = 7.8$dB. This required average SNR is higher than those in the proposed consensus scheme, both of which are approximately 6.8dB.

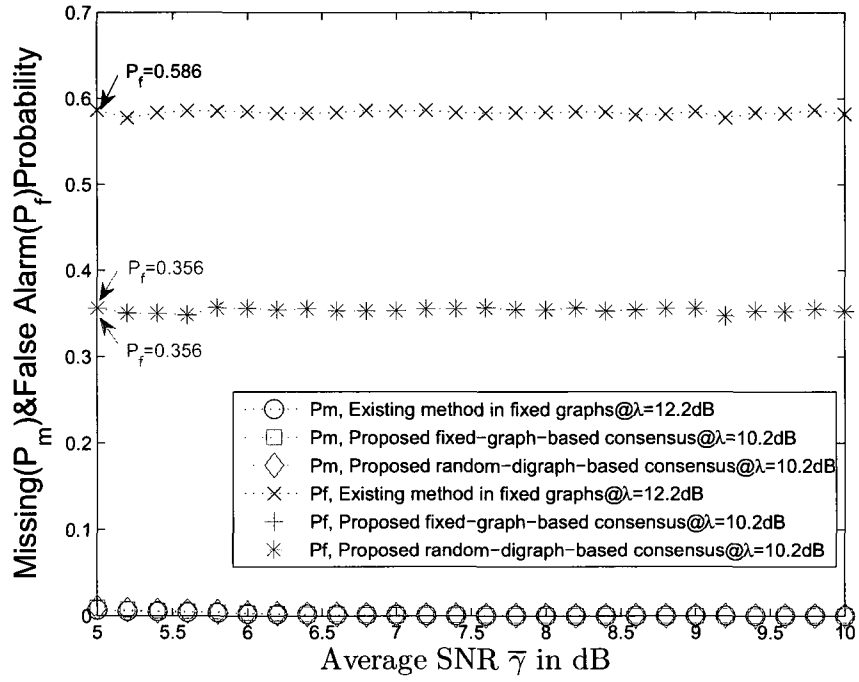
7.1.5 Scenario Three

In reality, it is unlikely to adjust the threshold λ on demand with regard to the different average SNR. Rather, a fixed threshold that can work in any $\bar{\gamma}$ is much more desirable. We can call it as threshold robustness. Therefore, in this scenario, we use condition one and intend to set a pre-defined threshold λ by using (4.5) so as to achieve a certain goal. In fact, there are three options when we choose such a goal to keep missing detection probability (P_m) below a certain level, to keep false alarm probability P_f around a certain level, or to keep both P_m and P_f as low as possible.

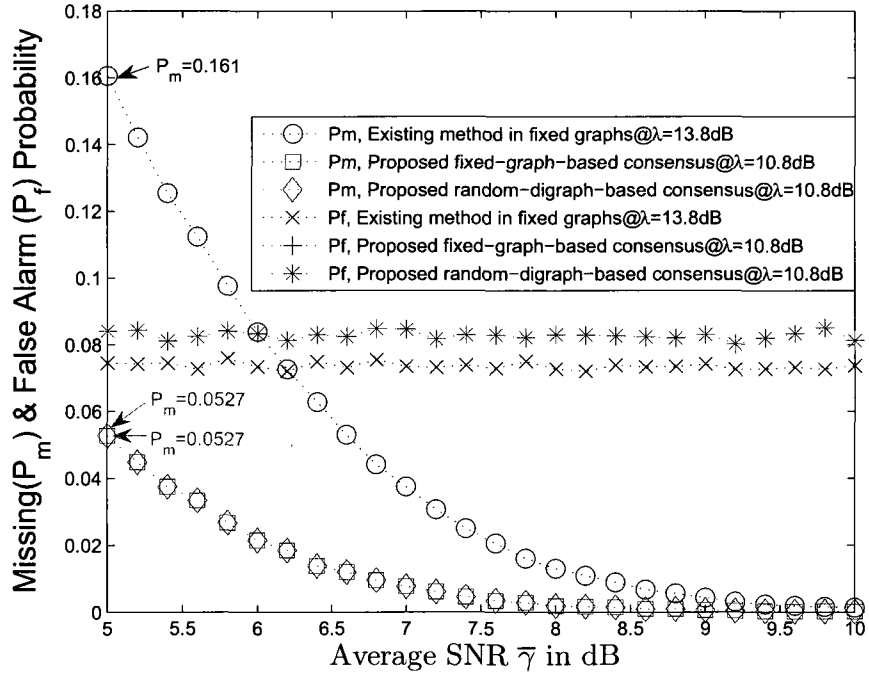
We first keep P_m below 10^{-2} when all the ten users undergo the same $\overline{\gamma}$ varying from 5dB to 10dB. Figure 7.10(a) shows a fixed λ that lets P_m below 10^{-2} for the average SNR ranging from 5dB to 10dB. As the result, the worst P_f decreases from 0.586 by using the existing method to 0.356 in both the random graph and the fixed graph by using the proposed scheme.

The second option is to let P_f always around 10^{-1} when all the ten users undergo $\overline{\gamma}$ varying from 5dB to 10dB. The result is shown in Figure 7.10(b), where P_f keeps around 10^{-1}. The proposed consensus algorithm has the better performance in terms of P_m, down from 0.161 in the existing method to 0.0527 in the proposed method.

In the third option, keep both P_m and P_f as low as possible. When determining a threshold, we refer to Figure 7.11(a), which shows the worst case when all the ten users suffers $\overline{\gamma} = 5$dB. For the consensus scheme to have better missing detection performance, the threshold chosen in the proposed scheme should be lower than that in the OR-rule scheme. In Figure 7.11(a), we can see that, with the same missing detection probability, the threshold is lower in the proposed scheme than that in the OR-rule scheme. On the other hand, with this lower threshold, a better false alarm probability can be achieved in the proposed scheme. The reason is that, when there is no primary user, the output of the energy detector, Y, of each secondary



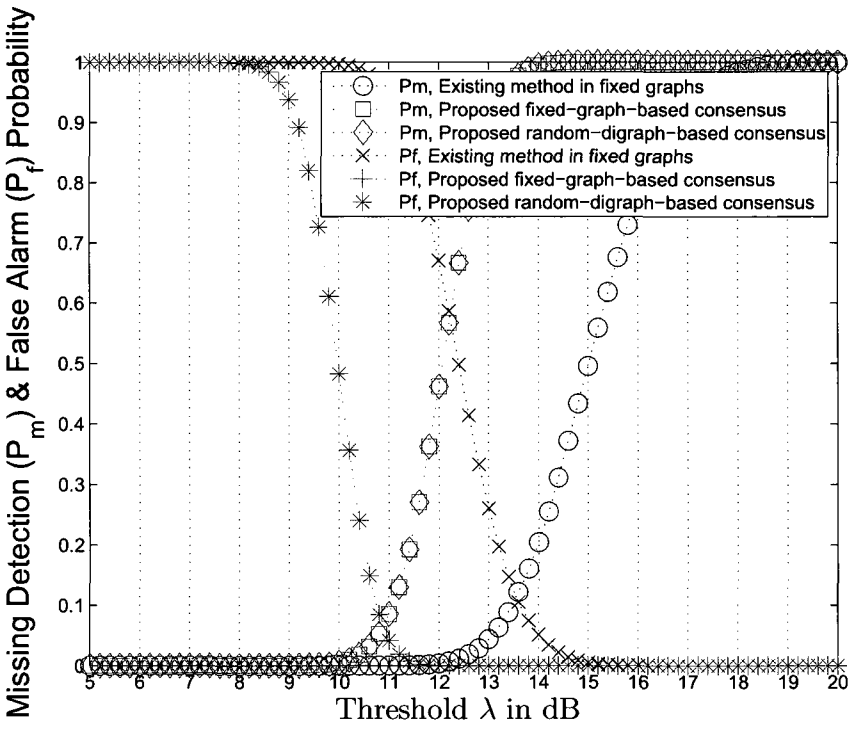
(a) Missing detection probability (P_m) and false alarm probability (P_f) vs. average SNR ($\overline{\gamma}$) with fixed threshold λ to keep P_m below 10^{-2}, when all the ten users undergo same $\overline{\gamma}$ varying from 5dB to 10dB.



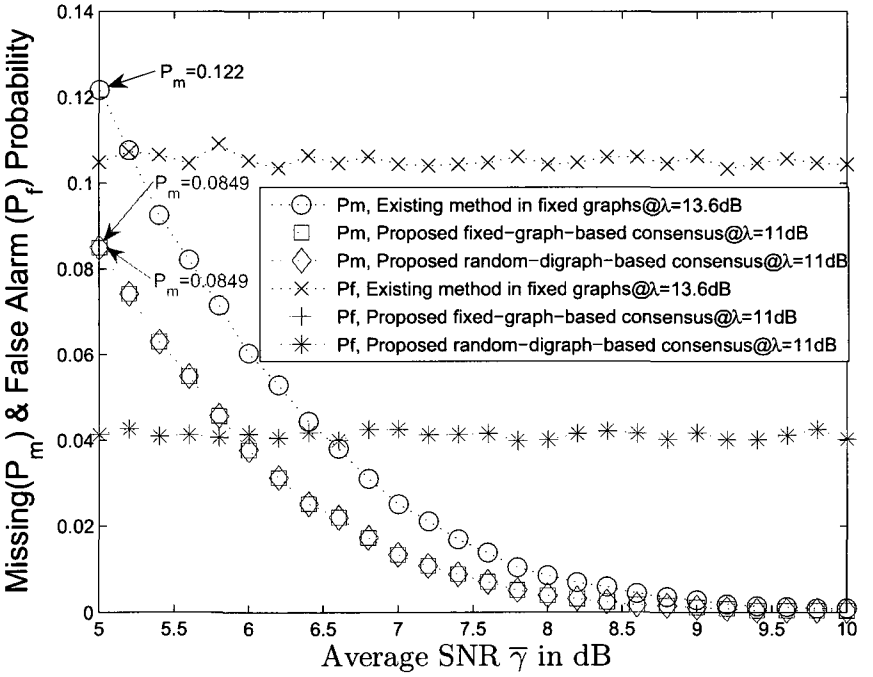
(b) Missing detection probability (P_m) and false alarm probability (P_f) vs. average SNR ($\overline{\gamma}$) with fixed threshold λ to keep P_f below 10^{-1}, when all the ten users undergo same $\overline{\gamma}$ varying from 5dB to 10dB.

Figure 7.10: Results in simulation scenario three: Part One.

user is a random quantity with central chi-square distribution (please see Eq. (2)). Since Y varies greatly, it is easy for a secondary user to have a false alarm in the OR-rule scheme. By contrast, the consensus scheme does not use the raw data Y to make decisions. Instead, it uses the consensus among the secondary users to make decisions, thus it can remove some randomness in the raw data Y. Therefore, the consensus scheme can have a better false alarm probability than the OR-rule scheme with the same threshold. This can be shown in Figure 7.11(a). From Figure 7.11(a), we can also observe that both missing detection and false alarm probabilities are low when the threshold is round 11dB for the consensus scheme and when the threshold is around 13.6 dB for the OR-rule scheme. In Figure 7.11(a), if we compare the performance of the consensus scheme with a threshold 11dB to that of the OR-rule scheme with a threshold 13.6 dB, we can see that both missing detection and false alarm probabilities are lower in the consensus scheme than those in the OR-rule scheme. We choose $\lambda = 11\text{dB}$ for the proposed consensus algorithm, and $\lambda = 13.6\text{dB}$ for the existing method to conduct our numerical studies. Figure 7.11(b) illustrates the result of such a fixed λ. It is seen that both P_m and P_f have better performance for the proposed algorithm than those of the existing method. P_m and P_f drops to a relatively low level. This highlights the overall advantage in so-called threshold robustness for the proposed consensus algorithm. That is, for a given λ, the proposed consensus algorithm can output less P_m and P_f than those of the existing method. The algorithm works well in both fixed graphs and random ones. Another observation in scenario three is, when the average SNR rises, P_m drops for a given threshold λ, but P_f remains more or less at the same level. This means, for a fixed λ, P_m is subject to the change of the average SNR. In contrast, P_f is stable, because this parameter deals with the condition of H_0, where only the collective noises exists.



(a) Missing detection probability (P_m) and false alarm probability (P_f) vs. threshold λ in dB when same $\overline{\gamma} = 5$dB for all users.



(b) Missing detection probability (P_m) and false alarm probability (P_f) vs. average SNR ($\overline{\gamma}$) with fixed threshold λ to keep both P_m and P_f below a certain level, when all the ten users undergo same $\overline{\gamma}$ varying from 5dB to 10dB.

Figure 7.11: Results in simulation scenario three: Part Two.

7.2 Distributed Consensus-Based Cooperative Spectrum Sensing With Malicious Attacks

In this section, we present simulation results to show the performance of the proposed scheme described in Chapter 6 to counter SSDF attacks.

7.2.1 Defense against SSDF Attacks

In the first part of the simulations with malicious attacks, we intend to demonstrate how the proposed consensus-based scheme works to counter SSDF attacks. The authentication scheme using ID-based cryptography is not considered in the first part. The simulations are based on a MANET with CRs shown in Figure 7.12, where 11 secondary users are doing cooperative spectrum sensing to check whether or not there is a primary user. There are 10 authentic secondary users. The sensed energy from the nodes is distributed according to (3.3) with an average SNR of 10. There is an attacker in the MANET. Figure 7.13 shows the estimated primary user energy with and without the Selfish SSDF. If there is no malicious attack, although the initially sensed energy varies greatly due to their different wireless channel conditions, a consensus will be reached that the energy is very low and there is no primary user. With the Selfish SSDF attack, node 11 keeps sending falsified data $x_{11}(k) = 20$. A wrong decision will be made in the CR network that there is a primary user. Figure 7.14 illustrates that when using our consensus-based scheme to filter out the attack data, all the authentic users can reach the consensus and make the correct decision that there is no primary user.

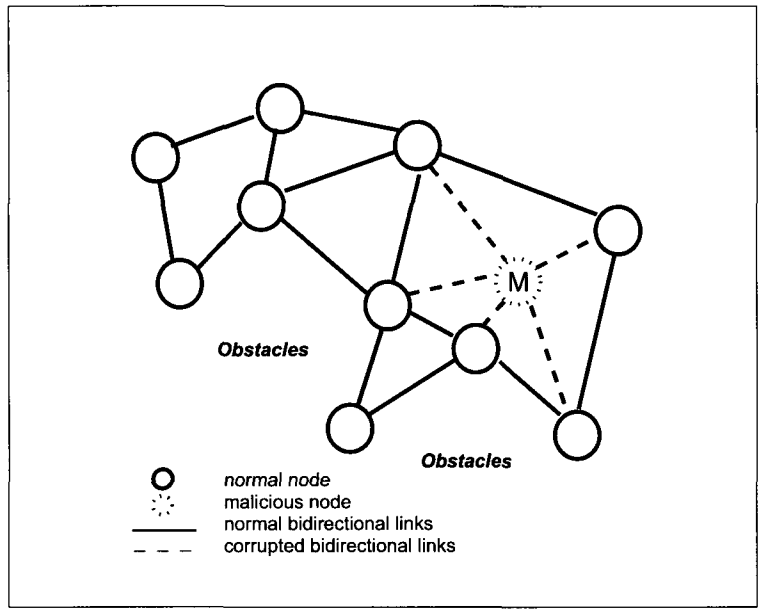


Figure 7.12: A 11-node MANET with one SSDF attack.

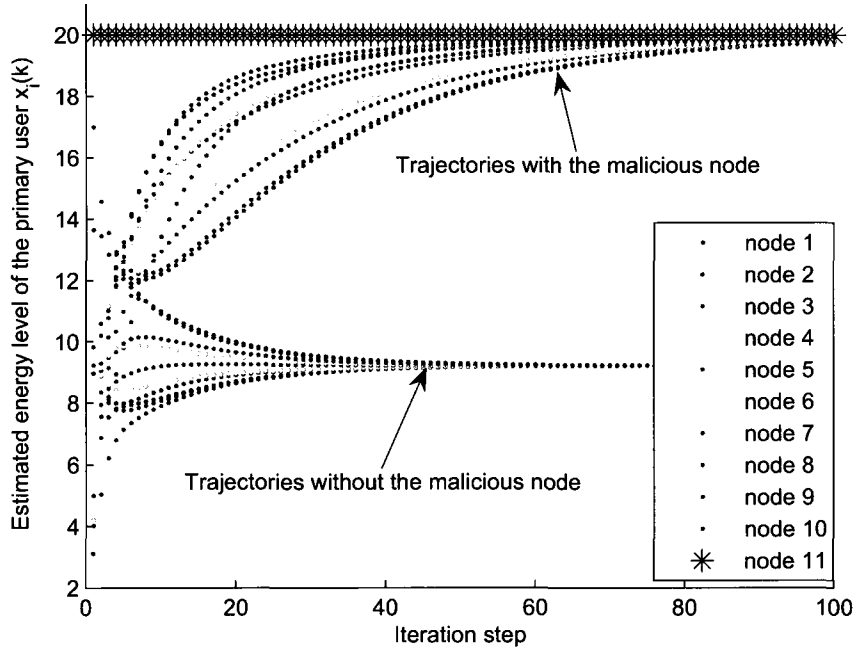


Figure 7.13: Estimated primary user energy with and without selfish SSDF attacks.

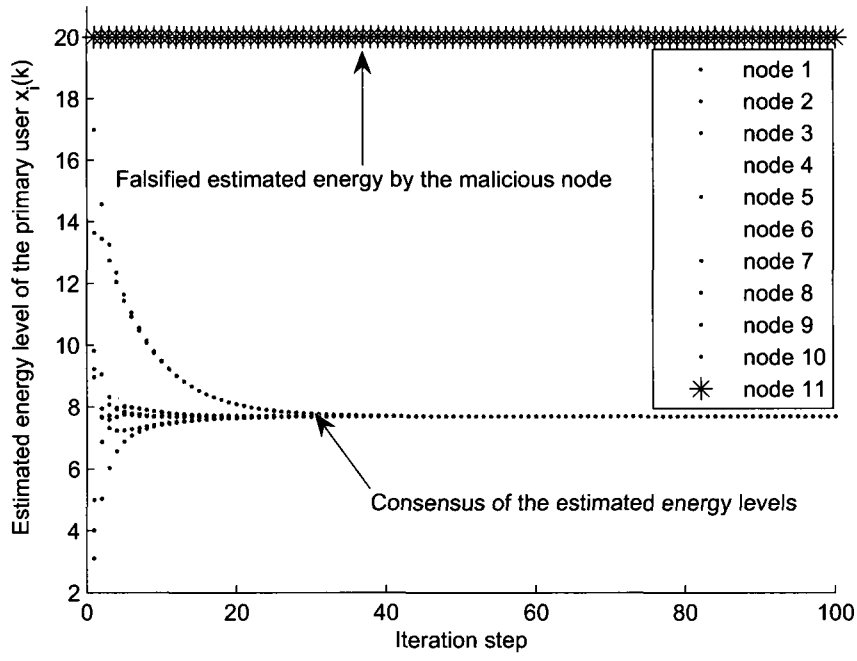


Figure 7.14: Estimated primary user energy in the proposed consensus-based scheme to mitigate Selfish SSDF attacks.

7.2.2 False Alarm Probabilities and Miss Detection Probabilities

In the second part of the simulations with malicious attacks, we focus on the performance in terms of false alarm probabilities and miss detection probabilities. The simulations are based on a MANET with 17 CRs shown in Figure 7.15, in which there are 15 authentic nodes and 2 malicious attackers. We focus on presenting the simulation results with the Selfish SSDF attack.

We compare the performance of the proposed scheme with that of the centralized decision fusion scheme [13]. In the centralized decision fusion scheme, each sensing terminal senses the spectrum and makes a local decision by comparing the sensed energy against a predefined energy threshold λ. Then, all sensing terminals send the local decisions to a common receiver, which sums all of the collected local spectrum sensing results. A threshold value is defined. If the sum of local decisions is equal to or greater than the threshold value, then the final result is the presence of primary

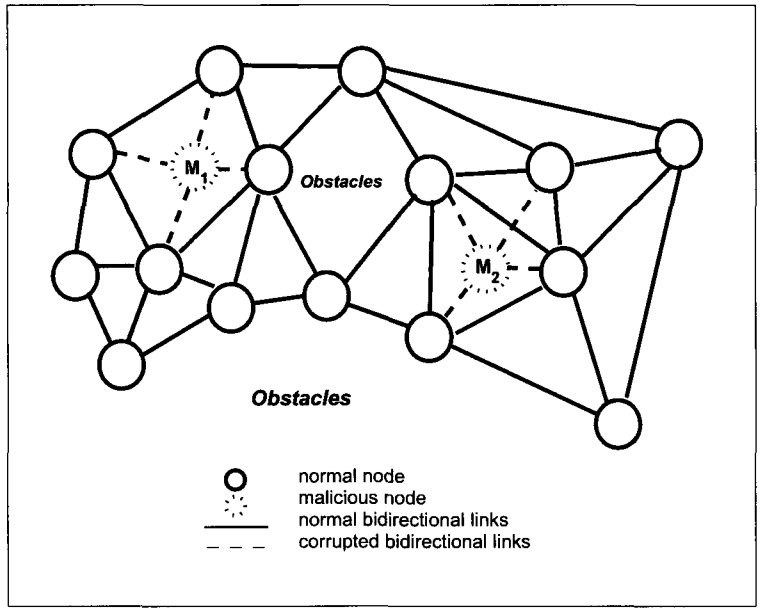


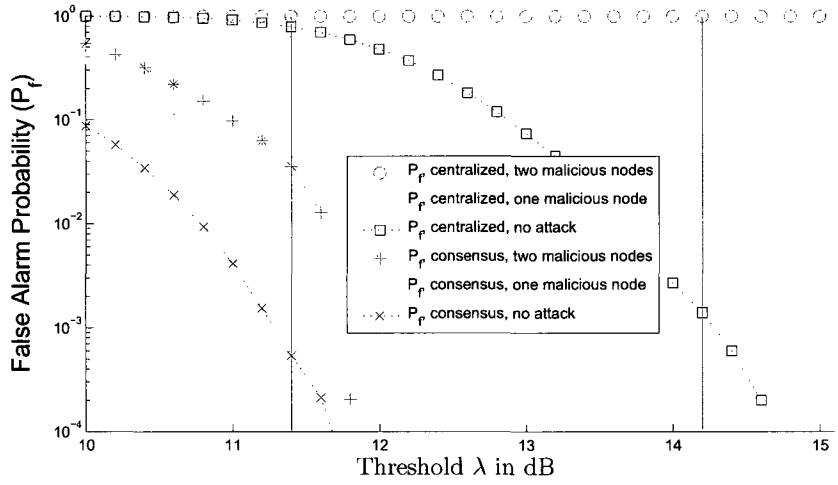
Figure 7.15: A 17-node MANET with two SSDF attacks.

users; Otherwise, the band is free. In our simulations, the threshold value is set to two in the centralized fusion scheme. To make a fair comparison, we need to determine the threshold λ, under which the centralized decision fusion scheme and the proposed consensus-based scheme have the best performance, when there is no malicious attack. In the simulations, we find that the best performance happens when we set local threshold $\lambda = 14.2$dB for the centralized decision fusion, and $\lambda = 11.4$dB gives the best performance for the proposed scheme. This shows the proposed consensus-based scheme has significantly improvement in terms of the required average SNR for detection. The system can make a better detection when secondary users undergo worse fading channels (low average SNR). We will use these threshold values in the following simulations.

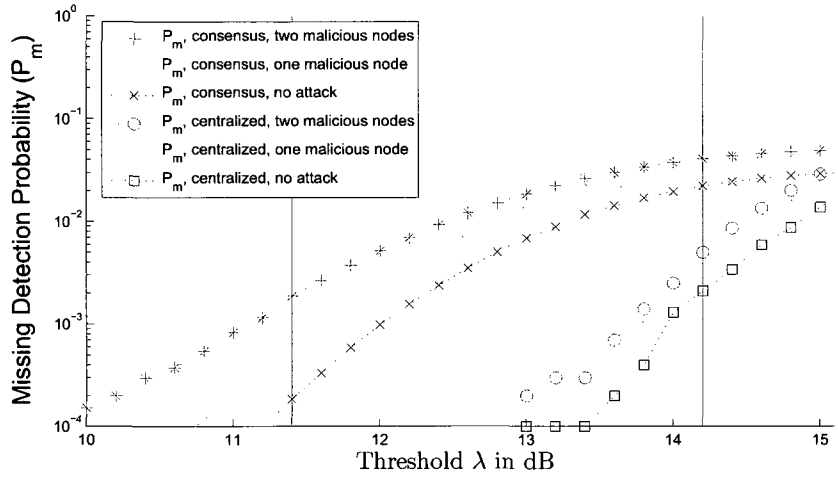
Two Selfish SSDF attacks are conducted. In the first attack, user M_1 is compromised and sends out falsified data 20. In the second attack, both user M_1 and user M_2 are compromised, they send out falsified data 20 and 15, respectively. Figure

7.16(a) shows the results in terms of false alarm probabilities, and Figure 7.16(b) shows the results in terms of miss detection probabilities. From Figure 7.16(a), we can see that the consensus-based scheme is more robust than the existing centralized fusion scheme. When $\lambda = 11.4$dB, the false alarm probability in the consensus-based scheme is lower than that in the centralized scheme in all of the following three cases: no attack, one attack and two attacks. The centralized scheme is very vulnerable to the Selfish SSDF attacks, particularly in the two attacks case, where the false alarm probability is 1. This will result in severe performance degradation of the MANET. The spectrum utilization will be very low since false alarms increase the number of missed opportunities (white space). When the false alarm probability is 1, the MANET with CRs cannot find any spectrum opportunity under two malicious attacks. From Figure 7.16(b), we can see that the miss detection probability is low in the centralized fusion scheme, even with two malicious attacks. This is because the centralized fusion scheme is a conservative scheme. That is, whenever there are some terminals (including the Selfish SSDF attacks) sensing the presence of primary users, it will not access the spectrum band, resulting in a low miss detection probability. Nevertheless, the consensus-based scheme has lower miss detection probabilities compared to the centralized scheme in all of the three different cases, which means that the consensus-based scheme can decrease the interference to primary users.

To further improve the security of MANETs with CRs, an authentication scheme using ID-based cryptography can be used when exchanging the estimated energy levels between secondary users to identify and eliminate malicious attackers. Figure 7.17(a) and Figure 7.17(b) show the results in terms of false alarm probabilities and miss detection probabilities, respectively. Compared to Figure 7.16(a), where authentication is not used, the false alarm probability in the consensus-base scheme with



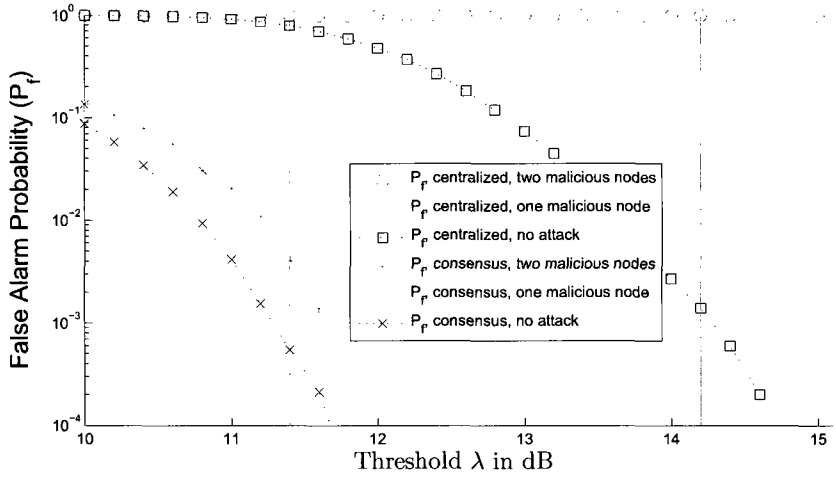
(a) False alarm probability comparison between the centralized decision fusion scheme and the consensus-based scheme without ID-based authentication.



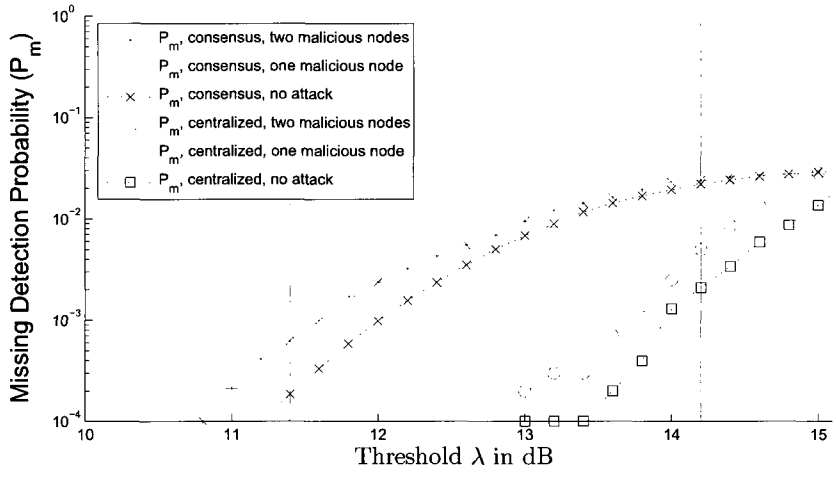
(b) Miss detection probability comparison between the centralized decision fusion scheme and the consensus-based scheme without ID-based authentication.

Figure 7.16: Results without using ID-based cryptography

authentication can be further reduced in Figure 7.17(a). We can have similar observation about miss detection probabilities when comparing Figure 7.17(b) with Figure 7.16(b), which demonstrates the effectiveness of the proposed schemes.



(a) False alarm probability comparison between the centralized decision fusion scheme and the consensus-based scheme with ID-based authentication.



(b) Miss detection probability comparison between the centralized decision fusion scheme and the consensus-based scheme with ID-based authentication.

Figure 7.17: Results when using ID-based cryptography

Chapter 8

Conclusion and Future Work

In this thesis, we have presented a fully distributed and scalable scheme for spectrum sensing based on recent advances in consensus algorithms. Cooperative spectrum sensing is modeled as a multi-agent coordination problem. Secondary users can maintain coordination based on only local information exchange without a centralized receiver. Simulation results are presented to show the effectiveness of the proposed consensus-based scheme. It is shown that both missing detection probability and false alarm probability can be significantly reduced in the proposed scheme compared to those in the existing schemes.

Also, as the real network topologies undergo random changes and the primary user may randomly enter and leave the network, a protocol is necessary to quickly decide when the consensus is considered to be practical reached. If the secondary users cannot efficiently form a decision in finite steps, the energy measurements obtained at the beginning may become obsolete. To address this finite time detection issue, in implementations a certain toleration threshold may be used by the users. A secondary user may stop the iteration if it finds the difference between the states of each neighbor and itself has fallen below the threshold. The choice of threshold depends on empirical studies. Our simulation indicates that the threshold may be chosen to be around a

fraction of 1 dB or close to 1 dB.

One limitation of the proposed scheme is that the choice of the step size ϵ depends on the maximum number of neighbors of a node in the network. In other words, each node needs to have the prior knowledge of an upper bound of the maximum degree of the network. To solve this problem, an alternative approach may be used, which is based on so called Metropolis weights [36]. This approach does not need the knowledge of the maximum degree of the network. Future work is in progress in this direction. We also want to simplify the data format of detection statistics from each secondary user to save the wireless bandwidth. In addition, as energy detection does not work well for spread spectrum signals, other approaches will be studied to deal with such networks.

As a second part of our work, security issues are studied in MANETs with CRs, where malicious CRs can send false local spectrum sensing results in cooperative spectrum sensing. Taking this into our considerations, we made a little modification on our consensus-based spectrum sensing scheme to counter SSDF attacks in MANETs with CRs. Using the consensus of secondary users, the modified scheme can differentiate the trustworthiness of spectrum sensing terminals, which makes it is robust against SSDF attacks. A common receiver is not needed for the final decision in the proposed scheme. Simulation results have been presented to illustrate the effectiveness of the proposed schemes.

Future work is in progress to use other bio-inspired algorithms, such as those in [26–28], to improve the quality of service and security in MANETs with CRs.

List of References

[1] J. Mitola, *Cognitive radio: An integrated agent architecture for software defined radio.* Doctor of Technology Thesis, Royal Inst. Technol. (KTH), Stockholm, Sweden, 2000.

[2] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio, part I: two user networks," *IEEE Trans. Wireless Commun.*, vol. 6, pp. 2204–2213, June 2007.

[3] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, pp. 201–220, Feb. 2005.

[4] C. Sun, W. Zhang, and K. B. Letaief, "Cluster-based cooperative spectrum sensing in cognitive radio systems," in *Proc. IEEE ICC'07*, pp. 2511–2515, 2007.

[5] A. Ghasemi and E. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in *Proc. IEEE DySPAN'05*, pp. 131–136, 2005.

[6] D. Cabric, S. Mishra, and R. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Proc. Thirty-Eighth Asilomar Conference on Signals, Systems and Computers*, vol. 1, pp. 772–776, 2004.

[7] J. Hillenbrand, T. Weiss, and F. Jondral, "Calculation of detection and false alarm probabilities in spectrum pooling systems," *IEEE Commun. Letters*, vol. 9, no. 4, pp. 349–351, 2005.

[8] J.-F. Chamberland and V. V. Veeravalli, "Wireless sensors in distributed detection applications," *IEEE Signal Proc. Mag.*, vol. 24, pp. 16–25, May 2007.

[9] R. Niu and P. Varshney, "Performance analysis of distributed detection in a random sensor field," *IEEE Trans. Signal Proc.*, vol. 56, no. 1, pp. 339–349, 2008.

[10] V. Veeravalli, "Decentralized quickest change detection," *IEEE Trans. Inform. Theory*, vol. 47, no. 4, pp. 1657–1665, 2001.

[11] S. Mishra, A. Sahai, and R. Brodersen, "Cooperative sensing among cognitive radios," in *Proc. IEEE ICC'06*, pp. 1658–1663, 2006.

[12] R. Chen, J.-M. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, pp. 25–37, Jan. 2008.

[13] R. Chen, J.-M. Park, Y. Hou, and J. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Comm. Mag.*, vol. 46, pp. 50–55, Apr. 2008.

[14] W. Ren, R. Beard, and E. Atkins, "A survey of consensus problems in multi-agent coordination," in *Proc. American Control Conference'05*, pp. 1859–1864, 2005.

[15] J. Mitola and G. Q. Maguire, "Cognitive radio: Making software radios more personal," *IEEE Pers. Commun.*, vol. 6, pp. 13–18, Aug. 1999.

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

[17] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio - part II: multiuser networks," *IEEE Trans. Wireless Commun.*, vol. 6, pp. 2214–2222, June 2007.

[18] G. Ganesan and Y. G. Li, "Agility improvement through cooperative diversity in cognitive radio," in *Proc. IEEE GLOBECOM'05*, pp. 2505–2509, 2005.

[19] E. Peh and Y.-C. Liang, "Optimization for cooperative sensing in cognitive radio networks," in *Proc. IEEE WCNC'07*, pp. 27–32, 2007.

[20] J. Unnikrishnan and V. V. Veeravalli, "Cooperative sensing for primary detection in cognitive radio," *IEEE J. Sel. Topics Signal Proc.*, vol. 2, no. 1, pp. 18–27, 2008.

[21] Z. Quan, S. Cui, and A. H. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio networks," *IEEE J. Sel. Topics Signal Proc.*, vol. 2, no. 1, pp. 28–40, 2008.

[22] Y.-C. Liang, Y. Zeng, E. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1326–1337, 2008.

[23] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pp. 1876–1884, 2008.

[24] W. Zhang and K. Ben Letaief, "Cooperative communications for cognitive radio networks," *Proc. IEEE*, vol. 97, no. 5, pp. 878–893, 2009.

[25] C. S. R. Murthy and B. S. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols.* Upper Saddle River, NJ: Prentice Hall, 2004.

[26] T. Nakano and T. Suda, "Applying biological principles to designs of network services," *Appl. Soft Comput.*, vol. 7, no. 3, pp. 870–878, 2007.

[27] I. Carreras, I. Chlamtac, F. D. Pellegrini, and D. Miorandi, "Bionets: Bio-inspired networking for pervasive communication environments," *IEEE Trans. Veh. Tech.*, vol. 56, pp. 218–229, Jan. 2007.

[28] F. Dressler, Ö. B. Akan, and A. Ngom, "Guest Editorial - Special Issue on Biological and Biologically-inspired Communication," *Springer Trans. on Computational Systems Biology (TCSB)*, vol. LNBI 5410, Dec. 2008.

[29] R. Olfati-Saber, J. Fax, and R. Murray, "Consensus and cooperation in networked multi-agent systems," *Proc. IEEE*, vol. 95, no. 1, pp. 215–233, 2007.

[30] J.-M. Amé, J. Halloy, C. Rivault, C. Detrain, and J. L. Deneubourg, "Collegial decision making based on social amplification leads to optimal group formation," *Proc. Natl. Acad. Sci.*, vol. 103, no. 15, pp. 5835–5840, 2006.

[31] L. Conradt and T. J. Roper, "Consensus decision making in animals," *Trends in Ecology and Evolution*, vol. 20, pp. 449–456, Aug. 2005.

[32] T. Vicsek, "A question of scale," *Nature*, vol. 441, p. 421, May 2001.

[33] I. D. Couzin, "Collective cognition in animal groups," *Trends in Cognitive Sciences*, vol. 13, pp. 36–43, Dec. 2008.

[34] P. K. Visscher, "How self-organization evolves?," *Nature*, vol. 421, pp. 799–800, Feb. 2003.

[35] W. Ren and R. Beard, "Consensus seeking in multiagent systems under dynamically changing interaction topologies," *IEEE Trans. Auto. Control*, vol. 50, no. 5, pp. 655–661, 2005.

[36] L. Xiao, S. Boyd, and S. Lall, "A scheme for robust distributed sensor fusion based on average consensus," in *Proc. Fourth International Symposium on Information Processing in Sensor Networks*, pp. 63–70, 2005.

[37] M. Huang and J. H. Manton, "Stochastic consensus seeking with measurement noise: convergence and asymptotic normality," in *Proc. American Control Conference'08*, pp. 1337–1342, 2008.

[38] A. Shamir, "Identity based cryptosystems and signature schemes," in *Proc. CRYPTO'84*, Aug. 1984.

[39] Y. Zhao, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," *IEEE Trans. Dependable and Secure Computing*, vol. 3, pp. 386–399, Oct.–Dec. 2006.

[40] W. Irving and J. Tsitsiklis, "Some properties of optimal thresholds in decentralized detection," *IEEE Trans. Auto. Control*, vol. 39, no. 4, pp. 835–838, 1994.

[41] J. Proakis and M. Salehi, *Digital communications*. McGraw-hill New York, 1995.

[42] A. Sahai, N. Hoven, and R. Tandra, "Some fundamental limits on cognitive radio," in *Allerton Conference on Communication, Control, and Computing*, Citeseer, 2004.

[43] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proc. IEEE*, vol. 55, no. 4, pp. 523–531, 1967.

[44] F. Digham, M.-S. Alouini, and M. Simon, "On the energy detection of unknown signals over fading channels," in *Proc. IEEE ICC'03*, vol. 5, pp. 3575–3579, 2003.

[45] V. Kostylev, "Energy detection of a signal with random amplitude," in *IEEE Proc. ICC'02*, vol. 3, pp. 1606–1610, 2002.

[46] M. Huang and J. H. Manton, "Coordination and consensus of networked agents with noisy measurements: stochastic algorithms and asymptotic behavior," *SIAM J. Control and Optimization*, vol. 48, pp. 134–161, Jan. 2009.

[47] C. Godsil and G. Royle, *Algebraic Graph Theory*. New York: Springer-Verlag, 2001.

[48] E. Seneta, *Non-negative Matrices and Markov Chains.* New York: Springer-Verlag, 1981.

[49] L. Elsner, I. Koltracht, and M. Neumann, "On the convergence of asynchronous paracontractions with applications to tomographic reconstruction from incomplete data," *Linear Algebra and its Applications*, vol. 130, pp. 65–82, 1990.

[50] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM J. Computing*, vol. 32, pp. 586–615, Mar. 2003.

[51] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Networks*, vol. 13, no. 6, pp. 24–30, 1999.

[52] K. Hoeper and G. Gong, "Bootstrapping security in mobile ad hoc networks using identity-based schemes with key revocation," tech. rep., University of Waterloo, Canada, 2006.

[53] N. Saxena, G. Tsudik, and J. H. Yi, "Identity-based access control for ad hoc groups," in *Proc. Int'l Conf. Info. Security and Cryptology*, Dec. 2004.

[54] A. Shamir, "How to share a secret," *Comm. ACM*, vol. 22, pp. 612–612, Nov. 1979.

[55] Y. Desmedt and Y. Frankel, "Threshold cryptosystems," in *Proc. CRYPTO'89*, Aug. 1989.

[56] G. Yin and V. Krishnamurthy, "Analysis of LMS algorithm for markovian parameters with infrequent jumps – applications to tracking hidden markov models and adaptive multiuser detection in DS/CDMA," *IEEE Trans. Inform. Theory*, 2003. (submitted).

[57] H. Deng, A. Mukherjee, and D. Agrawal, "Threshold and identity-based key management and authentication for wireless ad hoc networks," in *Proc. Int'l Conf. Info. Tech.: Coding and Computing (ITCC'04)*, Apr. 2004.

[58] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: Ubiquitous and robust access control for mobile ad hoc networks," *IEEE/ACM Trans. Netw.*, vol. 12, pp. 1049–1063, Dec. 2004.

[59] P. Whittle, "Multi-armed bandits and the Gittins index," *J. R. Statist. Soc. B*, vol. 42, no. 2, pp. 143–149, 1980.

[60] V. Krishnamurthy, "A value iteration algorithm for partially observed markov decision process multi-armed bandits," *Math. of Oper. Res.*, pp. 133–152, May 2005.

[61] A. Ghasemi and E. Sousa, "Opportunistic spectrum access in fading channels through collaborative sensing," *Journal of Communications*, vol. 2, no. 2, p. 71, 2007.