PhD Dissertation

International Doctorate School in Information and Communication Technologies

DIT - University of Trento

TOWARDS ENERGY EFFICIENT COOPERATIVE SPECTRUM SENSING IN COGNITIVE RADIO NETWORKS

by

Saud Althunibat

Advisor:

Dr. Fabrizio Granelli

Universita degli Studi di Trento

November 2014

TOWARDS ENERGY EFFICIENT COOPERATIVE SPECTRUM SENSING IN COGNITIVE RADIO NETWORKS

Saud Althunibat, Ph.D.
University of Trento 2014

Cognitive radio has been proposed as a promising technology to resolve the spectrum scarcity problem by dynamically exploiting underutilized spectrum bands. Cognitive radio technology allows unlicensed users, also called cognitive users (CUs), to exploit the spectrum vacancies at any time with no or limited extra interference at the licensed users. Usually, cognitive radios create networks in order to better identify spectrum vacancies, avoid resultant interference, and consequently, magnify their revenues. One of the main challenges in cognitive radio networks is the high energy consumption, which may limit their implementation especially in battery-powered terminals.

The initial step in cognitive transmission is called spectrum sensing. In spectrum sensing, a CU senses the spectrum in order to detect the activity of the licensed users. Spectrum sensing is usually accomplished cooperatively in order to improve the reliability of its results. In cooperative spectrum sensing (CSS), individual sensing results should be exchanged in order to make a global decision regarding spectrum occupancy. Thus, CSS consumes a significant a mount of energy, representing a challenge for CUs. Moreover, the periodicity of CSS and increasing the number of channels to be sensed complicates the problem. To this end, energy efficiency in CSS has gained an increasing attention recently.

In this dissertation, a number of energy-efficient algorithms/schemes for CSS is proposed. The proposed works include energy efficient solutions for low energy consumption in local sensing stage, results' reporting stage and decision-making stage. The proposed works are evaluated in terms of the achievable energy efficiency and detection accuracy, where they show a significant improvement compared to the state-of-the-art proposals. Moreover, a comprehensive energy-efficient approaches are proposed by combining different algorithms presented in this dissertation. These comprehensive approaches aim at proving the consistency of the proposed algorithms to each other and maximizing the achievable energy efficiency in the whole CSS process.

Moreover, high energy consumption is not the only challenge of CSS. Another important problem in CSS is the vulnerability of the security risks which can effectively degrade the energy efficiency of cognitive radio networks. In this dissertation, we propose three different strategies against security attackers. Specifically, authentication protocol for outsider attackers, elimination algorithm for insider attackers, and a punishment policy are presented in this dissertation. While designing these strategies, an eye is kept on energy efficiency such that increasing immunity against attacker does not affect energy efficiency. Therefore, the tradeoff between energy efficiency and security in CSS has been achieved.

I dedicate my dissertation work to my parents, wife and kids for their endless love, support and encouragement.

ACKNOWLEDGEMENTS

I would like to express my deepest appreciation to all those who provided me the possibility to complete this dissertation. A special gratitude I give to my advisor, Dr. Fabrizio Granelli, for his contribution in stimulating suggestions, giving necessary advices and guidance and arranging all facilities, which helped me to coordinate my PhD research.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Part I

Introduction, Outline and Literature Review

CHAPTER 1

INTRODUCTION

1.1 Cognitive Radio and Cognitive Radio Networks

The frequency spectrum is organized by a regulatory body in each country. This regulatory body divides the spectrum into bands, and defines the spectrum usage, the licensed users, the allowed application, and the operating policies in each band. Some examples of these bands are TV bands, cellular bands, military bands and paging bands. An observation has been reported by FCC, the regulatory body in United States, that some bands are overloaded while others are underutilized [1]. Most of the other regulatory bodies over the all world have confirmed this observation. Based on spectrum assignment agreements, the users of the overloaded bands cannot use the spectrum allocated for the underutilized bands. On the other hand, the users of the overloaded bands still ask for more spectrum resources to satisfy their growing demands. To this end, innovative solutions for spectrum scarcity are highly needed.

Cognitive radio (CR) has been proposed as a promising technique that offers a solution of the spectrum scarcity problem by dynamically exploiting the underutilization of the spectrum among the bands [2]. A cognitive radio was defined as a radio or system that senses, and is aware of its operational environment and can dynamically and autonomously adjust its radio operating parameters accordingly [3]. This definition was generalized by the FCC to be a radio or system that senses its electromagnetic environment and can dynamically and autonomously adjust its radio operating parameters to modify system operation, such as maximize throughput, mitigate interference, facilitate interoperability, access secondary markets [4]. Following these definitions, CR technology has been developed to a spectrum sharing process between licensed and unlicensed users. CR technology implies that the unlicensed users for a band, also called cognitive users (CUs) can exploit the spectrum vacancies in that band at any time without providing extra interference to the licensed users [5]. Doing so, both spectrum scarcity an spectrum underutilization problems can be solved.

Recently, CR technology has received a huge amount of research from several sides. Also, Several standardization organizations have developed CR standards or modified their standards with the objective of including this novel technology [6, 7, 8, 9, 10, 11]. The increasing attention paid to CR is due to the high demand in spectrum resources representing by increasing the number of high data rate devices over the whole world. In this chapter, a general introduction about CR technology is presented, including the most important related issues.

1.1.1 Access Techniques of Cognitive Radio

As CR is a sharing process between the CUs and the licensed users, there are three different access techniques that determine the sharing process. The three techniques are Underlay, Overlay and Interweave.

Underlay CR approach

Underlay approach allows CUs to access the licensed spectrum concurrently with the licensed users. However, the generated interference to the licensed users must be kept within an acceptable range. The induced interference can be managed by controlling the transmit power of CUs. This requires that and licensed users are perfectly known at the CUs side. However, other techniques, rather than adapting the transmit power, can be used to avoid high level of interference, such using multiple antennas or spreading the transmitted signals over a wide bandwidth [12]. Due to the interference constraints, underlay approach has been restricted to short range communications [13].

Overlay CR approach

Similar to the underlay approach, overlay approach allows CUs to use the licensed spectrum simultaneously with the licensed users. Hence, a concurrent transmission will occur from the two user sets, indicating interference to the licensed users. As a compensation , CUs should act as relays for the transmitted signals of the licensed users. Particularly, CUs will use a part of its transmit power for their own communications, while the remainder is used to relay the transmitted signals from the licensed users [14]. By a proper power allocation at the CU side, the increase in the signal-to-noise ratio of the licensed users can be exactly offset the induced interference. However, overlay approach requires a full knowledge of the channel gains and the licensed signal as well at the CU side.

Interweave approach

The third CR access technique follows an interweave approach [15]. Unlike the previous two approaches, interweave approach bans concurrent transmission.

Thus, CUs can only use the spectrum if it is unoccupied by licensed users. Interweave approach is based on the opportunistic communications, where spectrum is periodically monitored and detected vacancies are opportunistically used.

1.1.2 Cognitive Radio Networks

A key function of a cognitive transmission consists in the capability of acquiring the knowledge of the instantaneous spectrum status. Three main methods have been defined to gain such capability: (*i*) By using geo-location techniques, (*ii*) By receiving control and management information or (*iii*) By performing spectrum sensing [10, 16, 17]. Geo-location methods require a central database, self-locating capability and frequently updates of the database by license-holders. Likewise, control and management information techniques require both infrastructure elements and a database. On the other hand, spectrum sensing is considered the most promising solution for spectrum awareness [11].

The reliability of obtained results from the spectrum sensing process is an important factor in the success of the cognitive transmission [18]. Low reliable sensing results affect the performance of both CUs and licensed users. False sensing results, which indicate that the spectrum is occupied, lead to inefficient spectrum utilization, and hence reduced throughput for the CUs. On the other hand, false sensing results, which indicate that the spectrum is free, cause collision between cognitive and licensed users, wasting their energy-spectrum resources. Thus, it is of a paramount importance to ensure reliability in spectrum sensing. However, due to multi-path fading and shadowing that may face individuals, individual spectrum sensing can not guarantee the desired reliability. Especially, strict constraints on detection time and accuracy have been defined in order to avoid interference to the licensed users [19]. As a solution seeking accurate sensing results, cooperative spectrum sensing (CSS) has been proposed [20, 21, 22, 23]. CSS implies that individual cognitive radios should cooperate to create a cognitive radio network (CRN). The ultimate goal of a CRN is to share local sensing results among CUs in order to improve their reliability. The several types of CRNs, the stages of CSS, and the associated difficulties and the induced challenges of CSS will be discussed in the following.

1.1.3 Types of Cognitive Radio Networks

The CRNs are classified based on the architecture used to build the network. The architecture of the network affects the information exchange among the members of the CRN during the CSS and the way they make the global decision regarding the spectrum availability. Basically, there are three different popular architectures in the literature, namely, Infrastructure-based CRN, Ad-Hoc CRN and Mesh CRN.

Infrastructure-based CRN

This type of architectures includes a central entity that is in charge of controlling all the information exchange among CUs, and coordinating the transmission activities [24, 25]. Usually, the central entity is a base station (BS) which is responsible for collecting local sensing results form individuals, making a unique global decision regarding the spectrum occupancy, and coordinating the cognitive transmission. In addition, the BS is in charge of the regular tasks such as user scheduling, synchronization...etc. Fig. 1.1 shows the architecture of infrastructure-based CRN. Notice that in such type of CRNs, the cooperation is achieved only through the BS, where CU can not communicate each other.

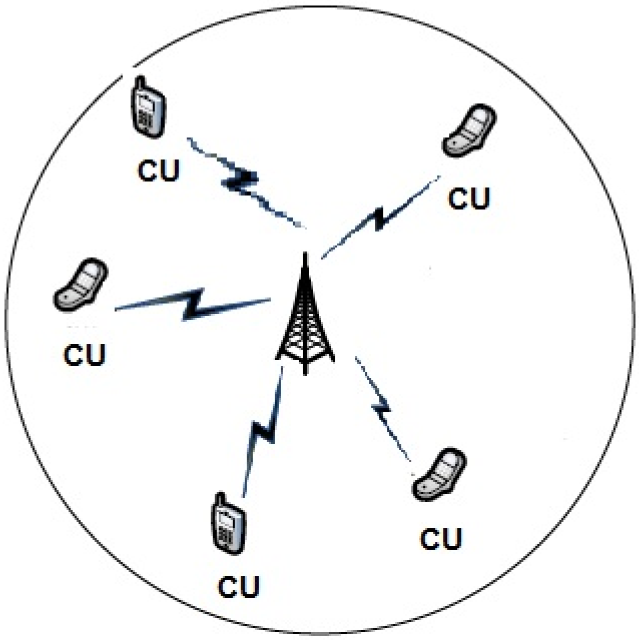


Figure 1.1: *An example of infrastructure-based CRN.*

Ad-Hoc CRN

As in the typical Ad-Hoc networks, the communication among CUs in Ad-Hoc CRNs is performed directly without a need for a BS [26, 27]. In this type of CRNs, each pair of CUs can initiate a communication link using different communications protocols, where they can exchange their local sensing results [28]. Notice that due to the absence of a central entity, each CU makes its own spectrum decision and it could be different from the others. Moreover, data transmission is not globally coordinated. Although Ad-Hoc CRN gives CUs more freedom to make the decision to target the spectrum, it cost individual resource consumption for information exchange and probable transmission collisions. Fig. 1.2 depicts an example of Ad-Hoc CRNs.

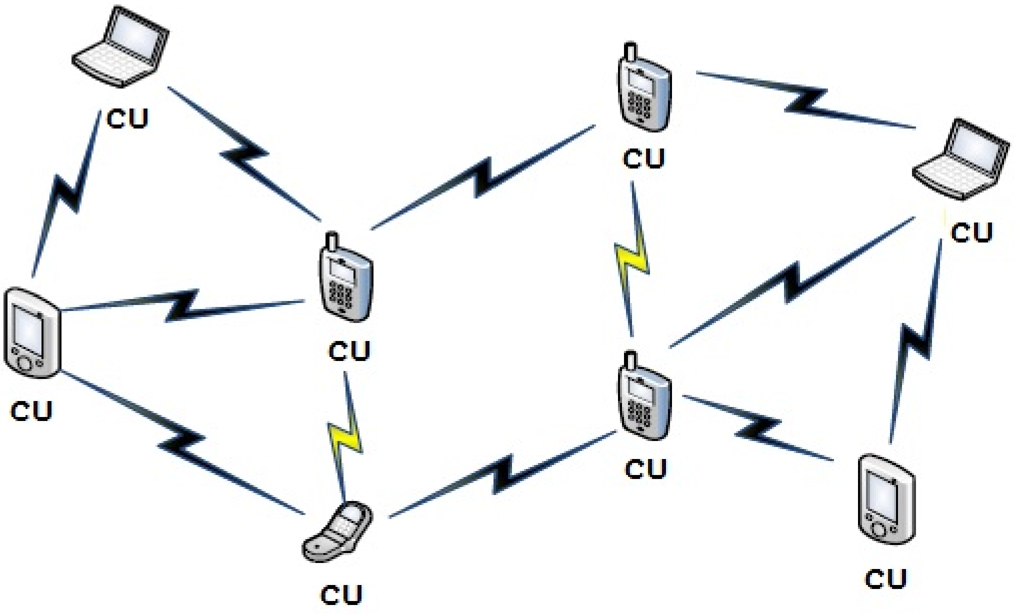


Figure 1.2: *An example of Ad-hoc CRN.*

Mesh Architecture

Another available architecture that is considered as a combination between Infrastructure-based and Ad-Hoc architectures is Mesh architecture [29, 30]. CUs in Mesh CRNs act as relay-nodes between their neighbors and the BS. Such an inter-cooperation avoid large energy consumption during communication with the base station. Notice that the decision regarding the spectrum occupancy is still globally made. Fig. 1.3 shows an example of Mesh CRNs.

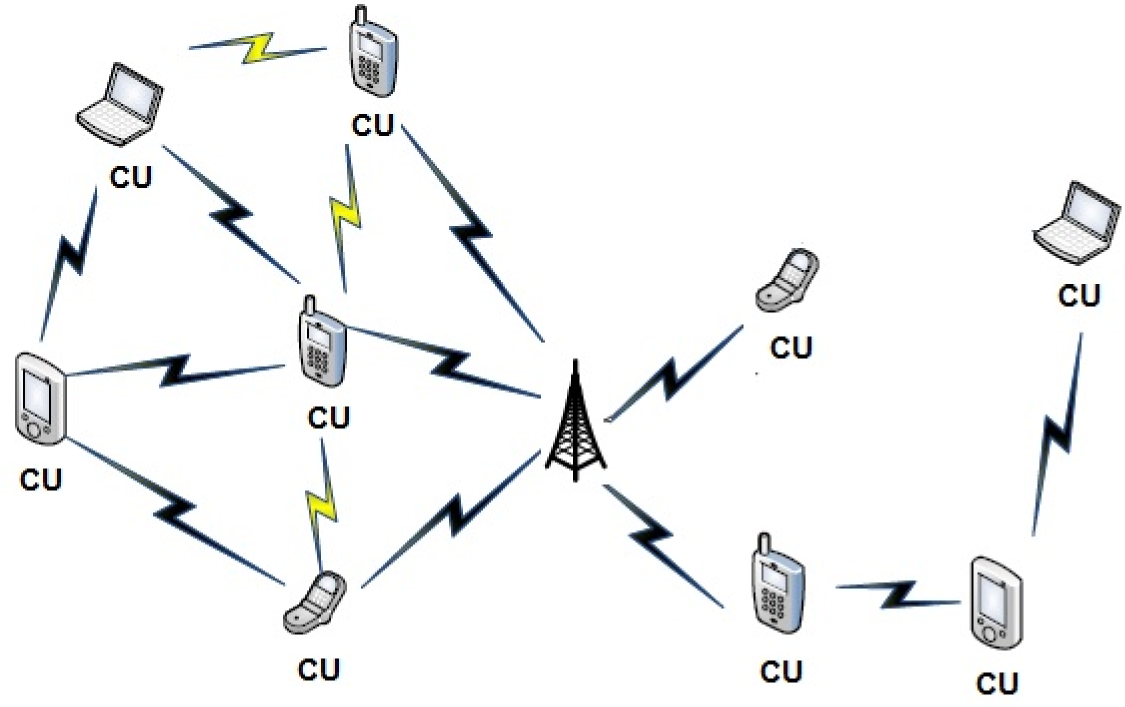


Figure 1.3: *An example of Mesh CRN.*

1.2 Cooperative Spectrum Sensing

In this dissertation, we concentrate on the centralized CSS, where the considered CRN is infrastructure-based CRN. A typical frame structure of a cognitive transmission is shown in Fig. 1.5. CSS starts by a local sensing performed by each CU individually. Different methods to sense the spectrum are available in the literature, such as energy detection [31], matched filters based sensing [32], cyclostationarity-based sensing [33] and waveform-based sensing [34]. Energy detection is the most popular method due to its low computational and implementation complexity. Besides, it does not require any prior knowledge about the signal to be detected, while the others depend mainly on the prior knowledge of the signals to be identified. However, energy detection achieves the worst detection accuracy compared to the other available techniques [35, 36].

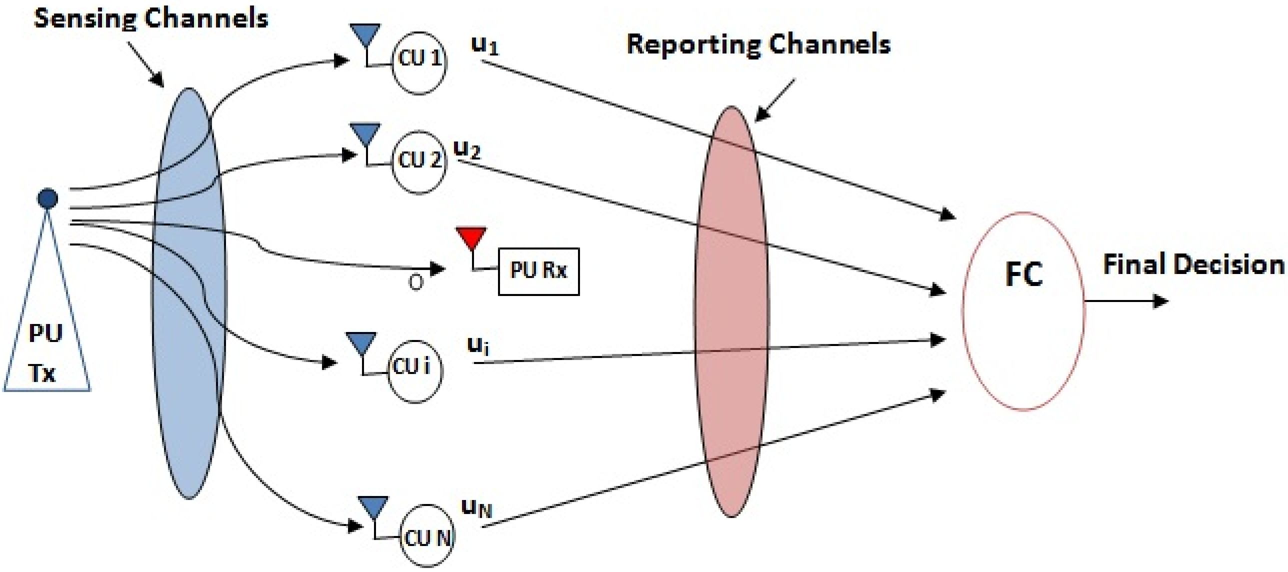


Figure 1.4: *Cooperative Spectrum Sensing Process*

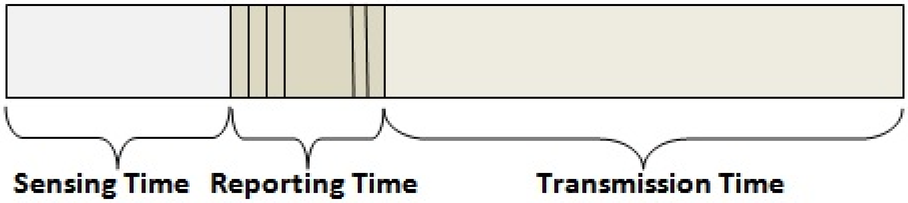


Figure 1.5: *The frame structure of the cognitive transmission.*

1.2.1 Local Sensing Stage

Considering the energy detection method, each CU collects a number of samples from the target spectrum. Each sample actually represents a measurement of the contained energy in the spectrum. The number of collected samples depends on the time dedicated for local sensing, called sensing time. The received signal for any sample by the i^{th} CU ($r_i(t)$) is represented as follows

$$r_i(t) = \begin{cases} h(t)x(t) + n(t) & H_1 \\ n(t) & H_0 \end{cases} \tag{1.1}$$

where H_0 and H_1 represent the two possible spectrum statuses: used or unused, respectively. $x(t)$ is the transmitted signal of the licensed user, $h(t)$ is the channel effect, and $n(t)$ is the complex additive white Gaussian noise with zero mean. Let us denote the average of the collected samples by Y which is expressed as follows

$$Y_i = \sum_{s=1}^{S} \mid r_{i,s} \mid^2 \tag{1.2}$$

where S is the total number of samples.

There are mainly two metrics to assess the local sensing process, namely, local detection probability and local false-alarm probability. Both probabilities evaluate a local decision issued by the CU itself. The local decision is *"used"* if the average of the collected samples is larger than a predefined threshold, called local detection threshold and denoted by λ. Otherwise, the local decision is *"unused"*. Mathematically, the local decision of the i^{th} CU, denoted as u_i, is obtained according to the following formula [69]:

$$u_i = \begin{cases} \textit{unused} & \text{if } \ Y_i < \lambda \\ \textit{used} & \text{if } \ Y_i \geq \lambda \end{cases} \tag{1.3}$$

The local detection probability (P_{di}) is the probability of identifying the spectrum as *used* given that it is actually used, while the local false-alarm probability (P_{fi}) is the probability of identifying the spectrum as *used* given that it is unused.

The mathematical closed form expressions of both probabilities follow the channel fading distribution (h). Considering an additive white Gaussian noise channel, the local detection probability and the local false-alarm probability are both respectively given as follows

$$P_d = Q(\sqrt{2S\gamma}, \sqrt{\lambda}) \tag{1.4}$$

$$P_f = \frac{\Gamma(S, \lambda/2)}{\Gamma(S)} \equiv \Phi_S(\lambda/2) \tag{1.5}$$

where S is the number of samples, and γ is the signal to noise ratio defined as $\gamma = \frac{\sigma_x^2}{\sigma_n^2}$, where σ_x^2 is the variance of $x(t)$, and σ_n^2 is the variance of $n(t)$. Both signals ($x(t)$ and $n(t)$) are assumed to be complex Gaussian distributed with zero mean. $Q(a, b)$ is the generalized Marcum Q-function [38], and $\Gamma(.)$ is the gamma function [39]. However, mathematical expressions of P_{di} and P_{fi} based on other assumptions and different fading channels can be found in [31] [40].

1.2.2 Reporting Stage

The next stage is to report the local sensing results to a common receiver, called fusion center (FC), that is responsible for processing them and for making a global decision of the spectrum occupancy. The reporting of the results is usually accomplished through a common control channel based on either a centralized time-division multiple access (TDMA) [41] or a random access [42]. In a centralized TDM access, each CU has its own time slot for reporting its local result, while in a random access reporting scheme the CUs transmit their reports without any coordination.

Upon having the obtaining the local sensing results, each CU, before sharing the local results with other CUs, has to find a way to represent its local result. There are two popular schemes to this end: hard-based scheme [40] ND soft-based scheme [43].

Hard-based Scheme

According to the hard-based scheme, each CU compares its sensing result to a predefined threshold (λ), and makes a local binary decision about spectrum availability ($u_i \in \{1 \equiv used, 0 \equiv unused\}$). In reporting stage, all CUs convey their local decisions, a single bit per CU, towards the FC consecutively. As will described later, counting rules are used to make the global decision at the FC when hard-based scheme is employed. The hard-based scheme has been proven to be an resource-efficient in terms of time and energy as the reported result is only a single bit. However, reporting only a single bit degrades the overall detection accuracy of the CSS.

Soft-based scheme

Unlike the hard scheme, the local sensing result is reported as it is in soft scheme without any processing at the local level. The sensing result is usually quantized by a large number of bits that is enough to ignore the resulting quantization distortion. Received sensing results are usually summed up at the FC (weighted or unweighted) to make the global decision.

Soft-based scheme provides more accurate sensing results to the FC, which improves the overall detection accuracy. However, this causes a high cost of network resources including time and energy.

1.2.3 Decision-Making Stage

The decision-making stage has an important role in the whole cognitive transmission as it decides whether to use the spectrum or not. At the FC, which is located at the base station, the results received from different CUs are processed by employing a specific fusion rule (FR) in order to make the global decision.

The employed FR follows the reporting scheme, hard or soft, due to the difference in the reporting data type. In general, the results received in soft-based CSS scheme are weighted and averaged, and then, the outcome is compared to a threshold to make a global decision. FRs for soft-based scheme can be classified according the weights used, such as equal-gain combining rule (EGC), where the weights of the all CUs are identical, maximal ratio combining (MRC) [43], where each CU is weighted by its signal-to-noise-ratio (SNR) and likelihood-ratio (LR) [44], where the likelihood ratio statistical test is used to obtain the most likely decision of the spectrum availability. It is worth mentioning that some FRs require additional information to be reported from the CUs together with the sensing results.

As for hard-based CSS scheme, the general rule is called *K-out-of-N* rule [45], where the number of CUs that detect a signal is compared to a threshold (K), where N is the total number of CUs. Depending on K, several rules can be derived for the *K-out-of-N* rule, such as the OR rule ($K = 1$) [46], the AND rule ($K = N$) [47] and majority-logic rule ($K = N/2$), also called voting rule [48].

A general formula that is used to make the global decision (U) for any FR can be given as follows:

$$U = \begin{cases} \textit{unused} & \text{if } \delta' < \delta \\ \textit{used} & \text{if } \delta' \geq \delta \end{cases} \tag{1.6}$$

where δ' is the rule metric and δ is the global detection threshold. For example, in *K-out-of-N* rule, δ' is the number of CUs that detect a licensed signal, and δ is K.

According to the interweave CR approach, which is adopted in this dissertation, the spectrum is used and data transmission is commenced only if the FC has decided that the spectrum is unused. Otherwise, all CUs should wait the next sensing round.

The global decision is usually evaluated by two quantities: global detection probability (P_D) and global false-alarm probability (P_F), which are expressed for any FR as follows

$$P_D = Prob.\{U = 1/H_1\} \tag{1.7}$$

$$P_F = Prob.\{U = 1/H_0\} \tag{1.8}$$

where U is the global decision issued at the FC.

Another widely used probability is the global missed-detection probability (P_{MD}) which is the complementary probability of global detection probability, defined as follows

$$P_{MD} = 1 - P_D = Prob.\{U = 0/H_1\} \tag{1.9}$$

From their definitions, high values of P_D and low values of P_F are desired in order to ensure the efficient exploitation of spectrum vacancies and protect licensed users from unacceptable interference. However, an increase in P_D is accompanied by an increase in P_F, which represents a challenge for network performance. Thus, such a trade-off should be carefully addressed in order to avoid any degradation in the performance of either licensed users or CUs.

1.2.4 Performance Metrics of Cooperative Spectrum Sensing

In the literature, the overall performance of CSS has been evaluated by the detection accuracy of the global decision. As the detection accuracy is a combination of the detection and false-alarm probabilities, a comprehensive metric should include both of them. The false-decision probability (ϵ) is widely used for such a purpose, which is expressed as follows

$$\epsilon = P_0 P_F + P_1(1 - P_D) = P_0 P_F + P_1 P_{MD} \tag{1.10}$$

Sometimes, ϵ is called error probability or erroneous-decision probability in some references. Low values of ϵ indicates that high accuracy of the global decision, which positively influences the other aspects of the network performance.

As any another communication network, the achievable throughput and total energy consumption represent important evaluation metrics of the whole CRN performance. The average achievable throughput (D) is defined as the average successfully transmitted data by the scheduled CUs, while the energy consumption (E) is defined as the average energy consumed during local sensing, results' reporting and data transmission by all CUs. Usually, the achievable throughput is measured by *bits*, whereas energy consumption is measured by *Joule*. Notice that both metrics, throughput and energy, are directly affected by the detection accuracy. However, since high achievable throughput may cause large energy consumption and vice versa, there is a trade-off between the two metrics. Thus, a general metric that combines both of them is recently used, called energy efficiency. Energy efficiency is defined as the ratio between the achievable throughput to the total energy consumption, and measured in *bits/Joule* [49]. Mathematically, energy efficiency (μ) is expressed as follows

$$\mu = \frac{D}{E} \tag{1.11}$$

It is worth noting that energy efficiency metric is a comprehensive metric that involves all the other metrics including detection accuracy, achievable throughput and energy consumption. Apparently, energy efficiency represents a fair indicator of the whole CRN performance from its all aspects. Thus, it has been widely accepted as a metric that can achieve the balance between the different aspects of CRN performance.

1.2.5 Induced Challenges of Cooperative Spectrum Sensing

As described earlier, spectrum sensing is a necessary process prior to the cognitive transmission in order to identify temporally unused portions of the spectrum. This process brings some challenges to the network designers, especially if spectrum sensing is performed cooperatively. The associated challenges of CSS includes extra resource expenditure [50] and additional security threats [51].

Resource Expenditure in Cooperative Spectrum Sensing

Apart of the regular resource consumption in typical wireless networks, additional consumption in terms of energy and time (or bandwidth) is caused by CSS. Performing the CSS in its all stages delays the data transmission, affecting the overall revenue gained by the cognitive transmission. Similarly, sensing the spectrum and reporting the results to the FC consume a significant amount of energy resources, which represents a serious challenges especially for battery-powered users. Moreover, in case of a large number of CUs/channels, these challenge become complicated and highly influence the overall performance of the CRN.

Security Threats in Cooperative Spectrum Sensing

As any other wireless network, CRNs is threatened by typical security attacks. However, other special attack types have been widely discussed as potential attackers for CRNs. There are two popular types of attacks in CRNs, namely, primary user emulation (PUM) and spectrum sensing data falsification (SSDF). PUM attack refers to some malicious users that intentionally act as licensed users (aka primary users) by generating its transmitted signal during the local sensing stage. In presence of PUM attack, CUs will detect the fake signal and will not use the spectrum as it is occupied. Such type of attack definitely degrades the overall performance since the CUs will lose their resources without revenue from the spectrum vacancies.

SSDF attack is represented by malicious users that report false sensing results about spectrum availability, aiming to mislead the global decision of the

CRN. Similar to PUM attack, SSDF attack wastes both energy and throughput resources of the CUs. Moreover, SSDF attack may introduce unacceptable interference to the licensed users, which heightens the negative influence of SSDF attacks.

In this dissertation, high attention is paid in order to address the first challenge, where a set of algorithms/techniques/schemes are proposed to improve the energy efficiency of CSS. The proposed energy-efficient CSS schemes include different solutions for each stage of CSS. Besides, the security threats have been addressed in this dissertation as well. Several secure algorithms and protocols are presented in order to alleviate the affects of attackers and protect the CRNs against them. Moreover, the trade-off between energy efficiency and security has been taken into consideration, where the proposed secure CSS schemes are kept energy-efficient as well.

CHAPTER 2

OUTLINE AND SCIENTIFIC PRODUCT

As we have introduced cognitive radio networks and cooperative spectrum sensing, in this chapter we present the outline of this dissertation and its scientific products in terms of publications.

2.1 Dissertation Outline

This dissertation is divided into seven parts as follows:

Part I: Introduction, Outline and Literature Review.

Part II: Improving Energy Efficiency in Local Sensing Stage.

Part III: Improving Energy Efficiency in Results' Reporting Stage.

Part IV: Improving Energy Efficiency in Decision-Making Stage.

Part V: The Trade-off between Security and Energy Efficiency.

Part VI: Towards Energy Efficient Cooperative Spectrum Sensing: Comprehensive Frameworks.

Part VII: Conclusions.

Part I includes three chapters. **Chapter 1** presents an introduction to CR and CSS, followed by the outline of the dissertation and its scientific products in **Chapter 2**. In **Chapter 3**, an in-deep literature review for the energy-efficient cooperative spectrum sensing approaches is provided.

The parts **II, III and IV** describe the proposed energy-efficient CSS approaches in this dissertation. The proposed approaches are divided based on the target stage. **Part II** proposes three different algorithms in three separated chapters (**Chapter 4-6**) aiming at improving energy efficiency in the local sensing stage. In **Chapter 4**, a centralized algorithm to limit the number of sensing users to the number that satisfies predefined threshold on detection accuracy is presented , while **Chapter 5** presents an energy-efficient CSS algorithm where the participation decision is taken distributively by each CU. An optimization problem of the number of sensing users for energy efficiency maximization is proposed in **Chapter 6**.

Part III discusses four energy-efficient approaches for the reporting stage in **Chapter 7-10**. An energy efficiency performance of hard and soft CSS schemes is analyzed in **Chapter 7**, while **Chapter 8** proposes a novel energy-efficient reporting scheme by reducing the number of reporting CUs. An objection-based reporting scheme is presented in **Chapter 9** in order to reduce the number of reporting CUs. A novel report form that exploits the time dimension is proposed in **Chapter 10**.

The proposed approaches for improving energy efficiency in the decision-making stage are discussed in **Part IV**. Particularly, in **Chapter 11**, an energy efficiency comparison between several fusion rules is performed, while the thresholds of the *K-out-of-N* rule are optimized for energy efficiency maximization in **Chapter 12**.

The trade-off between security and energy efficiency is addressed in **Part V**, where three different secure and energy-efficient CSS algorithms are presented in **Chapter 13-15**. A weighted CSS that is able to eliminate the effects of malicious attackers is presented in **Chapter 13**. In **Chapter 14**, a punishment policy for malicious attacker is proposed, aiming to degrade their individual energy efficiency while improving the energy efficiency of honest CUs. Finally, a novel secure CSS protocol is discussed in **Chapter 15**, where it employs an authentication process to protect the CRN against outsider attackers.

Part VI is dedicated for more comprehensive energy efficient solutions that combines some of the proposed algorithms earlier. The conclusions are drawn in **Part VII**.

2.2 Scientific Product

During three years of research (2011-2014), the research of this dissertation has yielded in many scientific papers in international journals, conferences, symposiums, workshops and books. First, we list the works that are already published , and then we list the works under evaluation.

Book-Chapters

1. Althunibat, S.; Narayanan, S.; Di Renzo M.; Granelli, F., "Energy-Efficient Cooperative Spectrum Sensing for Cognitive Radio Networks", a book chapter in "Software-Defined and Cognitive Radio Technologies for Dynamic Spectrum Access and Management", 2014, IGI Global.

Journals

1. Althunibat, S.; Di Renzo, M.; Granelli, F., “Towards Energy-Efficient Cooperative Spectrum Sensing for Cognitive Radio Networks - An Overview”, Telecommunication Systems, Springer, Accepted for publication.
2. Althunibat, S.; Granelli, F., “An Objection-based Collaborative Spectrum Sensing in Cognitive Radio Networks,” Communications Letters, IEEE, vol.18, no.8, August 2014.
3. Althunibat, S., M. Di Renzo, and F. Granelli. ”Cooperative spectrum sensing for cognitive radio networks under limited time constraints.”Computer Communications 43 (2014): 55-63.
4. Althunibat, S.; Sucasas, V.; Marques, H.; Rodriguez, J.; Tafazolli, R.; Granelli, F., “On the Trade-Off Between Security and Energy Efficiency in Cooperative Spectrum Sensing for Cognitive Radio,” Communications Letters, IEEE , vol.17, no.8, pp.1564,1567, August 2013
5. Althunibat, S.; Palacios, R.; Granelli, F., “Performance Optimisation of Soft and Hard Spectrum Sensing Schemes in Cognitive Radio,” Communications Letters, IEEE , vol.16, no.7, pp.998,1001, July 2012.

Conferences

1. Althunibat, S.; Vuong, T.M.; Granelli, F.,“Multi-Channel Collaborative Spectrum Sensing in Cognitive Radio Networks”,Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2014 IEEE 19th International Workshop on, December 2014, Athens-Greece, Accepted for publication.

2. Althunibat, S; Denise, B.; Granelli, F., “Secure Cluster-based Cooperative Spectrum Sensing Against Malicious Attackers”, Second workshop on trusted communications with Physical Layer Security (TCPLS2014), December 2014, Austin-USA, Accepted for publication.

3. Althunibat, S; Denise, B.; Granelli, F., “A Punishment Policy for Spectrum Sensing Data Falsification Attackers in Cognitive Radio Networks,” In Proceedings of the 2014 IEEE Vehicular Technology Conference-Fall, September 2014, Vancouver-Canada

4. Althunibat, S; Di Renzo M.; Granelli, F., “Robust Algorithm Against Spectrum Sensing Data Falsification Attack in Cognitive Radio Networks,” In Proceedings of the 2014 IEEE Vehicular Technology Conference-Spring, May 2014, Seoul-Korea.

5. Althunibat, S; Granelli, F., “Energy Efficiency Analysis of Soft and Hard Cooperative Spectrum Sensing Schemes in Cognitive Radio Networks ,” the 2014 IEEE 79th Vehicular Technology Conference, May 2014, Seoul-Korea.

6. Althunibat, S.; Di Renzo, M.; Granelli, F., “Optimizing of the K-out-of-N rule for cooperative spectrum sensing in cognitive radio networks,” Global Communications Conference (GLOBECOM), 2013 IEEE , 9-13 Dec. 2013, Atlanta-USA.

7. Althunibat, S.; Granelli, F., “Energy-Efficient Reporting Scheme for Cooperative Spectrum Sensing,” Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2013 IEEE 18th International Workshop on , 25-27 Sept. 2013, Berlin-Germany.

8. Althunibat, S.; Granelli, F., “Novel energy-efficient reporting scheme for spectrum sensing results in cognitive radio,” Communications (ICC),

2013 IEEE International Conference on , pp.2438,2442, 9-13 June 2013, Budapest-Hungary.

9. Althunibat, S.; Narayanan, S.; Di Renzo M.; Granelli, F., ”Energy-Efficient Partial-Cooperative Spectrum Sensing in Cognitive Radio over Fading Channels,” In Proceedings of the 2013 IEEE 77th Vehicular Technology Conference-Spring, 2-5 June 2013, Dresden-Germany.

10. Althunibat, S.; Granelli, F., “On the reduction of power loss caused by imperfect spectrum sensing in OFDMA-based Cognitive Radio access,” Global Communications Conference (GLOBECOM), 2012 IEEE , pp.3383,3387, 3-7 Dec. 2012, California-USA.

11. Althunibat, S.; Narayanan, S.; Di Renzo, M.; Granelli, F., “On the Energy Consumption of the Decision-Fusion Rules in Cognitive Radio Networks,” Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2012 IEEE 17th International Workshop on, pp.125,129, 17-19 Sept. 2012, Barcelona-Spain. BEST PAPER-AWARD.

12. Althunibat, S.; Palacios, R.; Granelli, F., “Energy-efficient spectrum sensing in Cognitive Radio Networks by coordinated reduction of the sensing users,” Communications (ICC), 2012 IEEE International Conference on, pp.1399,1404, 10-15 June 2012, Ottawa-Canada.

Papers under Evaluation

1. Althunibat, S; Denise, B.; Granelli, F., “Identification and Punishment Policies for Spectrum Sensing Data Falsification Attackers Using Delivery-based Assessment”, IEEE Transaction on Vehicular Technology.

2. Althunibat, S; Granelli, F., “On Results’ Reporting of Cooperative Spectrum Sensing in Cognitive Radio Networks”, Telecommunication Systems, Springer.

3. Sucasas, V.; Althunibat, S.; Radwan, A.; Marques, H.; Rodriguez, J.; Vahid, S.;Tafazolli, R.; Granelli, F., “Lightweight Security Against IE and SSDF Attacks in Cooperative Spectrum Sensing”, Wireless Communication and Mobile Computing Journal, Wiley.

4. Althunibat, S.; Vuong, T.M.; Granelli, F.,“Optimizing the Number of Samples for Multi-Channel Spectrum Sensing”, IEEE International Conference in Communications 2015.

CHAPTER 3

LITERATURE REVIEW

Energy efficiency (EE) has gained an increasing importance and has received a lot of interest. This attention is due to the limited energy resources at the CRs, which is often accompanied with a big demand for data rates. The EE is considered to be a comprehensive metric that is able to represent the overall performance of a CR system because it is capable of jointly taking into account the achievable throughput, the overall energy consumption and the detection accuracy. The combination of these indicators in a single metric has made the EE metric a relevant indicator of the quality of cognitive transmission. This chapter provides an overview of available research activities that are aimed at reducing energy consumption of CSS applied to CR networks.

3.1 Energy-Efficient CSS Approaches

The energy consumption of CR system is related to: (i) the periodic nature of the process, (ii) its increase with the number of CUs, and (iii) the increase of the number of channels. Moreover, the energy loss in the case of missed-detection magnifies the problem. Thus, energy-efficient approaches for CSS are mandatory.

Many approaches aiming at improving the energy efficiency of CSS have been presented in the literature. In this section, we review these approaches. The presented approaches are classified, as shown in Fig. 3.1, according to the CSS stage that they are aimed at optimizing. As such, they can be split in three categories: (i) EE approaches for the local sensing stage, (ii) EE approaches for

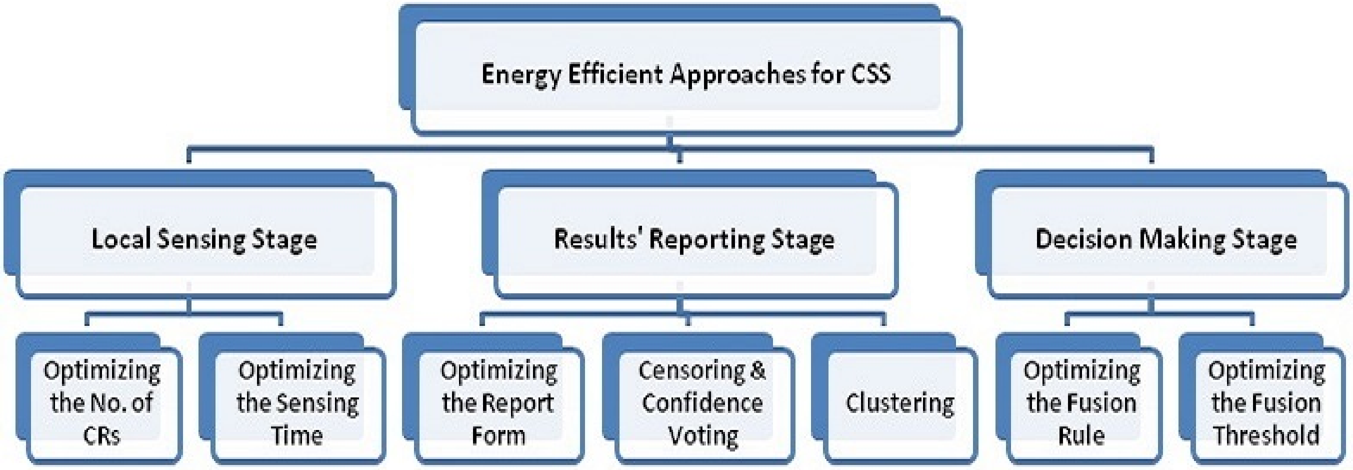

Energy Efficient Approaches for CSS
Local Sensing Stage
Results' Reporting Stage
Decision Making Stage
Optimizing the No. of CRs
Optimizing the Sensing Time
Optimizing the Report Form
Censoring & Confidence Voting
Clustering
Optimizing the Fusion Rule
Optimizing the Fusion Threshold

Figure 3.1: *The classification of the several energy-efficient CSS approaches found in the literature.*

the reporting stage and (iii) EE approaches for the decision-making stage.

3.1.1 Energy-Efficient Approaches for The Local Sensing Stage

The energy consumed for local sensing is equal to the product of the number of sensing users, the sensing time and the sensing power. Thus, reducing energy consumption in the sensing stage can be accomplished in two different ways, either reducing the number of sensing users or by reducing the sensing time.

Optimizing the number of sensing users

The number of sensing users plays a significant role in the energy consumed in CSS. This is related to the fact that any reduction in the number of sensing users leads to a reduction in all the preceding stages. In [52, 53], the energy consumption is reduced based on different scenarios by using the minimum number of CUs that satisfies predefined thresholds on the detection accuracy. In [52], an energy efficiency optimization problem is formulated by minimizing the number of sensing CUs while satisfying predefined constraints on the detection and false-alarm probabilities. However, considering a limited frame length, minimizing the number of sensing CUs does not necessarily maximize energy efficiency. In limited frame length, modifying the time given for a stage will affect the time distribution for other stages in CSS. Hence, minimizing the the number of sensing CUs may decease the reporting time but it gives more time for data transmission which consumes more energy. In [53], the minimum number of sensing CUs that satisfies two constraints on detection and false-alarm probabilities is mathematically formulated. Unlike [52], in [53] only the energy consumed in sensing stage is considered, while energy consumed in results' reporting and data transmission have not been taken into consideration. It is worth mentioning that the attention in [52, 53] has been focused to energy consumption not to energy efficiency, representing a drawback in all of them. Moreover, they assume identical sensing performance for all CUs, which is unrealistic assumption in light of different channel conditions including the multi-path fading and shadowing.

In [54], the CUs are divided into non-disjoint subsets such that only one subset senses the spectrum while the other subsets enter a low power mode. The energy minimization problem is formulated as a network lifetime maximization problem with constraints the detection accuracy. However, the mapping between network life time and energy consumption is not investigated. Similarly, the authors of [55] propose an algorithm that divides the CUs into subsets. Only the subset that has the lowest cost function and guarantees the desired detection accuracy is selected. The desired detection accuracy is defined by two thresholds on detection and false-alarm probabilities, while the cost function is represented by the total energy consumption. The proposed algorithm is built based only on the OR rule. Although OR rule can limit the interference at the licensed users, but it causes a high false-alarm rates. Moreover, the achievable throughput of the proposed algorithm is not discussed in the paper. In both works [54, 55], the proposed algorithms assume that the local sensing performance of each CU is available at the FC in advance, which requires extra resource expenditure in terms of time and energy due to the accompanied overhead.

A distributed approach for selecting the sensing CUs is presented in [56]. The proposed algorithm is based on excluding CUs that have high correlated spectrum sensing results. In detail, it is assumed that each CU has the ability to overhear the sensing results of other CUs. Thus, each CU calculates its correlation is within an acceptable range, it will participate in the sensing stage. Otherwise, the corresponding CU will not participate. Besides its additional complexity, the ability to overhear the sensing result of other CUs is not always possible.

In [57], the instantaneous battery level is considered as a base for selecting the participating CUs in CSS. Particularly, the FC classifies the CUs into two groups based on their battery level which is assumed to be known at the FC. The minimum number of sensing CUs is determined such that a predefined threshold on detection probability is satisfied. The minimum number of the sensing users is selected form the second group (which has th battery highest level). If the number of CUs in the second group is less than the minimum required number of CUs, the rest is selected form the first group (which has the lowest battery level)with equal probabilities. Although the algorithm shows a good performance in extending the lifetime of the CRN by considering the battery level, it does not guarantee the achievable energy efficiency.

In [58], a two-stage CSS is proposed, where CUs are divided into two groups. In the first stage, the first group senses the spectrum and reports the local decisions to the FC. If the FC decides that the spectrum is occupied, the CSS will be terminated. Otherwise, a second stage will be commenced, where the second group of CUs senses and reports the results to the FC. At the FC, the sensing results of both stages are processed in order to issue a global final decision. The energy efficiency is maximized by optimizing the number of CUs in each group and the fusion thresholds. A suboptimal solution for the maximization problem is found using the well-known particle swarm optimization algorithm. A practical drawback is in combining sensing results obtained at different time instants. This might degrade the reliability of the global decision as it is based on results gathered from two different stages.

Three different energy-efficient CSS algorithms for multi-channel systems are proposed in [59]. The three approaches select the sensing users based on their SNRs. In the first algorithm, the minimum number of CUs that satisfies the desired false-alarm probability and minimizes the the energy consumption is assigned to sense a specific channel. The energy consumption includes the energy consumed in sensing and reporting. The second algorithm assigns the CUs with the highest SNRs over a specific channel to sense it, while, in the third algorithm, it is assumed that CUs already sensed the channel, and only the CUs with the highest SNRs will report their sensing results. However, the three proposed algorithms assume the availability of the SNRs at the FC which is unrealistic assumption. Moreover, the energy consumed in data transmission is not taken into account.

Optimizing the sensing time

Optimizing the sensing time/period constitutes another approach that can be adopted for enhancing the energy efficiency of CSS. In [60, 61, 62], the sensing time/period is investigated for individual sensing systems. An adaptive sensing period based on the past spectrum occupancy pattern is presented in [60]. Also, they propose a sequential sensing policy that enforces the CUs to extend the sensing time when its sensing result lies in a specific range. In [61], the CU switch to a non-sensing mode (sleep mode) when a primary user is detected. The non-sensing time is optimized for maximizing a utility function that combines energy saving and throughput loss. The sensing and transmission durations are optimized in [62] with the aim of maximizing the energy efficiency while satisfying constraints on detection accuracy and maximum available power. However, the proposals in [60, 61, 62] consider only a single CU and do not investigate their proposal based on CSS scenario.

As for CSS, [63, 64] and [53] consider the sensing time as a possible approach to reduce the energy consumption. In [63], the CUs perform an initial short sensing stage called coarse sensing. If the sensing result of a CU lies outside a specific predefined range, a binary local decision will be reported from the corresponding CU to the FC. In the case that the sensing result lies in the predefined range, no local decision will be reported from the corresponding CU. At the FC, a global decision (either used or unused) can be made only if the majority decide it. The global decision cannot be made if no majority exists, and therefore, a another sensing stage is commenced by all CUs, called fine sensing. The fine sensing stage is two times longer that the coarse stage. Regardless of the fine sensing results, all CU will report their binary decision to the FC where the global decision should follow the majority decision. Although this two-stage sensing scheme can affectively reduce sensing time, it causes extra energy consumption in reporting stage since it is repeated twice, which is not taken into account. Moreover, the influence of waiting the first global decision on the achievable throughput is not investigated in [63], which might degrade energy efficiency.

In [64], a utility function that consists of the difference between the achievable throughput (revenue) and the consumed energy (cost) is maximized by optimizing the sensing time. A constraint is kept on the detection probability.However, only the utility function does not consider the energy/time spent during reporting the results to the FC. Also, only the AND rule is adopted at the FC, which causes a high missed detection rate. The optimal sensing time that minimizes energy consumption is obtained in [53]. Two constraints on the false alarm and detection probabilities are set, while only the sensing energy is considered in the formulated problem. In [65], energy efficiency is maximized by optimizing the number of sensing users, the sensing time, the transmit power and the local detection threshold jointly and individually. An iterative algorithm is presented to solve the joint optimization. An interesting property of [65] is considering the energy efficiency as a performance metric to be maximized with a constraint on the detection probability. However, the energy consumed in reporting are not considered in energy consumption calculations.

A utility function that includes the difference between the achievable throughput and the consumed energy is maximized in [66] by a joint optimizing of the sensing time and the number of sensing users. The optimal solution is found using an iterative algorithm. However, the energy and time consumed in reporting the results to the FC are not taken into consideration.

In [67] the sensing time is optimized in order to maximize the energy efficiency. The energy consumption function includes all the energy consumed in sensing, reporting and data transmission. However, no closed form expression of the optimal sensing time is given. Instead, the golden section search algorithm is used to find the optimal value.

A related work is in [68], where the sampling rate of the sequential sensing is optimized in order to reduce the energy consumption. The optimization problem is subject to constraints on detection and false alarm probabilities. However, the work only considers a single CU, and energy expenditure during CSS have not been considered in formulating the optimization problem.

3.1.2 Energy-Efficient Approaches for The Reporting Stage

The second stage of CSS is the reporting stage, where the CUs transmit their local sensing results to the FC. Compared to the sensing power, the power consumed in the reporting could be higher. On the other hand, the time spent in sensing is much longer than the time spent in reporting. Therefore, the energy consumed in the reporting stage may be comparable to the energy consumed during the sensing stage. Several works have studied techniques for reducing the energy consumption during the reporting stage, as summarized as follows

Optimizing the report form

In order to report the local result to the FC, each CU has to represent its own result by using a finite a number of bits. The reporting load has a contrasting impact on the overall performance of the CSS. On the one hand, increasing the number of bits enhances the amount of knowledge that is available at the FC, which improves the detection accuracy. On the other hand, a larger number of bits requires more bandwidth and increases the energy consumption. A single-bit reporting scheme is called hard-decision scheme, while multiple-bit reporting schemes are called soft-based reporting schemes. Although many works have compared them under different setups and assumptions [69, 70, 71, 72], none of them has investigated the resulting energy efficiency.

Censoring and Confidence Voting

Censoring is a promising approach that can significantly reduce the reporting CUs. In censoring, a CU does not report its sensing result unless it lies outside a specific range [46, 73, 74]. The censoring thresholds are optimized for minimizing the energy consumption with constraints on the detection accuracy in [41]. Two setups for the availability of the prior information about the probability of spectrum occupancy are considered,namely, blind setup and knowledge-aided setup. However, the considered problem would show more effectiveness if the energy efficiency maximization was considered rather than energy consumption minimization as a problem objective. Besides, energy consumed in data transmission is not considered while computing the total energy consumption.

Recently, in [75], censoring and truncated sequential sensing are combined in order to reduce the energy consumption in CSS. Specifically, the spectrum is sequentially sensed, and once the accumulated energy of the sensed samples lies outside a certain region, the sensing is stopped and a binary decision is sent to the FC. If the sequential sensing process continues until a timeout, censoring is applied an no decision is sent. The thresholds of the censoring region are optimized in order to minimize the maximum energy consumption per CU subject to a constraint on the detection accuracy. Similar to [41], transmit energy is not considered. Moreover, only two FRs are investigated instead of considering the general K-out-of-N FR.

In [76], a confidence voting scheme is presented. It works as follows: if the spectrum sensing of a specific CU agrees with the global decision, it gains its confidence; otherwise, it loses its confidence. When a user's confidence level drops below a threshold, it considers itself as unreliable and stops sending its results. But it keeps sensing the spectrum and tracking the global decision. As long as the result matches, it gains its confidence. Once its confidence level passes beyond the threshold, it rejoins the voting. The energy saving and the detection accuracy of this approach are investigated in [76]. However, confidence level is based on the global decision which is in some cases not reliable enough, especially in case of malfunction or malicious CUs. Moreover, detection accuracy cannot be guaranteed since the number of reported CUs is varying in each sensing round.

A simple approach is presented in [77], where the reported sensing statistics from CUs will processed sequentially at the FC. The FC performs a hypothesis test each time after receiving a statistic from a CU. The FC stops the reporting process when statistics gathered is sufficient for making a decision at a specified reliability level. Otherwise, it will acquire an additional statistic from another CU and repeat the above procedures until it terminates. The FC employs Neyman-Pearson decision strategy instead of *K-out-of-N* FR. The analytical and simulation results in [77] do not show the performance of the proposed algorithm in terms of improving energy efficiency.

Clustering

Clustering is a popular approach to reduce the overhead load between the CUs and the FC. In clustering, CUs are separated into clusters and one from each cluster is nominated as cluster-head, which is in charge of collecting sensing results from cluster-members and reporting a cluster-decision to the FC on behalf of the cluster-members [78]. The cluster-head can be dynamically changed in each CSS round. The energy saving and the accuracy loss are investigated in [76]. In addition to energy consumption analysis, time delay is conducted in [79]. In [80] and [81] clustering and censoring approaches are combined in one energy-efficient algorithm considering the noisy reporting channels. In [82], a multi-level cluster-based CRN is proposed, where the cluster-head that are far away from the FC can forward their cluster decisions to the near CH rather than the FC. Such a technique aims at reducing energy consumption in reporting process, however, it may generate synchronization challenges.

Although clustering reduces reported information to the FC, it induces extra energy consumption during results exchange inside the cluster itself. Besides, creating clustering is a complicated process that adds a significant amount of complexity to the CRNs, especially in mobile CUs scenario.

3.1.3 Energy-Efficient Approaches for The Decision-Making Stage

Every CSS round ends by making a global decision about the spectrum occupancy. The global decision is made by processing the received local results/decisions, where a fusion rule is applied. Regardless of the form of the received results, a predefined fusion threshold is needed to make a decision. In [83], the fusion threshold of the *K-out-of-N* rule is optimized for maximizing energy efficiency without constraints. In [84], the optimal fusion threshold that maximizes the throughput of CRN is obtained with constraints on the consumed energy per CU and the overall detection probability.

Part II

Improving Energy Efficiency in Local Sensing Stage

CHAPTER 4

ENERGY-EFFICIENT COOPERATIVE SPECTRUM SENSING BY COORDINATED REDUCTION OF THE SENSING USERS

4.1 Introduction

An important factor of the amount of energy consumed during local sensing stage is the number of participating CUs. In conventional CSS scheme, the total consumed energy in local sensing stage is proportionally increased as the number of sensing CUs increases. Therefore, reducing the number of sensing CUs should highly limit the energy consumption.

In this chapter, we propose an algorithm to reduce the consumed energy to the minimum value, while keeping the detection accuracy over the desirable bound. The detection accuracy is measured in terms of the detection probability and the false alarm probability. The algorithm is based on maintaining the minimum number of users to sense the spectrum and report the results to the FC. Notice that our proposal helps to reduce the energy consumed in both local sensing and reporting stages. Furthermore, we present a practical way to select the users which sense the spectrum without complicated selection's conditions. The selection of the sensing users depends on a predefined parameter which represents the fulfillment of the detection accuracy. Then, when a new user contends for the spectrum, the FC checks the parameter and decides if there is a need to let it sense or not. Likewise, when a currently sensing user leaves the network, the FC checks the parameter in order to decide if there is a need to invite another user to sense the spectrum or not. In case that a new sensing user needs to be invited, the priority is given to those users which do not occupy the spectrum. This priority preserves the local energy of the users which have a channel and already spent a part of their energy in data transmission.

The contributions of this work are extended to study the performance of the proposed algorithm in different scenarios of fusion rules. The proposed algorithm is run according to the most popular rules, namely, OR-Rule [85] and Majority Rule [86], and a comparison between them is performed in terms of energy efficiency.

4.2 System Model

Consider an infrastructure-based CRN consisting of N CUs. The CUs do not have any prior information about the transmitted signal of the licensed users, hence, the optimal sensing technique is just the energy detector itself, which provides a simple and low cost hardware implementation [69]. For simplicity, the sensing channel is assumed to be Gaussian channel, and the reporting channel is considered error-free channel.The hard-based CSS scheme is adopted as a reporting scheme in this chapter. The received local binary decisions form sensing CUs will be processed at the FC based on the *K-out-of-N* rule. Specifically, two special FRs derived from *K-out-of-N* rule will be discussed: OR rule and Majority rule. Two quantities are used to evaluate the overall detection accuracy, namely, the overall detection probability (P_D) and overall false-alarm probability (P_F). Both are defined in (1.7) and (1.8), respectively.

Before proceeding to our algorithm in the next section, let us define the total consumed energy (E_{css}) in CSS process, which can be expressed as follows:

$$E_{css} = N_s(\rho_s T_s + \rho_r \tau) \tag{4.1}$$

where N_s the actual number of sensing users, ρ_s is the sensing power, T_s is the sensing time, ρ_r is the consumed power during the result's reporting to the FC, and τ is the reporting solt for each CU ($N_s \tau = T_r$).

4.3 The Proposed Algorithm

The proposed algorithm is based on reducing the consumed energy in the local sensing stage by reducing the number of sensing users, while guaranteeing the sensing accuracy. The accuracy of the sensing process is guaranteeing by satisfying two conditions. The first condition is to keep the overall detection probability above a predefined threshold (P_D^{th}), while the second is to keep the false-alarm probability below a predefined threshold (P_F^{th}). Let us define a parameter (I), which represents an indicator of the fulfillment of the two thresholds. When ($I = 1$) the two conditions are satisfied, and when ($I = 0$) at least one of the conditions is not satisfied. Thus, I can be expressed as follows:

$$I = \begin{cases} 0 & \text{if } \ P_D < P_D^{th} \ or \ P_F > P_F^{th} \\ 1 & \text{if } \ P_F \geq P_F^{th} \ and \ P_F \leq P_F^{th} \end{cases} \tag{4.2}$$

The idea is to reduce the number of sensing users to the minimum number of users (N_S^{min}), while keeping the I-indicator equals to "1". The selection of the users sensing the spectrum will be random, providing priority to those users which currently do not use a channel. This priority is given for the aim of saving the local energy of those users which have already transmit data and consume power in data transmission. Fig. 4.1 describes the proposed algorithm.

As shown in Fig. 4.1, assume the I-indicator in random state (0 or 1). Then, for any new CU which contends for the access to the spectrum, the FC will check; if ($I = 1$), the CU will not sense the channel and will be considered in the scheduling of the data transmission. If ($I = 0$), the CU will participate in the sensing process. On the contrary, for any CU which leaves the CRN, the FC will immediately check I. If it is 1, no need to take any action. Otherwise, the FC will invite a CU (from the non-sensing CUs) to sense the spectrum. The priority of inviting will be given to those CUs that do not use the licensed spectrum, as explained above. In addition to the overall energy saving objective, with the proposed priority of invitation we try to balance the consumed energy between the sensing users, which represents another advantage of this algorithm.

As a result, the consumed energy during the CSS in the proposed algorithm will be different from that of the classical approach, derived in Eqn.(4.1), due to the reduction of the number of sensing users. We can write the resulting overall amount of consumed energy during CSS in the proposed algorithm as follows:

$$E_{css}^{min} = N_s^{min}(\rho_s T_S + \rho_r \tau) \tag{4.3}$$

Where N_s^{min} is the minimum number of sensing CUs which can satisfy the two thresholds (P_D^{th} and P_F^{th}).

The percentage of saved energy as compared with the classical approach can be derived as follows:

$$E_{saved} = 1 - \frac{N_s^{min}}{N} \tag{4.4}$$

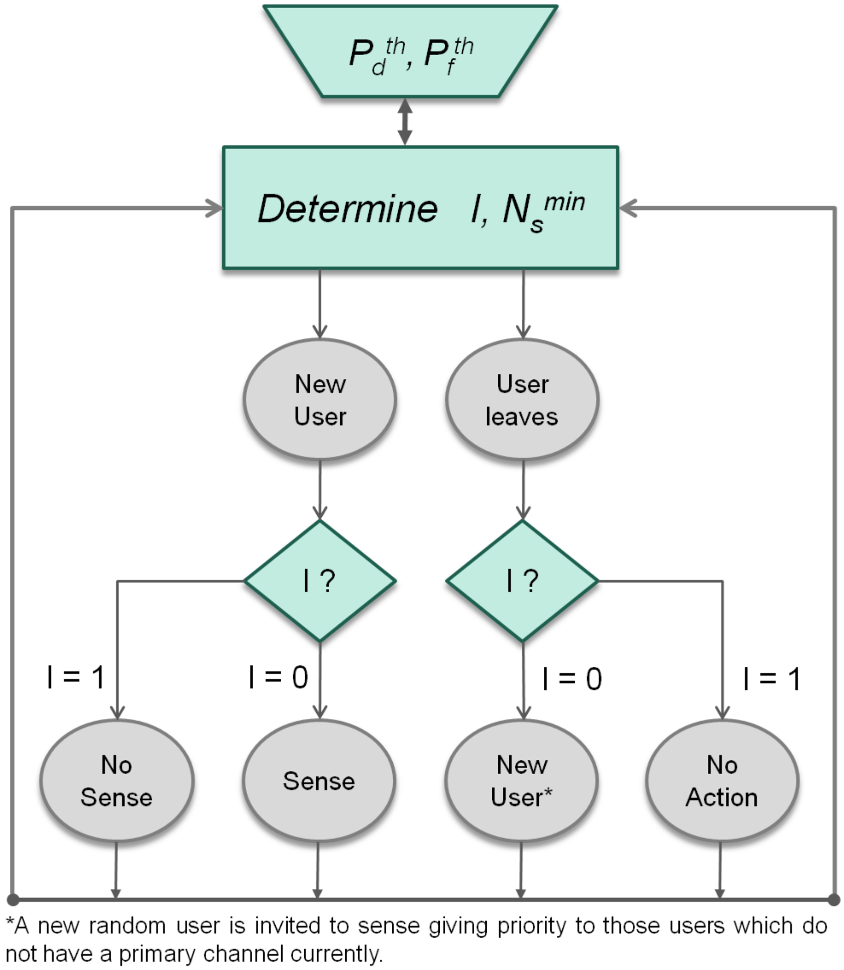


Figure 4.1: *The flow chart of the proposed algorithm .*

There are many of decision-making rules, for each rule, we need a different number of CUs to attain the desired performance. As a result, The exact value of N_S^{min} in (4.4) needed to determine the amount of energy saving depends on the applied FR, which will be discuss soon.

4.4 Analytical Description of Decision Making Scenarios

Energy saving in the proposed algorithm is achieved by satisfying the system requirements represented by P_D^{th} and P_F^{th} according to the minimum number of sensing users. Hence, the amount of consumed energy depends on how the global decision is made at the FC side regarding the availability of the spectrum. In this sense, the global decision relies on the FC which is applied over the collected local reports by the FC. This section is devoted to discuss our algorithm in accordance with two different FRs for the decision making, namely, OR rule and Majority rule. The discussion includes analytical description of the amount of saved energy in each scenario.

4.4.1 OR Rule

In this scenario, each sensing user, after finishing the sensing process, makes a local decision on the spectrum availability. This decision is based on predefined threshold (λ) and it is reported to the FC by a single bit "$1 = busy$", or "$0 = free$". When all the local decisions reach the BS, the BS applies the OR rule in order to output the global decision. The Or rule implies that if at least one CU makes a local decision of *busy* (or 1), the global decision will be *busy* (or 1). Otherwise; the global decision will be *free* (or 0). In other words, the global decision will not be *free*, unless all the users decide it, which is simply like the logical OR operation [85].

According to this scenario, the local detection probability for each user P_{dn}, i.e. the probability of a local decision "1" when the channel is, in fact, busy, can be written as:

$$
\begin{aligned}
P_{dn} &= Pr\{"1"/"channel\,is\,busy"\} \\
&= Pr\{Y_n(t) \geq \lambda/"channel\,is\,busy"\}
\end{aligned}
\tag{4.5}
$$

Notice that, $Y_n(t)$ is the average of S samples taken by each local detector. The exact mathematical expression of P_{dn} is given in (1.4). However, by using the central limit theorem, P_{dn} can be approximated as follows [86],

$$
P_{dn} = Q\left(\frac{\lambda - \left(\sigma_x^2 + \sigma_n^2\right)}{\left(\sigma_x^2 + \sigma_n^2\right)/\sqrt{S}}\right) \tag{4.6}
$$

where

$$
Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} exp\big(\frac{-t^2}{2}\big)\,.dt
$$

and the false alarm probability for each user P_{fn}, which is the probability of a local decision ”1” when the channel is free, is given as:

$$
\begin{aligned}
P_{fn} &= Pr\{"1"/"channel\,is\,free"\} \\
&= Pr\{Y_n(t) \geq \lambda/"channel\,is\,free"\}
\end{aligned}
\tag{4.7}
$$

Also, by using the central limit theorem, the exact expression of P_{fn}, given in (1.5), can be approximated as follows[86]

$$
P_{fn} = Q\left(\frac{\lambda - \sigma_n^2}{\sigma_n^2/\sqrt{S}}\right) \tag{4.8}
$$

Regarding the OR rule, the overall detection probability (i.e. the probability of a global decision of ”1” when the channel is busy) is defined as the probability that at least one of the users reports a local decision of ”1” when the channel is busy. Mathematically, we can express the overall probability of detection as :

$$
P_D^{OR} = 1 - \left(1 - P_{dn}\right)^{N_s} \tag{4.9}
$$

The overall false alarm probability can then be defined as the probability that at least one of the users reports ”1” when the channel is free.

$$P_F^{OR} = 1 - \big(1 - P_{fn}\big)^{N_s} \tag{4.10}$$

By analyzing these two equations, we can conclude that decreasing the number of sensing users will decrease the detection and false-alarm probabilities. Hence, the number of sensing users must be within a specific range $[N_s^{min} \quad N_s^{max}]$ to maintain the desired performance of the system given by $[P_D^{th}, P_F^{th}]$. Thus, as P_D^{th} is a lower threshold, N_s^{min} is determined as follows:

$$\begin{aligned} P_D^{OR} = 1 - \big(1 - P_{dn}\big)^{N_s} &\geq P_d^{th} \\ 1 - \big(1 - P_{dn}\big)^{N_s^{min,OR}} &= P_D^{th} \\ N_s^{min,OR} &= \frac{\log(1 - P_D^{th})}{\log(1 - P_{dn})} \end{aligned} \tag{4.11}$$

Similarly, we can obtain N_s^{max} from the upper threshold P_F^{th} as follows:

$$\begin{aligned} P_F^{OR} = 1 - \big(1 - P_{fn}\big)^{N_s} &< P_F^{th} \\ 1 - \big(1 - P_{fn}\big)^{N_s^{max,OR}} &= P_F^{th} \end{aligned}$$

$$N_s^{max,OR} = \frac{\log(1 - P_F^{th})}{\log(1 - P_{fn})} \tag{4.12}$$

As a result, we can state the range for the number of sensing user that satisfies the performance requirements as follows:

$$\frac{\log(1 - P_D^{th})}{\log(1 - P_{dn})} < N_s < \frac{\log(1 - P_F^{th})}{\log(1 - P_{fn})} \tag{4.13}$$

4.4.2 Majority Rule

In this case, the Majority rule is employed, where the majority of the local decisions will decide the global decisions. In other words, if the majority of the sensing CUs ($\geq N_s$)have decide that the channel is used, the FC will agree with them. Otherwise; the global decision will be *free* [86].

The individual false alarm and detection probabilities are similar to (1.4) and (1.5) because the same procedure has been applied to obtain the local decision. Nevertheless, the global decision is taken according to different rules. Thus, the overall probabilities will be different from (4.9) and (4.10).

The overall detection probability based on the majority rule (P_D^{Maj}) can be expressed as follows

$$P_D^{Maj} = \sum_{i=N_s/2}^{N_s} \binom{N_s}{i} (P_{dn})^i \big(1 - P_{dn}\big)^{N_s - i} \tag{4.14}$$

The overall false alarm probability based on the Majority rule (P_F^{Maj}) is given as follows

$$P_F^{Maj} = \sum_{i=N_s/2}^{N_s} \binom{N_s}{i} (P_{fn})^i \big(1 - P_{fn}\big)^{N_s - i} \tag{4.15}$$

To find the minimum number of sensing users that satisfies the desired performance of the CRN (i.e. the accuracy thresholds), we define two quantities $N_s^{min,D}$ and $N_s^{min,F}$. Whereas $N_s^{min,D}$ is the minimum number of sensing users that fulfills the detection probability threshold (P_D^{th}), $N_s^{min,F}$ is the minimum number of sensing user that complies with the threshold of false alarm probability (P_F^{th}). Hence, the minimum number of users being selected for acceptable performance of the system is:

$$N_s^{min,Sum} = Max\left\{N_s^{Min,F}, N_s^{Min,D}\right\} \tag{4.16}$$

Notice that the number of minimum sensing users in the equations (4.14), (4.15) and (4.16) are analytically invisible.

4.5 Simulations Results

The proposed algorithm is simulated for a CRN Of 20 CUs. During simulation, the local detection threshold has been set to ($\lambda = \sigma_n^2 + 0.1\sigma_x^2$), as this value gives a good results for both rules. The variance of the nose signal is assumed($\sigma_n^2 = -10dB$), and the variance of the licensed signal is assumed (σ_x^2) within the range $[-5dB\ 15dB]$.

The amount of saved energy is calculated as the difference from the consumed energy in the classical scheme, where all the CUs participate in the sensing. The relationship between the amounts of saved energy in spectrum sensing stage versus the channel condition (σ_x^2) is shown in Fig. 4.2 for both rules of decision making: Majority rule and OR rule. The detection probability and the false alarm probability thresholds are given as ($P_D^{th} = 0.9$) and ($P_F^{th} = 0.1$) respectively as in IEEE P802.22 standard.

Clearly, that the amount of saved energy increases as σ_x^2 increases, where it reaches 95% when σ_x^2 equals to 13 dB. Comparing between both rules in terms

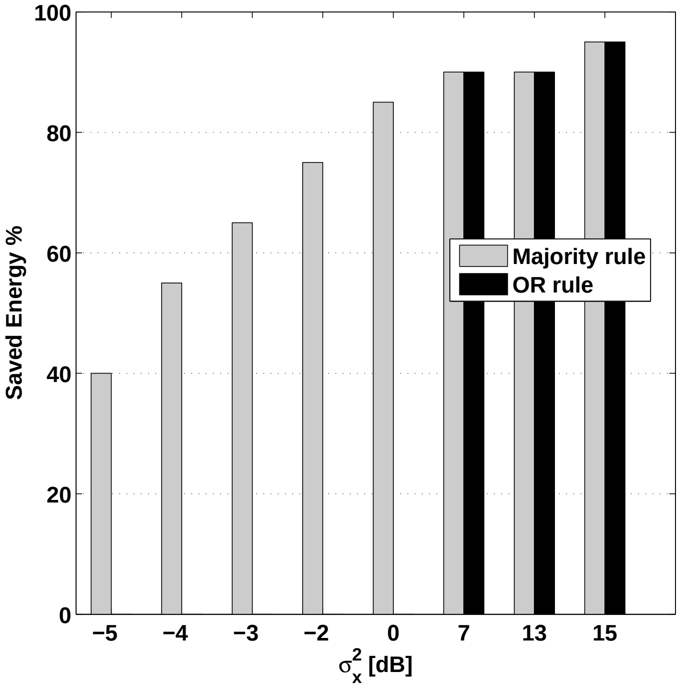


Figure 4.2: *The amount of saved energy versus σ_x^2 for both FRs at $P_D^{th} = 0.9$ and $P_F^{th} = 0.1$.*

of energy efficiency, both have the same performance in good channel conditions. But, in poor conditions (less than $7dB$), Majority rule is still saving a good amount of energy (40%) when the channel worsens ($-5dB$). On the contrary, Or rule results show that there is no saving gain at poor channel conditions (less $0dB$), due to the inability of this rule to fulfill the thresholds of detection accuracy.

Despite high detection accuracy thresholds and bad channel conditions, simulation results, shown in Fig. 4.2, claim that huge amounts of energy saving are achieved in the spectrum sensing stage by means of our approach, especially by the Majority rule. Indeed, final results have lived up to initial expectations in energy savings. In Fig. 4.3, we apply less detection accuracy, and show the performance of the proposed algorithm in terms of energy efficiency versus σ_x^2.

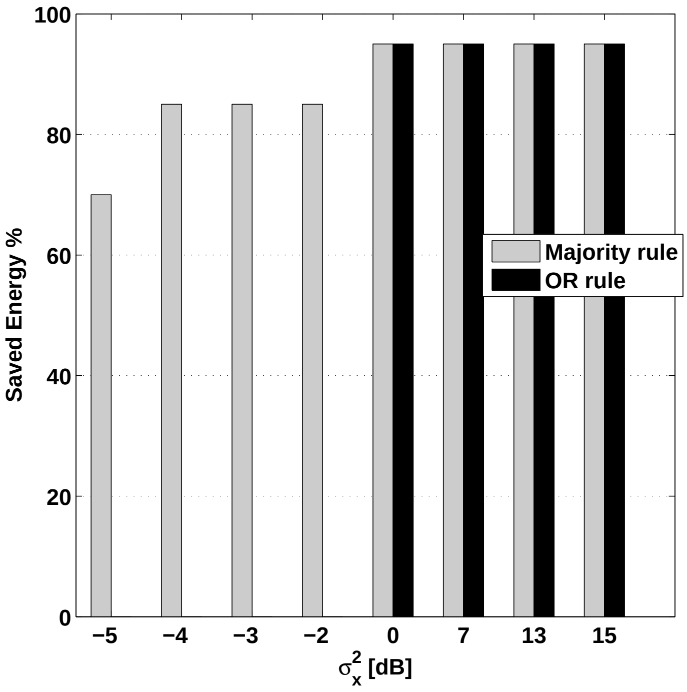


Figure 4.3: *The amount of saved energy versus σ_x^2 for both rules at $P_D^{th} = 0.8$ and $P_F^{th} = 0.2$.*

In Fig. 4.3, we choose the thresholds of detection accuracy to be: $P_D^{th} = 0.8$ and $P_F^{th} = 0.2$, obtaining that the percentage of saved energy at ($\sigma_x^2 = -5dB$) is increased to 60%. This is due to the low restriction on the detection accuracy which can be achieved by lower number of sensing users. Notice also that the performance of OR rule is enhanced at ($\sigma_x^2 = 0dB$), which refers to the ability of the rule to fulfill the less performance thresholds.

Fig. 4.4 is a generalization of the last two figures, where a 3D view of the saved energy versus the detection and false alarm probabilities at $\sigma_x^2 = 0dB$. Fig. 4.4 summaries the obtained results from Fig. 4.2 and Fig. 4.3, which shows the high percentage of saved energy in slight detection accuracy requirements for both rules and with the same percentage. Otherwise, in heavy requirements of detection accuracy, the Majority rule outperforms the OR rule in energy saving according to our proposed algorithm.

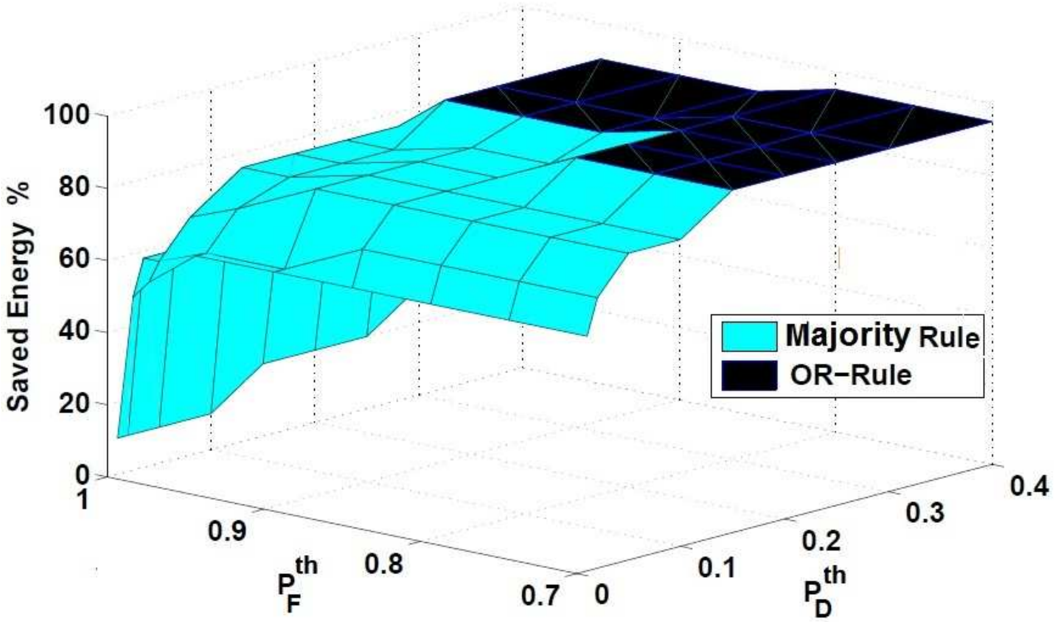


Figure 4.4: *The amount of saved energy versus P_D^{th} and P_F^{th} for both rules at $\sigma_x^2 = 0dB$* .

4.6 Summary

Aiming to reduce the energy consumed in CSS, an algorithm for reducing the number of participating CUs in the sensing process has been proposed in this chapter. The proposed algorithm implies involving only the minimum number of CUs in sensing that guarantees the desired detection accuracy. The detection accuracy is considered satisfied if two thresholds on detection and false-alarm probabilities are satisfied. The proposed algorithm has been evaluated according to two different FRs, namely, OR rule and Majority rule. Compared to OR rule, simulation results show that the Majority rule experiences a high performance being able to achieve huge amounts of saved energy even under harsh channel conditions and high detection accuracy requirements.

CHAPTER 5

ENERGY-EFFICIENT PARTIAL-COOPERATIVE SPECTRUM SENSING IN COGNITIVE RADIO OVER FADING CHANNELS

5.1 Introduction

In the previous chapter, an algorithm is proposed to randomly exclude a number of the CUs from participation in CSS. Likewise, in this chapter, a novel algorithm to reduce the number of participating CUs is proposed. However, the selection of the excluded CUs is not random, where the CUs who consume a high amount of energy during CSS are excluded.

It is normally accepted that not all of CUs spend the same amount of energy in CSS process. Specifically, as CUs are distributed around the FC at different distances, the mount of energy needed to report the sensing results should be different among CUs. Considering the total energy consumption by all CUs, preventing the set of CUs that heavily contributes in energy expenditure from sensing and reporting will effectively reduce the total consumption.

The idea behind our proposal is to prevent the CUs which consume a larger amount of energy from participating in the CSS. The participation decision of each CU is taken individually by the CU itself. In detail, each CU estimates the expected amount of energy that will be consumed if it participates, and compares it to a predefined threshold. If it is less than the threshold, the corresponding CU will participate in CSS. Otherwise, it will not participate. Doing so, not only the number of sensing CUs is reduced, but also the CUs that greatly increase the energy consumption will be prevented from participating, resulting in lower energy consumption.

It is worth mentioning that the proposed approach improves the energy efficiency not only by reducing energy consumption, but also by increasing the amount of successfully transmitted data. The increase in amount of successfully transmitted data is due to the decrease in the overall false alarm probability, as the number of involving users in CSS decreases. As the number of the involving CUs depends on the participation threshold, an optimization of this threshold is carried out to maximize energy efficiency.

The proposed approach includes all the required calculations to expect the amount of energy consumed in CSS. Moreover, a detailed energy consumption model is presented, that includes energy expenditure in all stages of the sensing, reporting and transmission.

5.2 System Model

We consider a centralized CRN of N CUs. The channels between the CUs and the licensed users and the channels between the CUs and the FC are modeled as narrow-band Rayleigh fading with additive white Gaussian noise (AWGN). The channel variance between any CU and the target spectrum is denoted by μ^2, while the channel variance between any CU and the FC is denoted as σ_i^2. The CUs are distributed randomly around the FC . The distance between i^{th} CU and the FC , denoted as (d_i), is uniformly distributed $d_i \sim U[d^{min}, d^{max}]$, where d^{min} and d^{max} are the minimum and the maximum distances, respectively. The adopted sensing technique is energy detection method, and the reporting scheme is hard scheme. Thus, each sensing CU, after sensing makes a binary local decision $u_i\{1,0\}$ about spectrum status is made. if $u_i = 1$, then the i^{th} CU decides it is used. Otherwise, the spectrum is identified as unused by the i^{th} CU.

The local performance is measured by the detection probability ($P_{d,i}$) and the false-alarm probability ($P_{f,i}$). For simplicity, we assume an identical performance among the CUs, and hence, $P_{d,1} = P_{d,2} = ... = P_d$ and $P_{f,1} = P_{f,2} = ... = P_f$. P_d and P_f for Rayleigh fading channels are given in [31] and [87].

Aiming at comparing with the proposed approach, we consider the conventional approach of CSS. In the conventional CSS, all CUs should participate in the spectrum sensing process. Therefore, after a local decision is issued individually by each CU, all local decisions should be reported to the FC. Without loss of generality, we consider OR rule as the FR at the FC. The overall performance is measured by the overall detection probability (P_D) and the overall false alarm probability (P_F), which are given in (4.9) and (4.10), respectively, in Chapter 4.

Regarding the total energy consumed in the conventional CSS approach, if we denote the energy consumed by the i^{th} CU during sensing and reporting by $E_{s,i}$, $E_{r,i}$, respectively, and the energy consumed by the scheduled user is E_t, the total energy consumed is given as:

$$E_{tot} = \sum_{i=1}^{N} E_{s,i} + \sum_{i}^{N} E_{r,i} + P_{unused}E_t \tag{5.1}$$

where P_{unused} is the probability of identifying the spectrum as *unused* (or free), and is given as:

$$P_{unused} = 1 - P_0 P_F - P_1 P_D \tag{5.2}$$

where P_0 and P_1 are the probabilities that the spectrum is actually *unused* and *used*, respectively.

Notice that the sensing energy is identical for all CUs and equal to E_s, thus, (5.1) can be simplified as:

$$E_{tot} = NE_s + \sum_{i}^{N} E_{r,i} + P_{unused}E_t \tag{5.3}$$

As the energy is defined as the consumed power multiplied by the time, (5.3) can be rewritten as:

$$E_{tot} = N\alpha_s T_s + \sum_{i=1}^{N} \alpha_{r,i} T_r + P_{unused}\alpha_t T_t \tag{5.4}$$

where T_s, T_r, and T_t are the time consumed by a CU in sensing, reporting and transmission, respectively. α_s, α_r and α_t are the consumed power during sensing, reporting and transmission, respectively.

Another important quantity that should be defined is the amount of the successfully transmitted data (D) measured in bits. Notice that D depends on the correct identification of the unused spectrum. D is given as:

$$D = P_0(1 - P_F)RT_t \tag{5.5}$$

where R is the data rate in bps, and the factor $P_0(1 - P_F)$ represents the probability of the correct identification of the unused spectrum. From (5.5), it is also clear that the D increases as P_F decreases.

Finally, for the purpose of assessing the energy efficiency in $[Joule/bit]$, we define the consumed energy per bit (EpB) as follows:

$$EpB = \frac{E_{tot}}{D} \tag{5.6}$$

5.3 The Proposed Approach

Motivated by improving the energy efficiency in cognitive radio systems, we propose a novel approach for spectrum sensing which reduces energy consumption during this process with a constraint on the achievable detection accuracy. The idea is to reduce the number of users participating in spectrum sensing, which results in a partial cooperative spectrum sensing. The novelty of our proposal is that the participation decision is taken individually by each CU, and on a base of expected energy consumption. In other words, each CU calculates its expected energy consumption in case of participating in spectrum sensing, and compares it to a predefined threshold called participation threshold (γ_p). If it is lower than γ_p, the CU will participate. Otherwise, the CU will not participate. By such mechanism, we try to reduce energy consumption by an effective way that implies preventing the CUs who will consume large amount of their energy in spectrum sensing from participation.

If we denote the estimated energy consumed during spectrum sensing by the i^{th} CU by E_i, the following equation describes the participation decision (S_i)

$$S_i = \begin{cases} 1\,(Participate) & \text{if} \;\; E_i < \gamma_p \\ 0\,(Don't \;\; participate) & \text{if} \;\; E_i \geq \gamma_p \end{cases} \tag{5.7}$$

Next, we discuss the calculation of E_i, the resulting performance based on our proposal, and finally, we address the energy efficiency improvement achieved by the proposed approach.

5.3.1 Calculations of E_i

E_i includes the energy consumed during local sensing and decision reporting by the CU. Thus, E_i is given as:

$$E_i = E_s + E_{r,i} \tag{5.8}$$

as E_s is identical for all CUs, then the determinant factor in E_i is $E_{r,i}$ that can be written as a product of the reporting time T_r and the power consumed during reporting $\alpha_{r,i}$, as follows:

$$E_r^i = \alpha_{r,i} T_r \tag{5.9}$$

In results' reporting, the user is in transmission status, and hence, $\alpha_{r,i}$ mainly depends on the distance from the FC and the desired bite error rate. $\alpha_{r,i}$ is given as [88]:

$$\alpha_{r,i} = \alpha^c + \alpha_i^{PA} \tag{5.10}$$

where α_i^{PA} is the power consumed in the power amplifier stage of the i^{th} user, and α^c is the power consumed by the other circuit elements. α^c is identical in all users and can be modeled as:

$$\alpha^c = \alpha^{DAC} + \alpha^{filt} + \alpha^{mix} + \alpha^{syn} \tag{5.11}$$

where α^{DAC}, α^{filt}, α^{mix}, and α^{syn} are the power consumption at the digital-to-analog converter (DAC), the transmit filters, the mixer, and the frequency synthesizer, respectively. α^{filt}, α^{mix}, and α^{syn} can be modeled as constants, while α^{DAC} can be approximated as:

$$\alpha^{DAC} = \left(\frac{1}{2} V_{dd} I_0 (2^{n_1} - 1) + n_1 C_p (2B + f_{cor}) V_{dd}^2 \right) \tag{5.12}$$

where I_0 is the current supply, n_1 is the number of bits in the DAC, C_p is the parasitic capacitance, V_{dd} is the voltage supply, f_{cor} is the corner frequency, and B is the symbol bandwidth.

The second part of (5.10), α_i^{PA} is given as:

$$\alpha_i^{PA} = \frac{\zeta}{\delta}\alpha_i^{out} \tag{5.13}$$

where δ is the drain efficiency of the RF power amplifier, ζ is the Peak-to-Average Ratio (PAR) which is dependent on the modulation scheme and the constellation size, and α_i^{out} is the transmitted power from the amplifier. When the channel only experiences a square-law path loss we have:

$$\alpha_i^{out} = \bar{E}^b R_b \tag{5.14}$$

where $\bar{E}^b$ is the required energy per bit at the receiver for a given BER requirement, and R_b is the bit rate. Under Rayleigh fading, $\bar{E}^b$ in (5.14) for BPSK modulation can be given as follows:

$$\bar{E}^b = \frac{N_o(1-2P_e)^2}{4\sigma_i^2 P_e(1-P_e)} \tag{5.15}$$

where P_e is the BER and σ_i^2 is channel variance that is given as:

$$\sigma_i^2 = \frac{(4\pi d_i)^2}{G_t G_r \lambda^2} M_l N_f \tag{5.16}$$

where G_t is the transmitter antenna gain, G_r is the receiver antenna gain, λ is the carrier wavelength, M_l is the link margin compensating the hardware process variations and other additive background noise or interference, and N_f is the receiver noise figure defined as $N_f = \frac{N_r}{N_o}$ with $N_o = 171\ dBm/Hz$ the single-sided thermal noise Power Spectral Density (PSD) at room temperature and N_r is the PSD of the total effective noise at the receiver input.

5.3.2 The achievable performance

Let us consider the estimated energy of each CU (E_i) as a random variable with a Probability Density Function (pdf), f_e, and Cumulative Distribution Function

(CDF), F_E. Therefore, for any CU, the probability of participation in the spectrum sensing equals to $F_E(\gamma_p)$. Also, the number of CUs who have decided to participate (N^*) follows a binomial distribution described as:

$$Prob.(N^* = n) = \left(\begin{array}{c} N \\ n \end{array} \right) (F_E(\gamma_p))^n \big(1 - F_E(\gamma_p)\big)^{N-n} \tag{5.17}$$

where the average number of sensing users $\overline{N^*}$ is given by

$$\overline{N^*} = N F_E(\gamma_p) \tag{5.18}$$

After reporting the local decisions made by N^* CUs, OR-rule is applied and a final decision is made. In case of $N^* = 0$, i.e., no users have participated, a random final decision is made at the FR. Therefore, the average overall detection probability (P_D^*) and the average overall false alarm probability (P_F^*) can be written as:

$$P_D^* = \begin{cases} 1 - (1 - P_d)^{N^*} & \text{if } \; N^* \geq 1 \\ 0.5 & \text{if } \; N^* = 0 \end{cases} \tag{5.19}$$

$$P_F^* = \begin{cases} 1 - (1 - P_f)^{N^*} & \text{if } \; N^* \geq 1 \\ 0.5 & \text{if } \; N^* = 0 \end{cases} \tag{5.20}$$

where $N^* = 1, 2, ..., N$.

5.3.3 Energy Efficiency Optimization

The total energy consumed by the whole system by following the proposed approach (E_{tot}^*) can be written as follows:

$$E_{tot}^* = \sum_{i=1}^{N} S_i E_i + P_{unused}^* E_t^* \tag{5.21}$$

where the first term represents the consumed energy during spectrum sensing process, which equals to 0 for the CUs who have not participated because it is multiplied by $S_i = 0$. The second term represents the energy consumed during data transmission (E_t^*) which is conditioned by P_{unused}^*. P_{unused}^* is the probability of identifying the spectrum as unused in our approach, which can be obtained by substituting P_D^* and P_F^* instead of P_D and P_F in (5.2).

Regarding the calculation of E_t^*, we assume that a CU is randomly scheduled for data transmission. Therefore, the calculation of E_t^* follows the same procedure as E_r with a proper substitution of the values of f_{cor}, B, and P_e.

The amount of successfully transmitted data in bits, D^* depends mainly on the performance of the spectrum sensing, and can be given as:

$$D^* = RT_t\Bigg(P_0(1 - P_F^*)\Bigg) \tag{5.22}$$

Hence, the total energy consumed per successfully transmitted bit based in the proposed approach (EpB^*) is given as:

$$EpB^* = \frac{E_{tot}^*}{D^*} \tag{5.23}$$

Remember that the resulting EpB depends mainly on the number of participating users which is a function of γ_p. Therefore, in order to minimize EpB^*, an optimization of γ_p is highly motivated.

5.4 Simulation Results

In this section, we present some simulation results in order to illustrate the advantage of the proposed partial-cooperative spectrum sensing scheme. In particular, we are interested in finding an optimal value of the energy threshold, γ_p, which minimizes the total energy consumed per successfully transmitted bit in partial CSS, EpB^{*}. Table 5.1 lists the simulation parameters used in this section [88].

Table 5.1: Simulation Parameters

Parameter	Value	Parameter	value
N	10	P_0	0.5
P_d	0.8	P_f	0.2
T_s	$3\,ms$	T_r	$0.01\,ms$
T_t	$40\,ms$	d^{min}	100m
d^{max}	7Km	α_s	$106\,mW$
α^{syn}	$50.0mW$	α^{filt}	$2.5mW$
α^{mix}	$30.3mW$	I_0	3μA
V_{dd}	$3V$	f_r	$2.5GHz$
R_b	$10Kbps$	n_1	10
C_p	$1pF$	G_tG_r	$5dBi$
N_f	$10dB$	M_l	$40dB$
δ	0.35	f_{cor}	$1KHz$
P_e	10^{-5}	ζ	514×10^{-3}

Fig. 5.1 shows the average number of participating CUs in CSS versus the participation threshold . The x-axis is shown in terms of E_{min}, E_{max} and Δ, where E_{min} and E_{max} are the energy consumed in spectrum sensing by a CU at a distance equals to d^{min} and d^{max}, respectively. The constant Δ is the step between each two consecutive lines and equals to 1×10^{-14} . Obviously, as γ_p increases, the probability of participating in CSS for each CU increases as well, and hence, the number of participating will increase. Different numbers of available CUs in the network are shown in Fig. 5.1. However, such change in the participating CUs will undoubtedly influence the transmitted data, energy consumption and energy efficiency, as we will see in the next results.

As the number of participating CUs is variable depending on the participation threshold, it is expected that both the false alarm and detection probabilities

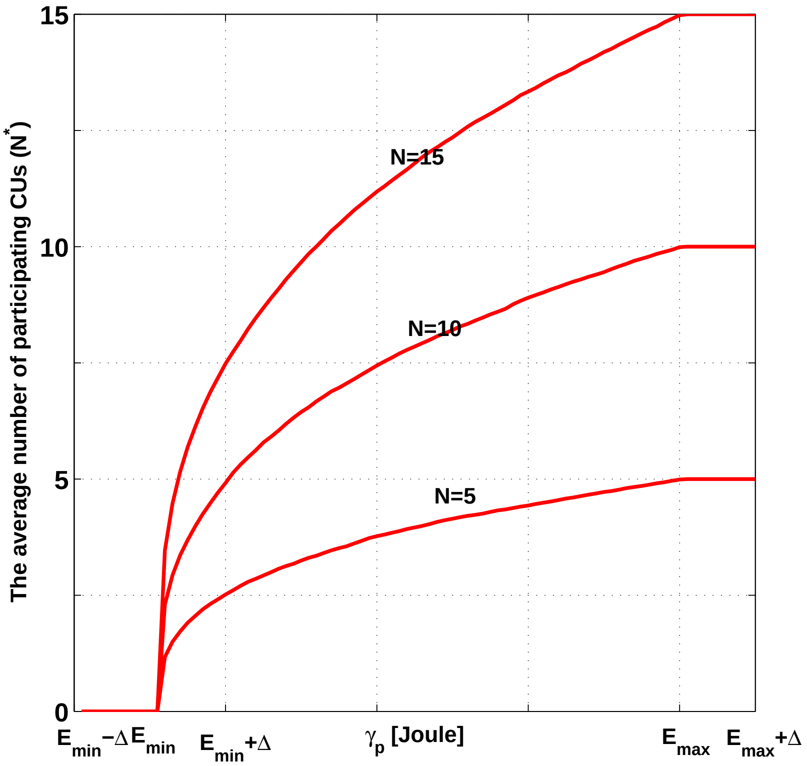


Figure 5.1: The average number of participating CUs versus γ_p. ($\Delta = 1 \times 10^{-14}$)

will be affected. In order to show the effect of the participation threshold on the sensing accuracy, we use the false-decision probability (ϵ) as an evaluation metric. ϵ, as given in (1.10), is defined as the weighted sum of false alarm probability and the missed detection probability.

Fig. 5.2 plots the false-decision probability versus participation threshold at $N = 10$. At low values of the participation threshold, ϵ is equal to 0.5 since the decision is random when no CUs participate in the CSS process. Optimizing the participation threshold yields in a minimum false-decision probability as shown in Fig. 5.2. Notice that the minimum false-decision probability attained by our approach is much less than the attained by the conventional approach.

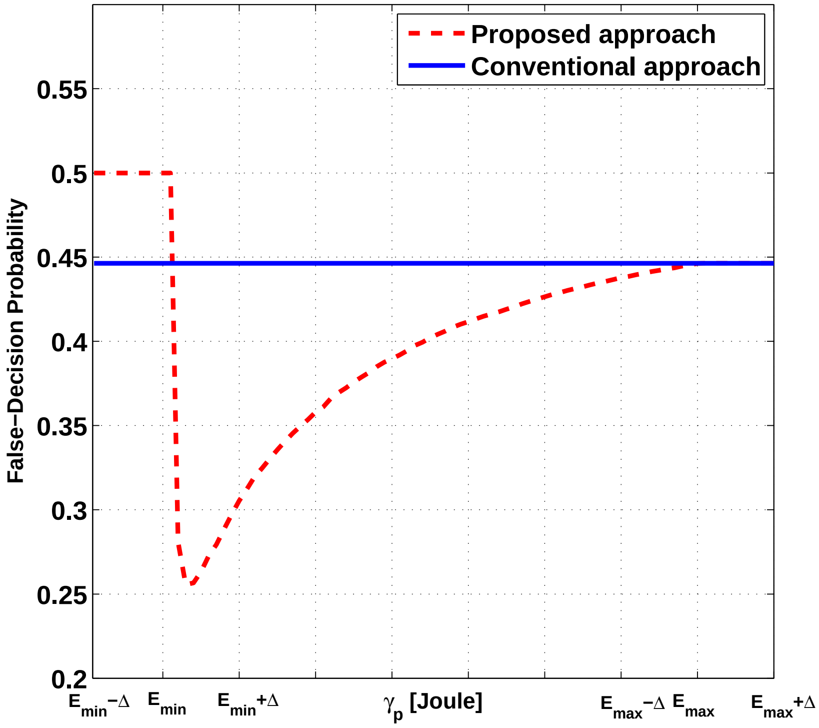


Figure 5.2: The false decision probability versus γ_p. ($\Delta = 1 \times 10^{-14}$)

Fig. 5.3 shows the achievable amount of successfully transmitted data versus the threshold γ_p. For low values of γ_p, all CUs will not participate in CSS since they have E_i larger than γ_p, which results in $P_F^* = 0.5$, according to (5.20). Hence, D^* is constant since it depends mainly on P_F^*, as stated in (5.22).

As γ_p increases so that the number of sensing users equals to 1, P_F^* improves, and consequently, the transmitted data increases. As γ_p increases, D^* decreases since P_F^* increases. For comparative purposes, Fig. 5.3 also shows the plot for the achievable amount of successfully transmitted data using the conventional approach, D, where all the users take part in CSS. Since in conventional approach, D is independent of the value of γ_p, the plot will be a constant with respect to γ_p. In Fig. 5.4, the total energy consumed by the system in partial

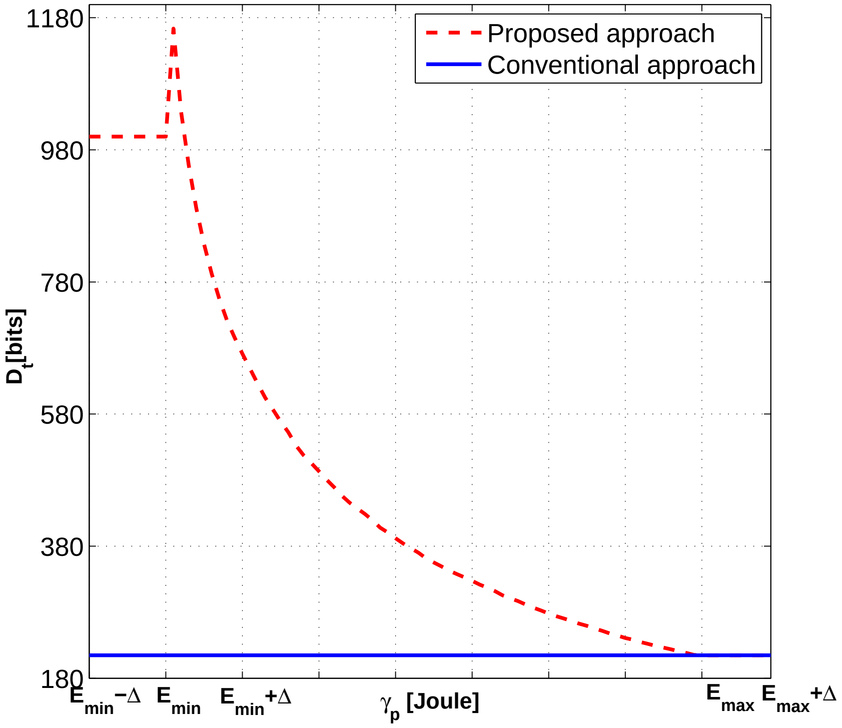


Figure 5.3: The amount of transmitted data versus γ_p. ($\Delta = 1 \times 10^{-14}$)

CSS, E^*_{tot} over different values of γ_p is plotted. We can see that, as γ_p increases, E^*_{tot} first remains the same, but then decreases and then gradually becomes stable for larger values of γ_p. The initial flat region in the plot is due to the fact the estimated energy, E_i of all the CU's is above γ_p. Hence, all the CU's will not participate in spectrum sensing, and energy is consumed only in transmission. As γ_p is increased, E^*_{tot} decreases even though more CUs participate in CSS. This is due to the decrease in P_{unused}. The plot for total energy consumed by the system in conventional approach, is also shown in Fig. 5.4. From the previous figures, it is clear that increasing γ_p lowers the energy consumption but with lower transmitted data. Thus, in order to find the optimal value of γ_p that balances the two contrasting effects, the total energy consumed per successfully transmitted bit in partial CSS, EpB^* versus different values of γ_p is plotted in Fig. 5.5. As γ_p

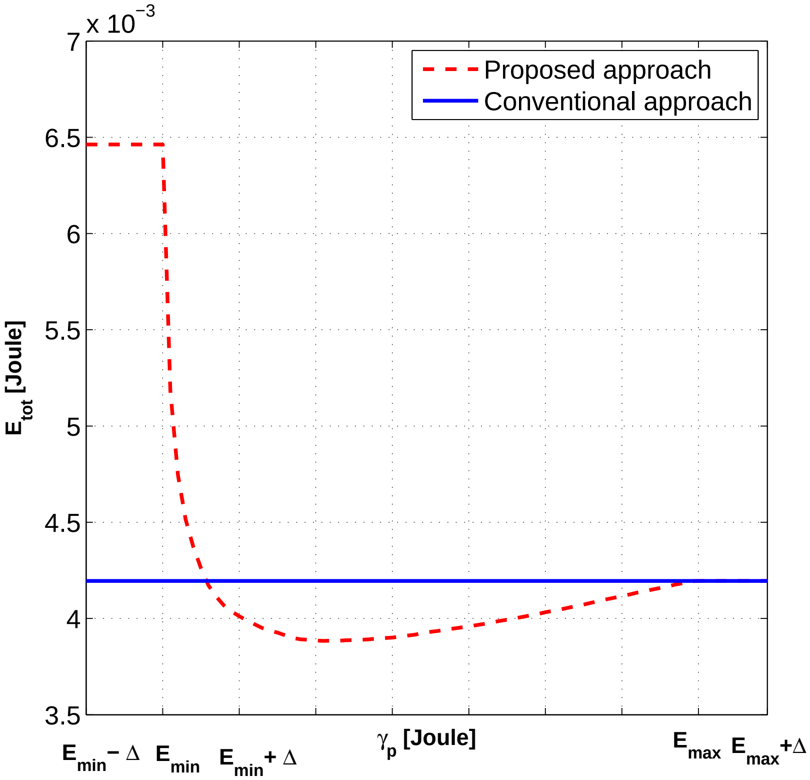


Figure 5.4: Total consumed energy of the whole system versus γ_p. ($\Delta = 1 \times 10^{-14}$)

increases, EpB^* first remains the same, but then decreases and then increases after a particular value of γ_p. The value of γ_p, where EpB^* is minimum gives the optimal value of γ_p. The plot for total energy consumed per successfully transmitted bit is also shown in Fig. 5.5. The results in Fig. 5.5 clearly shows the potential gain of using the proposed partial-CSS scheme over the conventional approach. More precisely, when the optimal value of γ_p is used, partial CSS provides a Relative Average Energy Reduction(RAER) per successfully transmitted bit of approximately 80% with respect to the conventional approach.

The threshold γ_p plays a key factor in the performance of the proposed approach. In Fig. 5.6, we plot the percentage of RAER compared to the conventional approach versus the total number of CUs, where RAER is expressed as

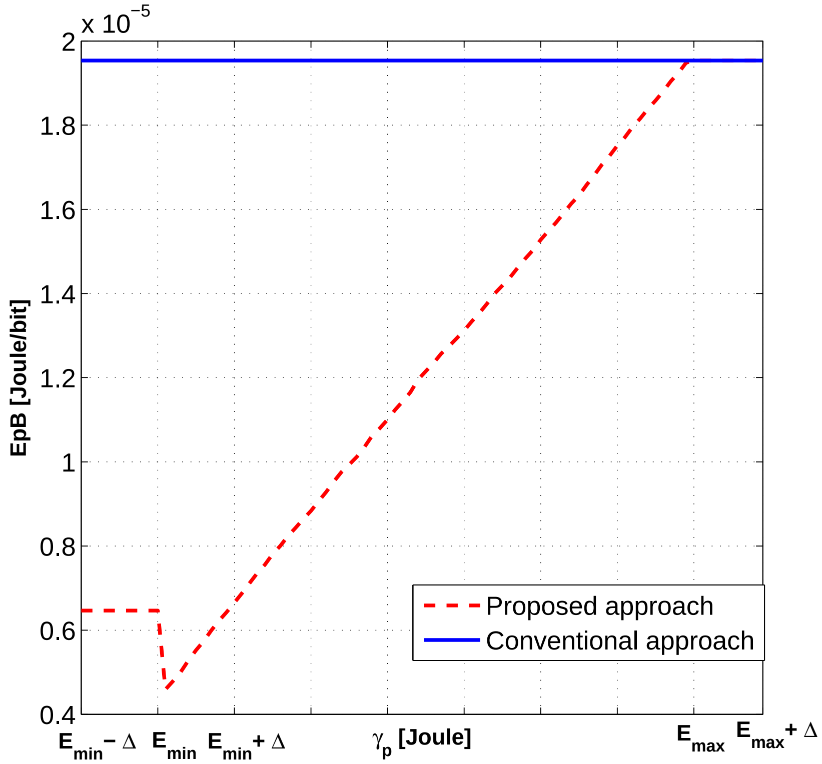


Figure 5.5: Total energy consumed per successfully transmitted bit versus γ_p. ($\Delta = 1 \times 10^{-14}$)

follows:

$$RAER\% = \frac{EpB_{conventional} - EpB_{proposed}}{EpB_{conventional}} \times 100\% \tag{5.24}$$

5.5 Summary

A partial cooperative spectrum sensing approach is presented in this chapter, which aims to reduce the energy consumption in cognitive radio networks. The proposed approach is based on reducing the number of sensing users. Each user decides to participate in spectrum sensing if its expected energy consumption during this process is less than a threshold. An energy consumption model is discussed in order to compute the total energy consumption. The participation

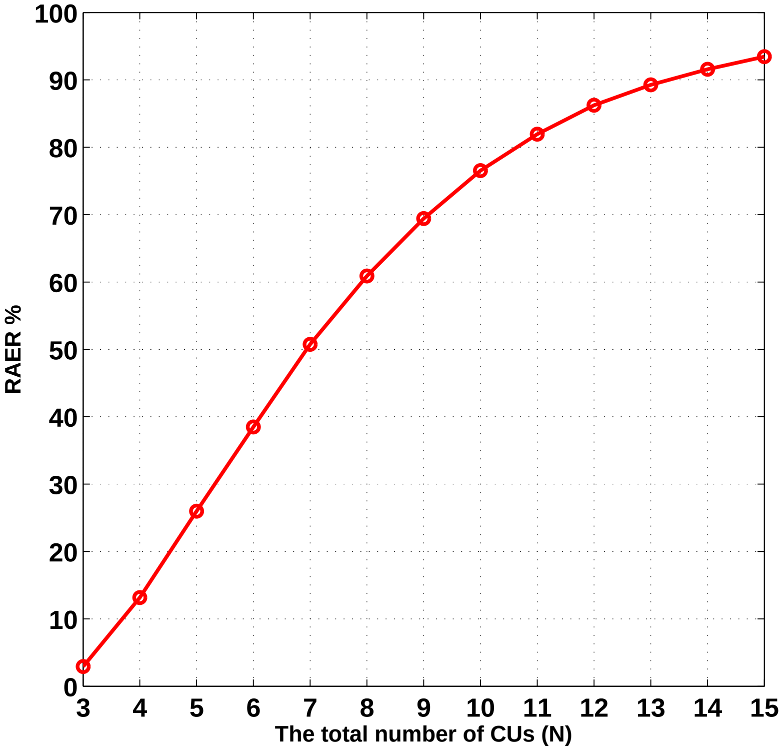


Figure 5.6: The Relative Average Energy Reduction per bit versus the total number of CUs.

threshold is optimized to minimize the energy consumption through computer simulations.

CHAPTER 6

OPTIMIZING THE NUMBER OF USERS IN COOPERATIVE SPECTRUM SENSING UNDER LIMITED TIME CONSTRAINTS

6.1 Introduction

In this chapter, we investigate the problem of optimizing the number of sensing users for CSS under three different setups: throughput maximization, energy minimization, and energy efficiency maximization, while satisfying a predefined constraint on the detection probability. The optimization problems are based on a pragmatic limited time resources constraint. More specifically, we assume that the total frame has a finite and fixed duration. A fixed part of it is dedicated for data transmission, while the rest is distributed between local sensing and results' reporting as a function of the number of sensing users. With this finite frame duration assumption, if the number of users increases, the reporting time has to be longer, and, thus, a shorter time is left for local sensing. Compared with the state-of-the-art, we assume that the time duration of data transmission is kept fixed and sensing/reporting times are variable. State-of-the-art papers sometimes assume a fixed sensing time and a variable data/reporting times [52, 89, 90]. Our assumption does not affect data transmission, and, thus, makes CSS a less invasive process.

Although the work in [52] is related to ours, there are three main differences between both works : (i) Different time distribution mechanisms are assumed, where in [52] the sensing time is fixed so that the overhead load affects the transmission time, while we fix the transmission time and the overhead load affects the sensing time, (ii) No closed form expression are presented in [52] for the two considered setups, while we present simple closed forms for the optimal number of sensing users that maximizes throughput and minimizes energy consumption, (iii) Unlike our work, neither energy minimization nor energy efficiency maximization are tackled in [52]. Nevertheless, since both works are based on different assumptions, our approach can be considered as parallel contribution to those presented in [52]. Another related work is [91], where the sensing time is optimized for throughput maximization. However, the optimal number of CUs has not been investigated in [91], and the optimization is confined on throughput maximization setup. Moreover, the time distribution assumption is different form ours, where the transmission time is left variable and the reporting time has not been considered.

The contributions of the work in this chapter can be summarized as follows:

- Deriving, in closed-form, the optimal numbers of sensing users that maximize the achievable throughput and minimize energy consumption, while limiting the resulting interference by satisfying a predefined constraint on detection probability.
- Proposing a simple iterative algorithm that is able to find the optimal number of sensing users that maximizes the energy efficiency while limiting the resulting interference by satisfying a predefined constraint on detection probability
- Proposing a novel scheme that is able to improve energy efficiency by finding the optimal number of sensing users that minimizes energy consumption while keeping the same throughput as when all available users cooperate, and satisfying a predefined threshold on the detection probability.

6.2 System Model

A CR network with N CUs is considered. The sensing channel is assumed to be additive white Gaussian noise channel with σ_w^2 noise variance. The transmitted signal by the licensed users is assumed to be circularly symmetric complex Gaussian (CSCG) distributed with variance σ_x^2. This assumption is reasonable for signals with rich inter-symbol interference, for orthogonal frequency division multiplexing (OFDM) signals with linear precoding [91], and under the assumption that the PUs are operating close to capacity [92] [93]. The adopted sensing technique is energy detection, and the employed reporting scheme is soft-based scheme. Also, we assume that the local results are reported to the FC in different time slots based on a time division multiple access scheme (TDMA) [52].

6.2.1 Detection Accuracy

According to the soft-based CSS, the overall detection probability (P_D) and the overall false alarm probability (P_F) can be approximated using the central-limit theorem as follows [45]

$$P_D = Q\left(\frac{\lambda - (\sigma_x^2 + \sigma_w^2)}{(\sigma_x^2 + \sigma_w^2)/\sqrt{nS}}\right) \tag{6.1}$$

$$P_F = Q\left(\frac{\lambda - \sigma_w^2}{\sigma_w^2/\sqrt{NS}}\right) \tag{6.2}$$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} exp\left(\frac{-t^2}{2}\right) dt$, S is the total number of collected samples by all CUs, and n is the actual number of sensing users with $1 \leq n \leq N$.

Let us assume that the threshold λ is chosen in order to guarantee a given detection probability P_D^{th}. Therefore, using (6.1), λ can be computed as follows:

$$\lambda = \frac{Q^{-1}(P_D^{th})(\sigma_x^2 + \sigma_w^2)}{\sqrt{nS}} + \sigma_x^2 + \sigma_w^2 \tag{6.3}$$

The constraint P_D^{th} is employed in order to limit the resulting interference at the licensed users, caused when a missed detection occurs. According to (6.3), P_F, given in (6.2), can be rewritten as:

$$P_F = Q\bigg(Q^{-1}(P_D^{th})(1+\zeta) + \zeta\sqrt{nS}\bigg) \tag{6.4}$$

where $\zeta = \frac{\sigma_x^2}{\sigma_w^2}$.

The transmission is organized in frames of fixed time duration. The frame duration (T) is divided into three sub-frames: i) the sensing sub-frame of duration T_s, during which local sensing is performed; ii) the reporting sub-frame of duration T_r, where local results are reported to the FC; and iii) the data transmission sub-frame of duration T_t, where data transmission occurs if the channel is identified as free according to (14.8). As a consequence, $T = T_s + T_r + T_t$. [1]

It is assumed that T_t is given and fixed, while T_s and T_r are chosen in order to trade-off sensing and reporting reliabilities, respectively, such that T is kept fixed. If we consider τ is the time needed by each CU to report the sensed result to the FC, then the total reporting time for all CUs is $T_r = n\tau$. Since T_t is assumed fixed, the duration of the sensing sub-frame can be expressed as a function of the number of sensing users as follows:

$$T_s(n) = T - T_t - n\tau \tag{6.5}$$

[1] Notice that the energy consumed during the idle state is small compared to the total energy consumption in CSS, thus we neglect it [52].

Hence, the maximum number of collected samples per user as a function of the number of sensing users is:

$$S(n) = \big(T - T_t - n\tau\big) f_s \tag{6.6}$$

where f_s is the sampling frequency.

Likewise, the total number of collected samples of all sensing users (S_T) is given:

$$S_T(n) = nS(n) = \big(T - T_t\big) f_s n - f_s \tau n^2 \tag{6.7}$$

It can be observed that as n increases, T_r increases, and, consequently, T_s and S decrease.

6.2.2 Energy Consumption

The energy consumed for CSS by all CUs is made of three contributions: i) the energy consumed during local sensing (E_s); ii) the energy consumed during results' reporting (E_r); and iii) the energy consumed during data transmission (E_t). While E_s and E_r are always non–zero, E_t is equal to zero if no data is transmitted. The probability of transmitting data is given by the probability of identifying the spectrum as unused during CSS, regardless the actual status of the spectrum. This probability is denoted by P_{unused}, and it was given in (5.2).

Since $P_D = P_D^{th}$, according to (6.3), and $P_0 + P_1 = 1$, then P_{unused} (given in (5.2)) can be rewritten as follows:

$$P_{unused} = 1 - P_1 P_D^{th} - P_0 P_F \tag{6.8}$$

Therefore, the energy consumed as a function of n is given as follows:

$$E(n) = E_s(n) + E_r(n) + P_{unused}E_t \tag{6.9}$$

where the energies E_s, E_r and E_t are expressed as follow:

$$E_s(n) = nT_s(n)\rho_s \tag{6.10}$$

$$E_r(n) = n\tau\rho_r \tag{6.11}$$

$$E_t = T_t\rho_t \tag{6.12}$$

where ρ_s, ρ_r and ρ_t are the powers consumed per each CU for local sensing, results' reporting, and data transmission, respectively.

It is worth mentioning that increasing n does not necessarily increase the total energy consumption. This is due to the contrasting effects on E_s, E_r and P_{unused}.

6.2.3 Achievable Throughput

The achievable throughput of CSS can be defined as the average amount of the successfully-delivered transmitted bits. A successful transmission occurs only in the case of correct identification of the unused spectrum. In other words, the transmitted bits are successfully delivered if the channel is unused and it is correctly identified as free [94]. Hence, the achievable throughput (D), measured in bits, is given in terms of N as :

$$D(n) = P_0(1 - P_F(n))RT_t \tag{6.13}$$

where the factor $P_0(1-P_F(n))$ represents the probability of correct identification of the unused spectrum, and R is the data transmission rate in *bits/s*.

Finally, the energy efficiency is defined as the average throughput over the average consumed energy (as in (1.11)) as follows [83]

$$\mu(n) = \frac{P_0(1 - P_F(n))RT_t}{E_s(n) + E_r(n) + P_{unused}E_t} \tag{6.14}$$

6.3 Optimization of the Number of Sensing Users

The number of CUs that participate in CSS plays a significant role in the overall performance of the cognitive radio network. This role is initiated due to the effect of the number of sensing users on time resources distribution, Eqn.(6.5), detection accuracy performance, Eqn.(6.4), energy consumption, Eqn.(6.9), and transmitted data, Eqn.(6.13). In this section, we optimize the number of sensing users for three different setups, throughput maximization, energy consumption minimization, and energy efficiency maximization.

6.3.1 Throughput Maximization

Increasing the number of sensing users leads to a higher diversity in the received sensing results, which improves the achievable throughput. On the other hand, larger number of sensing users consumes more time for reporting process, which, consequently, decreases the number of collected samples by each CU. This influences the false alarm probability, and hence, lower throughput will be achieved. Therefore, it is necessary to optimize the number of sensing users so that the throughput is maximized.

Using (6.13), the throughput maximization problem can be expressed as follows

$$\max_{n} P_0(1-P_F)RT_t \tag{6.15}$$

since P_0, R and T_t are independent of n, and using (6.4), the problem can be simplified to

$$\max_{n} -P_F = \min_{n} Q\Bigg(Q^{-1}(P_D^{th})(1+\zeta)+\zeta\sqrt{nS}\Bigg) \tag{6.16}$$

The optimal n that maximizes D can be obtained by setting $\frac{\partial P_F}{\partial n}=0$. However, $Q(\cdot)$ is an integral, therefore, we should use Leibniz integral rule [95] to find its derivative as follows:

$$\frac{\partial P_F}{\partial n} = \frac{-1}{\sqrt{2\pi}} \frac{\zeta f_s(T-2n\tau-T_t)}{2\sqrt{nf_s(T-n\tau-T_t)}} e^{-\frac{(Q^{-1}(P_D^{th})(1+\zeta)+\zeta\sqrt{nS})^2}{2}} \tag{6.17}$$

Since $\sqrt{nS}\neq\infty$, i.e., the total number of samples is limited, (6.17) will equal zero only if the following condition is satisfied [2]:

$$T-2n\tau-T_t=0 \tag{6.18}$$

that can be solved to obtain the optimal number of sensing users that maximizes throughput (n^{optTh}) as follows

$$n^{optTh} = \lfloor \frac{T-T_t}{2\tau} \rfloor \tag{6.19}$$

where $\lfloor\cdot\rfloor$ is the flooring operator. Since the number of sensing users is limited by the total available CUs (N), then n^{optTh} can be rewritten as follows

$$n^{optTh} = \min\Bigg\{\lfloor \frac{T-T_t}{2\tau} \rfloor, N\Bigg\} \tag{6.20}$$

[2] It is possible to employ the fact that the Q-function is a monotonic decreasing function of its argument, and hence, maximizing (6.18) is equivalent to (6.16).

According to (6.20), if the number of available users is $N > \frac{T-T_t}{2\tau}$, then the maximum throughput is achieved by dividing the time resources dedicated for CSS equally between local sensing (T_s) and reporting (T_r). Also, notice that for $N > \frac{T-T_t}{2\tau}$, the optimal number of users that achieve the maximum throughput is independent of N.

6.3.2 Energy Consumption Minimization

Another important objective for optimizing the number of sensing users is energy consumption minimization. Different numbers of sensing users lead to different time distribution between sensing and reporting, and hence different energy consumption. Besides, increasing n results in a lower P_F which increases the energy consumed during the data transmission subframe. In this subsection we optimize the number of sensing users for the minimum energy consumption.

The energy minimization problem can be formulated as follows:

$$\min_n E(n) = \min_n E_s(n) + E_r(n) + P_{unused}E_t \tag{6.21}$$

by substituting the values of E_s, E_r and P_{unused} that are given in (6.10), (6.11) and (6.8), we get

$$\min_n n(\rho_s T_s(n) + \rho_r \tau) + (1 - P_0 P_F - P_1 P_D^{th})\rho_t T_t \tag{6.22}$$

It is easy to prove that E_T is a concave function[3] of $n \in [1, N]$. Hence, the local minimum values occur at the bounds of the interval, i.e., $n = 1, N$. Then,

[3] The concavity of E_T can be shown using the second derivative test ($\frac{\partial^2 E_T}{\partial n^2} < 0$)

the optimal number of sensing users that minimizes energy consumption can be expressed as follows

$$n^{optE} = \begin{cases} 1 & \text{if } E_T(1) \leq E_T(N) \\ N & \text{if } E_T(1) > E_T(N) \end{cases} \tag{6.23}$$

where $E(1)$ and $E(N)$ the total energy consumption when the $n = 1, N$, respectively, and can be obtained using (6.9).

Notice that the number of the available CUs is bounded by n_{max} since the time resources are limited, the maximum number of sensing users can be expressed as follows:

$$n_{max} = \lceil \frac{T - T_t}{\tau} - 1 \rceil \tag{6.24}$$

where $\lceil \cdot \rceil$ is the ceiling operator. Using (6.5), we can obtain that $T_s(n_{max}) = \tau$, and using (11.11) we can find the number of samples collected by each CU as $S(n_{max}) = f_s\tau$. Hence, the total number of samples that can be obtained by the maximum number of users is given by

$$S_T(n_{max}) = S(n_{max})n_{max} = f_s(T - T_t - \tau) \tag{6.25}$$

Likewise, in the case of the minimum number of sensing users, i.e., $n = 1$, (6.5) gives $T_s(1) = T - T_t - \tau$, and (11.11) gives $S(1) = f_s(T - T_t - \tau)$. Then, the total number of samples that can be collected is expressed as follows

$$S_T(1) = S(1) = f_s(T - T_t - \tau) \tag{6.26}$$

As a result, $S_T(n_{max}) = S_T(1)$ which implies that $P_{unused}(n_{max}) = P_{unused}(1)$. According to this, we conclude that the energy consumed during data transmission is equal whether $n = n_{max}$ or $n = 1$. Therefore, since the energy consumed in CSS is less when only one user is participated, we can obtain that

$E(1) < E(n_{max})$. By applying this to (6.23), it can be reformulated to be as follows

$$n^{optE} = 1 \tag{6.27}$$

Similar to throughput maximization setup, the optimal number that minimizes energy consumption is independent of the number of available users and the time distribution between sensing and reporting.

6.3.3 Energy Efficiency Maximization

As we have optimized the number of sensing users into two different setups, throughput maximization and energy minimization, it is clear that optimizing each one of them may lead to high degradation on the other metric. e.g., maximizing the achievable throughput results in a high energy expenditure and vice versa. Therefore, since energy efficiency is defined as the ratio of throughput to energy consumption, maximizing it attains the balance point between the two contrasting performance indexes.

Energy efficiency, as defined in (6.14), could be maximized by the optimal number of sensing users using the following problem

$$\max_{n} \mu = \max_{n} \frac{P_0(1 - P_F)RT_t}{E_s(n) + E_r(n) + (1 - P_0P_F - P_1P_D^{th})E_t} \tag{6.28}$$

It is clear that obtaining the optimal n from (6.28) in a closed form expression is too hard. However, since n is bounded by the available time resources, i.e., $n_{max} = \frac{T-T_t}{\tau} - 1$, we propose a simple iterative bisection algorithm [96] to find the optimal number of users that maximizes energy efficiency, as described in Algorithm 1.

Algorithm 1 Proposed bisection algorithm to find $N^{opt\mu}$

```
Initialization: Set $N_{min} = 1$ and $N_{max} = \frac{T-T_t}{\tau} - 1$.
Define $i = 1$
**While** $i \neq 0$
    $N = \frac{N_{min}+N_{max}}{2}$
**Compute** $\mu(N-1)$, $\mu(N)$ **and** $\mu(N+1)$
    **If** $\mu(N+1) > \mu(N) > \mu(N-1)$
        $N_{min} = N$
    **If** $\mu(N+1) < \mu(N) < \mu(N-1)$
        $N_{max} = N$
    **If** $\mu(N+1) \leq \mu(N)$ & $\mu(N) \geq \mu(N-1)$
        $N^{opt\mu} = N$, $i = 0$
    **EndIf**
**EndWhile**
```

6.3.4 Sub-Optimal Energy-Efficient Approach

Since the optimal number of sensing users that maximizes energy efficiency can not be extracted in a closed mathematical form, we present in this subsection an energy-efficient approach that provides a suboptimal solution.

The idea is based on the fact that the achievable throughput is a symmetric function around the optimal value that maximizes throughput. Therefore, for large number of available users, the throughput achieved by the total available number of users can be attained by a less number of sensing users. Therefore, a huge amount of the consumed energy can be saved, and consequently, we can improve the overall energy efficiency.

Let us denote the number of sensing users that can achieve the same throughput as the total number of users by n'. In order to quantify n', we equalize the achievable throughput using all the available users ($Th(N)$) and the achievable throughput using ($Th(n')$, as follows

$$Th(N) = Th(n') \tag{6.29}$$

using (6.13), this can be rewritten as follows

$$P_0(1 - P_F(N))RT_t = P_0(1 - P_F(n'))RT_t \tag{6.30}$$

since P_0, R, and T_t are independent of the number of sensing users, (6.30) can be simplified as

$$P_F(N) = P_F(n') \tag{6.31}$$

According to (6.4), (6.31) can be rewritten as follows:

$$Q\Bigg(Q^{-1}(P_D^{th})(1+\zeta) + \zeta\sqrt{NS}\Bigg) = Q\Bigg(Q^{-1}(P_D^{th})(1+\zeta) + \zeta\sqrt{n'S}\Bigg)) \tag{6.32}$$

in order to achieve the equality between the two sides, we must equalize

$$NS(N) = n'S(n') \tag{6.33}$$

where $S(N)$ and $S(n')$ are the number of collected samples per user when the number of sensing users is N and n', respectively. By substituting the number of collected samples, given in (11.11), we get

$$N\Bigg(T - T_t - N\tau\Bigg)f_s = n'\Bigg(T - T_t - n'\tau\Bigg)f_s \tag{6.34}$$

which is simplified as a quadratic equation of n' as:

$$\tau n'^2 - (T - T_t)n' + \Bigg(T - T_t - N\tau\Bigg)N = 0 \tag{6.35}$$

where the two solutions (n'_1, n'_2) of this equation are computed as follows

$$n'_1 = N \tag{6.36}$$

$$n_2' = \frac{T - T_t - N\tau}{N\tau}N = \frac{T_s(N)}{T_r(N)}N \tag{6.37}$$

Thus, the number of sensing users that minimizes energy consumption while achieving the same throughput when all available users participate in CSS, is given as follows:

$$n' = min\{N, \frac{T_s(N)}{T_r(N)}N\} \tag{6.38}$$

Following this energy-efficient approach, a large reduction on the consumed energy can be achieved without degrading the achievable throughput, therefore, the overall energy efficiency of the network will be improved. Also, notice that the improvement in the energy efficiency mainly depends on the number of available users.

6.4 Analytical and Simulation Results

A cognitive radio network of N CUs is assumed. The probability that the target spectrum is used by a licensed user is 0.5. The ratio of the signal power of the licensed user to the noise power is assumed $\zeta = -20\,dB$. The total frame is assumed to be $T = 100\,ms$. During local sensing, each CU collects samples with sampling frequency $f_s = 1\,MHz$ and consumes power $\rho_s = 0.1\,W$. During results' reporting, each CU spends $\tau = 0.2\,ms$ and consumes power $\rho_r = 1\,W$. In data transmission, the data rate is assumed $R = 200\,Kbps$ and the transmit power is assumed $\rho_t = 1\,W$. The number of available users is set to the maximum, i.e., $N = n_{max}$ given in (6.24), unless otherwise is stated. These simulation parameters are summarized in Table 6.1. In all next figures, the markers represent the simulation results, while the analytical results obtained by the derived equations are represented by solid lines.

Fig. 6.1 shows the average total energy consumption versus the number of sensing users at a fixed predefined threshold in detection probability $P_D^{th} = 0.8$. Four different curves in Fig. 6.1 are corresponding to four different values of $T_s + T_r$ which represents the time dedicated for CSS. For all curves, the total energy consumption is a concave function of n, and the minimum energy consumption always occurs at $N = 1$. Increasing the number of CUs will increase the energy consumption, but at the same time, the energy consumed in local sensing and data transmission will be less due to the limited time constraint, which results in a concave curve of the energy consumption.

Fig. 6.2 plots the minimum energy consumption versus $T_s + T_r$ for different values of P_D^{th}. Increasing $T_s + T_r$ increases the minimum energy consumption because of the increased energy during CSS process. However, after a specific value of $T_s + T_r$, the minimum energy consumption decreases since the energy consumed during the data transmission subframe decreases. Another observation that can be derived from Fig. 6.2 is the decrease in the minimum energy consumption as P_D^{th} increases, which is due to increasing P_F as P_D^{th} increases, leading to lower energy consumed during the data transmission subframe.

Table 6.1: Simulation Parameters

Parameter	Value	Parameter	value
P_0	0.5	ζ	$-20\,dB$
f_s	$1\,MHz$	ρ_t	$1\,W$
ρ_s	$0.1\,W$	ρ_r	$1\,W$
τ	$0.2\,ms$	R	$200\,Kbps$
T	$100\,ms$		

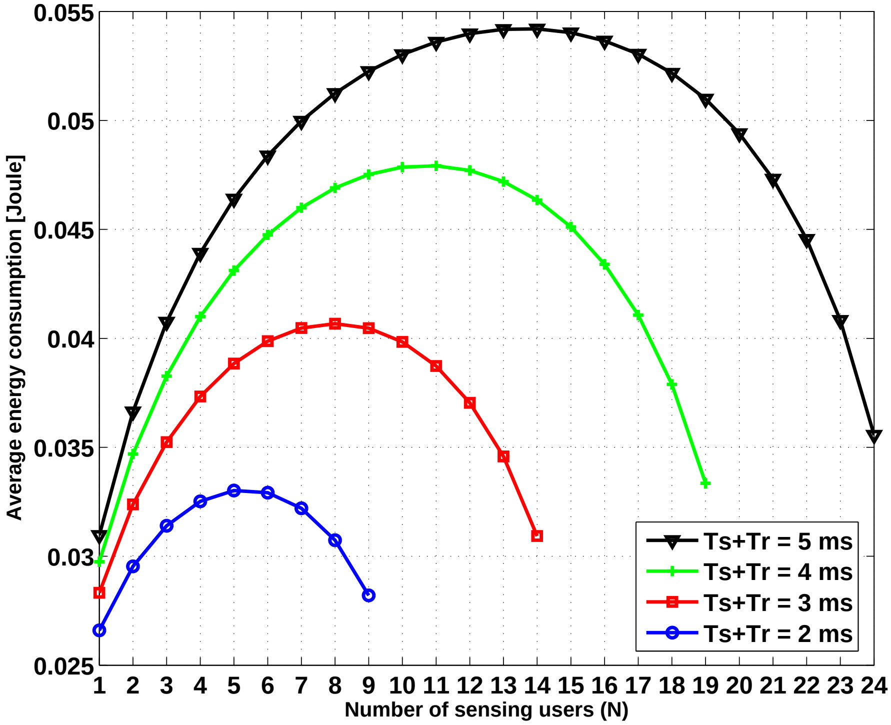


Figure 6.1: *The total consumed energy (E_T) versus the the number of sensing users (n) for different time distributions.(T=100 ms, Pd=0.8)*

The average achievable throughput versus the number of sensing users is plotted in Fig. 6.3 for multiple values of $T_s + T_r$. The concave shape of the curves can be interpreted as a result of two contrasting effects on the sensing performance caused by increasing n. In first part of each curve, the total number of collected samples increases as N increases, while in the second, the total number of samples decreases since the number of samples per CU decreases. The total number of samples affects P_F, as indicated in (6.4), which directly affects the average achievable throughput, as indicated in(6.13). Notice that the theoretical results, represented by the solid lines, exactly match the simulation results represented by markers.

The maximum achievable throughput is shown in Fig. 6.4 versus $T_s + T_r$ for $P_D^{th} = 0.9$, 0.8 and 0.7. Clearly, for a fixed total frame duration T, the increase

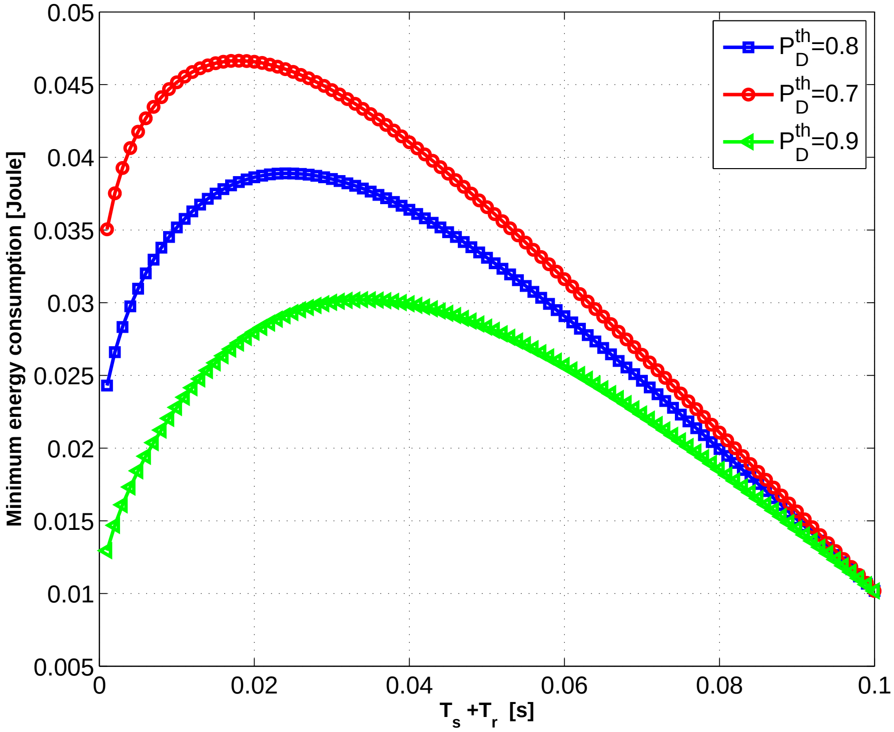


Figure 6.2: *The minimum energy consumption versus the time dedicated for CSS* ($T_s + T_r$) *for different values of* P_D^{th}. *(T=100 ms,* $N = n_{max}$*)*

in the time dedicated for CSS ($T_s + T_r$) increases the detection accuracy. On the other hand, increasing $T_S + T_r$ yields in lower transmission time T_t in view of the limited frame duration. Therefore, the maximum achievable curve follows a concave shape as appears in Fig. 6.4 regardless of P_D^{th}. Notice that for low values of $T_s + T_r$, the maximum achievable throughput is lower for higher P_D^{th} due to the higher P_F, while, for the high range of $T_s + T_r$, P_F can be reached to zero for all the considered values of P_D^{th}, implying equal maximum achievable throughput.

In Fig. 6.5 the energy efficiency versus the number of sensing users is plotted for multiple values of $T_s + T_r$. Notice that the maximum energy efficiency is achieved at a low value of n, usually $< N/2$, and it decreases as $T_s + T_r$ increases. The maximum energy efficiency is plotted versus $T_s + T_r$ for multiple values of

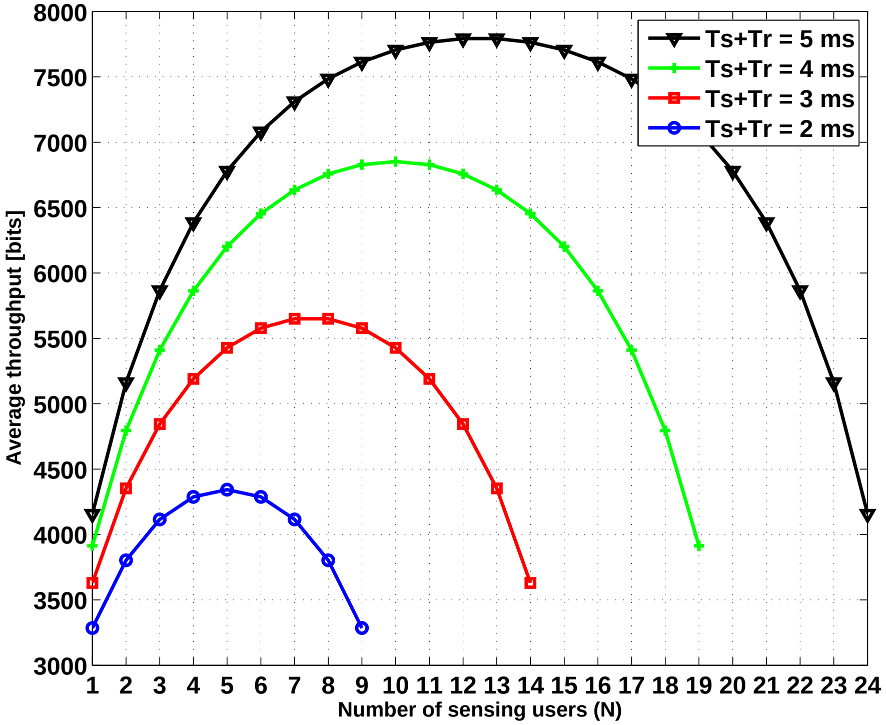


Figure 6.3: *The achievable throughput (Th) versus the the number of sensing users (n) for different time distributions. (T=100 ms, Pd=0.8)*

P_D^{th} in Fig. 6.6. Clearly, as $T_s + T_r$ increases the detection accuracy improves, which enhances the maximum energy efficiency. On the other hand, high values of $T_s + T_r$ decreases the transmission time, and consequently degrades the maximum energy efficiency. The theoretical results for the optimal number of users that maximizes energy efficiency are obtained using Algorithm6.3.3.

In Fig. 6.7, we compare the performance of the proposed sub-optimal energy-efficient approach presented in Section 6.3.4 to the optimal energy-efficient approach presented in Section 6.3.3. In Fig. 6.7 the energy efficiency of both approaches is shown versus the number of the available users (N) for different values of $T_s + T_r$. For each curve, N varies on the range $[1, n_{max}]$. The optimal approach uses the optimal number of sensing users that maximizes energy efficiency, while the sub-optimal approach uses the optimal number of

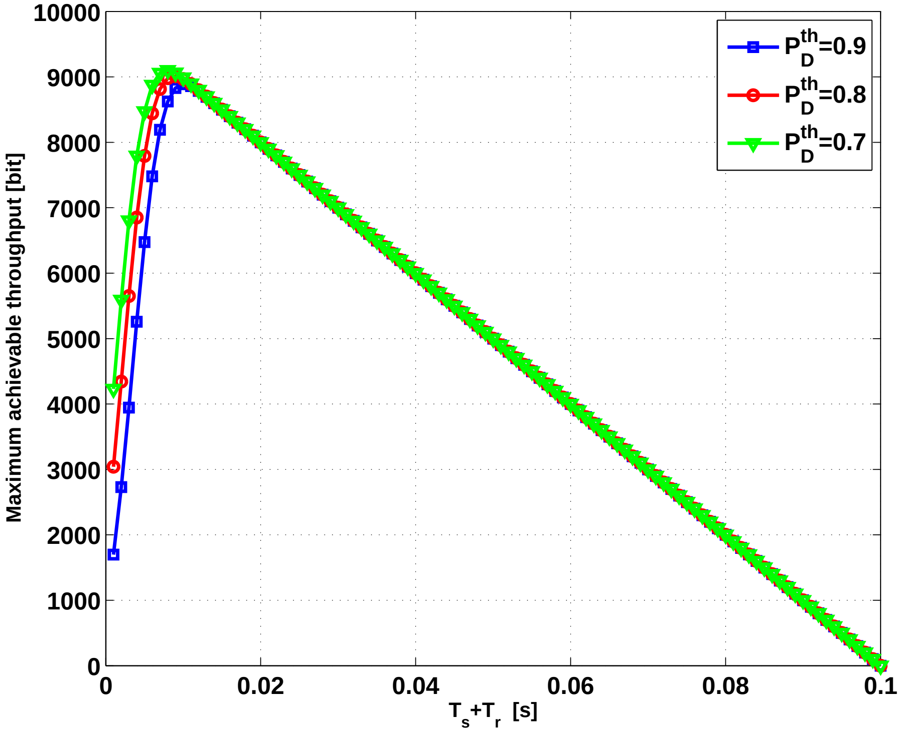


Figure 6.4: *The maximum achievable throughput versus the time dedicated for CSS ($T_s + T_r$) for different values of P_D^{th}. (T=100 ms, $N = n_{max}$)*

sensing users that minimizes energy consumption without affecting the achievable throughput, given in (6.38). The energy efficiency by the optimal approach, the red curves in Fig. 6.7, increases while $N \leq n^{opt\mu}$, then it keeps constant for the rest of the range $n^{opt\mu} \leq N \leq n_{max}$. In contrast, the energy efficiency in the sub-optimal approach is equal to the energy efficiency achieved by N while $N \leq n^{optTh}$. After that, for the range $N > n^{optTh}$, the energy efficiency will show a symmetric curve a round n^{optTh}. For example, on the curve $T_s + T_r = 5\,ms$, the energy efficiency of the sub-optimal approach for $N \leq 13$ equals to the energy efficiency achieved by N, see Fig. 6.5. Notice that for $T_s+T_r = 5\,ms$, $n^{optTh} = 12.5$ is obtained by (6.20) so that the achieved energy efficiency should be symmetric around $N = 12.5$, as exactly appears in Fig. 6.7. The maximum deviation of the sub-optimal approach from the optimal approach occurs when $N = n_{max}$ and it is within $2\% - 9\%$ for the considered values.

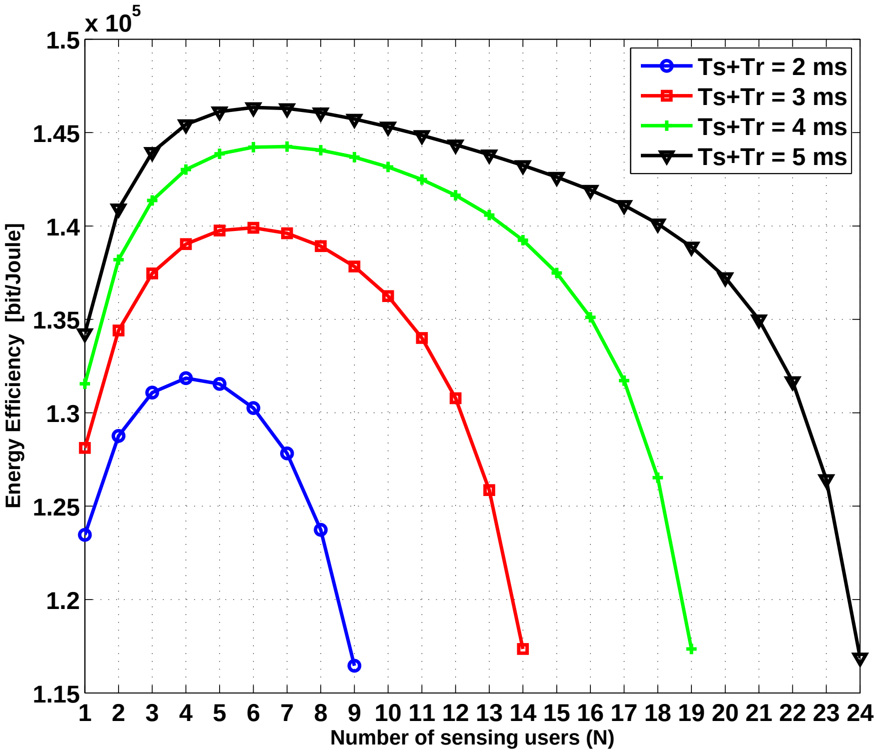


Figure 6.5: *The energy efficiency (μ) versus the the number of sensing users (n) for different time distributions. (T=100 ms, Pd=0.8)*

Also, for the purpose of comparison, in Fig. 6.8 we compare the achievable energy efficiency by our proposal and by the approach proposed in [52]. Briefly, in [52], they propose an energy efficient algorithm based on minimizing the number of sensing users while achieving two constraints on detection probability and false alarm probability. As mentioned in the introduction, in [52] the reporting time affects the transmission time while the sensing time is fixed. In Fig. 6.8, the total frame length is considered $100\,ms$ for both proposals. We consider $T_s = 1ms$ for the proposed approach in [52], and $T_s + T_r = 5ms$ in our approach. The constraint on the detection probability is set to a fixed value regardless of the number of users, as shown in the figure, while the constraint on the false alarm probability that should be satisfied by the other approach is tuned to be equal to the false alarm probability achieved by our approach.

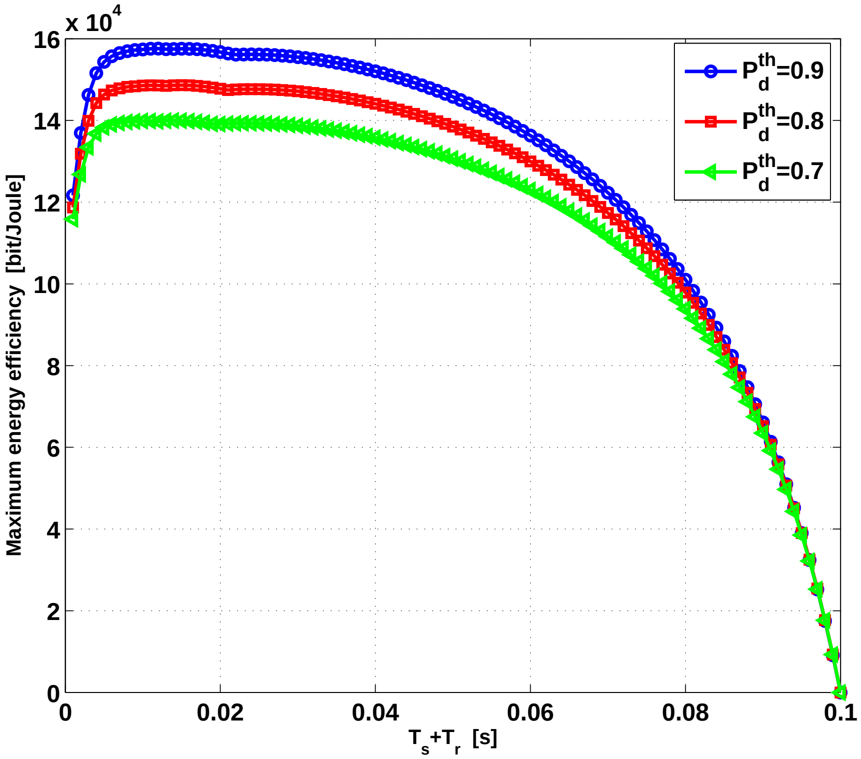


Figure 6.6: *The maximum energy efficiency versus the time dedicated for CSS ($T_s + T_r$) for different values of P_D^{th}. (T=100 ms, $N = n_{max}$)*

The circles on the two curves of the other approach indicate that the approach cannot satisfy the false alarm probability achieved by our proposal, so that the energy efficiency that is corresponding to the minimum false alarm probability is considered. Apparently, our proposal outperforms the approach presented in [52], this refers to the fact that in their proposal the number of sensing users is minimized without considering the achievable throughout, whereas in our approach we minimize the number of sensing users while keeping the achievable throughput above a threshold.

The effect of the constraint on detection probability (P_D^{th}) on the three approaches, the optimal energy efficient, Section 6.3.3, the proposed suboptimal energy efficient in Section 6.3.4, and the energy efficient approach proposed in [52], is shown in Fig. 6.9 for $N = 24$. As P_D^{th} increases, P_F increases, Th de-

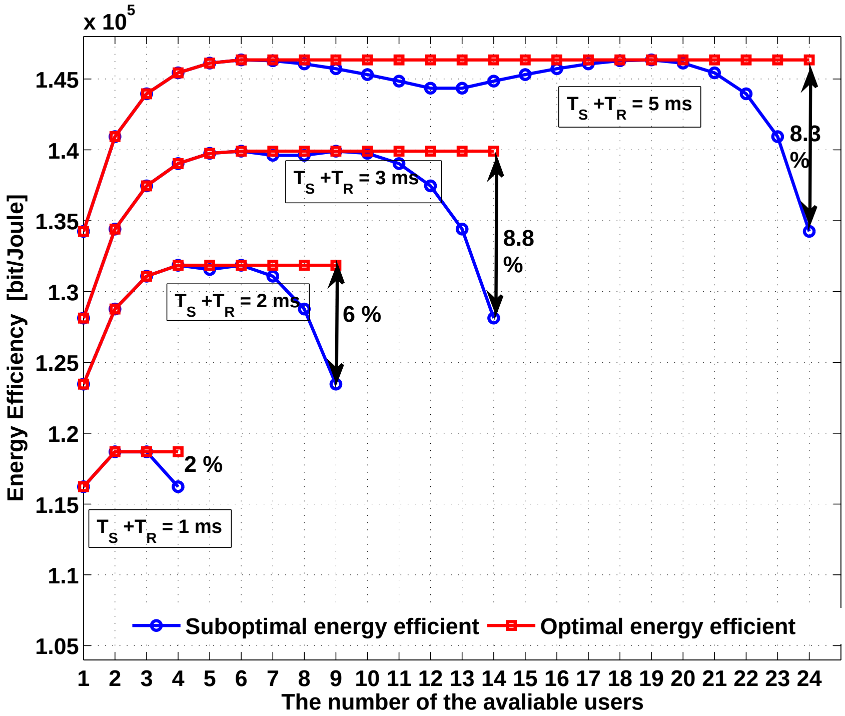


Figure 6.7: *The efficiency metric (μ) by the optimal number of of sensing users and by the proposed energy efficient approach versus the number of available users (n) for different time distributions.(T=100 ms, Pd=0.8)*

creases, E decreases, and μ improves. This is because the effect on reducing E is higher than the effect on reducing Th. Our approach can achieve higher energy efficiency, up to 3.5%, than that of the approach proposed in [52].

6.5 Summary

Optimization the number of sensing users in CSS has been investigated in this chapter for throughput maximization, energy consumption minimization and energy efficiency maximization. The optimization problems have been formulated under limited time assumption. This assumption implies that the total frame length is limited, where data transmission occupies a fixed part of it, and

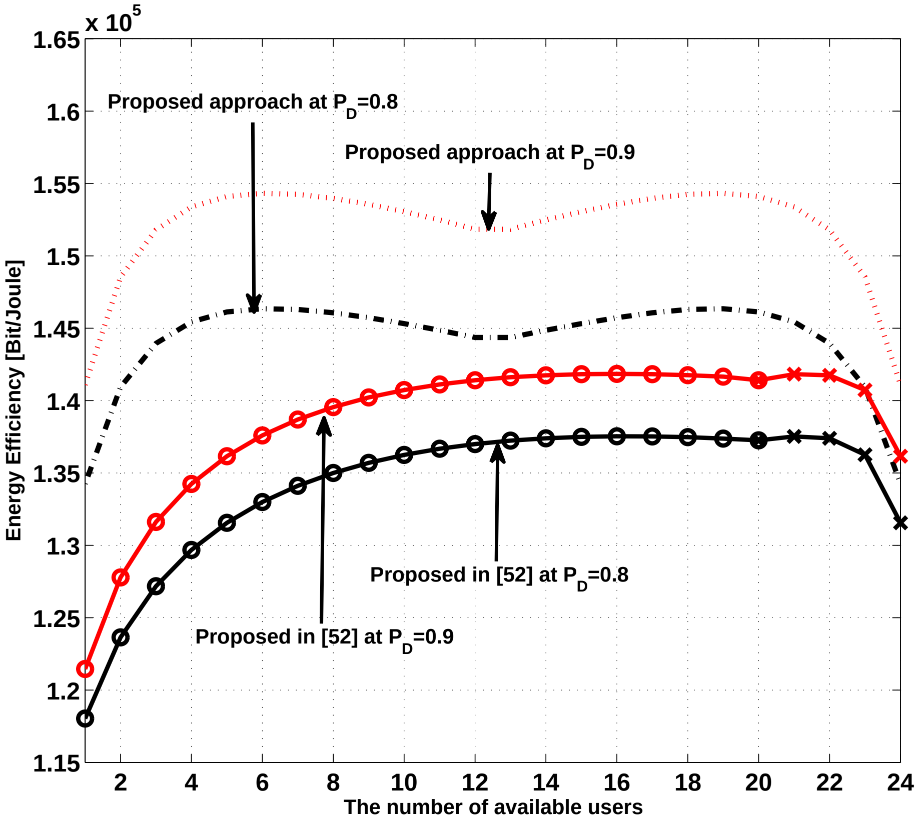


Figure 6.8: *The efficiency metric by the proposed energy efficient approach ($T_s + T_r = 5ms$) and the approach proposed in [52] ($T_s = 1ms$) versus the number of available users. (T=100 ms)*

the the rest of the frame is distributed between local sensing and results' reporting. Our results can be summarized into the following main conclusions:

- The optimal number of sensing users that maximizes the achievable throughput while satisfying a predefined threshold in detection probability should consume time for results' reporting equal to the time spent during local sensing.
- The optimal number of sensing users that minimizes energy consumption while satisfying a predefined threshold in detection probability is 1.

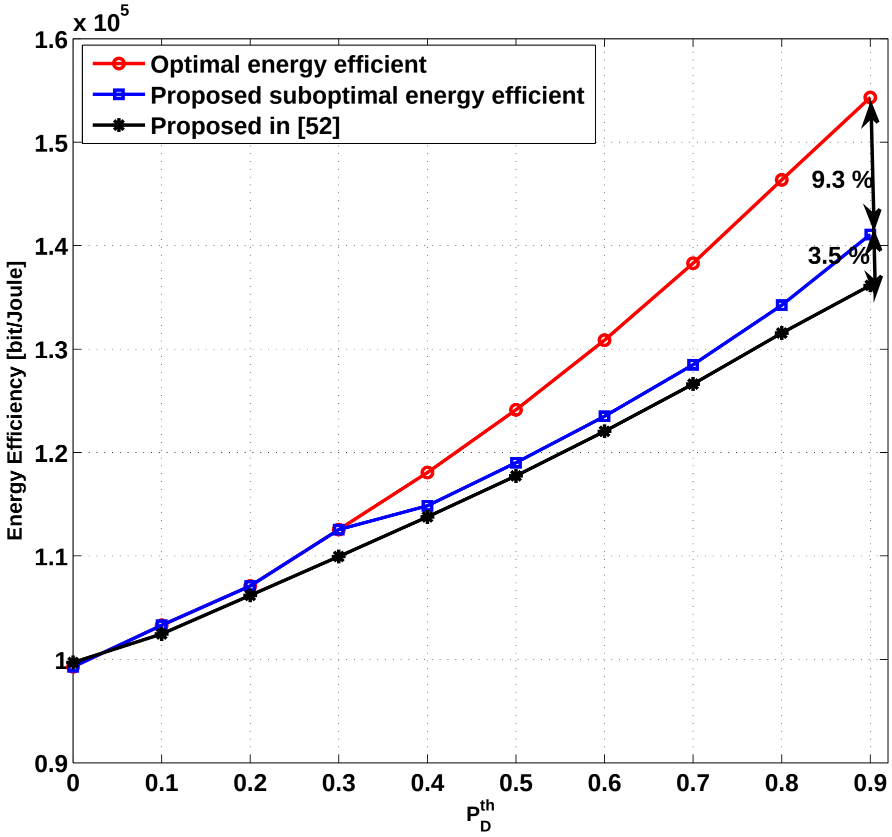


Figure 6.9: *The efficiency metric (μ) using the optimal number of sensing users, the energy efficient approach proposed in Section 6.3.4, and the energy efficient approach proposed in [52] versus the predefined threshold in detection probability (P_D^{th}) for different time distributions.(T=100 ms, N=24)*

- A simple bisection algorithm is proposed to find the optimal number of sensing users that maximizes energy efficiency while satisfying a predefined threshold in detection probability.

- A sub-optimal energy-efficient approach is presented that is able to achieve energy efficiency near to the optimal solution, while satisfying a predefined threshold in detection probability and attaining the same throughput when all the available users are participated in CSS.

Part III

Improving Energy Efficiency in Results' Reporting Stage

CHAPTER 7

ENERGY EFFICIENCY ANALYSIS OF SOFT AND HARD COOPERATIVE SPECTRUM SENSING SCHEMES

7.1 Introduction

Improving energy efficiency can be attained by several directions. The most energy consuming stage in CSS is the results' reporting stage. In literature there are two popular reporting schemes to convey the individual sensing results to the FC, namely, soft scheme and hard scheme. In soft scheme, each CU reports its sensing result as it is to the FC, usually by quantizing it with large number of bits, while in hard scheme, each CU makes a local decision according to its sensing result, and then, conveys the local decision by a single bit to the FC.

Several previous works have compared between both schemes with regard to the achievable detection accuracy. In [44], the authors conclude that the soft scheme provides higher detection accuracy, which also has been proved even in presence of noisy reporting channels in [70]. On the other hand, [69] shows that the gain of soft over the hard scheme is set lower than a fraction of a dB. Moreover, in [72], it has been demonstrated that the detection accuracy of both schemes will nearly converge under low SNR values when the ratio between the number of sensing users in hard and soft schemes equals 1.6. Indeed, as soft scheme provides more accurate sensing data to the FC, it is self-evident to have more reliable decisions at the FC. However, considering the larger time/bandwidth resources required in the soft scheme may change these results, especially, if we assume that increasing the reported data will affect the local sensing performance. In such a consideration, the frame length is assumed limited and any variation in the reporting time will vary the local sensing time, while the data transmission is kept fixed.

This chapter provides a fair comparison between the two schemes in terms of throughput, energy consumption and, most importantly, energy efficiency. The energy efficiency is defined as the ratio between the achievable throughput and the consumed energy [83]. As the throughput and energy consumption are influenced by the detection accuracy, the energy efficiency can be introduced as a comprehensive metric that combines all the affecting aspects on the overall performance of the cognitive transmission. The soft scheme provides higher detection accuracy, while hard scheme attains higher resources efficiency. Thus, this trade-off should be investigated. The contributions of the chapter include comparisons between both schemes in terms of throughput, energy consumption and energy efficiency metrics. For each metric, a closed form expression of the frame length that makes both schemes are identical is derived.

7.2 System Model

Consider a CRN consisting of N CUs. The sensing technique used in local sensing is energy detection. The sensing results are sent to the FC on a dedicated channel in a TDMA-based method, where each CU has its own reporting time slot [52]. At the FC, received reports form CUs are processed, and a global decision about spectrum occupancy is made by applying a specific fusion rule (FR). According the issued global decision, a CU will be scheduled for data transmission for the rest of the frame if the spectrum was identified as unused. Otherwise, all CUs stay idle during the rest of the frame.

According to Fig. 7.1, the time frame for the cognitive transmission T is divided into three sub-frames: the sensing sub frame T_s for spectrum sensing, reporting sub-frame for result reporting T_r, and transmission sub-frame T_t for data transmission. We assume that the frame duration is limited, and T_s consumes a fixed part of it. The rest of the frame, i.e., $T - T_s$, is divided between reporting and transmission sub-frames. Indeed, the reporting sub-frame is firstly computed and the rest of the frame will be dedicated for data transmission. Mathematically, T_r, which depends on number of CUs and the duration of the time slot (τ), is computed as follows

$$T_r = N\tau \tag{7.1}$$

which is used to obtain T_t as follows

$$T_t = T - T_s - N\tau \tag{7.2}$$

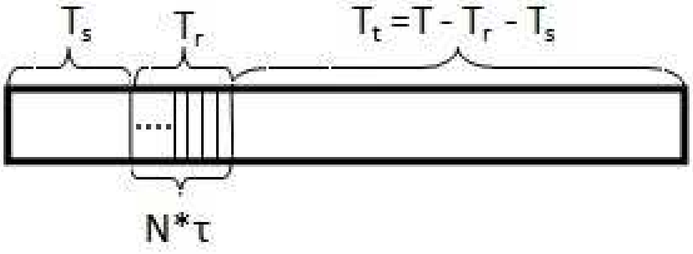


Figure 7.1: *The frame structure of the cognitive transmission.*

Three different metrics are used to evaluate the overall performance of the considered CRN, namely, the achievable throughput, the total energy consumption, and the energy efficiency. The formulas of theses quantities are respectively revised as follows

$$D = P_0(1 - P_F)RT_t \tag{7.3}$$

$$E = NT_s\rho_s + N\tau\rho_t + (1 - P_0P_F - P_1P_D)\rho_tT_t \tag{7.4}$$

$$\mu = \frac{D}{E} \tag{7.5}$$

As mentioned earlier, the local sensing results can be conveyed into two different popular schemes: hard or soft. Next, we discuss both schemes and investigate the related evaluation metrics for each scheme.

7.2.1 Hard-based CSS Scheme

According to the hard scheme, each CU compares its sensing result to a predefined threshold, denoted by λ_H, and makes a local binary decision about spectrum availability ($u_i \in \{1 \equiv used, 0 \equiv unused\}$). In reporting phase, all CUs convey their local decisions, a single bit per CU, towards the FC consecutively. If we consider that the duration of the time slot required for hard scheme is denoted by τ^H, then the total reporting time (T_r^H) and the transmission time (T_t^H) for hard scheme can be easily obtained by a proper substitution in (7.1) and (7.2), respectively.

Upon receiving the local decisions at the FC, a specific fusion rule should be applied to output the global decision. In this chapter, we consider the most popular FR that is called OR rule [72] since it causes the minimum interference to the licensed users. OR-Rule implies that the global decision will not be *used*, unless all CUs agree on that. Thus, the overall detection probability (P_D^H) and the overall false alarm probability (P_F^H) based on the OR-Rule were given in (4.9) and (4.10), and are revised here respectively as follows:

$$P_D^H = 1 - \big(1 - P_d\big)^N \tag{7.6}$$

$$P_F^H = 1 - \big(1 - P_f\big)^N \tag{7.7}$$

where P_d and P_f refer to the local detection probability and the local false alarm probability, respectively. Both are given for AWGN sensing channels in (1.4) and (1.5), and are rewritten as follows [31].

$$P_d = Q(\sqrt{2T_s f_s \gamma}, \sqrt{\lambda_H}) \tag{7.8}$$

$$P_f = \frac{\Gamma(T_s f_s, \lambda_H/2)}{\Gamma(T_s f_s)} \equiv \Phi_{T_s f_s}(\lambda_H/2) \tag{7.9}$$

where f_s is the sampling frequency, γ is the signal to noise ratio, $Q(a, b)$ is the generalized Marcum Q-function [38], and $\Gamma(.)$ is the gamma function [39].

7.2.2 Soft-based CSS scheme

Unlike the hard scheme, the local sensing result is reported as it is in soft scheme without any processing at the local level. The sensing result is usually quantized by a large number of bits that is enough to ignore the resulting quantization distortion. By denoting the time slot required for reporting the sensing result in soft scheme by τ^S ($> \tau^H$), the corresponding reporting time (T_r^S) and transmission time (T_t^S) can be easily obtained by replacing τ by τ^S in (7.1) and (7.2), respectively.

At the FC, in order to make the global decision, the received local sensing results are summed and compared to predefined threshold, denoted by λ_S. Thus, the detection probability (P_D^S) and the false alarm probability (P_F^S) for soft scheme are given for AWGN sensing channels in (6.1) and (6.2), and are rewritten as follows [31].

$$P_D^S = Q(\sqrt{2NT_s f_s \gamma}, \sqrt{\lambda_S})) \tag{7.10}$$

$$P_F^S = \frac{\Gamma(NT_s f_s, \lambda_S/2)}{\Gamma(NT_s f_s)} \equiv \Phi_{NT_s f_s}(\lambda_S/2) \tag{7.11}$$

7.3 Performance Analysis

As we have discussed both schemes and report their related evaluation metrics, this section provides a fair comparison between them in terms of several performance aspects. The comparison is established based on the assumption that both schemes attain the same false-alarm probability (P_F^{th}). To do so, both thresholds λ_H and λ_S should be tuned to obtain $P_F^H = P_F^S = P_F^{th}$, as follows

$$\lambda_H = 2\,\Phi_{T_s f_s}^{-1}\left(1 - \sqrt[N]{1 - P_F^{th}}\right) \tag{7.12}$$

$$\lambda_S = 2\,\Phi_{NT_s f_s}^{-1}\left(P_F^{th}\right) \tag{7.13}$$

where Φ_x^{-1} is the inverse function of Φ_x.

Since T_s identical in the both schemes, $T_r^S > T_r^H$ implies that more accurate sensing data will be available at the FC in the soft scheme, leading to higher detection probability:

$$P_D^S > P_D^H \tag{7.14}$$

However, due to the limited frame duration, $T_r^S > T_r^H$ will also implies that $T_t^S < T_t^H$, which consequently, affects the throughput D, energy consumption E and energy efficiency μ as well. Particularly, soft and hard schemes pose a trade-off between detection accuracy and resource efficiency. Next, we study this trade-off in all performance aspects, stating the sufficient condition on the number of participating CUs and time frame.

We start by comparing the achievable throughput. Specifically, we look for the case(s) when the achievable throughput of the hard scheme (D^H) is higher than it for the soft scheme (D^S), as follows

$$D^H \geq D^S \tag{7.15}$$

Notice the throughput can be obtained by replacing P_F and T_t in (5.5) by P_F^{th} and T_t^S for D^S, or by P_F^{th} and T_t^H for D^H, respectively.

$$P_0(1 - P_F^{th})RT_t^H \geq P_0(1 - P_F^{th})RT_t^S \tag{7.16}$$

Now, as $T_t^H > T_t^S$, we can conclude that (7.15) is always satisfied. This indicates that *the hard scheme always achieves more throughput than the soft scheme regardless of any factor*.

Regarding the average energy consumption, we identify the sufficient conditions by which the hard scheme consumes energy higher than the soft scheme by solving the following:

$$E^H \geq E^S \tag{7.17}$$

The energy consumption can be obtained by replacement τ, P_F, P_D and T_t in (7.4) by τ^H, P_F^{th}, P_D^H and T_t^H for hard scheme or by τ^S, P_F^{th}, P_D^S and T_t^S for soft scheme, respectively. Notice that the first term in (7.4) is identical for both schemes so that can be canceled out. The rest of (7.17) can be expressed as follows

$$\begin{aligned} N\tau^H + (1 - P_0P_F^{th} - P_1P_D^H)T_t^H \geq \\ N\tau^S + (1 - P_0P_F^{th} - P_1P_D^S)T_t^s \end{aligned} \tag{7.18}$$

Be denoting the difference in reporting time in both schemes by $\Delta\tau$ defined as follows

$$\Delta\tau = \tau^S - \tau^H \equiv \frac{T_t^H - T_t^S}{N} \tag{7.19}$$

(7.18) can be simplified to be

$$-N\Delta\tau(P_0P_F^{th} + P_1P_D^H) + P_1T_t^S(P_D^S - P_D^H) \geq 0 \tag{7.20}$$

that can be solved for T_t^s as follows

$$T_t^s \geq \frac{N\Delta\tau\big(P_0 P_F^{th} + P_1 P_D^H\big)}{P_1 \Delta P_D} \tag{7.21}$$

which can be solved for T by substituting the values of T_t^S as follows

$$T \geq T_s + N\tau^S + \frac{N\Delta\tau\big(P_0 P_F^{th} + P_1 P_D^H\big)}{P_1 \Delta P_D} \tag{7.22}$$

where $\Delta P_D = P_D^S - P_D^H$. Eqn.(7.22) can be solved for N as follows

$$N \leq \frac{T - T_s}{\tau^S - \frac{\Delta\tau(P_0 P_F^{th} + P_1 P_D^H)}{P_1 \Delta P_D}} \tag{7.23}$$

While (7.22) acts as a lower bound on the time frame duration by which the hard scheme consumes energy more than the soft scheme, (7.23) represents an upper bound on the number of participating CUs.

Another comprehensive metric that can better assess the performance of CSS is the energy efficiency. To compare between the both schemes in terms of energy efficiency, we investigate the satisfaction of the following case:

$$\frac{D^H}{E^H} \geq \frac{D^S}{E^S} \tag{7.24}$$

Using (7.3), (7.4) and some mathematical operations, (7.24) can be rewritten as a quadrature equation of T_t^S as follows

$$T_t^{s2} + AT_t^s + B \leq 0 \tag{7.25}$$

where A and B are constants defined as follows

$$A = -N\Delta\tau \frac{1 - P_1 \Delta P_D}{P_1 \Delta P_D} \tag{7.26}$$

$$B = -N^2 \Delta\tau \frac{P_s T_s + P_t \tau^s}{P_t P1 \Delta P_D} \tag{7.27}$$

Now, by using the general formula to solve quadrature equations, (7.25) can be solved as

$$T_t^s \leq \frac{-A}{2} + \sqrt{\frac{A^2}{4} - B} \tag{7.28}$$

where it can be written in terms of T using (7.2) as follows

$$T \leq \frac{-A}{2} + \sqrt{\frac{A^2}{4} - B} + T_s + N\tau^s \tag{7.29}$$

Notice that (7.29) represents the minimum frame length by which the soft scheme can achieve higher energy efficiency that the hard scheme.

7.4 Simulation Results

A cognitive radio network consisting N CUs is considered. All simulation parameters regarding local sensing performance, energy consumption and network specifications are summarized in Table 7.1. In this section, we compare both schemes in terms for throughput, energy consumption and energy efficiency in order to validate our analytical results previously.

Table 7.1: Simulation Parameters

Parameter	Value	Parameter	value
P_0	0.5	ρ_s	$10\, mW$
ρ_t	$100\, mW$	f_s	$0.1\, MHz$
γ	$-10\, dB$	R	$64K\, bps$
τ^H	$0.1\, msec$	τ^s	$0.8\, msec$
T_s	$1\, msec$	P_F^{th}	0.1

For a fair comparison we set the fusion thresholds, i.e., λ_H and λ_S, such that the false-alarm probability of both schemes equals to a specific threshold set to $P_F^{th} = 0.1$.

Fig. 7.2 shows the achievable throughput for both schemes versus the frame length. Clearly, the hard scheme achieves higher throughput than the soft scheme for the whole range of T, which insures our analytical result. The throughput difference between the two schemes should diminish as T increases.

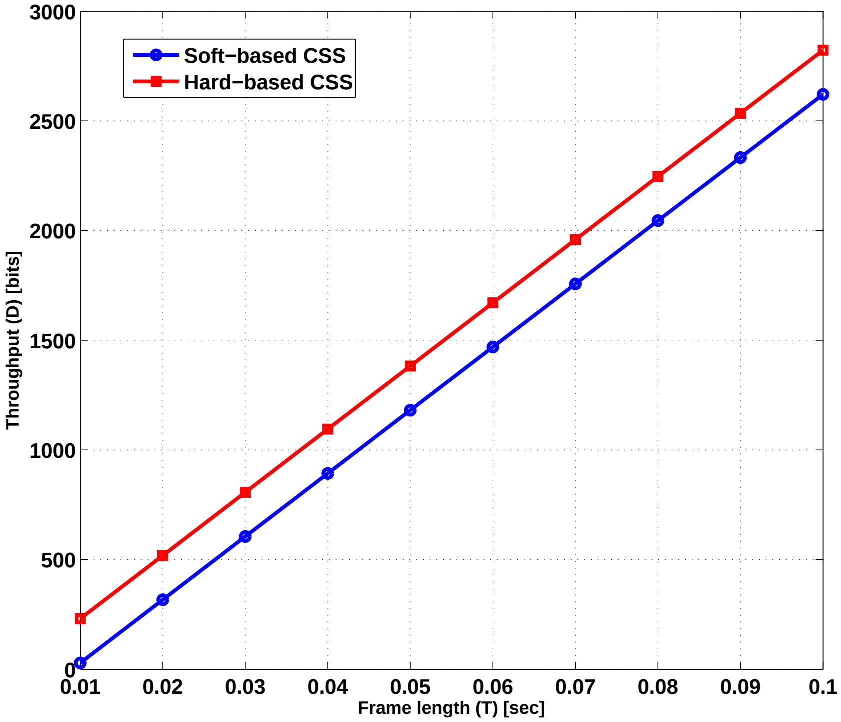


Figure 7.2: *The achievable throughput for both schemes versus the frame length (T). ($N = 10$)*

The total energy consumption versus T is plotted in Fig. 7.3 for both schemes. Notice that increasing T leads to increasing E because of the increase in the transmit energy. However, for low values of T, i.e., $T < 25\,msec$, the hard scheme consumes less energy that the soft, while for $T > 25\,msec$, soft scheme consumes less energy than the hard scheme. Notice that the inversion point is occurred exactly at the point given in (7.22) that is indicated by the black line in Fig. 7.3.

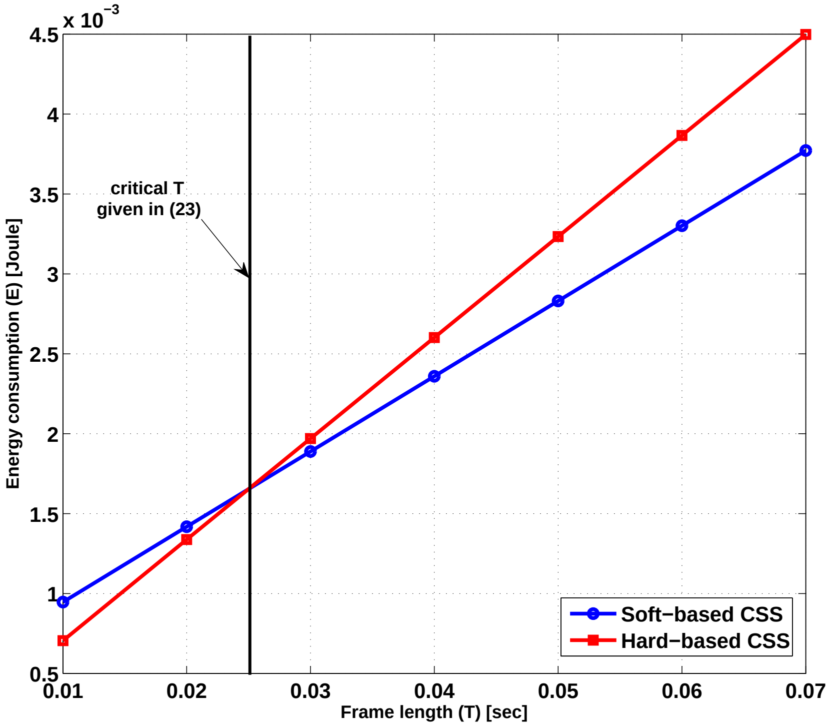


Figure 7.3: *The total energy consumption versus T for both schemes. ($N = 10$)*

Fig. 7.4 shows the energy efficiency versus T for both schemes. Likewise, the energy efficiency is higher for hard scheme at short time frames, while the soft scheme attains higher energy efficiency at longer frames. The critical frame length, at which both schemes achieve equal energy efficiency, is exactly as the one given in (7.29).

The achievable throughput versus the number of CUs is shown in Fig. 7.5 for both schemes. It is shown that the hard scheme always outperforms the soft scheme in amount of the achievable throughput. Also, the difference in throughput magnifies as the number of CUs increases because of the increase in the difference in T_t.

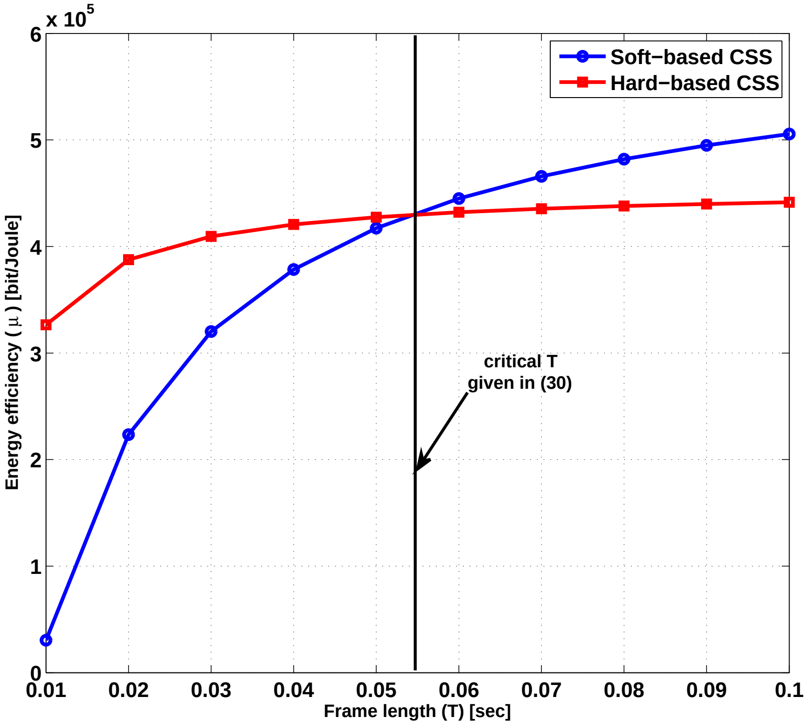


Figure 7.4: *The energy efficiency versus T for both schemes. ($N = 10$)*

Fig. 7.6 and Fig. 7.7 plot the total energy consumption and energy efficiency versus the number of CUs, respectively. For each figure, we plot the critical frame length at which the both schemes have the same performance. Clearly, the reversal in energy consumption (or energy efficiency) is occurred exactly when the condition (7.22) (or (7.29)) is satisfied. Notice that the critical frame length at $N = 1$ in both figures Fig. 7.6-b and Fig. 7.7-b is infinite value, and hence it does not appear in them.

7.5 Summary

Considering the difference in the required time resources between hard and soft CSS schemes, this chapter has investigated their performance in terms of the

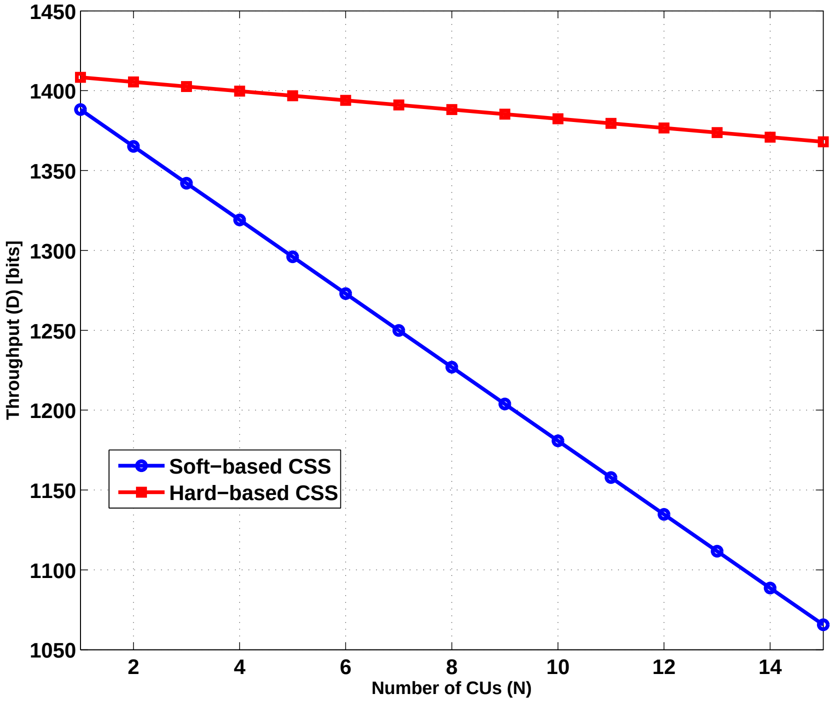


Figure 7.5: *The achievable throughput for both schemes versus the number of CUs* (N). *(*$T = 50\, msec$*)*

achievable throughput, consumed energy and energy efficiency. Our results have shown that hard scheme always provides higher throughput than soft scheme, and hard scheme consumes less energy and attains higher energy efficiency than soft scheme at short time-frames and large number of CUs. Moreover, the contributions of this chapter include deriving closed form expressions for the critical frame length that equalizes the energy consumption and energy efficiency in both schemes, which have been validated by simulation results.

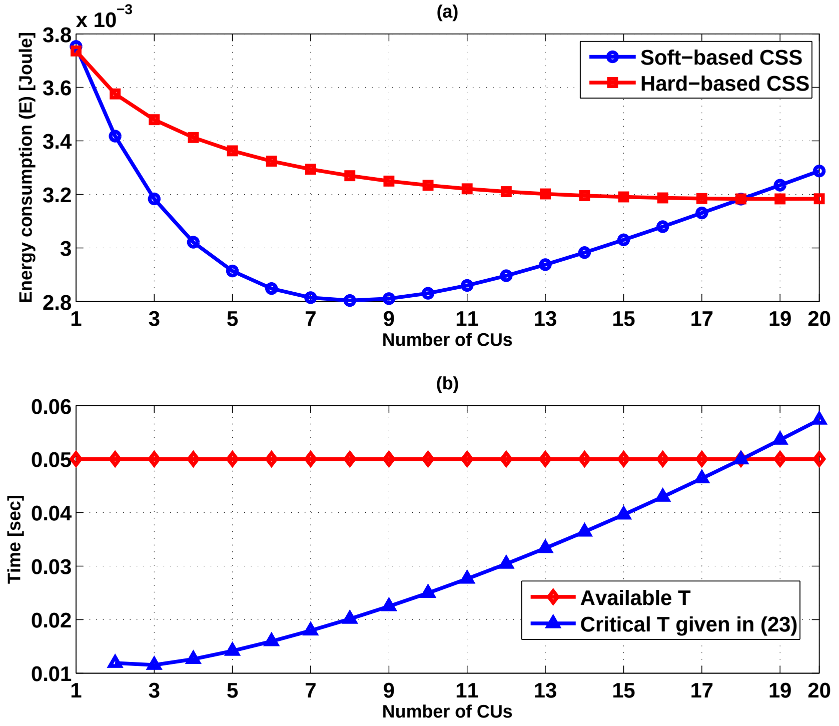


Figure 7.6: *(a) The total energy consumption versus N for both schemes at ($T = 50\,msec$), (b) The critical T given in* (7.22) *versus N*

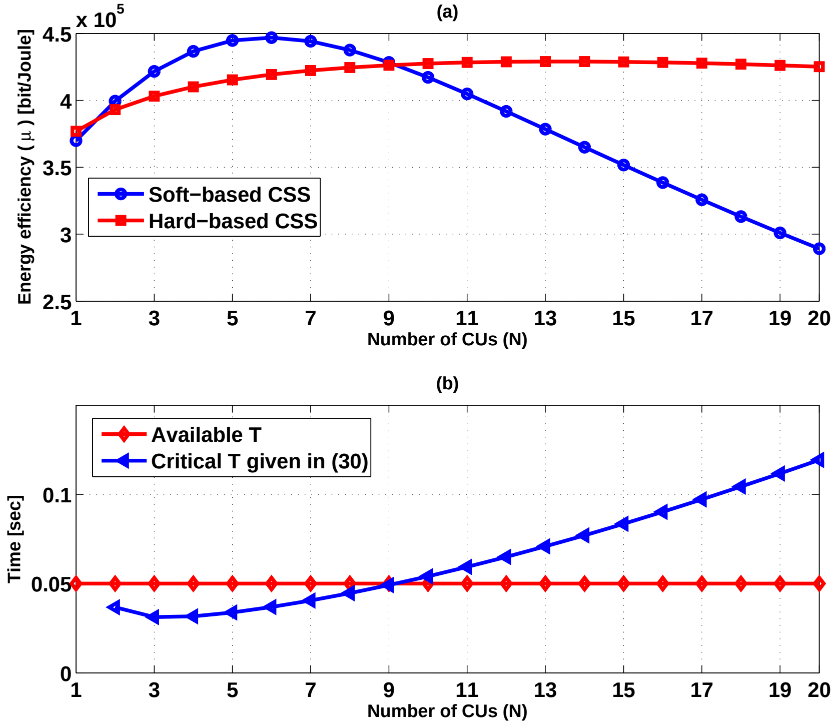


Figure 7.7: *(a) The energy efficiency versus N for both schemes at $T = 50\,msec$, (b) The critical T given in* (7.29) *versus N*

CHAPTER 8

ENERGY-EFFICIENT COOPERATIVE SPECTRUM SENSING BY TERMINATING THE REPORTING PROCESS

8.1 Introduction

In this chapter, a novel reporting scheme is proposed in order to reduce energy consumption in CSS without affecting the detection accuracy. The proposed reporting scheme is based on the assumption that the results are reported to the FC consecutively in a TDMA scheme. Hence, this assumption allows the FC to terminate the reporting process whenever the received results are enough to make a global decision according to the employed FR. In other words, the received results should be immediately processed at the FC, and the global decision should be made whenever the amount of information is enough to make it. Consequently, the reporting phase is terminated by broadcasting a message from the FC informing the CUs to quit reporting. Notice that the employed FR has a key role as it decides how much information is needed to make a global decision.

Considering the definition of the energy efficiency as the ratio of the average successfully transmitted bits to the average energy consumption, the properties of the proposed scheme are as follows; (i) The energy consumption reduction refers to preventing the rest of CUs, which wait their turn, from reporting, (ii) Since the reporting process will be terminated earlier, more time will be allocated to data transmission, which improves achievable throughput, and consequently, energy efficiency, (iii) The proposed scheme does not require/induce any energy consumption in preceding/following stages in the cognitive transmission, (iv) Most importantly, the proposed scheme does not affect the detection accuracy, and (v) The proposed scheme is consistent with most of the other energy-efficient CSS approaches presented in the literature, and can be jointly applied with any of them, which enhances the overall joint achievable energy efficiency.

The mathematical formulation of the proposed reporting scheme is presented in this chapter. Moreover, the proposed scheme is consistent with both types of sensing data: soft and hard, as will be explained later. Also, The significance of the order of the CUs during reporting phase is investigated, and the consistency with other energy efficient approaches is discussed and proved through computer simulations.

8.2 System Model

Consider a CRN consisting of N CUs. The adopted method for spectrum sensing is energy detection method. If we denote the received signal of the s^{th} sample by the i^{th} CU by $r_{i,s}$ (given in (1.1)), then the output of the energy detector can be expressed as follows

$$Y_i = \sum_{s=1}^{S} \mid r_{i,s} \mid^2 \tag{8.1}$$

where $S = T_s f_s$, and f_s is the sampling frequency during sensing.

According to [87] and [31], Y_i follows a central chi-square (χ^2) distribution with $2S$ degrees of freedom under H_0 hypothesis, and non-central chi-square distribution with $2S$ degrees of freedom and a non centrality parameter $2S\gamma_i$ under H_1 hypothesis. Therefore, the probability density function of Y_i is expressed as follows

$$f_{Y_i}(y) = \begin{cases} \frac{1}{2^S\Gamma(S)} y^{S-1} e^{-y/2} & H_0 \\ \frac{1}{2}\left(\frac{y}{2\gamma_i}\right)^{\frac{S-1}{2}} e^{-\frac{2\gamma_i+y}{2}} I_{S-1}(\sqrt{2\gamma_i y}) & H_1 \end{cases} \tag{8.2}$$

where $\Gamma(.)$ is the gamma function [39] and $I_v(.)$ is the v^{th} order modified Bessel function of the first kind [39].

As described in previous chapters, in soft-based CSS, CUs send their actual sensing information, i.e., Y's, to the FC without any local processing, and a global decision is made at the FC by combining them appropriately. The most popular combining scheme is the equal-gain combining (EGC) [97], where all the received results are summed up at the FC, as follows

$$Y_0 = \sum_{i=1}^{N} Y_i \tag{8.3}$$

Hence, the pdf of the statistic Y_0 follows the same distribution of Y_i, described in (8.2), with replacing each $2S$ by the product $2NS$, as follows [87] [31]

$$f_{Y_0}(y) = \begin{cases} \frac{1}{2^{NS}\Gamma(NS)} y^{NS-1} e^{-y/2} & H_0 \\ \frac{1}{2}\left(\frac{y}{2\gamma_0}\right)^{\frac{NS-1}{2}} e^{-\frac{2\gamma_0+y}{2}} I_{NS-1}(\sqrt{2\gamma_0 y}) & H_1 \end{cases} \tag{8.4}$$

where $\gamma_0 = \sum_{i=1}^{N} \gamma_i$. The overall detection and false alarm probabilities in soft-based CSS are given in (6.1) and (6.2), respectively.

In contrast to S-CSS, employing H-CSS implies that each CU processes its sensing result (Y_i) and issues a local binary decision $u_i\{1, 0\}$ about the spectrum status. If $Y_i \geq \lambda_{loc}$, then $u_i = 1$ (the spectrum is identified as used by the i^th CU). Otherwise, $u_i = 0$ (the spectrum is identified as unused by the i^{th} CU).

The detection accuracy of the local decision is also measured by local detection probability and local false alarm probability, which are given as follows [87]

$$P_{d,i}^{local} = Q_S(\sqrt{2\gamma_i}, \sqrt{\lambda_{loc}}) \tag{8.5}$$

$$P_{f,i}^{local} = \frac{\Gamma(S, \lambda_{loc}/2)}{\Gamma(S)} \tag{8.6}$$

According to H-CSS, all the obtained local decisions should be reported to the FC. At the FC, a specific fusion rule (FR) is employed to process these reported decisions in order to make a global decision. The general FR is *K-out-of-N* rule [98].

The overall detection probability and false alarm probability in hard-based CSS can be expressed in mathematical forms for arbitrary values of K as follows:

$$P_D^{hard} = \sum_{k=K}^{N} \sum_{j=1}^{\binom{N}{k}} \prod_{i \in A_j^{(N,k)}} P_{d,i} \prod_{i \notin A_j^{(N,k)}} \left(1 - P_{d,i}\right) \tag{8.7}$$

$$P_F^{hard} = \sum_{k=K}^{N} \sum_{j=1}^{\binom{N}{k}} \prod_{i \in A_j^{(N,k)}} P_{f,i} \prod_{i \notin A_j^{(N,k)}} \left(1 - P_{f,i}\right) \tag{8.8}$$

where $A_1^{(N,k)}, A_2^{(N,k)}, ..., A_{\binom{N}{k}}^{(N,k)}$ represent all the possible combinations of k integers drawn from the interval $[1, N]$, and the number of these combinations is $\binom{N}{k}$.

Depending on K, two popular FRs are derived from the *K-out-of-N* rule: OR rule ($K = 1$) and AND rule ($K = N$). The overall detection probability and false alarm probability for H-CSS based on OR rule are respectively given as follows

$$P_D^{or} = 1 - \prod_{i=1}^{N} \left(1 - P_{d,i}\right) \tag{8.9}$$

$$P_F^{or} = 1 - \prod_{i=1}^{N} \left(1 - P_{f,i}\right) \tag{8.10}$$

while for AND rule as follows

$$P_D^{and} = \prod_{i=1}^{N} P_{d,i} \tag{8.11}$$

$$P_F^{and} = \prod_{i=1}^{N} P_{f,i} \tag{8.12}$$

However, as a special case, when all CUs have identical sensing performance, i.e., $P_{d,i} = P_d \,\&\, P_{f,i} = P_f \;\forall i$, the overall detection and false-alarm probabilities are respectively given for any value of K as follows:

$$P_D^{hard} = \sum_{k=K}^{N} \binom{N}{k} P_d^k (1 - P_d)^{N-k} \tag{8.13}$$

$$P_F^{hard} = \sum_{k=K}^{N} \binom{N}{k} P_f^k (1 - P_f)^{N-k} \tag{8.14}$$

For both schemes, the energy efficiency (μ) is used as an evaluation metric as defined in (6.14).

8.3 The Proposed Energy-Efficient Cooperative Spectrum Sensing (EE-CSS)

The energy consumed during CSS represents a challenge that degrades the overall energy efficiency of cognitive transmission. The energy consumed in results' reporting dominates the energy consumption in CSS. Therefore, reducing the number of CUs that report their results to the FC represents a preferred energy-efficient approach since it leads to a huge reduction in the consumed energy [54]. However, such approach should not negatively affect the achievable performance represented by the detection accuracy of CSS. In this section, we present a novel reporting scheme by which the total amount of energy consumed is reduced, the achievable detection accuracy is kept unaffected, the amount of transmitted data is increased, and hence, higher energy efficiency is achieved.

The idea behind our proposal is that while the CUs report their results, the FC should process these local results immediately, and whenever the FC can make a global decision from the received results, a message is sent from the FC to the rest of CUs, preventing them from reporting their local results. In other words, according to the adopted FR, in some cases, the FC can make the global decision without hearing from all the CUs, and hence, the reporting process should be stopped and the data transmission process can be commenced earlier. Accordingly, the number of reporting CUs decreases, which reduces the consumed energy, and the data transmission can be started earlier, achieving higher amount of transmitted data. Notice that the performance of the CSS represented by the detection accuracy is not affected.

Let us denote the number of the reporting CUs based on our proposal by M. In the rest of this section, we formulate the average number of reporting CUs based on the proposed technique in both S-CSS and H-CSS. Afterward, a discussion on the resultant energy consumption, detection accuracy, transmitted data and energy efficiency is presented.

8.3.1 Energy-Efficient S-CSS

In S-CSS, the global decision is made by comparing the sum of received results to a predefined threshold (λ_s). Thus, at a specific point during the reporting phase, if the sum of the received results up to that point is larger than λ_s, then the decision can be made without waiting the other results of the rest of CUs.

In view of this, the number of reporting CUs will be m if the sum of the results of the first $m-1$ reporting CUs is less than λ_s and the sum of the results of the first m reporting CUs is larger than or equal λ_s. Mathematically, the probability of the number of reporting CUs in S-CSS is expressed as follows:

$$Pr.\{M=m\} = \begin{cases} F^{(m-1)}(\lambda_s)\big(1-F^{(m)}(\lambda_s)\big) & 1 \leq m < N \\ F^{(N-1)}(\lambda_s) & m = N \end{cases} \tag{8.15}$$

where $F^{(x)}(y)$ is the cumulative distribution function (CDF) of the sum of the sensing results for the first x reporting CUs. The pdf of $F^{(x)}(y)$, denoted by $f^{(x)}(y)$, is given as follows

$$f^{(x)}(y) = \begin{cases} \frac{1}{2^{xS}\Gamma(xS)} y^{xS-1} e^{-y/2} & H_0 \\ \frac{1}{2}\left(\frac{y}{2\gamma_x}\right)^{\frac{xS-1}{2}} e^{-\frac{2\gamma_x+y}{2}} I_{xS-1}(\sqrt{2\gamma_x y}) & H_1 \end{cases} \tag{8.16}$$

where $\gamma_x = \sum_{i=1}^{x} \gamma_i$ and $F^{(0)}(\cdot) = 1$.

The average number of reporting CUs ($\overline{M}^{soft}$) can be computed as follows

$$\overline{M}^{soft} = \sum_{m=1}^{N} m Pr.\{M=m\} \tag{8.17}$$

by using (8.15), (8.17) can be rewritten as follows

$$\overline{M}^{soft} = NF^{(1:N-1)}(\lambda_s) + \sum_{m=1}^{N-1} mF^{(1:m-1)}(\lambda_s)\big(1-F^{(1:m)}(\lambda_s)\big) \tag{8.18}$$

Fig. 8.1 shows the average number of reporting CUs of the proposed EES-CSS versus the global decision threshold for different numbers of the available CUs. The parameters used to generate this figure are listed in Table 8.1. All CUs are assumed to be identical $\overline{\gamma} = 10$. Clearly, the average number of reporting CUs according to the proposed scheme is lower than it in the conventional S-CSS, and it increases as the global decision threshold (λ_s) increases.

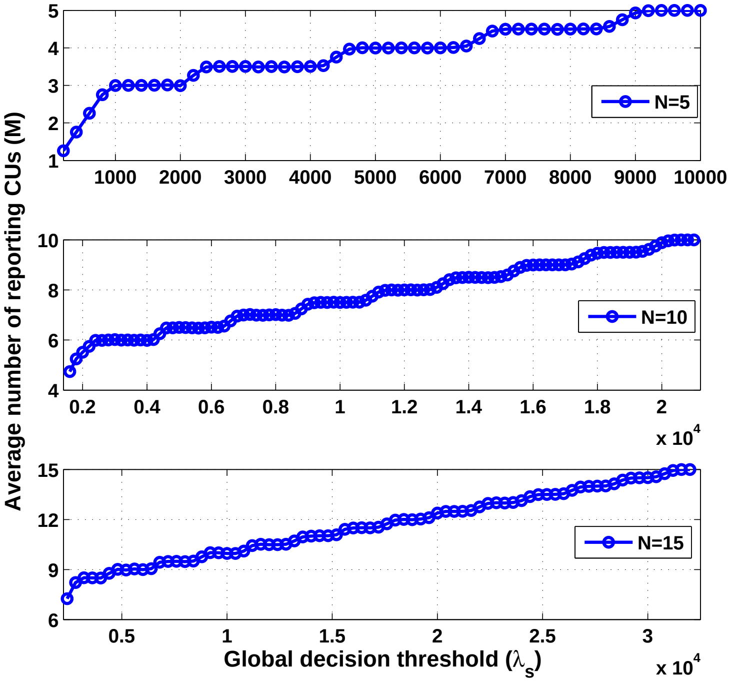


Figure 8.1: *The average number of reporting CUs versus the global decision threshold in the proposed Soft-based CSS for different numbers of CUs. All CUs have* $\overline{\gamma} = 10$

The decrease in the number of reporting CUs will affect the system in two ways: first it decreases the total energy consumed in CSS, and it makes the data transmission, if any, starts earlier. The former effect reduces the total energy consumption, while the latter increases the achievable throughput. Thus, both result in improved energy efficiency. Let us define Energy Efficiency Ratio (EER) as the ratio of the achievable energy efficiency of the proposed EES-CSS to the

Table 8.1: Simulation Parameters

Parameter	Value
P_0	0.5
F_s	$10^5\,Hz$
T	$30\,msec$
T_s	$1\,msec$
$\tau(soft)$	$0.8\,msec$
$\tau(hard)$	$0.1\,msec$
T_t	$T - N\tau - T_s$
ρ_s	$10\,mW$
ρ_t	$100\,mW$
ρ_r	$100\,mW$
R	$100\,Kbps$

achievable energy efficiency of the conventional S-CSS, as follows:

$$ERR = \frac{\mu'}{\mu} \tag{8.19}$$

where μ' is the achievable energy of the proposed approach, defined as follows:

$$\mu' = \frac{P_0(1-P_F)R\Big(T_t + (N-\overline{M})\tau\Big)}{N\rho_s T_s + \overline{M}\rho_r\tau + P_t\Big(T_t + (N-\overline{M})\tau\Big)\rho_t} \tag{8.20}$$

Compared to (6.14), in (8.20) the number of reporting CUs has been changed form N to $\overline{M}$ and the transmission time has been increased by $(N-\overline{M})\tau$.

In Fig. 8.2 the EER of the proposed EES-CSS is shown versus the global decision threshold for different number of the available CUs. The improvement in the energy efficiency is notable and significant due to the reasons we have discussed earlier. It is worthy mentioning that the detection accuracy is not affected by the proposed scheme.

In Fig. 8.1 and Fig. 8.2, all CUs are assumed to have equal SNR. Hence, the order of CUs during reporting phase does not affect the overall performance of the proposed scheme since all are identical at the FC side. In contrast, having CUs with non-equal SNRs implies that the reporting order has a significant

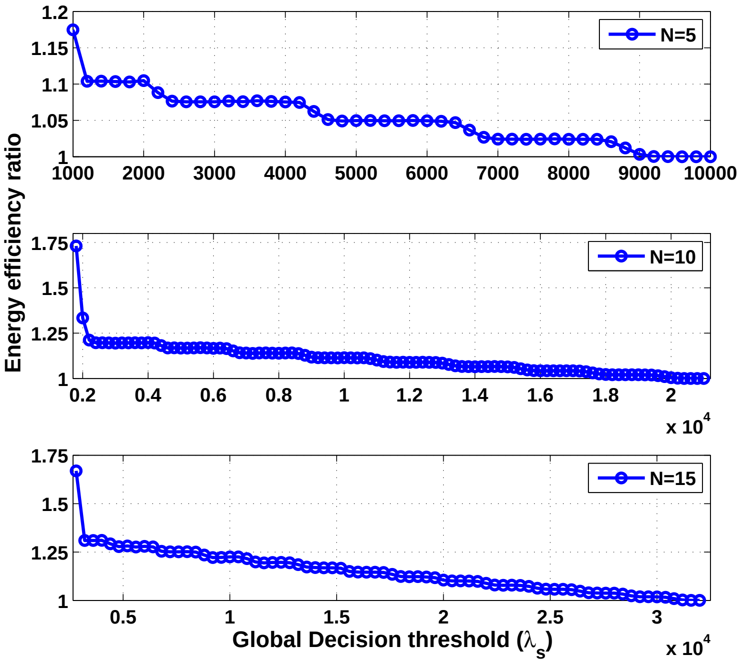


Figure 8.2: *The ratio of the achievable energy efficiency of the proposed S-CSS to the achievable energy efficiency of the conventional S-CSS versus the global decision threshold for different numbers of CUs. All CUs have* $\overline{\gamma} = 10$

influence on the achievable performance of the proposed scheme. Thus, the reporting order should be carefully designed in order to maximize the energy efficiency achieved by the proposed scheme.

Since the proposed scheme aims at terminating the reporting phase as fast as possible, then those CUs that are able to do so should report their results first. In S-CSS scheme, the global decision can be made earlier if the sum of the received results exceeds λ_s. Hence, the CUs should report their results to the FC according to a *descending* order of their average reported results, i.e., Y's.

Using (8.2), the average of Y_i can be expressed as follows

$$\overline{Y_i} = T_s F_s (2 + \gamma_i) \tag{8.21}$$

which implies that the optimal reporting order is equivalent to a *descending* order of the corresponding SNRs.

Fig. 8.3 and Fig. 8.4 show the average number of reporting CUs and EER of the optimal order (descending in SNRs) and the worst order (ascending in SNRs) versus the global decision threshold. 10 CUs are considered with SNR set $\gamma_{i=1}^{10} = \{1, 2, 3, 4, ..., 10\}$.

A significant gain can be noted between the optimal order and the worst word represented by the average number of reporting CUs, see Fig.8.3, which results in a higher energy efficiency, see Fig. 8.4.

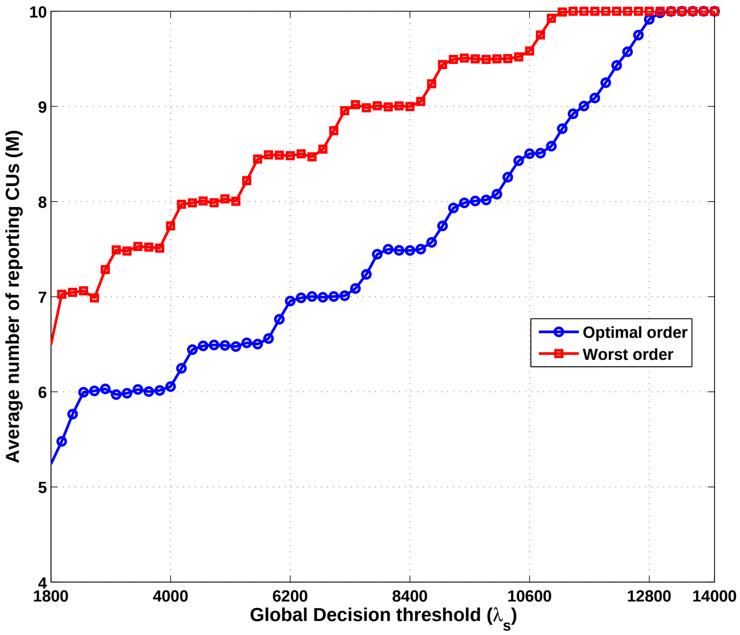


Figure 8.3: *The average number of reporting CUs versus the global decision threshold in the proposed Soft-based CSS for the optimal oder and the worst order.* $N = 10$ *and* $\gamma_{i=1}^{10} = \{1, 2, 3, ..., 10\}$

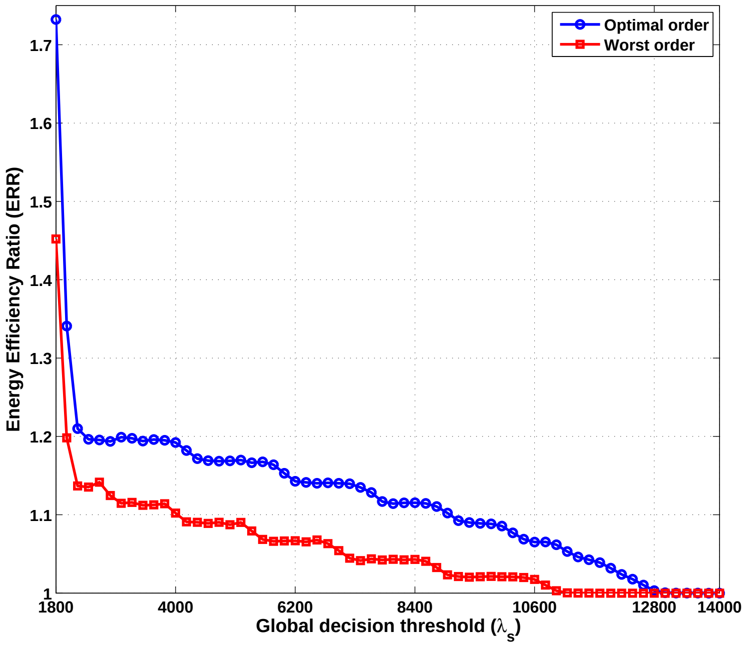


Figure 8.4: *The ratio of the achievable energy efficiency of the proposed S-CSS to the achievable energy efficiency of the conventional S-CSS versus the global decision threshold for the optimal order and the worst order.* $N = 10$ *and* $\gamma_{i=1}^{10} = \{1, 2, 3, ..., 10\}$

8.3.2 Energy-Efficient H-CSS

In H-CSS, the global decision can be made whenever the number of received $1'$s exceeds $K - 1$ or the number of received $0'$s exceeds $N - K$. Accordingly, the probability of the number of reporting CUs follows the threshold K in the *K-out-of-N* FR, as follows

$$P\{M = m\} = \begin{cases} \quad 0 & m < min\{K, N-K+1\} \\ P_{ad} + P_{af} & K \le m < N - K + 1 \\ P_{cd} + P_{cf} & N - K + 1 \le m < K \\ P_{ad} + P_{cd} + P_{af} + P_{cf} & max\{N-K+1, K\} \le m < N \\ \frac{P_{ad}}{P_{d,N}} + \frac{P_{af}}{P_{f,N}} & m = N \end{cases} \tag{8.22}$$

where

$$P_{ad} = P_1 P_{d,m} \sum_{j=1}^{\binom{m-1}{K-1}} \prod_{i \in A_j^{(m-1,K-1)}} P_{d,i} \prod_{i \notin A_j^{(m-1,K-1)}} \big(1 - P_{d,i}\big) \tag{8.23}$$

$$P_{af} = P_0 P_{f,m} \sum_{j=1}^{\binom{m-1}{K-1}} \prod_{i \in A_j^{(m-1,K-1)}} P_{f,i} \prod_{i \notin A_j^{(m-1,K-1)}} \big(1 - P_{f,i}\big) \tag{8.24}$$

$$P_{cd} = P_1 \big(1 - P_{d,m}\big) \sum_{j=1}^{\binom{m-1}{N-K}} \prod_{i \notin A_j^{(m-1,N-K)}} P_{d,i} \prod_{i \in A_j^{(m-1,N-K)}} \big(1 - P_{d,i}\big) \tag{8.25}$$

$$P_{cf} = P_0 \big(1 - P_{f,m}\big) \sum_{j=1}^{\binom{m-1}{N-K}} \prod_{i \notin A_j^{(m-1,N-K)}} P_{f,i} \prod_{i \in A_j^{(m-1,N-K)}} \big(1 - P_{f,i}\big) \tag{8.26}$$

where $A_1^{(x,y)}, A_2^{(x,y)}, ..., A_{\binom{x}{y}}^{(x,y)}$ represent all the possible combinations of y integers drawn from the interval $[1, x]$.

As a special case, when all CUs have identical performance, (8.23)-(8.26) can be rewritten as follows:

$$P_{ad} = P_1 \binom{m-1}{K-1} P_d^K (1 - P_d)^{m-K} \tag{8.27}$$

$$P_{af} = P_0 \binom{m-1}{K-1} P_f^K (1 - P_f)^{m-K} \tag{8.28}$$

$$P_{cd} = P_1 \binom{m-1}{N-K} P_d^{m-N+K-1} (1 - P_d)^{N-K+1} \tag{8.29}$$

$$P_{cf} = P_0 \binom{m-1}{N-K} P_f^{m-N+K-1} (1 - P_f)^{N-K+1} \tag{8.30}$$

In the following, we obtain the average number of reporting CUs according to the proposed technique for the two popular rules derived from *K-out-of-N* rule, OR rule and AND rule, when all CUs have identical sensing performance:

OR rule

In OR rule, $K = 1$, which means the global decision will be "$used$" if at least one CU reports "1". Eqn. (10.3) can be simplified in the case of OR rule by substituting $K = 1$ as follows

$$Prob.\{M^{or} = m\} = \begin{cases} P_{ad} + P_{af} & 1 \leq m < N \\ \frac{P_{ad}}{P_d} + \frac{P_{af}}{P_f} & m = N \end{cases} \tag{8.31}$$

The average number of reporting CUs in OR rule, denoted by $\overline{M}^{OR}$, can be derived after some algebra from (8.31), and is given as

$$\overline{M}^{or} = \frac{P_1 P_D^{or}}{P_d} + \frac{P_0 P_F^{or}}{P_f} \tag{8.32}$$

where P_D^{or} and P_F^{or} are given in (8.9) and (8.10), respectively.

AND rule

AND rule is another rule derived from the general *K-out-of-N* rule by substituting $K = N$, which means the global decision will be "$used$" only when all CUs report "1". Eqn. (10.3) can be simplified in the case of AND rule as follows

$$Prob.\{M^{and} = m\} = \begin{cases} P_{cd} + P_{cf} & 1 \leq m < N \\ \frac{P_{ad}}{P_d} + \frac{P_{af}}{P_f} & m = N \end{cases} \tag{8.33}$$

By the same way, we can write the average number of the reporting CUs based on our proposal for the AND rule ($\overline{M}^{and}$) as follows

$$\overline{M}^{and} = \frac{P_1(1 - P_D^{and})}{1 - P_d} + \frac{P_0(1 - P_F^{and})}{1 - P_f} \tag{8.34}$$

where P_D^{and} and P_F^{and} are given in (8.11) and (8.12), respectively.

Fig. 8.5 plots the average number of reporting CUs according to the proposed EEH-CSS versus the global decision threshold (K) for different numbers of the available CUs. Unlike the curve of EES-CSS in Fig. 8.1, the average number of reporting CUs shows a concave curve in terms of the decision threshold. This is due to the fact that in S-CSS the global decision can made earlier only if the sum of the received results is larger than a threshold, while in H-CSS the global decision can be issued earlier in two cases: i) if the number of received $1'$s is equal to K, or ii) if the number of the received $0'$s exceeds $N-K$. Thus, for low values of K, the reporting phase is early terminated due to the high probability of receiving K $1'$s, whereas for high values of K, the high probability of receiving $N-K+1$ $0'$s causes the early termination of the reporting phase.

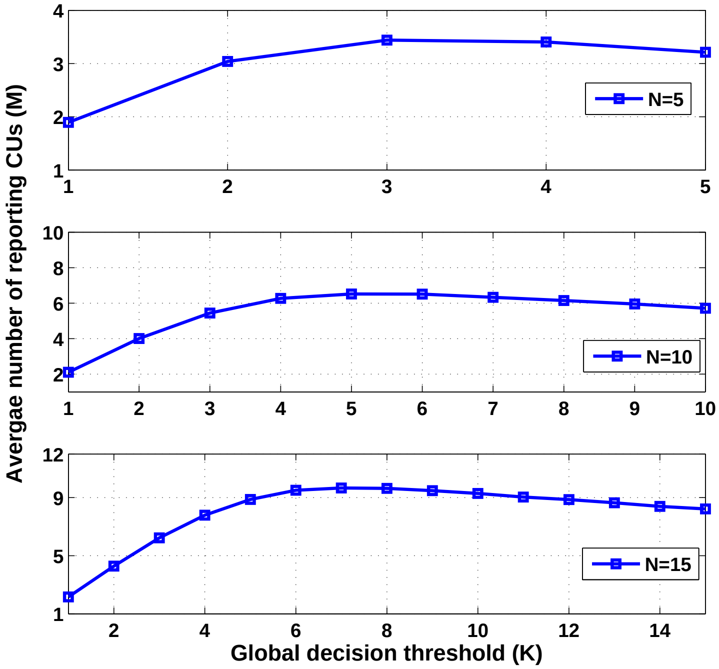


Figure 8.5: *The average number of reporting CUs versus the global decision threshold in the proposed Hard-based CSS for different numbers of CUs. All CUs have* $\overline{\gamma} = 10$

The decrease in the average number of reporting CUs, shown in Fig. 8.5, is reflected on the energy efficiency ratio of the proposed EEH-CSS to the conventional H-CSS as shown in Fig. 8.6. Notice that the curves do not take the same behavior that was followed in Fig. 8.5, i.e., concave shape, because of that although high values of K achieve low number of reporting CUs, the increase in P_t alleviate the resulting effect on the energy efficiency. The same parameters listed in Table 8.1 have been used except τ which has been set to $0.1\,msec$. The local decision threshold (λ_{loc}) has been set so that the resulting local false-alarm probability is $P_{f,i} = 0.3$.

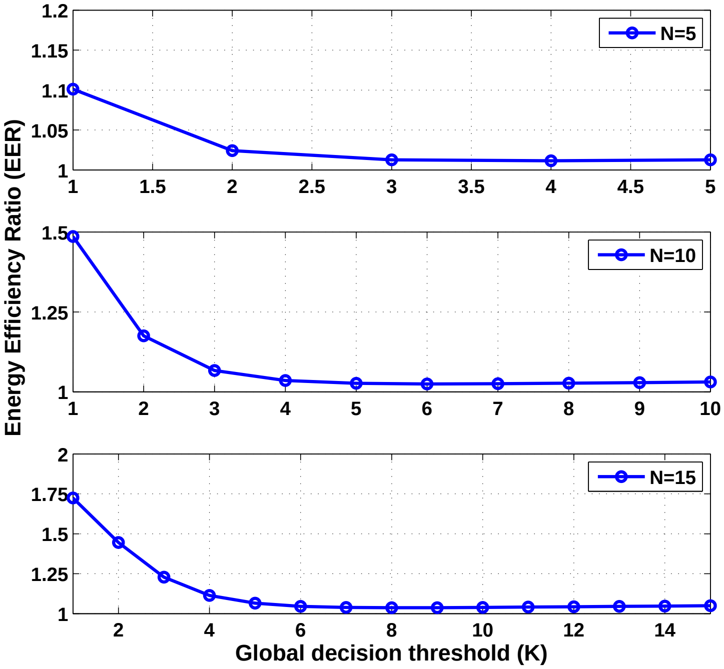


Figure 8.6: *The ratio of the achievable energy efficiency of the proposed Hard-based CSS to the achievable energy efficiency of the conventional Hard-CSS versus the global decision threshold for different numbers of CUs. All CUs have* $\overline{\gamma} = 10$

Similar to the proposed EES-CSS, in case of non-equal SNRs among CUs, the reporting order has a significant effect on the improvement of the overall performance of the proposed EEH-CSS scheme. A CRN of 10 CUs with the average SNRs $\gamma_{i=1}^{10} = \{0.03, 0.06, 0.09, ..., 0.3\}$. The local false-alarm probability is set to 0.3 for all CUs by controlling λ_{loc} as in (8.6), while the corresponding local detection probability for each CU is obtained using (8.5). Fig. 8.7 shows the average number of reporting CUs versus K for two different orders in the reporting phase; *ascending* order and *descending* order of the SNRs. Apparently, there is a significant difference in the average number of reporting CUs between the two orders. However, identifying the optimal order depends on K and the SNRs of the CUs. Fig. 8.8 shows the resulting EER for the considered CRN according to the different orders.

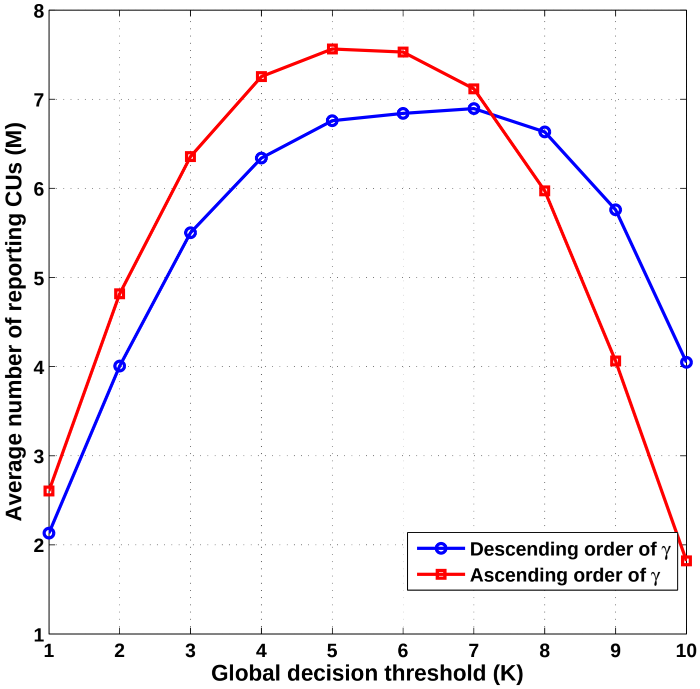


Figure 8.7: *The average number of reporting CUs versus the global decision threshold in the proposed Hard-based CSS for the ascending oder and the descending order.* $N = 10$ *and* $\gamma_{i=1}^{10} = \{0.03, 0.06, 0.09, ..., 0.3\}$

8.4 Consistency with Other Approaches

An interesting property of the proposed scheme is that it can be jointly applied with many other approaches for energy efficient CSS, enabling to improve the

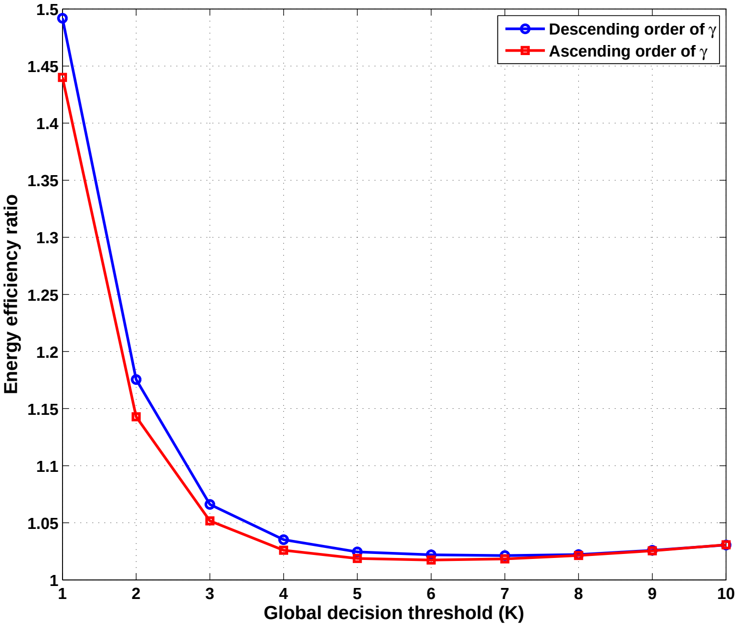


Figure 8.8: *The ratio of the achievable energy efficiency of the proposed Hard-based CSS to the achievable energy efficiency of the conventional Hard-CSS versus the global decision threshold for the ascending oder and the descending order.* $N = 10$ *and* $\gamma_{i=1}^{10} = \{0.03, 0.06, 0.09, ..., 0.3\}$

achievable energy efficiency of such approaches without any effect on their detection accuracy. Such approaches include most of the proposed energy efficient CSS proposed in the literature, such as cluster-based CSS [76] [79], dynamic-head cluster-based CSS [99], confidence-voting scheme [76], censoring scheme [100], minimizing the number of participating CU in CSS [52] [101] [53], and optimizing the sensing time [53] or the fusion rule. In this section, we prove the consistency of the proposed approach with only the energy-efficient cluster-based CSS approach as an example.

8.4.1 Cluster-based CSS

Cluster-based cooperative spectrum sensing method was proposed to improve the sensing performance [78]. By separating all CUs into a few clusters and selecting the most favorable user in each cluster, named cluster-head, to report to the FC, the proposed method can exploit the user selection diversity so that the sensing performance can be enhanced. Moreover, clustering technique is adopted to save energy consumed in reporting results, where each cluster-head processes the local decisions of its cluster-members and reports only one local decision to the FC in behalf of the whole cluster [76] [79].

The reader can notice that the proposed scheme is consistent with the cluster-based approach, and both can be applied together without affecting the detection accuracy of the network. The proposed scheme can be applied in both the reporting phase between the cluster-members and cluster-head, and the reporting phase between the cluster-heads and the FC.

For comparison, we consider 50 CUs are clustered into 10 clusters, each cluster contains 5 CUs. The members of each cluster report their local decisions to the cluster-head. The cluster-head makes a cluster-decision based on the majority decision. The cluster-decisions will be forwarded to the FC consecutively based on a TDMA scheme. Finally, the FC will make the final decision based on the employed fusion rule. The local threshold for each CUs λ_{loc} is set so that $P_{f,i} = 0.3$, and the power consumed in reporting the local decision between a cluster-member and a cluster-head is considered $50\,mW$. The other parameters are in Table 8.1.

Fig. 8.9 shows the achievable energy efficiency versus the overall false-alarm probability of the cluster-based CSS, the proposed approach and the conventional H-CSS. As an example, at $P_F = 0.1$, the cluster-based approach can improve the energy efficiency by 15% compared to the conventional H-CSS, while the proposed scheme achieves 11% improvement. However, since our proposal is consistent with the cluster-based approach, both can be applied together and an improvement up to 20% can be attained, as shown in Fig. 8.9.

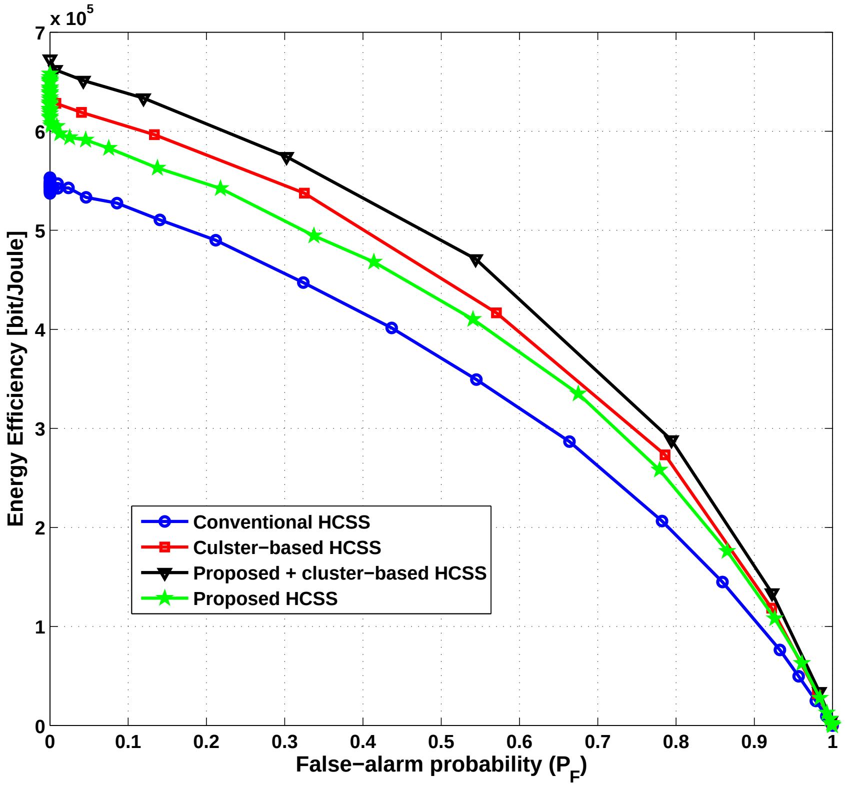


Figure 8.9: *The achievable energy efficiency versus the global false-alarm probability (P_F) for the compared approaches. All CUs have* $\overline{\gamma} = 10$

8.5 Summary

The problem of improving the energy efficiency of CSS by reducing the energy consumption in results' reporting phase has been investigated in this chapter, where a novel energy-efficient reporting scheme has been presented in this work. The idea of the proposed scheme is based on terminating the reporting phase whenever the final decision can be made and exploiting the remainder time for data transmission. The most interesting property of the proposed scheme is that it does not affect the detection accuracy. Moreover, the proposed scheme can be jointly applied with many other energy efficient proposals, enhancing their achievable energy efficiency. Analytical and simulation results show a considerable improvement in the energy efficiency, thus demonstrating the good potential of the proposed strategy.

CHAPTER 9

AN OBJECTION-BASED REPORTING SCHEME FOR COOPERATIVE SPECTRUM SENSING

9.1 Introduction

In this chapter, we propose a novel reporting scheme for CSS, called objection-based CSS scheme. The proposed scheme includes that one of the CUs will broadcast its local decision. Accordingly, the other CUs should object/agree with the announced decision. Each objecting CU will send an objection report to the FC on its reporting time slot, while the agreeing CUs will stay silent on their time slots. As a result, the number of reporting CUs should be reduced, leading to reduce the energy consumed in CSS while the detection accuracy is kept unaffected. The detection accuracy will not be degraded since all the made local decisions will be available at the FC without reporting all of them. Thus, the global decision will be identical to the conventional CSS when all CUs report their local decisions.

Notice that the number of the reporting CUs in the proposed scheme depends on the performance of the broadcasting CU. Hence, a practical and efficient method for selecting the broadcasting CU is presented in this chapter. Moreover, since the broadcasting CU consumes energy more than the other CUs, a novel schedluing algorithm is proposed, aiming to compensate the extra energy expenditure of the broadcasting CU by improving its achieved throughput. The chapter includes a mathematical framework and intensive analysis that have been made in order to investigate the performance of the proposed scheme.

9.2 System Model

A CRN of N CUs is considered. The sensing technique is assumed to be energy detection, and the hard-based scheme is adopted in this chapter. Accordingly, the local detection probability (P_{di}) and local false-alarm probability (P_{fi}) of the i^{th} CU are given in (1.4) and (1.5), respectively. We consider that the reporting phase is performed based on a TDMA approach, where each CU has its own time slot. At the FC, the *K-out-of-N* rule is employed as the FR for processing the local decisions and making the global decision. The overall detection probability (P_D) and the overall false-alarm probability (P_F) are both respectively expressed in (8.13) and (8.14).

9.3 The Proposed Objection-based Reporting Scheme

In the conventional CSS scheme, all CUs should report their local decisions to the FC, each on its time slot. This implies extra energy consumption that is continuous as long as the CRN lasts. The total energy consumption in a sensing round by the whole CRN is given in (6.9). According to (6.9), the energy consumption increases as the number of CUs increases, which may result in a huge energy expenditure in case of high number of CUs. To this end, we propose a novel CSS that is able to limit the number of reporting CUs, and to reduce the total energy consumption without affecting the global detection accuracy achieved by the CRN.

Following our proposal, only one CU will broadcast its local decision to the whole network on the first time slot in the reporting phase. As the other CU have heard the broad-casted local decision, the CUs that agree with it will stay silent during their time slots, while those CU who have different local decision should object and inform the FC during their time slots.Therefore, the number of reporting CUs should be less than N, and consequently, the energy consumption decreases. The total energy consumption based on the proposed CSS scheme can be given as follows

$$E^{pro} = NE_r + E_{bc} + N_i^* E_r + P_{free} E_t \tag{9.1}$$

where E_{bc} is the energy consumed in broadcasting and N_i^* is the number of the objecting CUs given that the i^{th} users is broadcasting. The energy consumed in receiving the broad-casted decision is considered to be included in the reporting energy (E_r).

It is worth noting that all the local decisions will be available at the FC by the end of the CSS process. Thus, the proposed scheme will not degrade the detection accuracy, and it still provides the same detection accuracy as in the conventional CSS scheme.

From (9.1), the total energy consumption depends on the number of objecting CUs. The probability that the i^{th} CU will send an objection report given that the j^{th} CU is the broadcasting CU can be expressed as follows

$$\begin{aligned} P_{obj_i} = P_0 \Bigg(& P_{fj}(1 - P_{fi}) + (1 - P_{fj})P_{fi} \Bigg) \\ & + P_1 \Bigg(P_{dj}(1 - P_{di}) + (1 - P_{di})P_{di} \Bigg) \end{aligned} \tag{9.2}$$

The four terms that appear in (9.2) represent the four probable cases of sending an object by the j^{th} CU, as follows: (i) The broadcasting CU makes a false-alarm while the j^{th} CU does not, (ii) The broadcasting CU correctly identifies a free channel while the j^{th} CU makes a false-alarm, (iii) The broadcasting CU correctly detects a licensed user while the j^{th} CU does not, and (iv) The broadcasting CU miss-detects a licensed user while the j^{th} CU correctly detects it.

The average number of the objecting CUs given that the i^{th} CU is broadcasting can be derived as follows

$$\overline{N^*}_i = \sum_{n=1}^{N-1} nP(N_i^* = n) \tag{9.3}$$

where

$$\begin{aligned} P(N_i^* = n) = \sum_{k=1}^{\binom{N-1}{n}} \Bigg(& P_0 P_{fi} \prod_{t \in A_k} (1 - P_{ft}) \prod_{l \notin A_k} P_{fl} \\ & + P_0 (1 - P_{fi}) \prod_{t \in A_k} P_{ft} \prod_{l \notin A_k} (1 - P_{fl}) \\ & + P_1 P_{di} \prod_{t \in A_k} (1 - P_{dt}) \prod_{l \notin A_k} P_{dl} \\ & + P_1 (1 - P_{di}) \prod_{t \in A_k} P_{dt} \prod_{l \notin A_k} (1 - P_{dl}) \Bigg) \end{aligned} \tag{9.4}$$

where A_k ($k = 1, 2, ...\binom{N-1}{n}$) represents the whole possible combinations of n CUs out of the total number of N CUs.

9.3.1 The selection of the broadcasting CU

The selection of the broadcasting CU is a key factor in the performance of the proposed scheme. Specifically, the local sensing accuracy of the broadcasting CU, i.e., P_{di} and P_{fi}, determines the amount of the saved energy obtained by the proposed scheme. A tricky point is that the broadcasting CU is not necessary to be the one that achieves the best sensing accuracy. On the contrary, the broadcasting CU should be selected so that its decision will most likely agree with the majority of the other CUs in the network.

The selection of the broadcasting CU should be performed in order to minimize the total energy consumption, which is attained by reducing the number of objecting CUs. Thus, the optimal broadcasting CU should be the CU that more accords with the majority of the other CUs. Notice that the majority decision can be different form the global decision taken at the FC. For example, if the FC employs AND rule or OR rule, it is likely that the global decision does not agree with the majority decision.

A practical algorithm to select the broadcasting CU is to initiate a counter for each CU at the FC. This counter is updated each CSS round based on the accordance with the majority decision. Specifically, if the local decision of a CU agrees with the majority decision, its corresponding counter will be incremented by one. If we denote the agreement counter of the i^{th} CU at the k^{th} CSS round by $\alpha_{i,k}$, then $\alpha_{i,k}$ should be updated as follows

$$\alpha_{i,k} = \begin{cases} \alpha_{i,k-1} + 1, & \text{if } u_{i,k} = M_k \\ \alpha_{i,k-1}, & \text{if } u_{i,k} \neq M_k \end{cases} \tag{9.5}$$

where M_k is the majority decision, and $\alpha_{i,0} = 0$.

Each CSS round, the FC will select the broadcasting CU based on the current state of the counters, where the broadcasting probability of the i^{th} CU is given as follows

$$P_{bc,i} = \frac{\alpha_{i,k}}{\sum_{i=1}^{N} \alpha_{i,k}} \tag{9.6}$$

The selected CU will act as a broadcasting CU on the first time slot. This implies that the FC should update the reporting order in each round to avoid any probable collision during reporting the local decisions.

9.3.2 Throughput Reward

The broad-casted decision should be transmitted to the whole CRN, while in normal reporting, the decision is sent only to the FC. Hence, broadcasting consumes more energy than normal reporting since it is adjusted to cover a wider area. Thus, those CUs that have high values at their α counters will suffer from high energy expenditure, while the others will save energy due to not even reporting the local decision. Motivated by this, the proposed scheme offers a throughput reward to the CUs broadcasting more often. Particularly, the scheduling policy adopted is not equally probable among CUs. Instead, the scheduled CU for data transmission in each frame, if any, will based on a new metric that is based on the contribution in the broadcasting process. Doing so, those CUs that lose their energy in broadcasting will be compensated by achieving higher throughput. According to this throughput reward, a proportional fairness can be attained among CUs in their achievable energy efficiency in $bit/Joule$.

The scheduling probability for a specific CU is equal to the broadcasting probability given as follows

$$P_{sch,i} = P_{bc,i} = \frac{\alpha_{i,k}}{\sum_{i=1}^{N} \alpha_{i,k}} \tag{9.7}$$

Notice that (9.7) does not imply that the broadcasting CU in a specific round is the scheduled CU on the corresponding data transmission frame.

The individual performance of each CU can be represented by the individual energy efficiency defined as the ratio between the achievable throughput to the consumed energy.

$$\mu_i = \frac{D_i}{E_i} \tag{9.8}$$

The average individual energy consumed by the i^{th} CU can be expressed as follows

$$E_i = E_s + P_{bc,i}E_{bc} + (1 - P_{bc,i})P_{obj,i}E_r + P_{sch,i}P_{unused}E_r \tag{9.9}$$

The individual achievable throughput can be given as follows

$$D_i = P_0(1 - P_F)P_{sch,i}RT_t \tag{9.10}$$

where the transmitted data are considered successfully delivered only if the free channel has been correctly identified as free, represented by factor $P_0(1 - P_F)$ in (9.10).

From (9.9) and (9.10), increasing the broadcasting probability increases the individual energy expenditure, but it also increases the individual achievable throughput, leading to a balance in the achievable energy efficiency among CUs.

The flow charts shown in Fig. 9.1 depict the procedure of the proposed objection-based CSS at FC side and CU side.

9.4 Numerical Analysis and Simulation Results

In this section, the performance of the proposed CSS scheme is proved by numerical and simulation results. All the necessary parameters regarding detection performance, energy consumption and network specifications are summarized in Table 9.1.

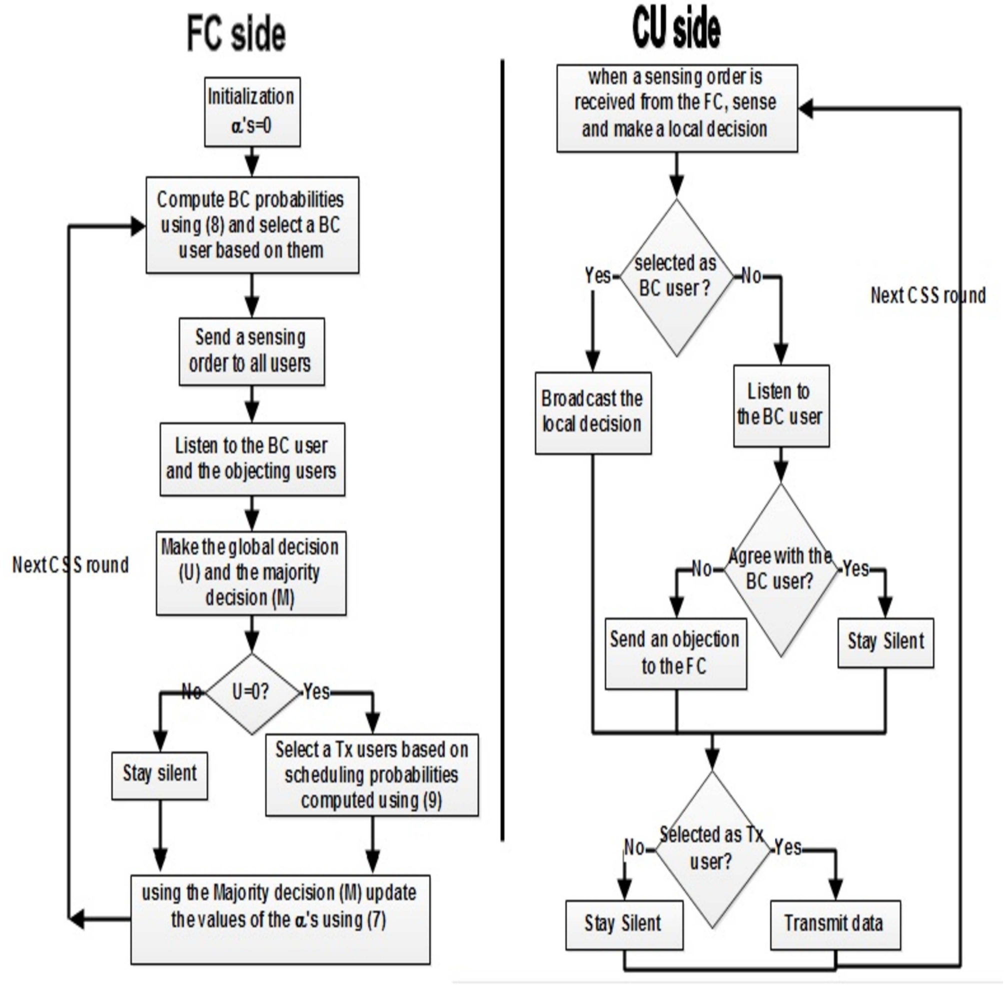

FC side
Initialization α's=0
Compute BC probabilities using (8) and select a BC user based on them
Send a sensing order to all users
Listen to the BC user and the objecting users
Make the global decision (U) and the majority decision (M)
U=0?
No
Yes
Stay silent
Select a Tx users based on scheduling probabilities computed using (9)
using the Majority decision (M) update the values of the α's using (7)
Next CSS round
CU side
when a sensing order is received from the FC, sense and make a local decision
selected as BC user?
Yes
No
Broadcast the local decision
Listen to the BC user
Agree with the BC user?
No
Yes
Send an objection to the FC
Stay Silent
Selected as Tx user?
No
Yes
Stay Silent
Transmit data
Next CSS round

Figure 9.1: *A flow chart of the proposed objection-based CSS*

Numerical results for a CRN that consists of 5 CUs are shown in Table 9.2 and Table 9.3. The first two columns in Table 9.2 list the individual sensing performance of each CU, which are selected randomly. The employed FR is considered majority rule ($K = N/2$). The individual energy consumption, achievable throughput and energy efficiency are shown in Table 9.2 for both the proposed scheme and the conventional scheme. The conventional CSS scheme refers to the scheme where all CUs sense and report their results to the FC, and the scheduled CU is randomly chosen where all CUs are equal probable.

.

Table 9.1: Simulation Parameters

Parameter	Value	Parameter	value
P_0	0.5	T_t	$0.2\,sec$
R	$1M\,bps$	E_s	$0.1m\,J$
E_r	$1.0m\,J$	E_{bc}	$1.8m\,J$
E_t	$6m\,J$		

Table 9.2: Numerical Results- Individual Performance

	P_d	P_f	$BC\%$	$E[mJ]$	$E_{conv}[mJ]$	$D[Kb]$	$D_{conv}[Kb]$	$\mu[Mb/J]$	$\mu_{conv}[Mb/J]$
CU1	0.6	0.1	21.30	1.58	1.86	20.61	19.28	13.04	10.37
CU2	0.5	0.4	17.08	1.43	1.86	16.39	19.33	11.46	10.39
CU3	0.6	0.3	18.74	1.49	1.86	18.23	19.42	12.23	10.44
CU4	0.8	0.05	21.97	1.61	1.86	21.39	19.32	13.29	10.38
CU5	0.55	0.1	20.91	1.56	1.86	19.89	19.16	12.75	10.30

Regarding the individual energy consumption shown in Table 9.2, the results show that all CUs have saved different amounts of energy compared to the conventional scheme. However, the different individual energy consumption among CUs refers to the different broadcasting and objecting probabilities. The distribution of the transmitted data is almost identical in the conventional scheme, whereas in the proposed scheme, the transmission opportunity is distributed based on the contribution in the broadcasting phase. Consequently, the individual energy efficiency for each CU has been improved in the proposed scheme compared to the conventional scheme.

A primary note on the global performance shown in Table 9.3 is that the global detection accuracy is equal in both schemes. Not effecting the detection accuracy is an interesting property that usually does not exist in most of the proposed schemes in the literature. The proposed scheme results in 17.5% saved energy for the whole CRN, leading to 21% energy efficiency improvement for the whole CRN.

Table 9.3: Numerical Results - Global Performance

	P_D	P_F	$E[mJ]$	$D[Kb]$	$\mu[Mb/J]$
Conventional Scheme	0.7	0.03	9.3	96.51	10.83
Proposed Scheme	0.7	0.03	7.67	96.51	12.55

For the purpose of comparison to other schemes, we choose the confidence voting scheme (CV) that is presented in [76]. Briefly, CV scheme implies that each CU has a confidence counter which is updated each CSS round as follows. If the local decision matches the global decision, the confidence counter is incremented by one, while if the local decision mismatches the global decision, it is decreased by one. When the confidence counter is below a specific threshold, the corresponding CU will not report its local decision. CV scheme attempts to reduce the energy consumption in reporting phase by limiting the number of reporting CUs. However, unlike our proposed scheme, CV scheme influences the global detection accuracy since not all the decisions will be present at the FC. The global energy efficiency versus the total number of CUs for the three schemes is shown in Fig.9.2. The detection and false-alarm probabilities for the CUs are selected uniformly from the periods $[0.4\ 0.95]$ and $[0.05\ 0.6]$, respectively. The voting threshold of CV scheme is set to zero. The global energy efficiency has been opted as a comparison base since it incorporates all the performance aspects, see (1.11)-(9.10).

Generally, the global energy efficiency of all schemes decreases due to the increase in the energy consumed in local sensing. However, the objection-based scheme still achieves higher energy efficiency than the other schemes. This is a result of reducing the number of reporting CUs without degrading the detection accuracy nor the global achievable throughput.

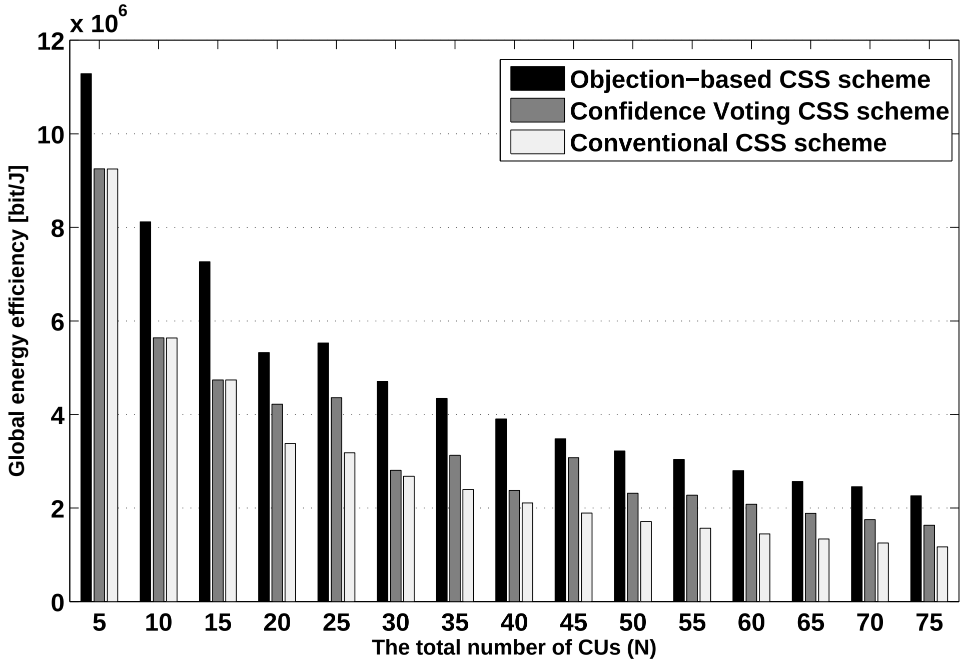


Figure 9.2: *The global energy efficiency (μ) versus the number of CUs (N). (The value at $N = 5$ is different form the obtained value in Table 9.3 because of the different P_d and P_f used.)*

9.5 Summary

In this chapter, a novel collaborative spectrum sensing scheme for cognitive radio networks has been proposed. The proposed scheme implies that one of the CUs broadcasts its local decision about the spectrum availability to the whole network. The other CUs that have a different local decision should send an objection to the FC, each on its corresponding reporting time slot, while the CUs that agree with the announced decision should stay silent. The amount of the saved energy refers to limiting the number of reporting CUs without affecting the overall detection accuracy. A practical algorithm to select the broadcasting CU in each round is presented. Moreover, a reward policy is proposed in order to compensate the broadcasting CUs by increasing their scheduling probabilities. Simulation and analytic results show the superiority of the proposed scheme compared to the conventional scheme and the confidence voting scheme.

CHAPTER 10

ENERGY-EFFICIENT REPORTING SCHEME FOR COOPERATIVE SPECTRUM SENSING BY EXPLOITING THE ARRIVAL TIME

10.1 Introduction

As mentioned earlier, Two main schemes have been proposed for reporting the local sensing results to the FC, soft-based scheme and hard-based scheme. In soft-based scheme, high accurate sensing results will be available at the FC since each CU reports its sensing result as it is without any local processing. In contrast, hard-based scheme suffers from the low accuracy since the each sensing result is conveyed by only a single bit. However, hard-based scheme is considered as a resource efficient scheme in terms of time and energy, while soft-based scheme requires more energy and time consumption in results' reporting. Such a trade-off between resource efficiency and detection accuracy has motivated us to propose a novel reporting scheme in this chapter. The proposed reporting scheme is able to approximately provide detection accuracy as in the soft-based scheme by reporting only a single bit as in the hard-based scheme.

The idea behind the proposed scheme is based on exploiting the time dimension as an indicator of the sensing results. Specifically, the arrival time of a single bit from each CU at the FC can be adjusted to indicate the actual sensing result. In detail, the proposed scheme implies splitting the reporting period to several time slots, and mapping these slots to specific intervals on the range of the local sensing result. Each CU (after obtaining the sensing result) will report a single bit on the time slot that is corresponding to the actual sensed value. At the FC, whenever a bit is received, the sensing result can be extracted by demapping the time slot on which the bit is received to the corresponding interval of the sensing result range. Doing so, each CU reports only one bit as in the hard-based scheme, while the actual sensing result can be extracted at the FC, providing a high accuracy as in the soft-based scheme.

However, according to this proposal, there is probability that more than a CU report on the same time slot, and hence, their reports will collide and appear as one report to the FC. Also, the division of the reporting period and spectrum sensing intervals affects the overall performance of the proposed scheme. These effects are intensively investigated in this chapter. Moreover, the performance of the proposed scheme is compared to the soft and hard schemes, where simulation results demonstrate that our proposal outperforms both schemes in terms of detection accuracy and energy efficiency.

10.2 System Model

A CRN consists of a set of CUs is considered. The energy detection is employed as the sensing technique in this chapter. The time frame (T) of the cognitive transmission is divided into three phases, sensing phase T_s where local sensing is performed by each CU, reporting phase T_r where local results are reported to the FC, and data transmission phase T_t where one of the CUs is scheduled for data transmission. The total energy consumption by the whole network, which includes the energy consumed during the three phases, is given in (6.9). The average achievable throughput in terms of the successfully transmitted bit is expressed in (6.13).

10.3 The Proposed Reporting Scheme

Motivated by the need for a reporting that achieve a balance between energy efficiency and detection accuracy, we propose a novel reporting scheme that is able to consume an amount of energy as in hard scheme while achieving a detection accuracy almost as in soft scheme. In this proposal, the reporting phase T_r is split into L time slots ($\{\tau_1, \tau_2, ...\tau_L\}$). Likewise, the possible range of the sensing result, which is represented by the average of the collected energy samples, is divided into L intervals using $L+1$ thresholds ($\gamma_1, \gamma_2, ..., \gamma_{L+1}$). Each interval is represented by a unique level v_l. Upon ending the local sensing and computing the samples' average (A_i) at each CU, if A_i is within the l^{th} interval, i.e., $\gamma_l \leq A_i < \gamma_{l+1}$, then, one bit will be reported to the FC on the l^{th} time slot. At the FC, whenever a bit is received on the i^{th} time slot, the FC will consider the samples' average of the reporting CU equals to v_l. Fig. 10.1 shows the mapping between the time slots and the samples' average.

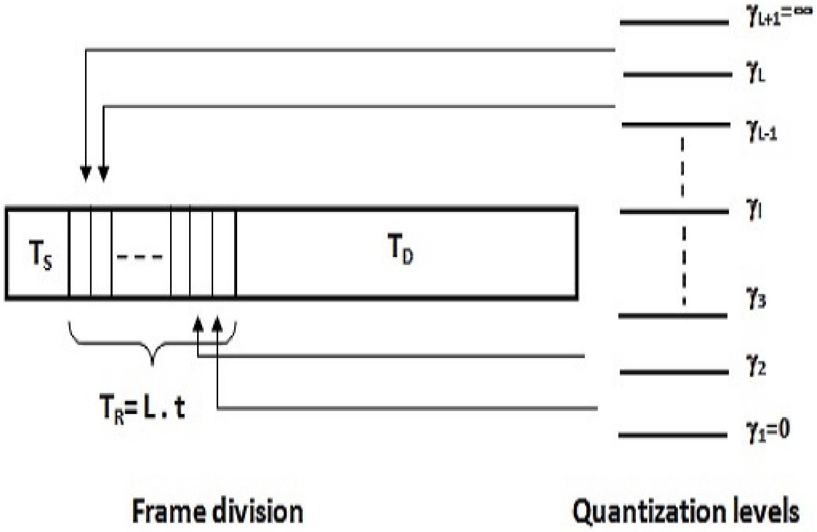


Figure 10.1: *Description of the quantization intervals used at the CU-end, frame division at the FC-end, and the mapping between them in the proposed scheme.*

In formulas, a CU that has obtained a samples' average A_i will report one bit on the time slot ($\tau^{(i)}$) given by

$$\tau^{(i)}(\gamma_l \leq A_i < \gamma_{l+1}) = \tau_l \tag{10.1}$$

At the FC, the recovered samples' average ($\hat{A}_i$) of a CU whose reported bit has been received at the FC on the l^{th} time slot is expressed as follows

$$\hat{A}_i(\tau^{(i)} = \tau_l) = v_l \tag{10.2}$$

Following this proposal, each CU reports only one bit to the FC so that the energy consumed in reporting is equal to the hard scheme. On the other hand, the resulting detection accuracy is affected by several factors, the thresholds γ's , the recovered values v's, and the number of levels L. In the following we discuss each one of them.

10.3.1 Quantizer Design

The process of representing the samples averages in discrete levels is considered as a scalar quantization process [102]. Thus, the selection of the thresholds γ's and the representing values v's follow the typical problem of quantization design. The optimal γ's and v's that minimize the squared-error distortion could not be formulated in analytical forms, and they are obtained using an iterative algorithm [32]. Therefore, in this work we consider an maximum-entropy quantization process in order to reduce complexity and smooth the following analysis [103]. According to the maximum-entropy quantization, the thresholds are selected so that the probability that the sensed valued lies in an interval is equal probable for all intervals, as follows

$$Pr(\gamma_l \leq A_i < \gamma_{l+1}) = \frac{1}{L} \qquad for\ \ l = 1, ..., L \tag{10.3}$$

where the notation $Pr(.)$ refers to the probability of an event. (10.3) can be rewritten using the cumulative distribution function of the samples' average (F_A) as follows

$$F_A(\gamma_{l+1}) - F_A(\gamma_l) = \frac{1}{L} \qquad for\ \ l = 1, ..., L \tag{10.4}$$

The optimal level v for each interval has been found to be the centroid (the conditional expected mean) of the corresponding interval [32]. Therefore, the representing level of any interval can be given as

$$v_l = \frac{\int_{\gamma_l}^{\gamma_{l+1}} x f_A(x) \cdot dx}{Pr(\gamma_l \leq A_i < \gamma_{l+1})} \qquad for\ \ l = 1, ..., L \tag{10.5}$$

which can be simplified as follows

$$v_l = L \int_{\gamma_l}^{\gamma_{l+1}} x f_A(x) \cdot dx \qquad for\ \ l = 1, ..., L \tag{10.6}$$

where f_A is the probability density function of A.

10.3.2 Reports Collision

Due to the absence of results exchange among CUs, there is a probability that two or more CUs report their bits on the same time slot. This implies that the sent reports on the same time slot will collide, and hence, the FC will be unable to recognize if the received signal from one or more CUs. Therefore, the FC will deal with them as one CU. Obviously, these collisions affect directly the achievable performance and the detection accuracy since the number of participating CUs in making the final decision will be lower than the total available CUs.

If we denote the number of reporting CUs in the l^{th} time slot by n_l, then the probability of n_l is expressed as follows

$$Pr.(n_l = i) = \sum_{i=0}^{N} \binom{N}{i} \left(\frac{1}{L}\right)^{i} \left(1 - \frac{1}{L}\right)^{N-i} \tag{10.7}$$

Notice that (10.7) is identical for all time slots because of the equal probable levels. Accordingly, the average number of reporting CUs in any time slot can be given as:

$$\bar{n} = \frac{N}{L} \tag{10.8}$$

It is worthy to mention that the average number of reporting CUs decreases as the number of levels increases. However, the increase in number of levels requires more time resources for the reporting process.

10.4 Performance Optimization

The proposed scheme for reporting the local results to the FC reduces the energy consumption in CSS. On the other hand, the achievable detection accuracy depends on the number of used quantization levels (time slots), where an increase in the number of levels improves the detection accuracy. However, increasing the number of time slots reserves more time resources for CSS (T_r), which, in turn, affects the time dedicated for transmission (T_t) since the total frame length T is fixed. Such decrease on T_t results into two contrasting effects on the achievable energy efficiency. First, shorter T_t results in lower throughput, as indicated in (6.13), which consequently, degrades the achievable energy efficiency. Second, lower T_t decreases the total energy consumption during data transmission, as appears in (6.9), and hence, energy efficiency is improved.

The number of the time slots should be optimized so that the achievable energy efficiency is maximized. To this goal, the resulting detection probability and false-alarm probabilities should be computed based on the proposed scheme. Both probabilities depend on the number of CUs (N) and the number of time slots (L). However, due to the possible collision among different CUs, the number of successfully received reports could be less than the total number of sent reports. If we denote the number of successfully received reports by x ($1 \leq x \leq N$)[1], then the probability of x is expressed as follows

$$Pr.(x = i) = \frac{L!}{L^N} \binom{L}{i} \sum_{k=1}^{K_i} \frac{S_k}{\prod_{j=1}^{i} d_{kj}!} \tag{10.9}$$

where d_{kj} ($j = 1, 2, .., i$ and $k = 1, 2, ..., K_i$) is the j^{th} element in the set D_k that contains i non-zero elements whose sum is N, i.e., $\left(\sum_{j=1}^{i} d_{kj} = N, \;\; d_{kj} \neq 0\right)$, K is the number of possible sets that satisfy D, and S_k is the number of different combinations of the set D_k. For example, consider $L = 10$ and $N = 6$ and we want to compute the probability that only two reports are received successfully, i.e., $Pr(x = 2)$. In other words, we compute the probability that 6 CU report on 2 time slots. In this case, 3 different sets can satisfy the condition of D, which are $D_1 = \{5, 1\}$, $D_2 = \{4, 2\}$ and $D_3 = \{3, 3\}$, and the number of the different combinations of each one is $S_1 = 2$, $S_2 = 2$ and $S_3 = 1$, respectively. Now, by substituting these values in (10.9), $Pr(x = 2)$ can be easily computed.

At the FC, if i CUs have reported on the same time slot, their reports will collide, and be considered as only one report. The final decision is made by comparing the sum of the received results to a predefined threshold. Thus, the average achievable detection probability and false-alarm probability are given

[1] Notice that if more than one report are sent on the same time slot, one of them will be consider as received successfully

respectively as follows:

$$\bar{P}_D(L,N) = \sum_{i=1}^{N} Pr(x=i)P_D(i) \tag{10.10}$$

$$\bar{P}_F(L,N) = \sum_{i=1}^{N} Pr(x=i)P_F(i) \tag{10.11}$$

where $P_D(i)$ and $P_F(i)$ are respectively the detection probability and false-alarm probability when i CUs are involved.

Now, let us investigate energy consumption and throughput. Following the proposed scheme, (6.9) can be rewritten as follows:

$$E_T = \rho_s T_s + \rho_r N\tau + P_{unused}\rho_t(T - T_s - L\tau) \tag{10.12}$$

where ρ_s, ρ_r and ρ_t are the consumed power during sensing, reporting and transmission, respectively. Notice that the energy consumption during sensing and reporting is independent of L, while the transmit energy is directly affected by increasing L. This effect is related to the change on P_{unused} and the decrease in transmission time.

Regarding the throughput, (6.13) can be rewritten as follows

$$Th = P_0(1 - P_F)R(T - T_s - L\tau) \tag{10.13}$$

Likewise, the throughput will be affected here also by increasing L due to the decrease in P_F and the decrease in the transmission time.

From (10.12) and (10.13), we can say that the achievable energy efficiency is influenced by L, and hence, L should be optimized so that the energy efficiency is maximized.

10.5 Simulation Results

A CRN of N CUs is considered. The sensing channel is assumed to be additive Gaussian noise channel with an average signal to noise ratio equals $SNR = -10dB$[2]. The proposed scheme is compared to the two classical schemes, Soft Scheme and Hard Scheme, in terms of the detection accuracy and energy efficiency. The common simulation parameters among the three schemes are shown in Table 10.1. In SS, the sensing results are reported using 8 bits, where the resulting quantization noise is ignored.

Table 10.1: Simulation Parameters

Parameter	Value	Parameter	value
P_0	0.5	F_s	0.1 MHz
τ	20 μs	ρ_r	1 W
ρ_t	1 W	ρ_s	$0.1W$
T	$50ms$	T_s	$1ms$
SNR	$-10dB$	R	$200Kbps$

Fig. 10.2 shows the missed-detection probability versus the false alarm probability for the proposed scheme ($L = 10$) and both HS and SS. It is clear that at a fixed false alarm probability, our proposal can achieve lower missed detection probability than the HS. This is due to the more accurate results provided by our proposal. On the other hand, the SS still attains lower missed detection than the proposed scheme, due to the perfect accuracy in the reported sensing results. It is obvious that the number of levels (L) have an important role in the detection performance since increasing the number of levels improves the accuracy in the reported information. In Fig 10.3, the detection probability is plotted versus the number of levels at a fixed false-alarm probability ($P_F = 0.1$). Clearly, the detection probability increases as the number of levels increases. The proposed

[2] All derived equations are applicable to any other fading model that could be considered.

scheme outperforms the HS with a small number of levels, while the achievable detection probability by the SS represents the maximum detection probability that can be attained by the proposed scheme. However, for $L \geq 12$, the difference in detection probability can be ignored between our proposal and the SS.

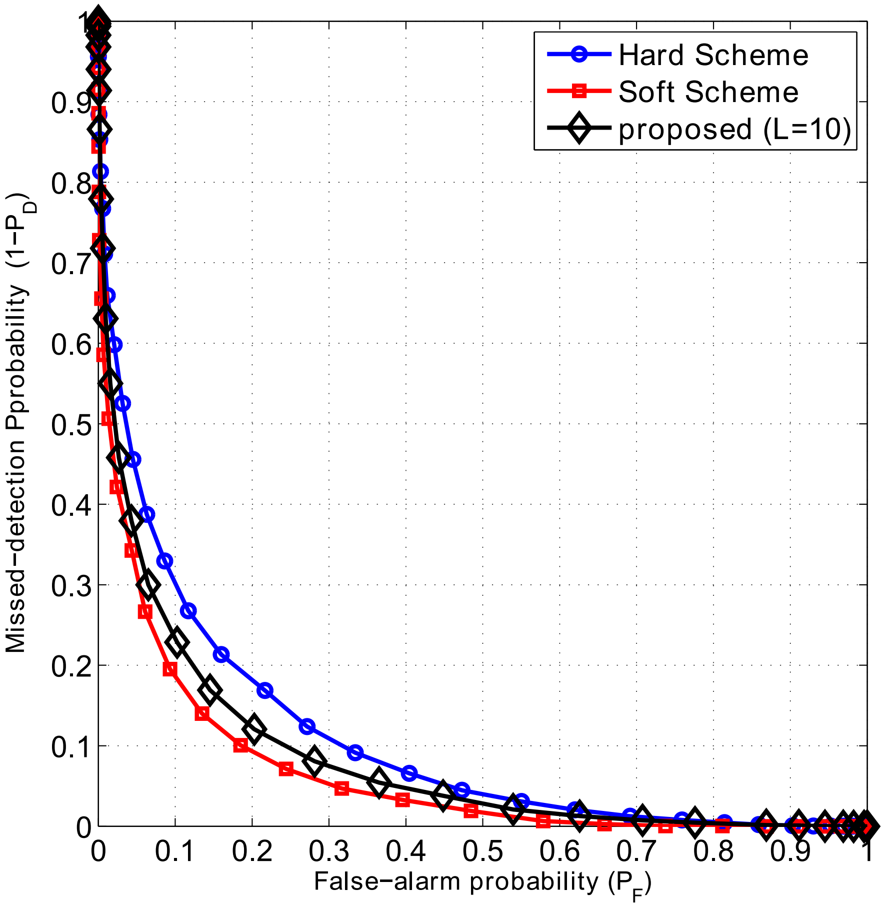


Figure 10.2: *The missed detection probability versus the false alarm probability for the three schemes.* $(N = 5)$.

The previous two figures show that the detection accuracy of the proposed scheme depends on the number of levels (time slots). However, in view of the limited time resources, increasing the number of time slots affects the energy consumption, achievable throughput and energy efficiency. This is due

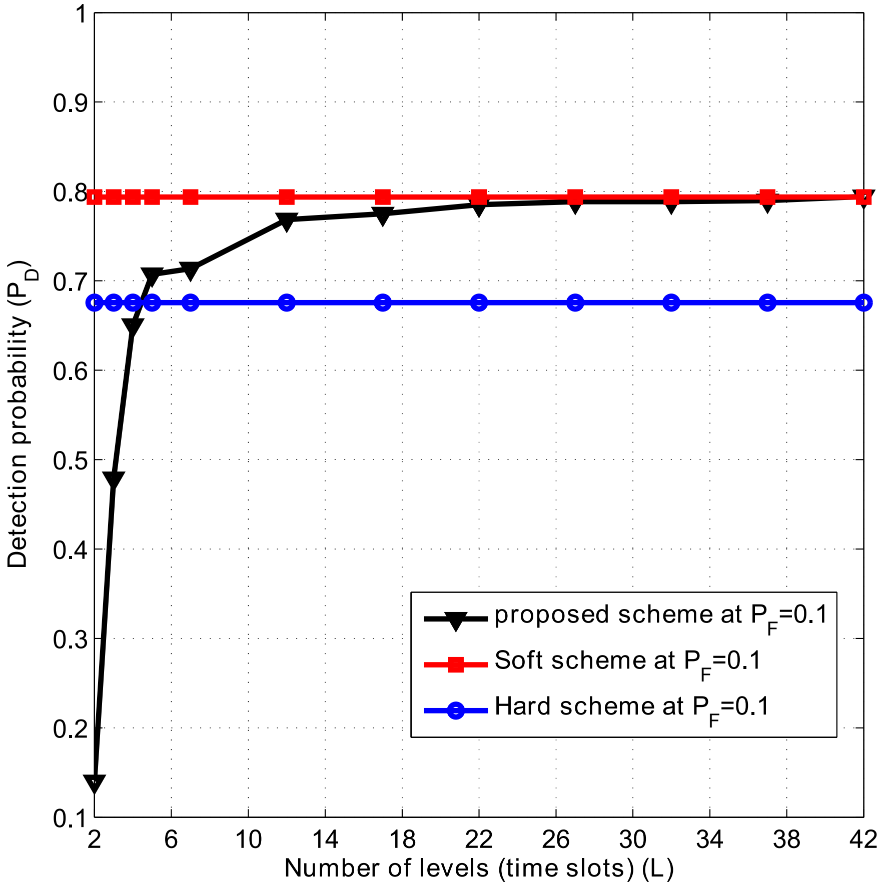


Figure 10.3: *The detection probability versus the number of levels (time slots) at a fixed false alarm probability ($P_F = 0.1$) for the three schemes.* $(N = 5)$.

to increasing the number of time slots that are dedicated for reports reception, which reduces the time spent in data transmission. Hence, energy consumption, throughput and energy efficiency will be affected. Also, since energy efficiency is affected by detection performance that mainly depends on L. Fig. 10.4 depicts the energy efficiency versus the false alarm probability for the proposed scheme (at $L = 20$) compared to the SS and the HS. Our proposal can achieve higher energy efficiency than the other two schemes for most of the range of P_F.

The achievable energy efficiency by the proposed scheme using the optimal L is shown in Fig. 10.5 versus the number of sensing users N. The proposed

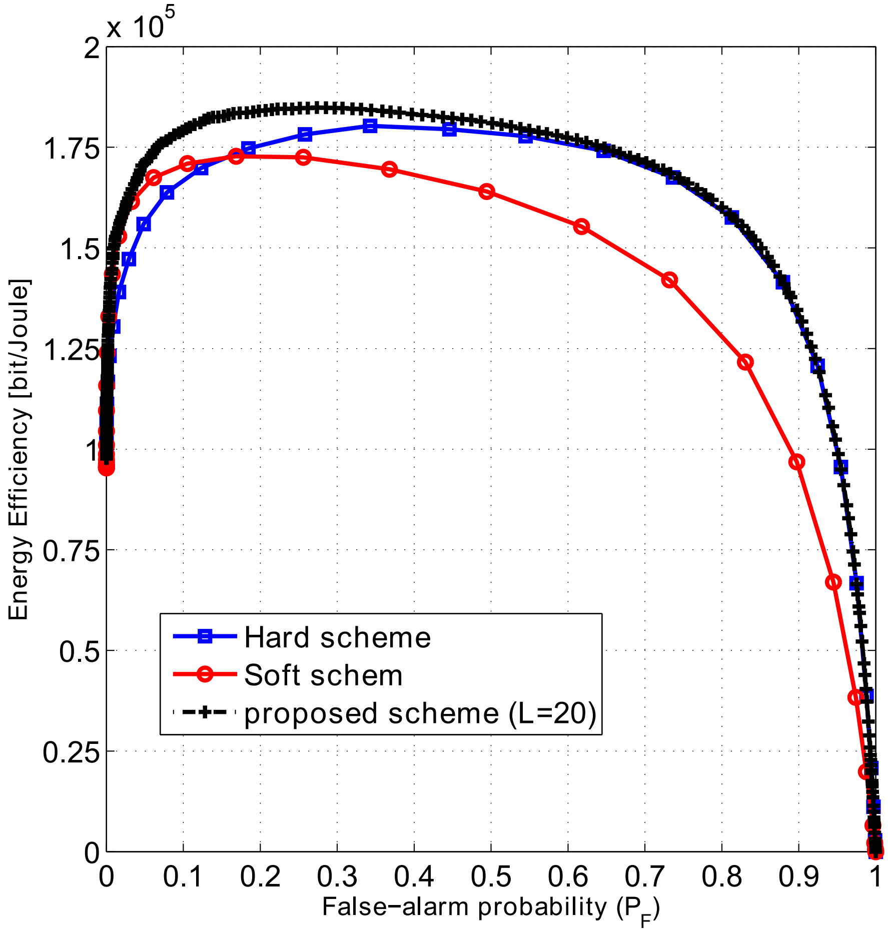


Figure 10.4: *The energy efficiency versus the false alarm probability for the three schemes.* $(N = 10)$.

scheme achieves higher energy efficiency than the other schemes due to the low energy consumption and the high accuracy in the reported results. The proposed scheme outperforms the other two schemes over the whole range of the number of CUs.

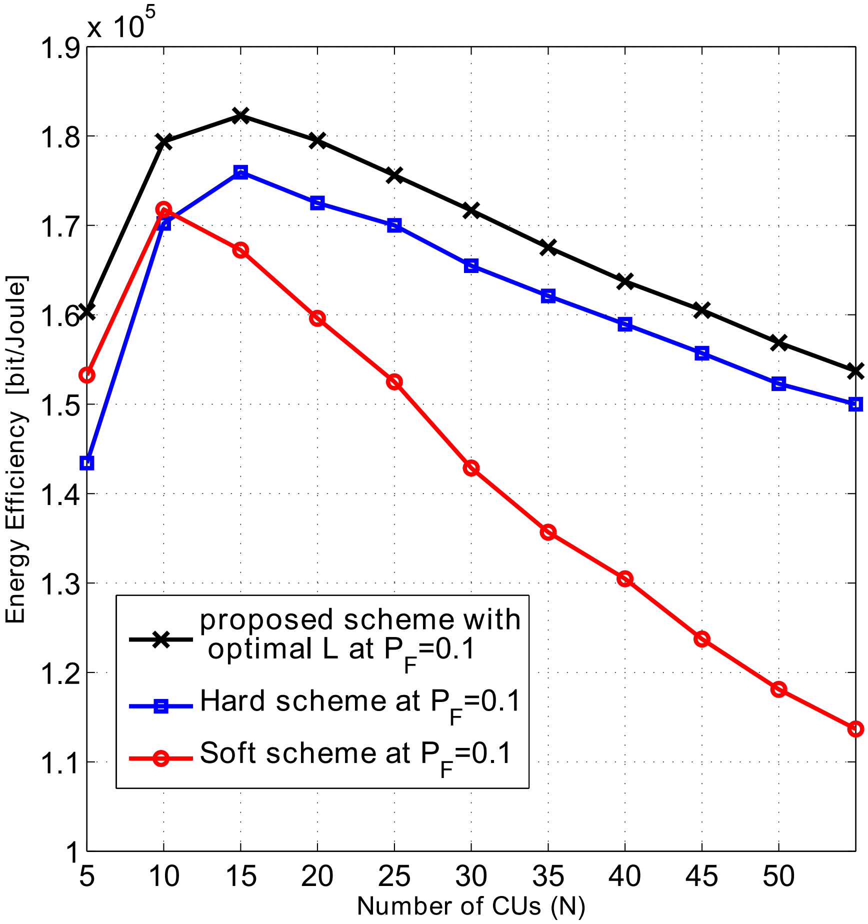


Figure 10.5: *The energy efficiency versus versus the number of available users N for the three schemes. The optimal number of levels is used in the proposed scheme.* ($P_F = 0.1$)

10.6 Summary

A novel energy-efficient reporting scheme for spectrum sensing results is presented in this work. The proposed scheme gets benefits from both soft-based scheme and hard-based scheme, where each CU reports only a single bit on a time slot related to its actual sensing result. At the FC, the sensing result is extracted based on the arrival time. Extended discussion and simulation results have demonstrated the superiority of the proposed scheme in terms of achievable energy efficiency over both hard-based scheme and soft-based scheme.

Part IV

Improving Energy Efficiency in Decision Making Stage

CHAPTER 11

ENERGY EFFICIENCY ANALYSIS OF DECISION FUSION RULES IN COOPERATIVE SPECTRUM SENSING

11.1 Introduction

In the decision-making stage, the FC applies a predefined fusion rule [97] in order to make a global decision based on the received local decisions. Considering noisy local decisions, there are several FRs, such as the Likelihood Ratio rule (LR), the Maximum Ratio Combining rule (MRC) or the Equal Gain Combining rule (EGC). However, In order to make a global decision, each FR requires a different amount of prior information about the detection performance of each user and the fading effect of the channels between the users and the FC. Neglecting the impact of required prior information and the consumed energy to this end, LR has been proved to be the optimal in terms of achievable performance [20].

As mentioned earlier, the total frame structure is divided into three phases: sensing, reporting and data transmission. The time dedicated for reporting phase mainly depends on the number of users and the amount of information that has to be reported to the FC. Thus, the difference in the amount of reported data for each FR implies a different reporting time, leading to a different time distribution among the three phases. For instance, LR requires knowledge of detection probability and false alarm probability of each CU at the FC, while MRC and EGC do not need this information. Consequently, time, bandwidth and energy requirement of each FR vary. To the best of our knowledge, this issue has not been addressed in the literature.

Motivated by such considerations, this chapter is aimed at comparing LR, MRC, and EGC decision FRs in CSS in terms of consumed energy and achievable performance. Unlike other previous works, this chapter builds the comparison under a limited time assumption, which implies an equal frame length for all the rules. According to this assumption, the time specified for data transmission is fixed and the rest of the frame is distributed between collecting the samples from the spectrum and reporting decision and prior information required for each rule. It is shown by simulation that consumed energy and achievable performance of decision FRs depend on various factors, such as the number of cognitive users, the frame length, and the Signal-to-Noise-Ratio (SNR). The role of every factor is discussed in detail in the next sections. In particular, our analysis shows that, *in critical conditions, the EGC rule has the best performance in both the achievable detection probability and in the consumed energy*. The critical conditions are represented by short frame time, large number of users and low SNR.

11.2 System Model

Consider a CRN consisting of N CUs. Energy detection is assumed to be the sensing technique. The reporting scheme adopted in this chapter is hard-based scheme. According to the hard scheme, each CU should report a local binary decision ($u_i = \{0, 1\}$) to the FC. The sensing channels are assumed additive white Gaussian noise channels, so that the local detection and false alarm probabilities are given as in (1.4) and (1.5). The reporting channel is assumed to be noisy channel, where the sent local decisions are received corrupted at the FC. The received decision from the i^{th} CU is given as follows

$$y_i = h_i u_i + w_i \tag{11.1}$$

where h_i is the channel envelope ($h_i > 0$) with variance $\sigma^2_{h,i}$, and w_i is the additive white Gaussian noise with variance $\sigma^2_{w,i}$. Let γ_i denote the SNR of user i given as:

$$\gamma_i = \frac{\sigma^2_{h,i}}{\sigma^2_{w,i}} \tag{11.2}$$

At the FC, three different FRs are considered, described in what follows.

LR rule:

LR rule is based on a complete knowledge of the channel envelop (h), the local performance indices (P_d, P_f), and the received decision (y). LR rule can be derived as [97]:

$$\delta^{LR} = \prod_{i=1}^{N} \frac{P_{di} e^{-\frac{(y_i - h_i)^2}{2\sigma_w^2}} + (1 - P_{di}) e^{-\frac{(y_i + h_i)^2}{2\sigma_w^2}}}{P_{fi} e^{-\frac{(y_i - h_i)^2}{2\sigma_w^2}} + (1 - P_{fi}) e^{-\frac{(y_i + h_i)^2}{2\sigma_w^2}}} \tag{11.3}$$

MRC rule:

In MRC rule, the global decision is issued by assuming a knowledge of the channel fading (h) and the received decisions (y) from the CUs. Notice that MRC does need the local performance indexes to obtain the global decision. The MRC is given as [97]:

$$\delta^{MRC} = \frac{1}{N} \sum_{i=1}^{N} h_i y_i \tag{11.4}$$

EGC rule:

Unlike the other rules, EGC need no knowledge of any information other than the received decisions (y). EGC rule is written as follows [97]:

$$\delta^{EGC} = \frac{1}{N}\sum_{i=1}^{N} y_i \tag{11.5}$$

For each FR, after calculating the corresponding δ , δ is compared to a predefined threshold (ζ) to obtain the global decision. Mathematically, the global decision (U) is computed as follows

$$U = \begin{cases} -1 & \text{if } \ \delta < \zeta \\ 1 & \text{if } \ \delta \geq \zeta \end{cases} \tag{11.6}$$

It worth noting that the threshold ζ is independent of the local detection threshold λ.

Notice that the assumed knowledge on some information in each rule is achievable by reporting it with the local decisions to the FC. However, this process consumes time, bandwidth and energy. Therefore, a fair comparison has to consider the amount of these prior information reported to the FC, and its effect on the overall performance of CSS.

11.3 Frame Structure and Energy Consumption

For a fair comparison among the three rules, and as they have different amount of prior information to be reported (which results in different performance in terms of detection probability and consumed energy), we propose to perform a fair comparison under a limited and fixed time frame duration. In this section, we discuss the limited time assumption in detail, and then quantify the consumed energy for each rule.

11.3.1 Limited Time Assumption:

Unlike state-of-the-art works, we assume that the total frame length is equal for all rules. This practical assumption gives all the rules the same time resources, which explicitly accounts for the difference in the amount of the required prior information, resulting in a fair comparison. The total frame (T) is divided into three sub-frames, namely; the sensing sub-frame (T_s), where the samples for spectrum sensing are collected; the reporting sub-frame (T_r), where local decisions and prior information are reported to the FC; and the transmission sub-frame (T_t), where data transmission starts if the channel is estimated to be available according to the outcome of the CSS, represented by (11.6). Our assumption implies an equal transmission sub-frame in all rules, and due to the different amounts of prior information among rules, the reporting sub-frame is different in each rule, and consequently, the sensing sub-frame is also variable among the rules.

The performance of the spectrum sensing depends on how many samples the users collect and how much information the users provide the FC. According to the limited time assumption, T_s and T_r are variable among the rules, which means different number of samples and different amount of information. While the prior information is predefined, T_r is easily calculated. The rest of the frame is equal to $T_s + T_t$. By subtracting the fixed amount T_t, the rest is T_s

, which can be used to compute the number of samples for each rule.

Assume the required bits to convey the local decision (u), the channel fading (h), and the performance indexes (P_d, P_f) are B_u, B_h and B_I respectively. Then the total required bits (B) to report all prior information for each rule can be computed as

$$B^{LR} = B_u + B_h + B_I \tag{11.7}$$

$$B^{MRC} = B_u + B_h \tag{11.8}$$

$$B^{EGC} = B_u \tag{11.9}$$

Notice that $B_u = 1$ because of using the hard scheme. It is clear that LR rule receives more prior information from the users, which improves its performance. However, this results in decreasing the number of samples, as we will see later, which negatively affects the achievable performance. T_r for all users is given as:

$$T_r = \frac{NB}{D} \tag{11.10}$$

where D is the reporting data rate. Notice that T_r is different for each rule due to the difference in B. Then, the number of samples per user S can be written as follows:

$$S = (T - T_t - NB/D)f_s \tag{11.11}$$

where f_s is the sampling frequency. Notice that the number of samples for a specific rule can be obtained by substituting the corresponding B for that rule. From the equations of the required bits and the available samples, a trade-off between the number of samples and the number of bits appears. This is due to the limited time assumption we consider in this chapter.

11.3.2 Consumed Energy Calculations:

By taking into account that the optimization of the FR to minimize the consumed energy in cognitive radio as the main goal of this chapter, in this section we present the necessary calculations to quantify the total energy consumption in each rule.

The consumed energy can be classified in three types, the consumed energy during sensing (E_s), during reporting (E_r), and during data transmission (E_t). Hence, the total consumed energy by all users, given in (6.9), is revised here:

$$E_{tot} = N\rho_s T_s + \rho_r T_r + P_1(1 - P_D)\rho_t T_t + P_0(1 - P_F)\rho_t T_t \tag{11.12}$$

Notice that E_s, E_r and E_t are computed by multiplying the time of each stage by the amount of power ρ_s, ρ_r and ρ_t for the three types respectively. Also, P_1 and P_0 are the probability of occupying the channel or not, respectively, where $P_0 + P_1 = 1$.

While the consumed energy during sensing and reporting always exists, the energy consumed during data transmission is conditioned by identifying the channel as free. The channel is identified as free in two cases, the missed detection and the non-false-alarm. Hence, the third and the fourth terms in (11.12) are multiplied by the probabilities of these two cases. As ($1 - P_D = P_{MD}$) and by assuming ρ_r and ρ_t are equal, (11.12) is simplified as follows:

$$E_{tot} = N\rho_s T_s + \rho_r(T_r + P_1 P_{MD} T_t) + P_0(1 - P_F)\rho_r T_t \tag{11.13}$$

By assuming E_0 is the energy consumed per unit time in transmission and reception, then ρ_s and ρ_r are given as:

$$\rho_s = xE_0 \tag{11.14}$$

$$\rho_r = (1-x)E_0 \tag{11.15}$$

where $0 < x < 1$ is the percentage of the power consumed in sensing per unit time to E_0. By using (15.31) and (11.15), (11.13) can be expressed as follows:

$$E_{tot} = xNE_0T_s + (1-x)E_0\bigg(T_r + T_t(1 - P_1P_D - P_0P_F)\bigg) \tag{11.16}$$

The normalized energy ($\frac{E_{tot}}{E_0}$) can be derived from (11.16) as follows:

$$E_N = xNT_s + (1-x)\bigg(T_r + T_t(1 - P_1P_D - P_0P_F)\bigg) \tag{11.17}$$

Eqn.(11.17) represents the normalized consumed energy per user during the cognitive transmission. For a specific rule, E_N can be obtained by substituting in (11.17) the corresponding parameters T_s, T_r and P_M.

We are interested in the consumed energy per bit. Therefore, we define the throughput in bits as the total number of bits has been successfully transmitted from all the users during T_t, given in (6.13). Using (6.13) and (11.17), we can write the normalized Energy per Bit (EpB) as follows:

$$EpB = \frac{xNT_s + (1-x)\bigg(T_r + T_t(1 - P_1P_D - P_0P_F)\bigg)}{RP_0T_t(1-P_F)} \tag{11.18}$$

11.4 Simulation and Evaluation

In this section we present the simulation results of the comparison of the three decision-fusion rules. The results show the performance of the rules in terms of achievable detection probability and consumed energy at a given false alarm probability (P_F^{th}). The simulation parameters are shown in Table 11.1. From the stated equations and the simulation results, it seems that the superiority of a rule among the others, either in P_D or E, depends mainly on three factors, namely, frame length (T), number of users (N), and the SNR. Next, we discuss the effects of these factors on the energy consumption and detection probability of the three considered decision rules.

11.4.1 Frame Length (T):

To show the effect of increasing the time resources on the achievable detection probability, we plot Figure 11.1. Remember that the detection probability is independent of the transmission time T_t, therefore, we plot the detection probability versus the sum of sensing and reporting sub-frames ($T_s + T_r$). For low values of ($T_s + T_r$), the difference in the number of samples is more effective than the difference in the amount of prior information, and hence, EGC achieves higher detection probability than LR and MRC. As ($T_s + T_r$) increases, the effect of the difference in the collected samples among the rules gets lower compared to the effect of difference in the amount of prior information, which yields in a higher detection probability for LR. Figure 11.2 is developed to show the normalized energy consumption per bit (EpB) for the three rules versus the total frame time (T). As expected, the rule with the highest detection probability is the most energy efficient rule, as shown in the figure. Hence, EGC consumes less energy

Table 11.1: Simulation Parameters

Parameter	Value	Parameter	value
P_0	0.5	σ_x^2/σ_n^2	-7 dB
B_u	1 bit	B_I	8 bits
B_h	4 bits	F_s	$1KHz$
D	$10Kbps$	P_F^{th}	0.1
R	$100Kbps$	x	0.1

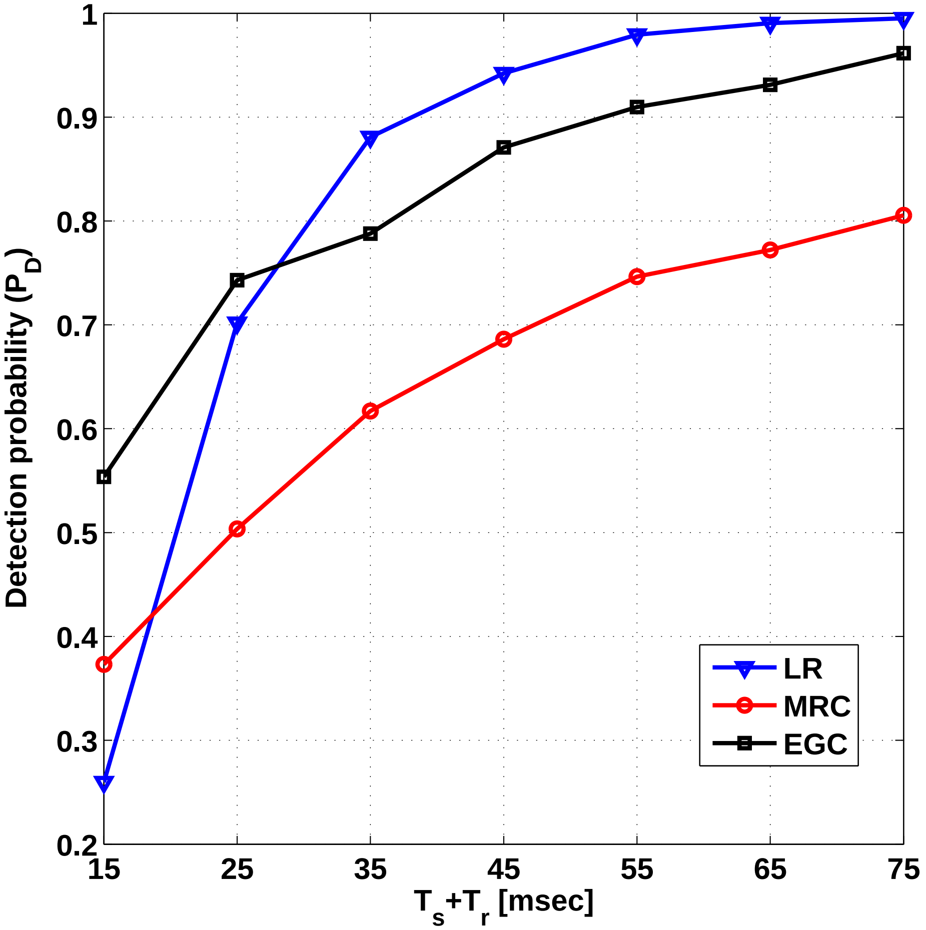


Figure 11.1: *The detection probability versus sensing and reporting time for all rules. ($N = 10$, $SNR = 7dB$)*

than the other rules for short frames, while, for long frames, the LR is the most energy efficient rule.

11.4.2 Number of Users (N):

The detection probability and the normalized energy consumption versus the number of users for all rules are shown in Figure 11.3 and Figure 11.4 respectively. For small number of users, LR rule achieves the highest detection prob-

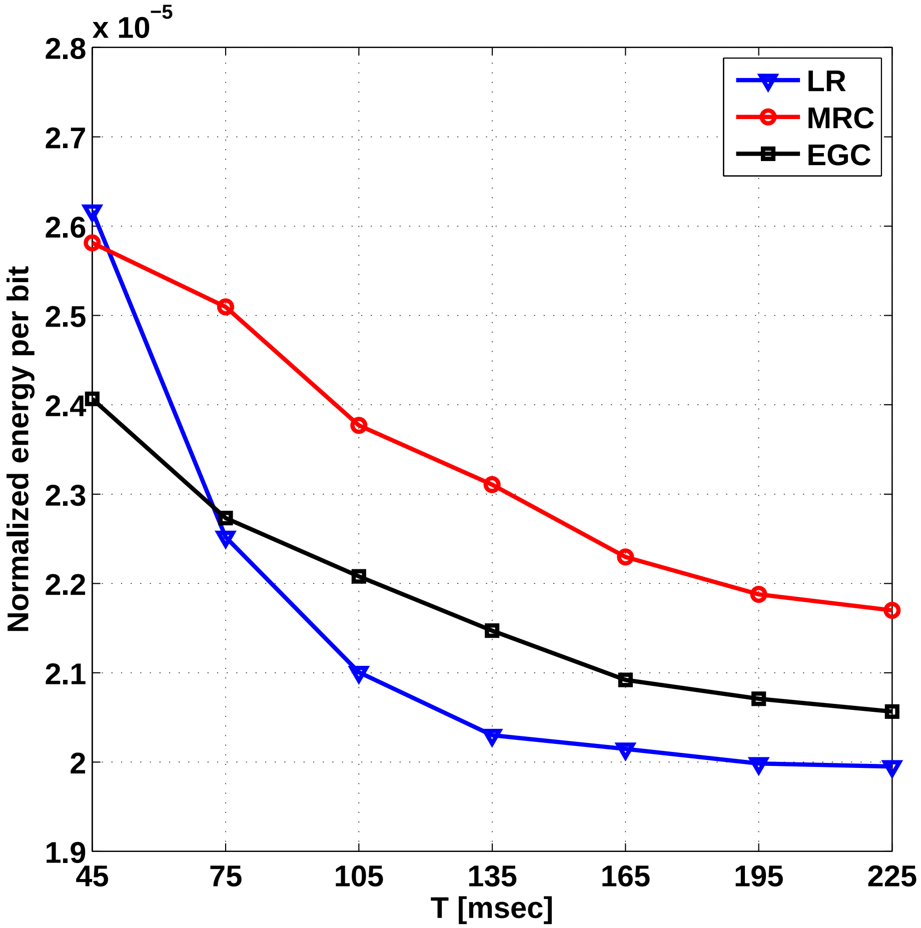


Figure 11.2: *The normalized consumed energy per bit versus the frame length for all rules. ($N = 10$, $SNR = 7dB$)*

ability. While, for large number of users, the detection probability achievable by EGC is the highest. This can be justified as follows, as the number of users increases, T_r increases, according to (7.1), resulting in less T_s, and consequently, less number of samples. As LR rule has the longest T_r, due to the large prior information, the detection probability of LR rule is negatively affected more than the other rules by increasing the number of users, as shown in Figure 11.3. Regarding the consumed energy, Figure 11.4 confirms the conclusions from the last subsection, the rule with highest detection probability at a given number of users is the most energy efficient rule. Even though more energy is consumed due to the large number of users, the amount of successfully transmitted data

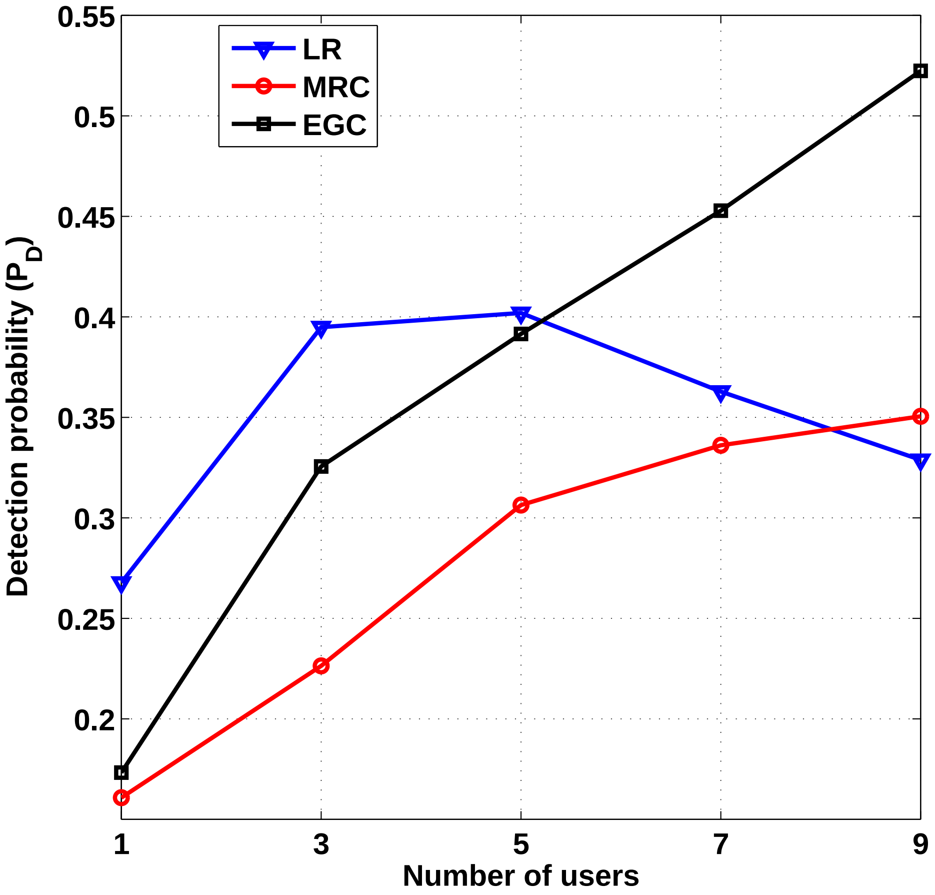


Figure 11.3: *The detection probability versus the number of users for all rules. ($T = 45msec$, $SNR = 7dB$)*

increases, which improves the energy efficiency.

11.4.3 The Signal-to-Noise-Ratio (SNR):

The SNR is an important parameter in optimizing the decision-fusion rule in terms of the detection probability or the consumed energy. Fig. 11.5 represents the achievable detection probability for all rules versus the SNR. At low SNR range, EGC has a better performance than the others, while, as SNR increases, the LR rule starts outperforming the other rules. Notice that, at low SNR val-

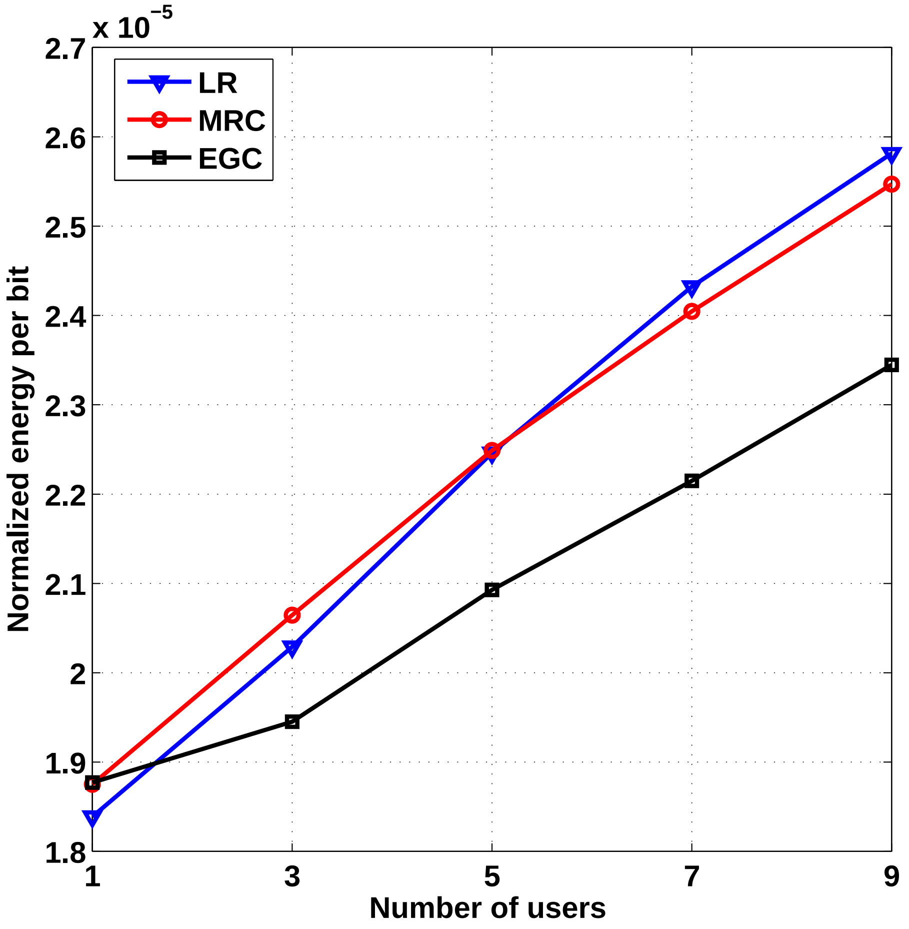


Figure 11.4: *The normalized consumed energy versus the number of users for all rules. ($T = 45msec$, $SNR = 7dB$)*

ues, the samples are almost similar due to the large noise signal affecting the reported decisions, which amplifies the effect of the difference in the number of collected samples, and as EGC has the largest number of samples, this implies the highest detection probability. Figure 11.6 represents the normalized consumed energy per bit versus the SNR for all rules. The rule with highest P_D is the most power efficient also in this case, where EGC consumes less energy at the low SNR range. From this discussion about the effect of the three factors, the simulation results indicate that EGC has the best performance at critical conditions. These critical conditions, which are most of the time encoun-

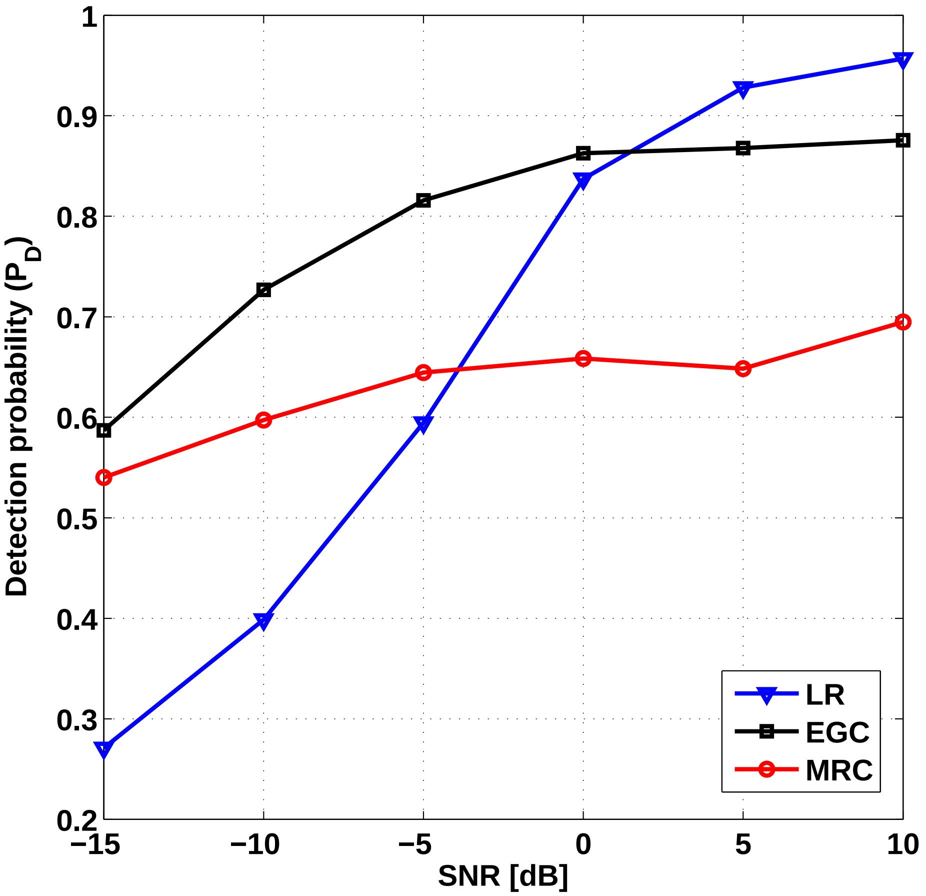


Figure 11.5: *The detection probability versus the average SNR for all rules.(*$T = 135msec$*,* $N = 10$*)*

tered in practical situations, are represented by short frames, large number of users and low SNR values.

11.5 Summary

An energy consumption analysis for three decision-fusion rules , LR, EGC and MRC, has been presented in this chapter. The chapter includes a comparison among the three FRs in terms of the achievable detection probability and energy consumption. The comparison is based on the limited time assumption, where

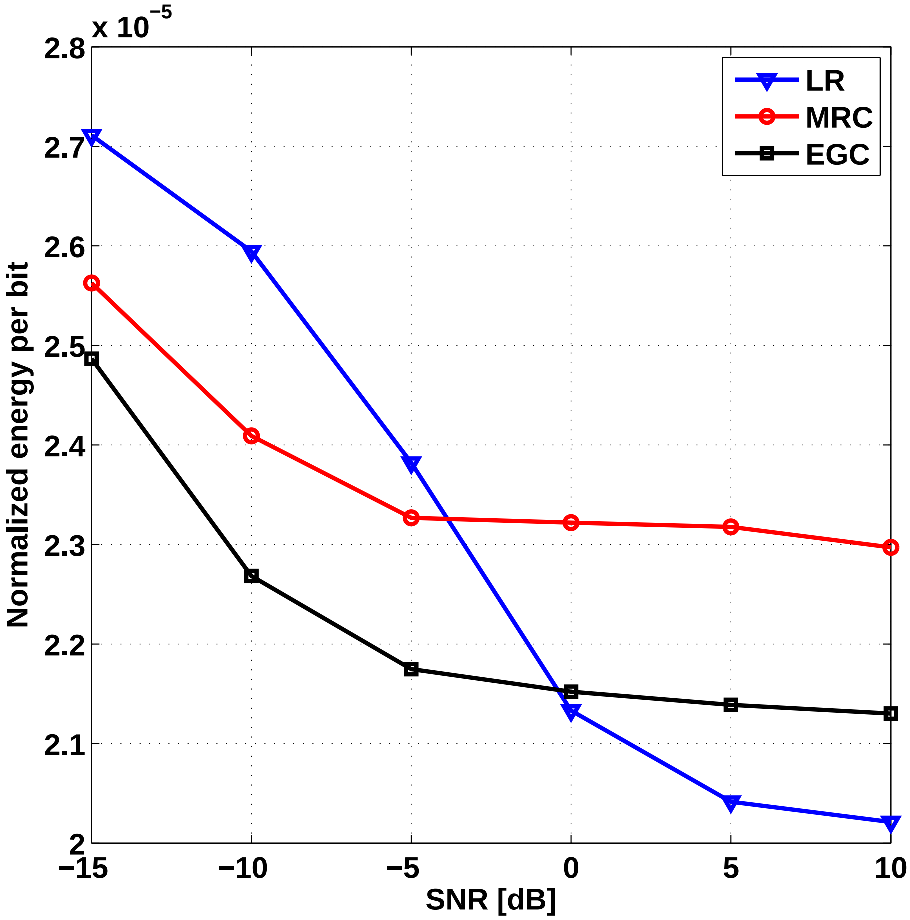


Figure 11.6: *The normalized consumed energy versus the average SNR for all rules.($T = 135msec$, $N = 10$)*

the time resources are equal and limited for all rules. The results show that EGC rule outperforms the other rules, either in detection probability or energy efficiency, in critical conditions. The critical conditions are represented by short frames, large number of users and low SNR values.

CHAPTER 12

OPTIMIZING THE *K-OUT-OF-N* FUSION RULE FOR COOPERATIVE SPECTRUM SENSING

12.1 Introduction

The general FR for hard-based CSS is called *K-out-of-N* rule [104], where N is the total number of reported local decisions, while K is a predefined threshold on the number of local decisions that identify the spectrum as used. Several authors have investigated the optimization of several parameters of the *K-out-of-N* rule aiming at different objectives. For example, in [105] the number of cooperative users (N), the FR (K), and the energy detection threshold are all optimized individually in order to minimize the error rate, while in [45], K is optimized for throughput maximization. The authors of [52], optimize N for two different setups, energy efficient setup and throughput maximization setup. In [106], K is optimized for throughput maximization and detection probability maximization. Also, K is optimized in [107] to minimize the erroneous decision probability.

However, optimizing the FR for throughput maximization can result in high energy consumption. Also, considering the minimization of energy consumption as an objective for optimizing the parameters of the FR will degrade the throughput. Therefore, in this chapter, the energy efficiency is chosen as an objective for optimizing the *K-out-of-N* rule, which represents the first effort in this direction to the best of our knowledge. The main benefit of using energy efficiency as an objective is to achieve the balance between the throughput and energy consumption since the energy efficiency is defined as the ratio between the achievable throughput to the consumed energy. However, to avoid a large interference at the licensed users, a constraint is put on the resulting missed detection probability so that the interference is kept within the acceptable range.

In this chapter, the achievable energy efficiency is compared between the false-decision minimization and energy efficiency maximization setups when both satisfy a specific missed detection probability. The results show that energy efficiency setup can achieve a better performance than the false decision minimization setup in terms of the achievable energy efficiency and resulting missed detection probability.

12.2 System Model

Consider a CRN of N CUs. The employed method for spectrum sensing is energy detection method, and the hard-based reporting scheme is considered. The local performance of each CU is measured by the local detection probability (P_{di}) and the local false-alarm probability (P_{fi}). For simplicity, we assume an identical performance among the CUs, and hence, $P_{d1} = P_{d2} = ... = P_d$ and $P_{f1} = P_{f2} = ... = P_f$.

The reporting channel between any CU and the FC is assumed to be noisy [108], and modeled as binary symmetric channel with error probability P_e, and it is identical among all CUs. At the FC, a specific FR is employed to process these received decisions in order to make the global decision. The general FR is *K-out-of-N* rule, where K is predefined integer (($1 \leq K \leq N$)), and N is the total number of received decisions to be processed. The idea behind this rule is to compare the number of CUs whose local decisions have been received as 1 to K. If it is larger than or equal K, then the spectrum is used. Otherwise, the spectrum is unused. After issuing the global decision, if it is *"unused"*, a CU will be scheduled for data transmission. Otherwise, the spectrum will not be used by any CU.

The overall performance of CSS can be evaluated by two indicators, the overall detection probability (P_D) and the overall false-alarm probability (P_F). Considering noisy reporting channels, P_D and P_F, which are given in (8.13) and (8.14), can be rewritten respectively as follows:

$$P_D = \sum_{i=K}^{N} \binom{N}{i} P_x^i (1 - P_x)^{N-i} \tag{12.1}$$

$$P_F = \sum_{i=K}^{N} \binom{N}{i} P_y^i (1 - P_y)^{N-i} \tag{12.2}$$

where P_x is the probability of receiving a local decision of "1" when the spectrum is used, and P_y is the probability of receiving a local decision of "1" when the spectrum is unused. Both P_x and P_y can be given respectively as follows

$$P_x = P_d(1 - P_e) + (1 - P_d)P_e \tag{12.3}$$

$$P_y = P_f(1 - P_e) + (1 - P_f)P_e \tag{12.4}$$

However, in order to evaluate the detection accuracy of CSS in one metric, both P_D and P_F are combined to define the probability of false global decision, denoted by ϵ, which is defined as follows

$$\epsilon = P_0 P_F + P_1(1 - P_D) \tag{12.5}$$

where P_1 is the probability of the spectrum being used by a licensed user ($P_1 = 1 - P_0$).

The energy efficiency (μ) of a CRN is also used as an indicator of the overall performance of the CRN. Energy efficiency is given as follows

$$\mu = \frac{P_0(1-P_F)RT_t}{NE_{css} + (1 - P_0P_F - P_1P_D)E_t} \tag{12.6}$$

where E_{css} the energy consumed during CSS by a CU, and E_t is the consumed energy during data transmission.

12.3 Optimizing the Fusion Rule Parameters (K and N)

Both parameters of the *K-out-of-N* rule, K and N, have an effect on the overall achievable detection accuracy of CSS, which directly affects the other performance metrics of the cognitive transmission, such as false-decision probability, achievable throughput, energy consumption, and energy efficiency. Therefore, K and N should be optimized in order to achieve the best achievable performance. In this section, we discuss the optimal K and N for different setups.

12.3.1 Minimizing the False-Decision Probability (ϵ)

The false decision probability is divided into two terms, as indicated in (12.5), the first term refers to the false alarm probability (P_F), while the second refers to the missed detection probability ($1-P_D$). For a fixed N, large values of K results in less false alarm probability which decreases ϵ. On the other hand, this leads to higher missed detection probability, and consequently, higher ϵ. Therefore, K should be optimized in order to minimize the overall false decision probability. However, minimizing the false-decision probability without a constraint on the missed detection probability may lead to a high interference at the licensed user. Thus, we optimize K and N for the minimum ϵ while guaranteeing an upper bound of missed detection, denoted by ζ.

The optimization of K to minimize the false decision probability with a constraint on the missed detection probability can be expressed as follows

$$\min_K \epsilon \equiv \min_K P_0 P_F + P_1(1 - P_D) \tag{12.7}$$

subject to

$$1 - P_D \leq \zeta \tag{12.8}$$

The K value that satisfies (12.7) without the constraint is obtained by equating the derivative of ϵ to zero, as follows

$$P_0 \frac{\partial P_F}{\partial K} - P_1 \frac{\partial P_D}{\partial K} = 0 \tag{12.9}$$

The derivatives of P_F and P_D can be computed approximately as follows

$$\frac{\partial P_F}{\partial K} = P_F(K+1) - P_F(K) = \binom{N}{K})P_y^K(1-P_y)^{N-K} \tag{12.10}$$

$$\frac{\partial P_D}{\partial K} = P_D(K+1) - P_D(K) = \binom{N}{K}P_x^K(1-P_x)^{N-K} \tag{12.11}$$

by substituting (12.10) and (12.11) in (16.40), and after some mathematical manipulations, the optimal K that minimizes the false decision probability without satisfying the constraint is given in a closed form expression as follows

$$K_1 = \frac{\ln \frac{P_0}{P_1} + N \ln(\frac{1-P_y}{1-P_x})}{\ln(\frac{P_x(1-P_y)}{P_y(1-P_x)})} \tag{12.12}$$

Notice that a similar formula has been reported in [105] without considering the prior knowledge about the activity of the licensed users, i.e. $P_0 = P_1 = 0.5$.

According to (12.12), for a given N, the optimal K that minimizes ϵ while satisfying the constraint on the missed detection probability is expressed as follows

$$K^{opt\epsilon} = min\{K_1, K_2\} \tag{12.13}$$

where K_2 is the value that satisfies the constraint on the missed detection probability given in (12.8). The closed-form expression of K_2 is difficult to be computed. Thus, an approximated expression is proposed in this chapter. To this end, we use the Demoiver-Laplace theorem [109] which approximates the binomial distribution with a normal distribution. Accordingly, P_D, given in (12.1), can be expressed as

$$P_D \approx Q\left(\frac{K - 0.5 - NP_x}{\sqrt{NP_x(1 - P_X)}}\right) \tag{12.14}$$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-u^2/2} \cdot du$. By substituting (12.14) in the constraint in (12.8), K_2 can be written as[1]

$$K_2 \approx Q^{-1}(1 - \zeta)\sqrt{NP_x(1 - P_X)} + NP_x + 0.5 \tag{12.15}$$

where $Q^{-1}(x)$ is the inverse function of $Q(x)$.

Also, for a given K, as the number of processed decisions (N) increases, P_F increases and P_{MD} decreases. Thus, these two contrasting effects should be balanced by optimizing N for the minimum false decision probability. The optimization of N to minimize the false decision probability with a constraint on the missed detection probability can be expressed as follows

$$\min_N \epsilon \equiv \min_N P_0 P_F + P_1(1 - P_D) \tag{12.16}$$

subject to

$$1 - P_D \leq \zeta \tag{12.17}$$

[1] This formula is accurate only if N is very large. For further information the reader is kindly referred to [109]

Assume N_1 is the value that solves the minimization problem without considering the constraint. Then, N_1 is obtained by equating the derivative of ϵ to zero, as follows

$$P_0 \frac{\partial P_F}{\partial N} - P_1 \frac{\partial P_D}{\partial N} = 0 \tag{12.18}$$

However, (16.41) is a transcendental equation, and it is too hard to obtain a closed form expression of the optimal N for any value of K. However, we can solve the optimization problem for two popular FRs as special cases, i.e., the OR-rule ($K = 1$) and the AND-rule ($K = N$), as follows:

$$N_1^{or} = \frac{\ln \frac{P_1}{P_0} + \ln \left(\frac{\ln(1-P_x)}{\ln(1-P_y)} \right)}{\ln (\frac{1-P_y}{1-P_x})} \tag{12.19}$$

$$N_1^{and} = \frac{\ln \frac{P_1}{P_0} + \ln \left(\frac{\ln(P_x)}{\ln(P_y)} \right)}{\ln (\frac{P_y}{P_x})} \tag{12.20}$$

For arbitrary FRs, however, an approximated solution for N_1 that minimizes ϵ can be derived from (12.12). The approximation is based on the fact that the optimal N is the value that makes K optimal as given in (12.12). Mathematically, N_1 is approximately given as:

$$N_1 \approx \frac{\ln \frac{P_1}{P_0} + K \ln \left(\frac{P_x(1-P_y)}{P_y(1-P_x)} \right)}{\ln (\frac{1-P_y}{1-P_x})} \tag{12.21}$$

By considering the constraint on the missed detection probability, the optimal N that minimizes ϵ and keeps the missed detection probability less than ζ is given as

$$N^{opt\epsilon} = max\{N_1, N_2\} \tag{12.22}$$

where N_2 is the value that satisfies the constraint. Using again the Demoiver-Laplace theorem, an approximated expression of N_2 can be computed as follows

$$\begin{aligned} N_2 \quad \approx \quad & \tfrac{2K+Q^{-1}(1-\zeta)}{2P_x} \\ + \quad & 0.5\sqrt{\left(\tfrac{2K+Q^{-1}(1-P_x)}{P_x}\right)^2 - 4\tfrac{K^2-K+0.25}{P_x}} \end{aligned} \tag{12.23}$$

12.3.2 Maximizing the Energy Efficiency

The maximum achievable throughput occurs at the minimum P_F, as indicated in (6.13). According to (6.9) and (5.2), low P_F increases energy consumption. Therefore, optimizing the parameters of the FR for the maximum throughput results in high energy consumption, leading to poor energy efficiency. On the other hand, optimizing the parameters of the FR for the minimum energy consumption degrades the achievable throughput, and consequently, leads to poor energy efficiency. However, in order to achieve a good trade-off between these contrasting objectives, and since energy efficiency combines the two performance metrics, throughput and energy consumption, it is more convenient to optimize the parameters of the FR for the maximum energy efficiency.

Furthermore, another important aspect that should be taken into account for the optimization of the *K-out-of-N* rule is the resultant interference at the licensed user caused by the missed detection during CSS. This effect can be controlled by introducing a constraint on the missed detection probability, so that the interference can be kept below an acceptable threshold.

Optimizing K for maximum energy efficiency and a constraint on the missed detection probability can be stated as follows

$$\max_{K} \mu \equiv \max_{K} \frac{P_0(1-P_F)RT_t}{NE_{css}+(1-P_0P_F-P_1P_D)E_t} \tag{12.24}$$

subject to

$$1-P_D \leq \zeta \tag{12.25}$$

The solution of (12.24) (without considering the constraint) cannot be derived in closed form. Thus, by applying similar methods used to derive (12.12), we write the sufficient condition that should be satisfied by the optimal K (without constraint) as follows

$$K_3 = \frac{\ln\left(\frac{NE_{css}+P_1E_t(1-P_D)}{P_1E_t(1-P_F)}\right) + N\ln(\frac{1-P_y}{1-P_x})}{\ln(\frac{P_x(1-P_y)}{P_y(1-P_x)})} \tag{12.26}$$

Then, since the missed detection probability increases as K increases for a given N, the optimal K that maximizes the energy efficiency while fulfilling the missed detection requirement is given as follows:

$$K^{opt\mu} = min\{K_3, K_2\} \tag{12.27}$$

where K_2 the value of the K that satisfies the constraint on missed detection, approximated in the previous section using Demoiver-Laplace theorem in (12.15)
.

The optimization of N in order to maximize the energy efficiency can be formulated similar to (12.24) by replacing K with N, as follows

$$\max_N \mu \equiv \max_N \frac{P_0(1-P_F)RT_t}{NE_{css} + (1-P_0P_F - P_1P_D)E_t} \tag{12.28}$$

subject to

$$1 - P_D \leq \zeta \tag{12.29}$$

However, it is very difficult to obtain the optimal N for the general *K-out-of-N* rule. Hence, we apply the same approximation used to find the optimal N that minimizes ϵ in (12.21). The approximation is based on the fact that the optimal N is the value that makes K optimal. Therefore, the solution of (12.28) (without considering the constraint) can be given be solving (12.26) for N, as follows

$$N_3 \approx \frac{\ln\left(\frac{P_1E_t(1-P_F)}{N_3E_{css}+P_1E_t(1-P_D)}\right) - K\ln(\frac{P_y(1-P_x)}{P_x(1-P_y)})}{\ln(\frac{1-P_y}{1-P_x})} \tag{12.30}$$

By considering the constraint on the missed detection, and since the missed detection decreases as N increases for a given N, the optimal N that solves (12.28) for the maximum energy efficiency while keeping the missed detection under the maximum allowed bound is expressed as follows

$$N^{opt\mu} = max\{N_3, N_2\} \tag{12.31}$$

where N_2 is the value that satisfies the required missed detection probability, approximated in the previous section using the Demoiver-Laplace theorem in (12.23).

12.4 simulation results

A CRN consisting N_T CUs is assumed. The parameters regarding the local performance, energy consumption, reporting channel, data rate and transmission time are all summarized in Table 12.1. These parameters are assumed identical among all CUs.

Table 12.1: Simulation Parameters

Parameter	Value	Parameter	value
N_T	10	P_d	0.7
P_f	0.2	P_e	0.1
E_t	1 Joule	E_{css}	12 mJoule
R	$100Kbps$	T_t	0.3 sec

The false-decision probability versus K for different values of N is shown in Fig. 12.1. It is clearly shown that for any value of N, ϵ is a convex function of K, and thus, a minimum exists. This behavior is common for all curves, and can be interpreted as follows. Increasing K reduces P_F and P_D. This creates two contrasting effects on ϵ, ϵ decreases as P_F decreases , and, at the same time, ϵ increases as P_D decreases. The two effects are balanced at the optimal K value, yielding the minimum ϵ.

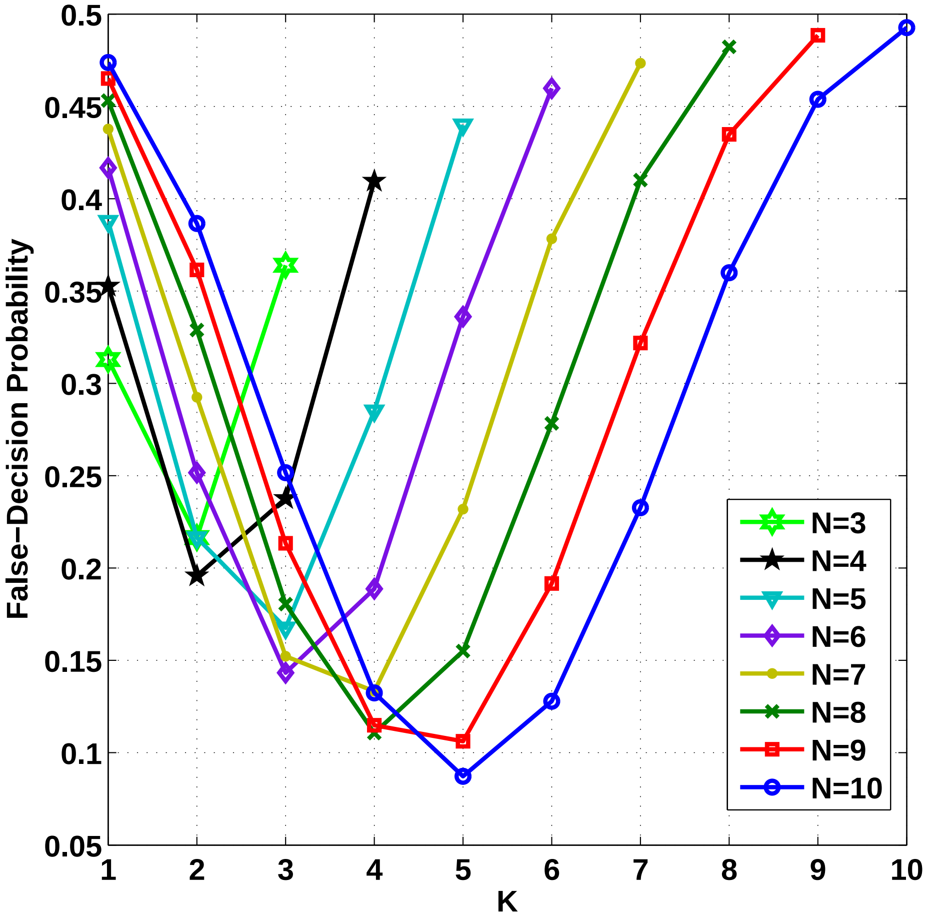


Figure 12.1: *The average false-decision probability (ϵ) of versus the threshold K for different values of N. The solid lines represent the simulation results, while the markers represent the analytical results.*

Another result can be observed in Fig. 12.1 is that for a given K, the optimal N that minimizes the false-decision probability is the value that makes the corresponding K optimal among all other K. For example, if $K = 2$, the optimal

N is at $N = 4$, and at the same time, for $N = 4$, the optimal K is 2. This observation confirms our approximated formula of the optimal N for minimizing false-decision probability given in (12.22).

Regarding the achievable energy efficiency, it is plotted in Fig. 12.2 for different pairs of (K, N). Approximately, μ has the same behavior of ϵ as in Fig. 12.1. However, for a given N, the value of K that maximizes μ is less than the value of K that minimizes ϵ by one in most cases. Also, Fig. 12.2 confirms the accuracy of the approximated formula given in (12.21), where it gives the optimal N, for a given K, as the value of N that makes K optimal, which is clearly proved by the results in Fig. 12.2.

Although the results in Fig 12.1 and Fig. 12.2 show the same behavior as K or N vary, the optimum values of μ and ϵ occur at different values for both setups. In Fig. 12.1, the minimum ϵ occurs at $N = 10$ and $K = 5$, while the maximum μ is achieved at $N = 3$ and $K = 1$, as shown in Fig. 12.2.

For the purpose of showing the importance of optimizing K and N for energy efficiency maximization on the overall system performance, we consider two scenarios as follows

- **Scenario 1**: where we use the optimal values of K and N that maximize the energy efficiency with a constraint on the missed detection probability.
- **Scenario 2**: where we use the optimal values of K and N that minimize the false-decision probability with a constraint on the missed detection probability.

Fig. 12.3 shows the achievable energy efficiency in both scenarios as a func-

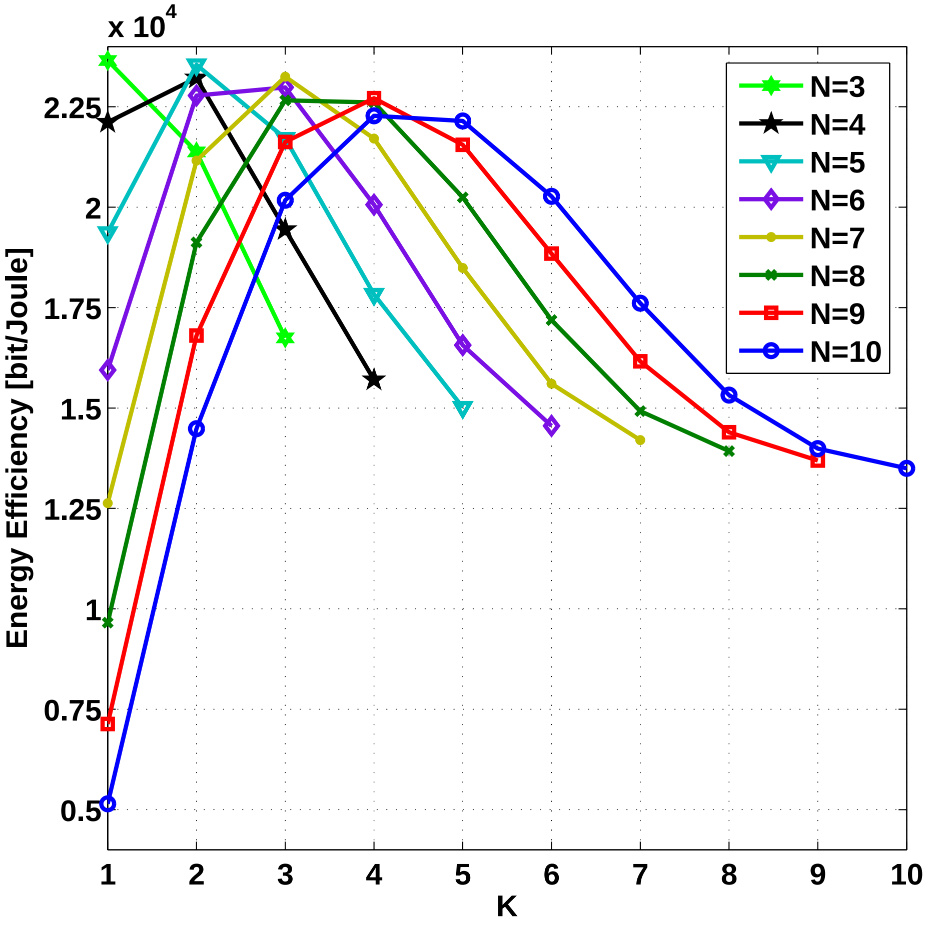


Figure 12.2: *The average energy efficiency (μ) of versus the threshold K for different values of N. The solid lines represent the simulation results, while the markers represent the analytical results.*

tion of the constraint on the missed detection probability (ζ) for a total number of CUs equals to 15. It is clearly shown that **Scenario 1** provides better energy efficiency than **Scenario 2** while keeping the missed detection probability below the acceptable value. The difference in energy efficiency increases as the acceptable missed detection probability (constraint) increases. Therefore, this comparison confirms that the K-out-of-N rule should be optimized for maximizing energy efficiency as in **Scenario 1**, which improves the overall network performance and, at the same time, limits the resultant interference at the licensed users caused by the missed detection.

In Fig. 12.4 both scenarios are compared in terms of the achievable energy efficiency versus the total number of CUs for a missed detection probability equals to 5%. Also in this case, **Scenario 1** achieves better energy efficiency than **Scenario 2**, and the difference between them increases as the N_T increases.

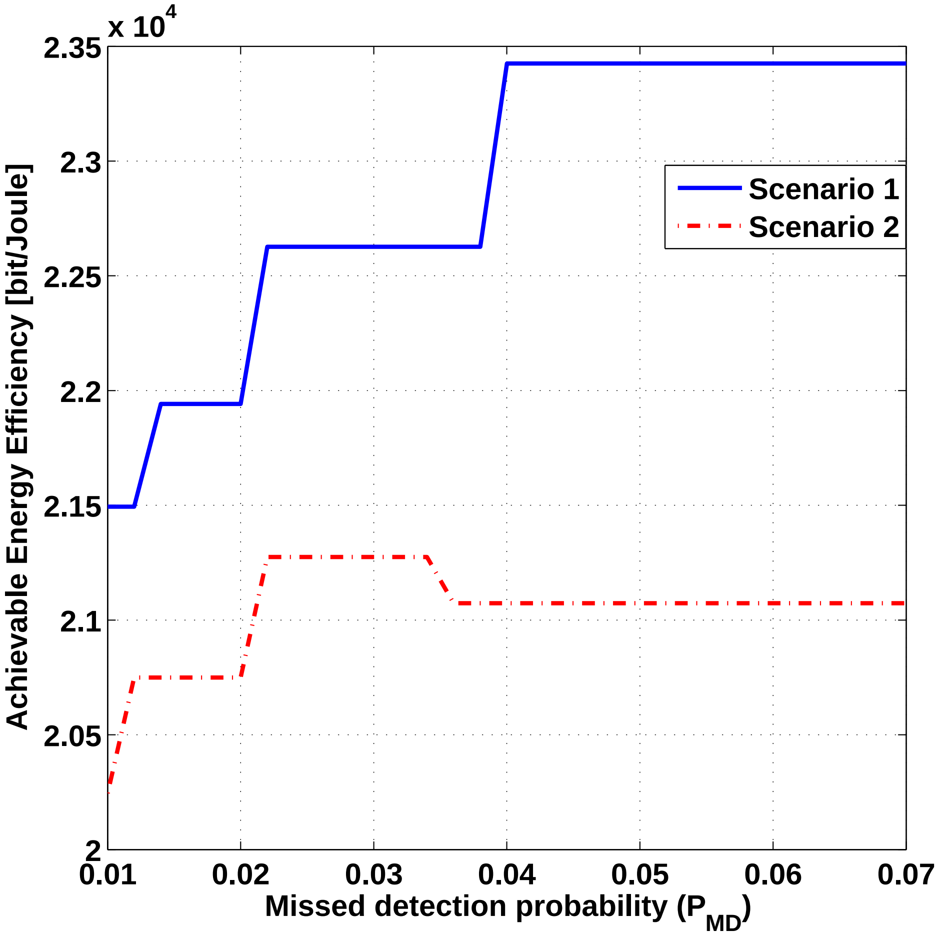


Figure 12.3: *The achievable energy efficiency versus the average missed detection probability for both **Scenario 1** (maximizing energy efficiency) and **Scenario 2** (minimizing false-decision probability). The total number of CUs is* 15.

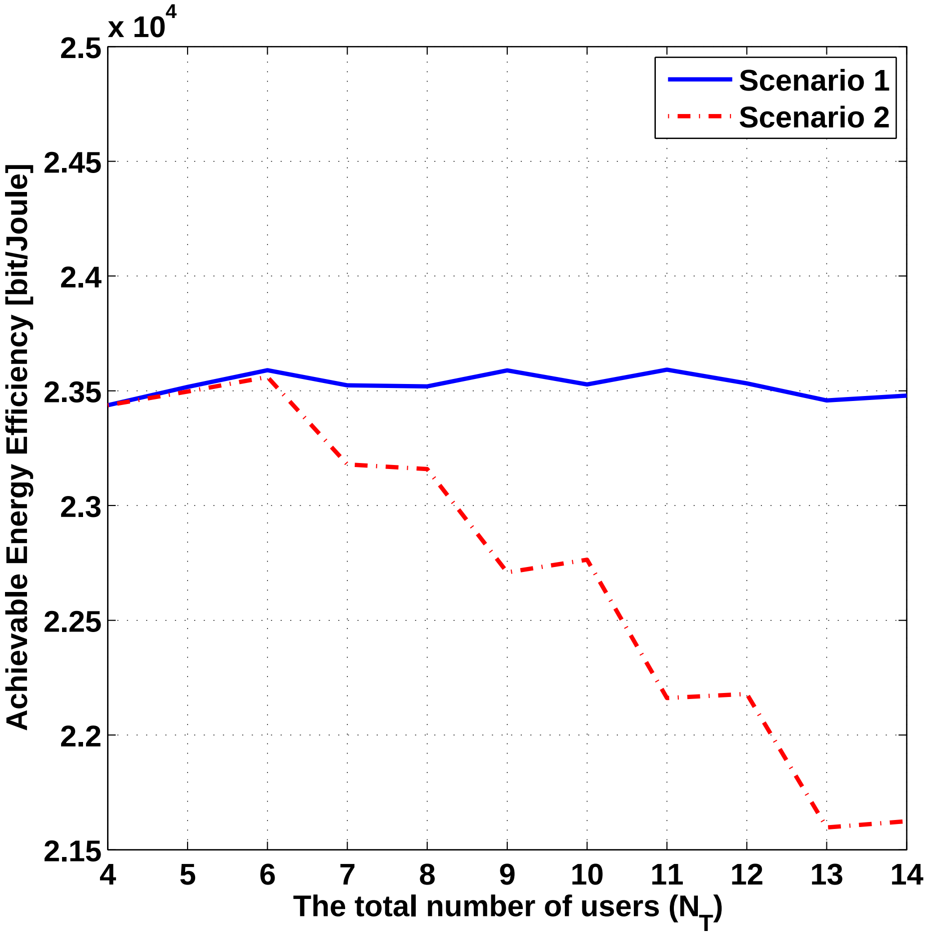


Figure 12.4: *The achievable energy efficiency versus the total number of CUs for both* ***Scenario 1*** *(maximizing energy efficiency) and* ***Scenario 2*** *(minimizing false-decision probability). The constraint on the average missed detection probability is* 5%.

12.5 Summary

In this chapter, we have optimized the *K-out-of-N* fusion rule in cooperative spectrum sensing for two different setups: maximizing the energy efficiency and minimizing the false decision probability. The optimization in both setups is performed with a constraint on the missed detection probability. Closed form expressions for N and K in both setups are provided. The results have shown that energy efficiency maximization setup significantly improves the network performance in terms of the achievable energy efficiency and the resulting interference.

Part V

The Trade-off Between Energy Efficiency and Security in Cooperative Spectrum Sensing

CHAPTER 13

AN INTRODUCTION TO SPECTRUM SENSING DATA FALSIFICATION ATTACK

Although CSS improves the reliability of spectrum sensing process, it introduces several challenges to CRNs. Beside the extra consumed energy resources, the security risks pose a significant challenge for CSS process [110] [111]. Due to the limited resources given for overhead exchange to the FC, applying typical security protocols against outsider attackers becomes infeasible. Moreover, it is possible to have insider malicious users that act as attackers based on different motivations. Thus, CSS is highly vulnerable for security attackers, which threatens the overall performance of the CSS process [112].

A popular attack is represented by reporting false data about the spectrum status in order to mislead the global decision of the CRN. In the case of making a false global decision about an unused spectrum, it gives the chance to the attacker to access the spectrum alone, whereas, in the case of making a false global decision about a used spectrum, a legitimate CU, also called honest CU, will lose its resources without throughput revenue, and more importantly, a severe interference to the licensed users. Notice that the former case causes inefficient exploitation of the unused spectrum, while the latter cases results in energy waste. Therefore, attackers have a relevant effect on the decision reliability as well as users' resources (including consumed energy and achievable throughput).

The attack in which a false information is reported is called Spectrum Sensing Data Falsification (SSDF) [110]. There are several types of SSDF attack, classified based on the employed strategy in reporting the false sensing data, as follows

1. Always-Yes Attacker (Greedy Attacker): this type of attackers always informs the FC that the spectrum is used regardless of its actual sensing result. The motivation of Always-Yes attacker is to prevent other CUs from accessing the spectrum, which gives him the chance to use the spectrum alone. Thus, it is usually called Greedy attacker [113].
2. Always-No Attacker: this type of attackers always informs the FC that the spectrum is unused regardless of its actual sensing result. The motivation behind such strategy is to degrade the performance of the CRN and the licensed users as well. An example of this attacker is Denial-of-Service (DoS) attack [114]
3. Malicious Attacker: A smarter attacker than the previous types is the malicious attacker. The malicious attacker builds his false report based on its sensing result, where it usually reports the opposite of its local sensing decision. Such a misbehaving might be conducted constantly or selectively. The motivation of this attacker can be a combination of the motivations of greedy and DoS attackers.

However, some honest (non-attacker) CUs may appear like attackers because of their bad sensing performance caused by either shadowing and fading, noisy reporting channel or malfunctioning sensor [69]. Such type of CUs is called unintentional attacker [115]. Nevertheless, both intentional and unintentional attackers degrade the detection accuracy, which, in turn, influences throughput and energy efficiency of the other honest CUs. Therefore, it is of a paramount importance to eliminate these attackers from the network.

The two well-known approaches, Bayesian detection [116] and Neyman-Person test [117], for signal detection are no longer optimal in the presence of SSDF attack [113]. In addition, both approaches require a prior knowledge about the local sensing performance. Several works have investigated the defense against SSDF attack. For example, [118] proposes an algorithm to identify attackers by counting the number of mismatches between each CU's local decisions and the global decision at the FC. Once, the number of mismatches exceeds a given threshold, the corresponding CU will be considered an attacker, and thus, its reports will be ignored. This approach however becomes unreliable when the the number of attackers is large giving an unreliable global decision. A detection scheme is proposed in [119], where it calculates a trust value as well as a consistency value for each CU based on its past reports. Once both values fall below predefined thresholds, the received reports from the corresponding CU are no longer considered in the fusion process. However, the algorithm is valid only for one attacker. In [120] the authors propose to correlate the received reports (spectrum sensing data) with the channel fading characteristics of the authenticated users, in such a way that reports from not authenticated users are filtered out. In [121] authors propose to compare every report with the rest by using uncertainty reasoning. A similarity degree is given to each report based on such a comparison, and reports are weighted according to their degree. In [122] a probabilistic model is used to detect the change in the behavior of a node and assign reputation to the nodes; the reputation is then used to weight the node's reports. A punishment policy for attackers is presented in [123] that can effectively prevent users from behaving maliciously.

This part of the dissertation is dedicating for combating against SSDF attackers. To this end, three independent works are proposed in this part. The first work is a weighted CSS algorithm that is able to totally eliminate the affects of the attackers, while the second work presents a detection and punishment polices for attackers. The third work represents a novel low-overhead security protocol for CSS against outsider attackers.

CHAPTER 14

ROBUST ALGORITHM AGAINST SPECTRUM SENSING DATA FALSIFICATION ATTACK IN COGNITIVE RADIO NETWORKS

14.1 Introduction

In this chapter a novel robust algorithm against SSDF attack is presented. The proposed algorithm is based on setting some evaluation frames by which the FC can assess the performance of each CU, and consequently, assigns a proper weight. In an evaluation frame, the target spectrum is used regardless of the local results reported by the CUs. As a consequence, a CU will be scheduled for data transmission in each evaluation frame. According to the success delivering of the transmitted data by the scheduled CU, the FC will be able to identify the actual spectrum status. In other words, if the scheduled CU successfully delivers its transmitted data, the spectrum is unoccupied. Thus, the FC will assess the local results that have been reported during that frame, and consequently, a proper weight related to the actual performance will be assigned for each CU. The most interesting thing is that the proposed algorithm is able to convert SSDF attackers to honest CUs, which highly improves the overall detection accuracy and energy efficiency.

The proposed algorithm is able to (i) completely eliminate the resulting effects on CSS caused by many types of SSDF attacks, (ii) convert some types of SSDF attackers to be honest users, and (iii) alleviate the influence of other honest users that suffer from poor sensing performance or/and very noisy reporting channels. Simulation results show that, compared to many previous works, a significant improvement in detection accuracy and energy efficiency can be attained by the proposed algorithm.

14.2 System Model

Consider an infrastructure-based CRN, e.g. IEEE 802.22 standard, consisting of a set of CUs that seek to exploit a specific spectrum where they are unlicensed. To avoid inducing interference to the licensed users, each CU senses the target spectrum for a specific time and issues a local binary decision $u_k\{-1, +1\}$ about the activity of the licensed users in the target spectrum. if $u_k = +1$, then the CU decides that the spectrum is used by a licensed user. Otherwise, the spectrum is identified as unused by the k^{th} CU.

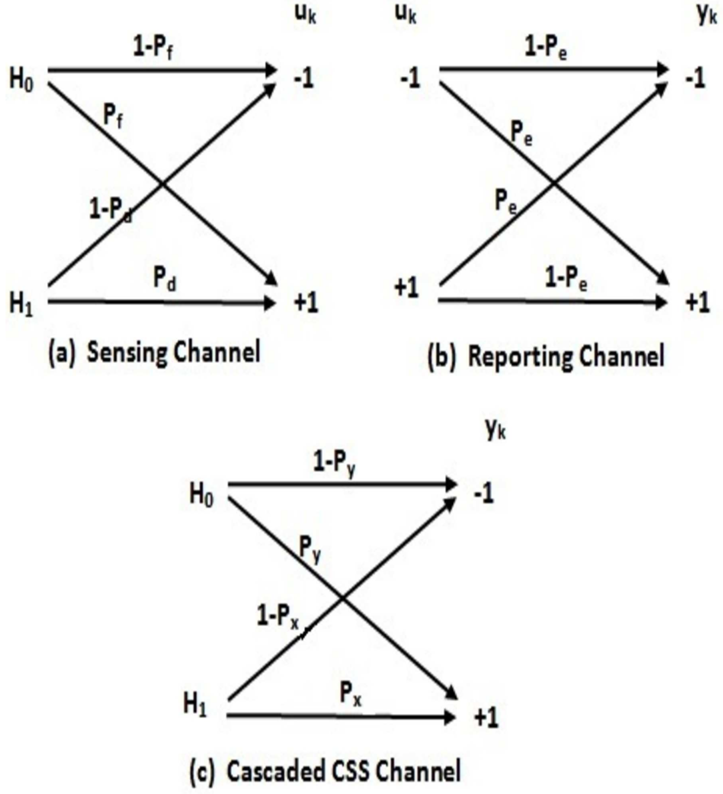
The local sensing performance of the k^{th} CU is evaluated by the detection probability (P_{dk}) and the false-alarm probability (P_{f_k}). During the reporting process, due to the fading and shadowing between the CUs and the FC, the reported decisions may be erroneous. Therefore, we consider a noisy reporting channel between the k^{th} CU and the FC with average error probability denoted by P_{ek}.

The local sensing process can be modeled as a non-symmetric binary channel as shown in Fig 14.1-(a), where H_1 denotes the event of the used spectrum, and H_0 denotes the event of the unused spectrum. Likewise, the reporting channel can be modeled as a symmetric binary channel as shown in Fig 14.1-(b). Both channels can be combined into a cascaded channel modeled as non-symmetric binary channel. P_{xk} and P_{y_k} that appear in Fig. 14.1-(c) are respectively defined as follows

$$P_{xk} = Pr.\{y_k = +1/H_1\} = P_{dk}(1 - P_{ek}) + (1 - P_{dk})P_{ek} \tag{14.1}$$

$$P_{y_k} = Pr.\{y_k = +1/H_0\} = P_{f_k}(1 - P_{ek}) + (1 - P_{f_k})P_{ek} \tag{14.2}$$

where $y_k\{-1, +1\}$ is the received decision form the k^{th} CU at the FC.



(a) Sensing Channel

(b) Reporting Channel

(c) Cascaded CSS Channel

Figure 14.1: *The representation of the (a) Sensing channel, (b) Reporting channel and (c) Cascaded channel (sensing and reporting)*

At the FC, a specific FR is employed to process these received decisions in order to make the global decision U$\{-1, +1\}$. If U $= -1$, the spectrum is identified as unused, and consequently, one of the CUs will be scheduled for data transmission during the rest of the frame denoted by T_t. Otherwise (U $= +1$), no data transmission will be commenced.

However, in such networks, it is possible to have some SSDF attackers that try to degrade the overall performance by reporting false data to the FC. The resulting influence of SSDF attack mainly depends on the adopted strategy. Therefore, the detection probability and/or the false alarm probability will be affected by the reported false information, and hence, the achievable energy efficiency will be degraded as well.

14.3 The proposed algorithm

In this section we propose a novel weighted cooperative spectrum sensing algorithm that is able not only to eliminate the resulting effects of the SSDF attacks, but also to take advantage from some types of the attackers, which consequently, improves the overall performance.

The proposed algorithm is based on setting a number of evaluation frames by which a proper weight for each CU is computed. The evaluation frames are randomly distributed over time. In an evaluation frame, the CUs perform their local sensing, and report their decisions to the FC. At the FC, the global decision is set to "unused" (-1) regardless the received decisions, and thereby, a CU will be scheduled for data transmission. As the considered CRN is infrastructure-based, the success of the transmission can be easily realized at the FC. According to the success in delivering the transmitted data of the scheduled CU, the actual status of the spectrum can be correctly defined. Therefore, all the reported decision from the CUs can be evaluated, and for each CU a specific weight will be assigned that is related to its actual performance. The above process is repeated in every evaluation frame. The random distribution of the evaluation frames will be discussed later.

Let us denote the number of the evaluation frames by L, and Γ_l as a counter that is updated on each evaluation frame, as follows

$$\Gamma_l = \begin{cases} \Gamma_{l-1} + 1 & \text{if } \; S_l = H_0 \\ \Gamma_{l-1} & \text{if } \; S_l = H_1 \end{cases} \tag{14.3}$$

where $\Gamma_0 = 0$, $l = 1, 2, ..., L$, and S_l represents the actual spectrum status of the l^{th} evaluation frame. S_l is decided according to the success of data transmission or not. Notice that the global value of the counter, i.e., Γ_L, represents the number of evaluation frames in which the licensed spectrum was unoccupied.

Likewise, let us set two counters for each CU, $b_{k,l}$ and $f_{k,l}$ that are updated in each evaluation frame. The index k represents the CU index, while l represents the evaluation frame index. These counters are related to the reliability of the local decision of the corresponding CU, and they are updated as follows

$$f_{k,l} = \begin{cases} f_{k,l-1} + 1 & \text{if } \; S_l = H_0 \;\&\; y_{k,l} = +1 \\ f_{k,l-1} & \text{if } \; S_l = H_1 \;\&\; y_{k,l} = +1 \end{cases} \tag{14.4}$$

$$b_{k,l} = \begin{cases} b_{k,l-1} + 1 & \text{if } \; S_l = H_1 \;\&\; y_{k,l} = +1 \\ b_{k,l-1} & \text{if } \; S_l = H_0 \;\&\; y_{k,l} = +1 \end{cases} \tag{14.5}$$

where $y_{k,l}$ is the received decision from the k^{th} CU on the l^{th} evaluation frame. Notice that, for any CU, the counter $f_{k,l}$ is equal to the number of false alarms that have been received by the corresponding CU during the evaluation frames, while the counter $b_{k,L}$, represents how many times the k^{th} CU detects successfully the licensed user during the evaluation frames.

Based on these counters, two indicators for each CU, α_k and β_k are computed at the FC as follows:

$$\alpha_k = \frac{b_{k,l}}{l - \Gamma_l} \tag{14.6}$$

$$\beta_k = \frac{f_{k,l}}{\Gamma_l} \tag{14.7}$$

It is worthy noting that α_k and β_k express estimated versions of the actual sensing and reporting performance of the corresponding CU, i.e., P_{xk} and P_{y_k} probabilities. Such estimation is improved as the number of evaluation frames increases.

During the normal time frames, i.e., non-evaluation frames, each local decision is weighted by a specific weight depending on α and β, so as the global decision is issued according to the following rule:

$$\mathrm{U} = \begin{cases} +1 & \text{if } \sum_{k=1}^{K} w_k y_k \geq \lambda \\ -1 & \text{if } \sum_{k=1}^{K} w_k y_k < \lambda \end{cases} \tag{14.8}$$

where λ is the fusion threshold chosen to satisfy a predefined false alarm probability, and w_k is the weight for the k^{th} CU as follows

$$w_k = \log \frac{\alpha_k(1-\beta_k)}{\beta_k(1-\alpha_k)} \tag{14.9}$$

14.3.1 The distribution of the evaluation frames

Motivated by enhancing the robustness of the proposed algorithm, the evaluation frames are randomly selected by the FC. Thus, the attackers that are aware of the employed evaluation strategy can not be aware in which frames the evaluation will be performed. Therefore, it will be difficult for the attackers to resist against the proposed algorithm.

For any frame, the probability to be an evaluation frame or not is expressed as follows

$$P_l^{eva} = \begin{cases} q & \text{if } l < L \\ 0 & \text{if } l = L \end{cases} \tag{14.10}$$

where q is predefined probability.

Notice that if $q = 1$, it implies that the L evaluation frames will take place in the first L frames, which achieves the best performance of the system. However, if an attacker is aware that $q = 1$, the attacker can act as an honest user and then the algorithm fails to combat it. Thus, q plays an important role in the overall performance of the proposed algorithm. As q decreases, those attackers that are aware of q need more frames to elude the FC. On the other hand, decreasing q results on a delay in assigning the proper weights for CUs, which leads to lower performance.

14.3.2 Effectiveness against SSDF attackers

SSDF attackers are different in their resulting affects. In this subsection, we discus the most popular types of SSDF attackers, and we show the effectiveness of our proposal against each type

- Greedy Attack [111]: this type of attackers always reports that the spectrum is occupied, i.e., $u_k = +1$, regardless of its sensing results ($P_{dk} = P_{f_k} = 1$). According to (14.4), (14.5), (14.6) and (14.7), by the end of the evaluation frames, the two indicators will approximately be $\alpha_k = \beta_k = 1 - P_{ek}$, which results in a zero weight $w_k = 0$ according to (14.9). Therefore, the resulting effect of greedy attackers can be completely eliminated whatever their number is. Another similar attacker type that always informs the FC that the spectrum is free can be handled by the same way.
- Malicious Attack [111]: this type of SSDF attack always reports the opposite of its local decision to the FC. Thus, its sensing performance can be

expressed as $P_{dk} = 1 - P_{dk}^{h}$ and $P_{fk} = 1 - P_{fk}^{h}$, where P_{dk}^{h} and P_{fk}^{h} represent the corresponding values if the CU is honest. Reflecting this to (14.4), (14.5), (14.6) and (14.7), we can get that the assigned values for a malicious attacker are approximately equal to $\alpha_k = 1 - \alpha_k^h$ and $\beta_k = 1 - \beta_k^h$, where α_k^h and β_k^h are the corresponding weights if the CU is honest. By substituting these findings in (14.9), the assigned weight for a malicious attacker is given as follows:

$$w_k^{mal} = -\log \frac{\alpha_k^h(1-\beta_k^h)}{\beta_k^h(1-\alpha_k^h)} \tag{14.11}$$

From (14.8), each local decision will be multiplied by its weight. Hence, according to (14.11), any decision received from a malicious attacker will be inverted and multiplied by a weight corresponding to its actual honest performance as in (14.9). This means that the malicious attacker will not be an attacker anymore since the proposed algorithm is able to convert it to an honest CU.

Notice that, whatever the followed strategy, our algorithm has the ability to identify the actual performance of each CU, and consequently, assign a suitable weight to its received decisions.

It is worth mentioning that the main disadvantage of the proposed algorithm is the resulting interference at the licensed users caused during the evaluation frames. The interference is caused because the spectrum is always targeted in the evaluation frames regardless of the reported local decisions. Thus, the number of the evaluation frames should be small enough not to degrade the performance of the licensed users. On the other hand, less number of evaluation frames will affect the accuracy of the resulting assigned weights. Therefore, the number of the evaluation frames should be tuned to satisfy the desired performance.

14.4 Simulation Results

A CRN consists of three different classes of CUs according to their sensing performance as shown in Table 14.1. CUs belonging to Class 1 or Class 2 are considered to be honest users (H), while CUs belonging to Class 3 are assumed to be SSDF attackers (Att.). The sensing and reporting performance of Classes 1 and 2 are fixed, while the performance of Class 3 is represented in terms of $\delta \in [0, 1]$.

Table 14.1: Classes' Performance

	Class 1	Class 2	Class 3
P_d	0.8	0.65	$1 - \delta$
p_f	0.1	0.3	δ
P_e	0.1	0.05	0.1

The performance of the proposed algorithm is compared to two popular algorithms described as follows:

- Equal Gian Combining (EGC): where all CUs have equal weights, i.e., $w_k = 1, \forall k$
- Attacker-Removal Algorithm (ARA) [118]: where a predefined threshold (ν) on the number of mismatches between the local decision and the global decision is set. Whenever the number of mismatches exceeds ν for a specific CU, it will be identified as an attacker, and its reported results will not be processed.

The performance of the three algorithms is assessed over a large time window W. The simulation results consider the attacker of malicious type since it is the most challenging attacker, and also because the greedy attacker is easy to be detected and removed by any of the three algorithms. All simulation parameters regarding the channel statistics, energy consumption and transmission rate are summarized in Table 14.2.

Table 14.2: Simulation parameters

Parameter	Value	Parameter	Value
P_0	0.5	E_{css}	$12\,mJ$
E_t	$0.1\,J$	R	$100\,Kbps$
T_t	$0.1\,sec$	W	$2 \times 10^3 \times T sec$
L	100		

Fig. 14.2 compares our proposal and EGC algorithms in terms of average detection probability. First, P_D is shown for a CRN of two honest users, one from Class 1 and the other form Class 2, at a given false alarm probability $P_F = 0.1$. The detection probability achieved by our proposal is higher than that is achieved by EGC. This is due to assigning proper weights that are related to the actual users performance. Also in Fig. 14.2, we show the achievable performance when a single malicious attacker form Class 3 joins the considered CRN. The achievable P_D is plotted versus δ which represents the sensing performance of the attacker as it appears to the FC. Since the attacker is a malicious attacker, it implies that its strategy consists in inverting its local decision and reporting the inverted local decision to the FC. Therefore, the effectiveness of such attacker depends on its honest sensing performance. In terms of δ, the honest (actual) performance of the malicious attacker is given by $P_d^h = \delta$ and $P_f^h = 1 - \delta$, while, due to the malicious strategy, its performance appears at the FC as $P_d = 1 - \delta$ and $P_f = \delta$. According to that, as δ increases, the effectiveness of the malicious attacker should be increased.

For EGC algorithm, as δ increases, the average detection probability decreases, which is expected since EGC does not assign weights to the CUs. However, according to our proposal, a proper weight is assigned for the attacker

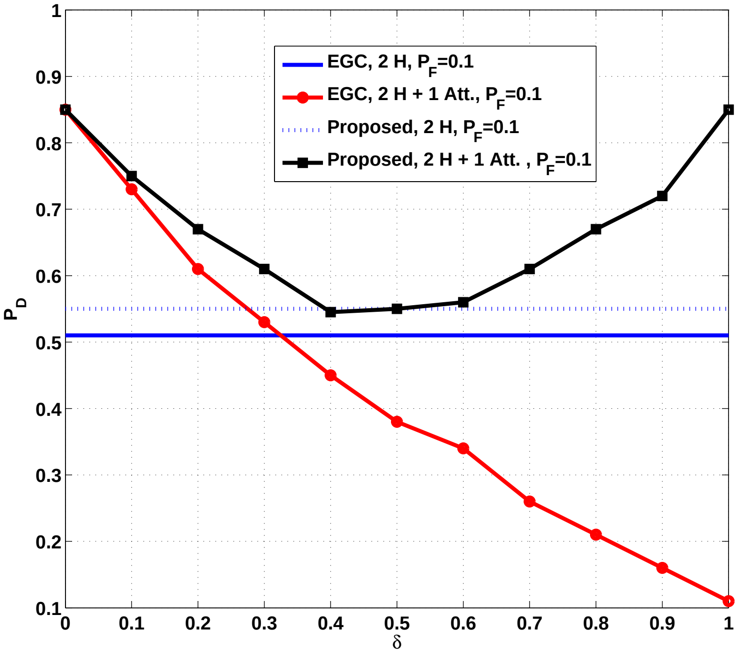


Figure 14.2: *The average detection probability P_D versus the performance of the attacker represented by δ. ($q = 1$).*

based on its performance (δ). For example, if $\delta = 0$, this means that the attacker has a very poor honest performance ($P_d^h = 0$ and $P_f^h = 1$) but due to its malicious type, its performance will be highly improved ($P_d = 1$ and $P_f = 0$). Hence, its reported decisions will enhance the global decision reliability. At $\delta = 0.5$, the assigned weight will be zero, and hence, the decisions reported by the attacker will be totally removed. In the case of $\delta > 0.5$ up to the worst case $\delta = 1$, our proposal still achieves an outstanding performance. Notice that the symmetry of the P_D around $\delta = 0.5$, which means that the assigned weight for any attacker can convert this attacker to be an honest user, which highly improves the overall performance.

It was stated in [118] that the performance of the their proposal improves as the percentage of the attackers to the honest CUs decreases. Fig. 14.3 depicts the average detection probability for the three algorithms (EGC, ARA and our pro-

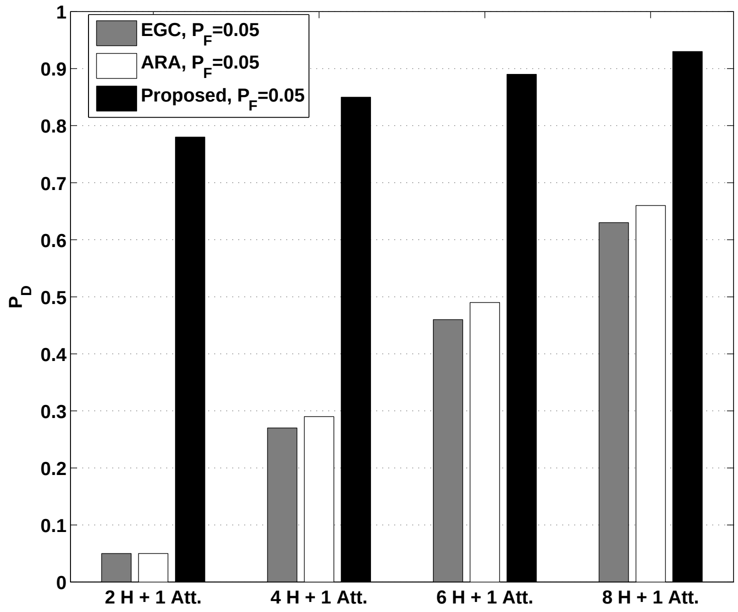


Figure 14.3: *The average detection probability P_D for a CRN consisting one malicious attacker and different number of honest CUs for the three algorithms. (In ARA ν is set to the optimal value) ($q = 1$).*

posal) versus different percentages of the attacker presence. Specifically, for all cases we consider only one malicious attacker with $\delta = 1$, while the number of honest CUs is variable (2, 4, 6 and 8) half of them belong to Class 1 and the other half belong to Class 2. In terms of percentages, the considered cases represent four different percentages of attacker presence as follows: 33.3%, 20%, 14% and 11%. The average detection probability of all algorithms should be improved since the number of honest users increases, which is shown in Fig. 14.3. However, the detection probability achieved by our proposal is higher than the other algorithms since our proposal is able to assign a proper weigh for the attacker, converting it to an honest user.

Fig. 14.4 explores the achievable energy efficiency for the three algorithm in the four considered cases. Since the false alarm probability is identical for all algorithms ($P_F = 0.05$), the determining factor in the achievable energy efficiency

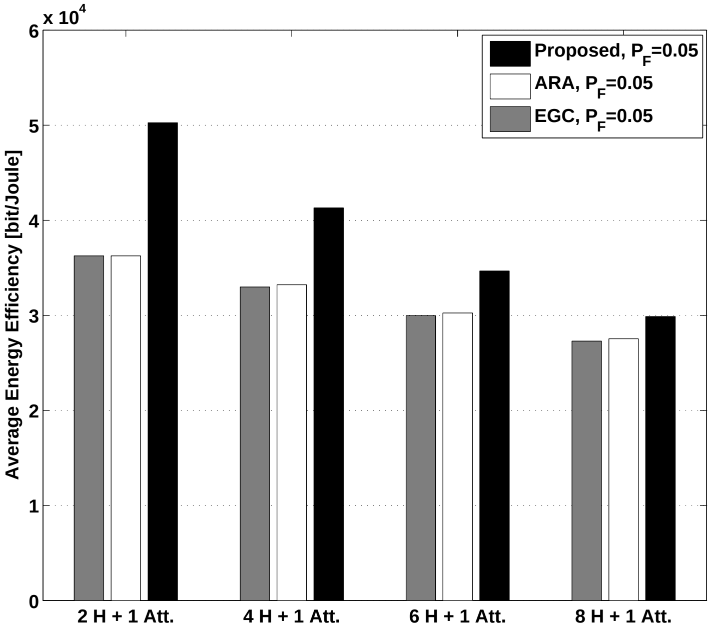


Figure 14.4: *The average energy efficiency μ for a CRN consisting one malicious attacker and different number of honest CUs for the three algorithms. (In ARA ν is set to the optimal value).*

is the average detection probability, as indicated in (16.2). The achievable energy efficiency for all algorithms decreases as the number of CUs increases because of the high energy consumption, while the achievable throughput is fixed. The proposed algorithm outperforms the other algorithms even though large energy is consumed during the evaluation frames.

Up to now, in all the obtained results we have assumed that $q = 1$, which means that the evaluation frames will be the first L frames. Accordingly, if we consider that the attacker is aware of q, the attacker can easily elude the FC and act as honest user during the first L frames. Thus, we should reduce q, resulting in spreading the L frames over time. By this way, it will be more difficult to the attacker to deceive the FC since being aware of $q < 1$ does not imply that the attacker is aware in which frames the evaluation takes place. Fig. 14.5 depicts the detection probability of the proposed algorithm for three

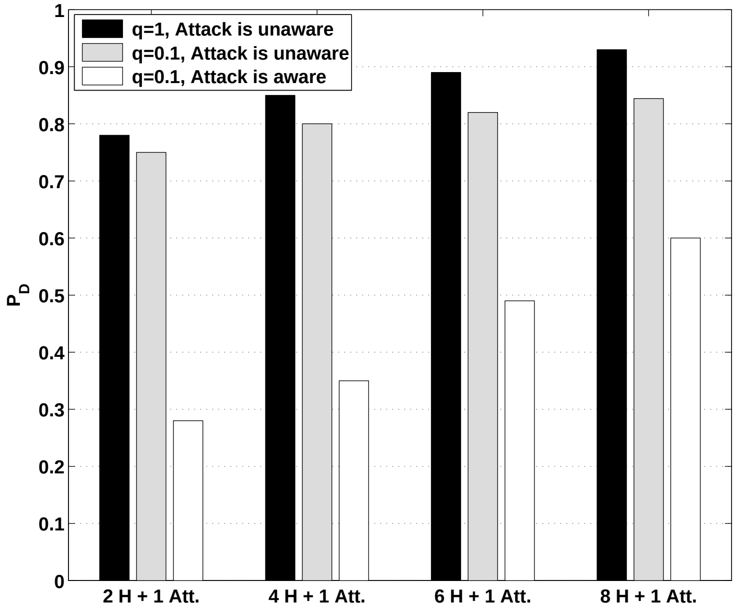


Figure 14.5: *The average detection probability P_D for a CRN consisting one malicious attacker and different number of honest CUs.*

different scenarios: i) $q = 1$ and the attacker is unaware of it, ii) $q = 0.1$ and the attacker is unaware of it, and iii) $q = 0.1$ and the attacker is aware of it. In the third scenario, since the attacker is aware of q we consider that the attacker will act as an honest user until the evaluation frames are finished. Using q, the attacker can predict the average number of frames that is required to perform the evaluation, which is approximately given by L/q. Notice that varying q from 1 to 0.1 slightly affects the detection probability. In the main while, the proposed algorithm still achieves a good performance compared to other algorithms (see Fig. 14.3) even though the attacker is aware of q.

14.5 Summary

In this chapter, a robust algorithm against SSDF attacker in CSS for infrastructure-based CRN has been presented. The proposed algorithm is based on setting a number of evaluation frames in which the actual performance for each CU is obtained, and a proper weight is derived for each CU. The proposed algorithm does not require any prior information about the spectrum or CUs. Moreover, the proposed algorithm takes advantage of attackers and converts them to honest users. Simulation results show that our algorithm outperforms other algorithms in detection accuracy and energy efficiency.

CHAPTER 15

IDENTIFICATION AND PUNISHMENT POLICIES FOR SPECTRUM SENSING DATA FALSIFICATION ATTACKERS USING DELIVERY-BASED ASSESSMENT

15.1 Introduction

Identifying attackers is a very crucial process that should be carefully carried out to avoid detecting honest CUs as attackers. Thus, attacker-identification should be built on a reliable base that cannot be affected if the number of attackers is large. In this chapter, we consider the delivery of the transmitted data as a base of evaluating the individual performance, and consequently, identifying attackers. Notice that in infrastructure-based cognitive radio networks, the data transmission is performed through the base station (BS) [124]. Thus, it is easy to ensure if the transmitted data is successfully delivered or not, and hence, the actual spectrum status will be known at the FC. Using the obtained spectrum status, all the individual sensing results can be evaluated accordingly. Based on the evaluated performance of each CU, attackers can be seamlessly detected and removed from the fusion process at the FC.

Identifying attackers possess an initial step to alleviate their effects on the network performance. However, a further action should be taken against identified attackers in the subsequent data transmission phase. Depriving attackers of scheduling opportunity in data transmission phase is a bad choice. This is due to the fact that the attacker-identification is an imperfect process, where a false identification of an honest CU as an attacker is probable. Moreover, an identified attacker could be an honest CU that suffers from poor sensing performance. On the other hand, keeping all CUs, honest and attackers, equal in scheduling probability is unfair with respect to the honest CUs. In this chapter, we propose a scheduling policy based on assigning a scheduling probability to each CU related to its sensing performance. For attackers, such policy establishes a punishment strategy, where a low scheduling probability is assigned to them, and hence, reduced individual throughput and energy efficiency. Thus, the proposed punishment policy is aiming at motivating attackers to quit reporting false reports. On the other hand, honest CUs will gain proportional fair distribution of data transmission corresponding to their local sensing performance.

Although the considered setup is challenging, as it will be described later, both proposed policies show promising results even in the worst case scenario where the number of attackers is very large. Mathematical analysis and simulation results explore the significant improvement in the overall performance achieved by the proposed policies compared to previous works.

The contributions of this chapter can be summarized as follows

- Introducing data delivery as a base for evaluating the performance of the individuals in infrastructure-based CRNs. Delivery-based assessment is a novel strategy and has never been proposed before to the best of our knowledge.
- Proposing a novel attacker-identification algorithm that is able to skillfully detect attackers and completely eliminate their influence on the CRN.
- Proposing attacker-punishment algorithm that is based on lowering the energy efficiency of the attacker, motivating it either to quit attacking or to

leave the CRN.

15.2 System Model

Consider a CRN consisting of N CUs cooperating in order to opportunistically access the licensed spectrum whenever it is free. The CRN is considered of infrastructure-based type [125], where the CSS and data transmission is coordinated by the BS. An example of such network is IEEE 802.22 [126]. For the sake of simplicity, the licensed spectrum is modeled as a single channel although it can be easily extended to multiple-channel scenario. The probability that the spectrum is not being used is denoted by P_0. In each CSS round, each CU senses the licensed spectrum and, depending on its sensing result, it solves a hypothesis testing problem deciding on one of two hypotheses, either H_0 that implies spectrum is unused, or H_1 for spectrum is used. It then reports its binary local decision $u_n = \{1 \equiv \text{``}used\text{''}, 0 \equiv \text{``}unused\text{''}\}$ to the FC that is located at the BS.

The reliability of the local decision of a CU is evaluated by two indicators: local detection probability (P_{dn}) and local false-alarm probability (P_{df}). After reporting the issued local decisions, the FC applies the *K-out-of-N* fusion rule to make the global decision. Upon issuing the global decision, a CU will be scheduled for data transmission only if the global decision is "unused", while in case of identifying the spectrum as "used", the FC will not schedule any of the CUs in order to avoid interference to the licensed users.

15.2.1 Attacker Model

As in other wireless networks, CRNs are usually vulnerable to different security threats. One of these threats, which is not typical in the other wireless networks, is SSDF attack. In SSDF attack, a malicious CU sends false reports about the spectrum availability to the FC in order to mislead the global decision. The motivation behind such attack is to exploit the spectrum holes for their own transmission. To satisfy this motivation, the optimal attack strategy is to always report the spectrum as “used”, also called ”Always-Yes” attack [127]. However, such strategy is easy-to-detect at the FC. Thus, smarter attackers usually follow a different strategy in order to elude the FC and avoid detection and negligence. The smart strategy is based on inverting the actual local sensing result in a selective manner. Specifically, an attacker decides in each CSS round to attack or not with a probability, denoted as P_m. If the attacker decides to attack in a specific round, it simply flips its own local decision and reports it to the FC. Such attacker model is usually termed as Byzantine attackers [127, 128, 129]. The sensing performance. i.e., P_{dn} and P_{fn}, of an attacker as it appears at the FC based on such strategy can be mathematically modeled as follows

$$P_{dn} = P_m(1 - P_{dn}^{ac}) + (1 - P_m)P_{dn}^{ac} \tag{15.1}$$

$$P_{fn} = P_m(1 - P_{fn}^{ac}) + (1 - P_m)P_{fn}^{ac} \tag{15.2}$$

where P_{dn}^{ac} and P_{fn}^{ac} represent the actual (honest) detection and false-alarm probabilities, respectively. Notice that this model is valid for an honest CU if we set P_m to zero.

For the sake of simplicity, let us assume that all honest CUs are identical in there sensing performance, i.e., $P_{dn} = P_{dh}$ and $P_{fn} = P_{fh}$. Likewise, the attackers are considered to have identical performance, i.e., $P_{dn} = P_{da}$ and $P_{fn} = P_{fa}$.

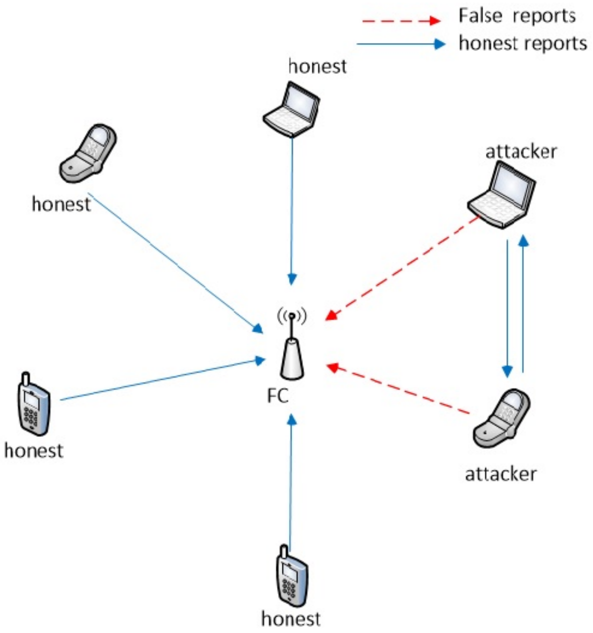


Figure 15.1: An example of a cognitive radio network in presence of SSDF attackers

Since the main motivation of attackers is to increase their achievable throughput while degrading the throughput of the honest CUs, the attacker will exploit the case of false-alarm to perform individual transmission without coordination from the BS. Specifically, we consider that the attackers will cooperate among themselves to make their own global decision based on their honest performance. Accordingly, once a false-alarm occurs at the FC, if their own global decision does not agree with the decision of the FC, the attackers will select one of them randomly to transmit its own data individually. From now on, we denote the detection and false-alarm probabilities of the global decision of attackers by P_D^A and P_F^A, respectively.

15.2.2 Throughput and Energy Efficiency

According to the considered CRN model, an honest CU has the chance to transmit only if it has been legitimately scheduled by the FC. On the other hand, an attacker can get a transmission opportunity in two cases: (i) if it has been legitimately scheduled by the FC, and (ii) if it has been selected by the other attackers to transmit in the case of a false-alarm at the FC. We call the achievable throughput in first case the legitimate throughput, while the illegitimate throughput is the throughput achieved in the second case.

Notice that increasing the false-alarm probability, which is a result of SSDF attackers, the illegitimate throughput of attackers will increase, which, in turn, degrades the achievable throughput of the honest CUs. However, increasing the throughput is always accompanied with more energy consumption. Therefore, for evaluation purpose, we use the individual energy efficiency of the CU as comparison metric between attackers and honest CUs. Individual energy efficiency of a CU is defined as the ratio of the individual throughput achieved in *bits* to the individual energy consumed in *Joule*. According to the considered setup, it is expected that the individual achievable throughput, the individual energy consumption and the individual energy efficiency will be different for an honest CU and an attacker.

15.2.3 An example

Let us consider a CRN of 5 honest CUs with identical detection and false-alarm probabilities equal to 0.8 and 0.1, respectively. The global decision is made based on Majority rule. In Fig. 15.2, we plot the effects on the detection accuracy and the achievable throughput if a number of attackers has joined the CRN. The local detection and false-alarm probabilities of attackers are identical and equal to 0.1 and 0.8, respectively. Fig. 15.2-a shows the error probability of the global decision, as an indicator of the detection accuracy, versus the number of joined attackers, while Fig. 15.2-b shows the achievable throughput of an attacker and an honest CU versus the number of joined attackers. The achievable throughout is divided into two parts: legitimate throughput resulting from scheduling by the BS, and illegitimate throughput achieved by individual transmission without coordination of the BS. Clearly, the increase in the error probability and the degradation in the achievable throughput of honest CUs increase as the number of attackers increases. On the other hand, the throughput of attackers increases due to the high false-alarm probability that they can cause. Such a simple example explores the importance of encountering the attackers in CRNs.

15.3 Delivery-based Assessment

Most of the previous work depends either on a prior knowledge about the local performance of the CUs or the global decision reliability to detect attackers and remove them. The prior knowledge is not always available and the global decision lacks reliability in the presence of large number of attackers. Instead, in this chapter, we propose a novel approach that can be seamlessly evaluate the sensing performance of each CU, and consequently, identify attackers. The proposed approach is based on the delivery of the transmitted data of the scheduled CU. Specifically, if the licensed channel has been decided as unused and one of the CUs has been scheduled for data transmission, the successful delivery of the

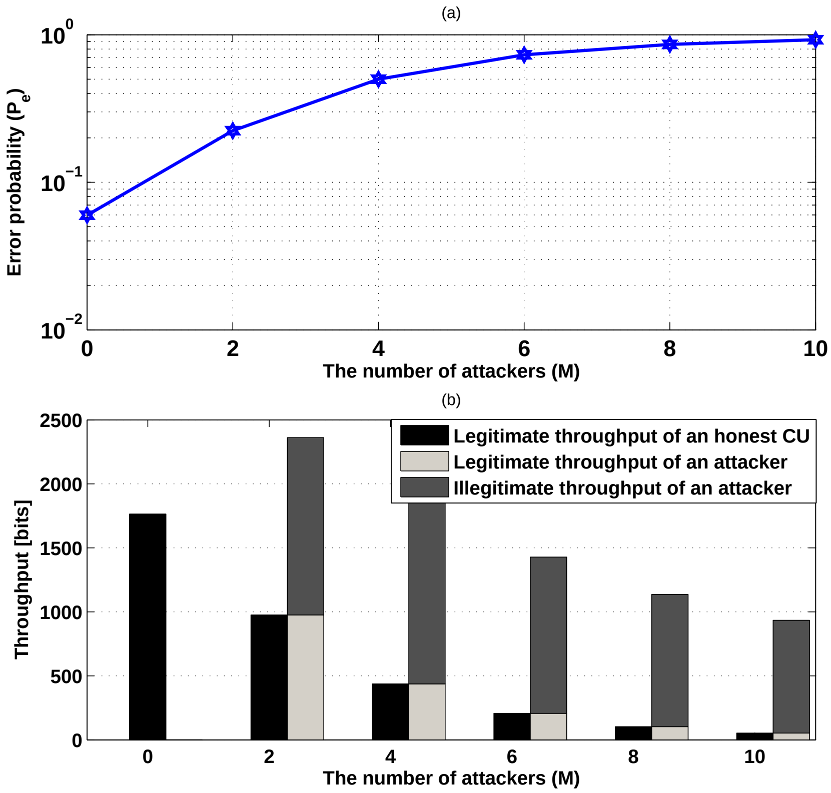


Figure 15.2: Example: (a) the error probability versus the number of attackers, and (b) the throughput versus the number of attackers

transmitted data reveals that the global decision was correct and the channel is actually unused. In the other case, if the transmitted data cannot be successfully delivered, the global decision is identified as incorrect and the channel is actually occupied. Notice that in both cases, the FC has doubtlessly realized the actual channel status, which can be used to assess all the received local decisions as correct or not.

Delivery-based assessment continues in each data transmission phase in order to formalize a performance indicator for each CU, which can be further employed to identify attackers and honest CUs. The reader should note that considering data delivery as an evaluation base is much more reliable than the global decision even in the case of large number of attackers.

From implementation point of view, the delivery-based assessment approach can be easily applied in infrastructure-based CRNs with a BS coordinating the data transmission, as assumed in this chapter. However, for centralized CRNs without a BS, where CUs individually access the spectrum, the data delivery can be verified by an additional monitoring process during data transmission performed by the FC itself or another delegated trusted CU. Notice that the monitoring process is much easier than spectrum sensing since the transmitting user is known at the FC. Another option which can verify the data delivery is requesting a feedback from the scheduled CU. However, it should be taken into account the probability that the scheduled CU is an attacker providing false feedback. In order to avoid any induced drawback in the delivery-based assessment approach, we consider only infrastructure-based CRNs in this chapter, which has been widely adopted in the literature [124, 130, 131, 132, 133, 45, 134], while the applicability of delivery-based approach on other mentioned CRN types is left as future work.

In the following sections, we describe two novel policies, attacker-identification policy and attacker-punishment policy. Both of them are developed based on the delivery-based assessment approach. While attacker-identification policy aims at detecting attackers and ignoring their reported local decision in the fusion process, the attacker-punishment policy is basically a scheduling policy that leads to a proportional resource distribution according to the evaluated individual performance of each CU. Such a fair scheduling policy acts as a punishment for attackers and a reward for honest CUs.

15.4 Attacker-Identification Policy

Attacker-identification is a key factor to improve the overall performance of the CRNs either in terms of detection accuracy or energy efficiency. Attacker-identification should be carefully carried out in order to avoid incorrectly identifying honest CUs as attackers. Once an attacker is identified, it should be removed out from the fusion process at the FC, where its reports should be ignored. In this section we propose a novel attacker-identification policy that is able to identify the attackers whatever their number in the network is.

The proposed policy is based on assessing the local decisions according to the delivery of the transmitted data of the scheduled CU. In detail, once the spectrum is identified as "unused", a CU will be scheduled for data transmission. Consequently, based on the success of delivering the transmitted data, the actual spectrum status can be correctly defined and used to evaluate the local decisions. Thus, the local decisions reported in that round can be classified false or correct. If the local decision is false, a corresponding counter will be incremented by one. After a sufficient amount of time, let us say W CSS rounds, if a counter of a specific CU exceeds a predefined threshold, it will be considered as an attacker, and hence, its reports will be ignored at the fusion process.

Following the proposed policy, a zero-initialized counter, denoted by $B_{n,i}$, for each CU is updated each CSS round as follows

$$B_{n,i} = \begin{cases} B_{n,i-1} + 1, & \text{if } U_i = 0 \;\&\; S_i \neq u_{n,i} \\ B_{n,i-1}, & \text{Otherwise} \end{cases} \tag{15.3}$$

where S_i represents the actual status of the spectrum. The global value of the counter after W rounds $B_{n,W}$ follows a binomial distribution function, as follows

$$Prob.\{B_{n,W} = b\} = \binom{W}{b} \lambda_n^b (1-\lambda_n)^{W-b} \tag{15.4}$$

where λ_n denotes the probability that the counter B will be incremented, which can be derived as follows

$$\lambda_n = P(B_{n,i} = B_{n,i-1}+1) = P(H_0 \cap u_{n,i} = 1 \cap U_i = 0) + P(H_1 \cap u_{n,i} = 0 \cap U_i = 0) \tag{15.5}$$

Using the following theorem on conditional probability [135]

$$P(A_1 \cap A_2 \cap A_3) = P(A_1)P(A_2|A_1)P(A_3|A_1 \cap A_2) \tag{15.6}$$

the first term in (15.5) can be expanded as follows

$$\begin{aligned} P(H_0 \cap u_{n,i} = 1 \cap U_i = 0) &= P(H_0)P(u_{n,i} = 1|H_0)P(U_i = 0|u_{n,i} = 1 \cap H_0) \\ &= P_0 P_{fn} P(U_i = 0|u_{n,i} = 1 \cap H_0) \end{aligned} \tag{15.7}$$

Likewise, the second term in (15.5) can be expanded as follows

$$\begin{aligned} P(H_1 \cap u_{n,i} = 0 \cap U_i = 0) &= P(H_1)P(u_{n,i} = 0|H_1)P(U_i = 0|u_{n,i} = 0 \cap H_1) \\ &= P_1(1-P_{dn})P(U_i = 0|u_{n,i} = 0 \cap H_1) \end{aligned} \tag{15.8}$$

by substituting (15.7) and (15.8) in (15.5), λ_n can be rewritten as follows

$$\lambda_n = P_0 P_{fn} P(U_i = 0|u_{n,i} = 1 \cap H_0) + P_1(1-P_{dn})P(U_i = 0|u_{n,i} = 0 \cap H_1) \tag{15.9}$$

The probability λ_n can be found for an honest CU, denoted by λ_h, by substituting the following probabilities in (15.9)

$$P(U_i = 0|u_{n,i} = 1 \cap H_0)\Big|_{honest} = 1 - \sum_{k=K-1}^{N-1} \sum_{j=a_1}^{a_2} f(j, M, P_{fa}) f(k-j, H-1, P_{fh}) \tag{15.10}$$

$$P(U_i = 0|u_{n,i} = 0 \cap H_1)\Big|_{honest} = 1 - \sum_{k=K}^{N-1} \sum_{j=a_1}^{a_2} f(j, M, P_{da}) f(k-j, H-1, P_{dh}) \quad (15.11)$$

where $a_1 = \max(0, k - H + 1)$, $a_2 = min(k, M)$, H is the number of honest CUs, M is the number of attackers and the function $f(\alpha, \beta, \gamma)$ denotes the binomial function [135], as follows

$$f(\alpha, \beta, \gamma) = \binom{\beta}{\alpha} \gamma^{\alpha} (1 - \gamma)^{\beta - \alpha} \quad (15.12)$$

By the same way, the probability λ_n can be found for an attacker, denoted by λ_a, by substituting the following probabilities in (15.9)

$$P(U_i = 0|u_{n,i} = 1 \cap H_0)\Big|_{attacker} = 1 - \sum_{k=K-1}^{N-1} \sum_{j=a_3}^{a_4} f(j, M-1, P_{fa}) f(k-j, H, P_{fh}) \quad (15.13)$$

$$P(U_i = 0|u_{n,i} = 0 \cap H_1)\Big|_{attacker} = 1 - \sum_{k=K}^{N-1} \sum_{j=a_3}^{a_4} f(j, M-1, P_{da}) f(k-j, H, P_{dh}) \quad (15.14)$$

where $a_3 = \max(0, k - H)$, $a_4 = min(k, M - 1)$.

Now, from (15.4), the average value of $B_{n,W}$ of the n^{th} CU, denoted by $\overline{B_{n,W}}$, can be derived as follows

$$\overline{B_{n,W}} = \sum_{b=0}^{W} b \cdot Prob.\{B_{n,W} = b\} = \sum_{b=0}^{W} b \cdot \binom{W}{b} \lambda_n^b (1 - \lambda_n)^{W-b} \quad (15.15)$$

which can be simplified using the binomial law as follows

$$\overline{B_{n,W}} = W\lambda_n \quad (15.16)$$

Also, if we denote the ignoring threshold by ζ, the ignoring probability of the n^{th} CU can be expressed as follows:

$$P_{ign,n} \equiv Prob.\{B_{n,W} \geq \zeta\} = \sum_{b=\zeta}^{W} \binom{W}{b} \lambda_n^b (1 - \lambda_n)^{W-b} \quad (15.17)$$

Accordingly, the average number of the remaining CUs after W CSS rounds, i.e. those CUs that have not been ignored, can be given as follows

$$\overline{N_W} = N - \sum_{n=1}^{N} P_{ign,n} = H(1 - P_{ign,h}) + M(1 - P_{ign,a}) \tag{15.18}$$

where $P_{ign,h}$ and $P_{ign,a}$ are the ignoring probabilities for an honest CU and an attacker, which can be obtained by substituting λ_h and λ_a instead of λ_n in (15.17), respectively.

15.4.1 Optimizing of ζ

It is worth noting that ζ has a significant role in the proposed policy. Low values of ζ may result in identifying some honest CUs as attackers, whereas some attackers can not be identified at high values of ζ. Therefore, ζ should be carefully optimized. An approach to optimize the threshold ζ is to maximize the difference between the ignoring probability of attackers and the ignoring probability of honest CUs. Mathematically, the maximization problem can be expressed as follows

$$\max_{\zeta} P_{igna} - P_{ignh} \tag{15.19}$$

by substituting the values of P_{igna} and P_{ignh} using (15.17), the maximization problem can be rewritten as follows

$$\max_{\zeta} \sum_{b=\zeta}^{W} \binom{W}{b} \lambda_a^b (1 - \lambda_a)^{W-b} - \sum_{b=\zeta}^{W} \binom{W}{b} \lambda_h^b (1 - \lambda_h)^{W-b} \tag{15.20}$$

The optimal value of ζ can be computed using Lagrange method, where the derivative of the function with respect to ζ is equalized to zero. Since ζ is an integer, then the derivative of P_{igna} and P_{ignh} are respectively given as follows

$$\frac{\partial P_{igna}}{\partial \zeta} = P_{igna}(\zeta + 1) - P_{igna}(\zeta) = -\binom{W}{\zeta} \lambda_a^{\zeta} (1 - \lambda_a)^{W-\zeta} \tag{15.21}$$

$$\frac{\partial P_{ignh}}{\partial \zeta} = P_{ignh}(\zeta+1) - P_{ignh}(\zeta) = -\binom{W}{\zeta}\lambda_h^{\zeta}(1-\lambda_h)^{W-\zeta} \tag{15.22}$$

Accordingly, the first derivative of the function under optimization in (15.19) can be given as follows

$$\frac{\partial}{\partial \zeta}(P_{igna} - P_{ignh}) = -\binom{W}{\zeta}\lambda_a^{\zeta}(1-\lambda_a)^{W-\zeta} + \binom{W}{\zeta}\lambda_h^{\zeta}(1-\lambda_h)^{W-\zeta} = 0 \tag{15.23}$$

The binomial coefficients can be canceled, and the equation can be rearranged as follows

$$\left(\frac{\lambda_a(1-\lambda_h)}{\lambda_h(1-\lambda_a)}\right)^{\zeta} = \left(\frac{1-\lambda_h}{1-\lambda_a}\right)^{W} \tag{15.24}$$

Now, by applying the natural logarithm for both sides, the optimal values of the ignoring threshold that maximizes the difference between the ignoring probabilities of attackers and honest CUs, denoted by ζ^*, can be given as follows

$$\zeta^* = \left\lceil W \frac{\ln\left(\frac{1-\lambda_h}{1-\lambda_a}\right)}{\ln\left(\frac{\lambda_a(1-\lambda_h)}{\lambda_h(1-\lambda_a)}\right)} \right\rceil \tag{15.25}$$

where $\lceil \cdot \rceil$ is the ceiling operator that should be applied to ζ^* to make it an integer.

15.4.2 Worst-case scenario

For the purpose of exploring the high performance of the proposed attacker-identification policy, we consider the worst case scenario. The worst case scenario is represented when a large number of attackers is present confronted by a low number of honest CUs (i.e., $M \gg H$).

The performance can be clearly shown in terms of the ignoring probability of attackers and hones CUs. From (15.17), the ignoring probability of a CU mainly depends on its corresponding λ_n probability. Considering the majority rule as the employed FR, notice that both probabilities given in (15.9) can be respectively approximated in such scenario as follows

$$P(U_i = 0|u_{n,i} = 1 \cap H_0)\Big|_{wc} \approx 0 \tag{15.26}$$

$$P(U_i = 0|u_{n,i} = 0 \cap H_1)\Big|_{wc} \approx 1 \tag{15.27}$$

These approximations are valid since in the case of $M \gg H$ the probability of making a correct global decision (as in (15.26)) is almost absent and the probability of making a false global decision (as in (15.27)) is almost one.

Now, by substituting (15.26) and (15.27) in (15.9), the probabilities λ_h and λ_a can be computed as follows

$$\lambda_h\Big|_{wc} \approx P_1(1 - P_{dh}) \tag{15.28}$$

$$\lambda_a\Big|_{wc} \approx P_1(1 - P_{da}) \tag{15.29}$$

Consequently, since $P_{dh} \to 1$ and $P_{da} \to 0$, then $\lambda_h \to 0$ and $\lambda_a \to P_1$. Using (15.17), it is easy to show that $P_{ignh} \approx 0$ while P_{igna} is still high, and hence, attackers can be easily detected with a proper choice of ζ even in the worst-case scenario.

The optimal ignoring threshold in the worst-scenario (ζ^*_{wc}) can be also approximated by substituting (15.28) and (15.29) in (15.25), as follows

$$\zeta^*_{wc} \approx \left\lceil W \frac{\ln\left(\frac{P_0 + P_1 P_{dh}}{P_0 + P_1 P_{da}}\right)}{\ln\left(\frac{(1-P_{da})(P_0+P_1 P_{dh})}{(1-P_{dh})(P_0+P_1 P_{da})}\right)} \right\rceil \tag{15.30}$$

15.5 Attacker-Punishment Policy

Ignoring the reports received from the identified CUs as attackers helps to improve the overall performance of the network. However, a false identification is probable, where some honest CUs might be identified as attackers by error. Moreover, as stated earlier, not all of attackers intentionally send false reports to the FC. Some honest CUs suffer from multi-path fading and shadowing during sensing or noisy reporting channels, leading to a bad sensing performance. This type of honest CUs will appear like attackers at the FC side. Thus, depriving CUs that are identified as attackers from data transmission represents a harmful action towards the unintentional attackers. On the other hand, providing the same transmission chance among all CUs does not attain fairness from honest CUs' point of view. Instead, in this section, we provide a novel scheduling policy that distributes the spectrum resources among CUs in a proportional fair manner. The proposed scheduling policy allocates scheduling probability to each CU based on its sensing performance that appears at the FC. Such policy can be deemed as punishment for attackers, while it provides a fair resource distribution for honest CUs.

The proposed policy is also based on delivery-based assessment as in the proposed attacker-identification policy. Therefore, the assigned scheduling probability for each CU depends on the instantaneous value of the counter B. The scheduling probability of the n^{th} CU is computed each CSS round as follows

$$P_{sn} = \frac{x_i - B_{n,i}}{\sum_{j=1}^{N}(x_i - B_{j,i})} \tag{15.31}$$

where x_i represents the number of times in which the spectrum was identified as "unused" by the global decision until the i^{th} CSS round, expressed as follows

$$x_i = \begin{cases} x_{i-1} + 1, & \text{if } U_i = 0 \\ x_{i-1}, & \text{if } U_i = 1 \end{cases} \tag{15.32}$$

According to (15.31), an increase in the counter $B_{n,i}$ for a CU implies a magnified punishment through reducing the scheduling probability. At i^{th} CSS round, the value of x_i follows a binomial distribution, where its average value can be given as follows

$$\overline{x_i} = i \cdot P(U_i = 0) \tag{15.33}$$

where $P(U_i = 0)$ is the probability that the spectrum will be identified as unused at the FC, expressed as follows

$$P(U_i = 0) = P_0(1 - P_F) + P_1(1 - P_D) = 1 - P_0 P_F - P_1 P_D \tag{15.34}$$

Consequently, using the average value of $B_{n,i}$ given in (15.16), the average value of P_{sn} at the i^{th} round can be easily derived as follows

$$\overline{P_{sn}} = \frac{i \cdot P(U_i = 0) - i \cdot \lambda_n}{\sum_{j=1}^{N} \left(i \cdot P(U_i = 0) - i \cdot \lambda_j \right)} = \frac{P(U_i = 0) - \lambda_n}{NP(U_i = 0) - \sum_{j=1}^{N} \lambda_j} \tag{15.35}$$

The reader should note that the computation of $P(U_i = 0)$ and λ_n are different before and after removing the identified attackers. scheduling probabilities are computed based on the accumulated counters B and x, should be kept updated as long as th CRN lasts.

According to the proposed punishment policy, the average achievable throughput for an honest CU, denoted by D_h, can be expressed as follows

$$D_h = P_0(1 - P_F)R \cdot T_t \overline{P_{sh}} \tag{15.36}$$

where R is the data rate, T_t is the transmission time and $\overline{P_{sh}}$ is the average scheduling probability for an honest CU. The factor $P_0(1 - P_F)$ represents the case of no false-alarm at the FC. On the other hand, the average achievable throughput for an attacker, denoted by D_a, is divided into two parts; legitimate and illegitimate, and can be expressed as follows

$$D_a = P_0(1 - P_F)R \cdot T_t \overline{P_{sa}} + P_0 P_F (1 - P_F^A)R \cdot T_t \cdot (1/M) \tag{15.37}$$

Notice that the first term (legitimate throughput) is identical to the honest CU except the difference in the scheduling probability, while the second term includes the illegitimate throughput. The factor $P_0 P_F (1 - P_F^A)$ represents the case that a false-alarm occurs at the FC and no false-alarm made by the attackers' global decision.

Likewise, the average energy consumption for an honest CU, denoted by E_h, is expressed as follows

$$E_h = E_{css} + P(U_i = 0) E_t \cdot \overline{P_{sh}} \tag{15.38}$$

where E_{css} and E_t are the energy consumed in spectrum sensing and data transmission, respectively. For an attacker, the average energy consumed (E_a) is given as follows

$$E_a = E_{css} + P(U_i = 0) E_t \cdot \overline{P_{sa}} + \big(P_0 P_F (1 - P_F^A) + P_1 P_D (1 - P_D^A)\big) E_t \cdot (1/M) \tag{15.39}$$

where the first, the second and the third terms refer to the energy consumed in spectrum sensing, legitimate transmission and illegitimate transmission, respectively.

As a comprehensive metric, the individual energy efficiency can be introduced as the ratio of the average achievable throughput to the average energy consumption, as follows

$$\mu = \frac{D}{E} \tag{15.40}$$

It is obvious from the proposed attacker-punishment policy that an attacker will be punished by reducing its scheduling probability that yields in lowering the achievable throughput, and consequently poor energy efficiency. Such punishment can generate a reaction at the attacker side if its energy efficiency falls below a specific threshold. The expected reaction is represented by either leaving the CR or quiting attacking ad switching to a honest mode.

15.5.1 Worst-case scenario

Considering the worst case scenario ($M \gg H$), the analysis can be divided into two cases, (i) before removing the identified attackers ($i \leq W$), and (ii) after removing the identified attackers ($i > W$):

Case I : $i \leq W$: as the number of attackers is very large, then both P_D and P_F approximately equal to 0 and 1, respectively. Substituting that in (15.34), it can be simplified as follows

$$P(U_i = 0)\Big|_{wcI} \approx P_1 \tag{15.41}$$

Using (15.41) and the approximated values of λ_h and λ_a, given in (15.28) and (15.29), the scheduling probability for an honest CU in the worst-case scenario before removing identified attackers can be approximated as follows

$$\begin{aligned}\overline{P_{sh}}\Big|_{wcI} &\approx \frac{P_1 - P_1(1 - P_{dh})}{NP_1 - MP_1(1 - P_{da}) - HP_1(1 - P_{dh})} \\ &\approx \frac{P_{dh}}{MP_{da} + HP_{dh}}\end{aligned} \tag{15.42}$$

Likewise, the scheduling probability for an attacker in the worst-case scenario before removing the identified attackers can be approximated as follows

$$\overline{P_{sa}}\Big|_{wcI} \approx \frac{P_{da}}{MP_{da} + HP_{dh}} \tag{15.43}$$

As P_{dh} is usually much larger than P_{da} , the scheduling probability for an honest CU should be larger than an attacker according to (15.42) and (15.43).

Case II: $i > W$**:** The analysis of this case is different form the previous one since the ignored attackers are no longer affecting the global decision. For sake of simplification, we consider that all attacker have been removed and none of the honest CUs are incorrectly removed. This assumption is reasonable and can be attained by th proposed attacker-identification policy with a proper adjustment of ζ. Also, we consider that the CRN contains a sufficient number of honest CUs that can attain high global detection probability (≈ 1) and low global false-alarm probability (≈ 0) after removing attackers. By applying these assumptions to (15.5) and (15.34), the following approximations can be obtained

$$\lambda_h\Big|_{wcII} \approx P_0 P_{fh} \tag{15.44}$$

$$\lambda_h\Big|_{wcII} \approx P_0 P_{fa} \tag{15.45}$$

$$P(U_i = 0)\Big|_{wcII} \approx P_0 \tag{15.46}$$

However, these approximation can be directly applied to (15.35) since the counters are affected by the first case ($i \leq W$). Instead, it can be applied to (15.31) with taking into account the effect of the first case. Accordingly, the scheduling probability for an honest CU in the worst-case scenario after removing the identified attackers can be approximated as follows

$$\begin{aligned}\overline{P_{sh}}\Big|_{wcII} &\approx \frac{WP_1 + (i-W)P_0 - TP_1(1-P_{dh}) - (i-W)P_0P_{fh}}{N(WP_1 + (i-W)P_0) - M(WP_1(1-P_{da}) + (i-W)P_0P_{fa}) - H(WP_1(1-P_{dh}) + (i-W)P_0P_{fh})} \\ &\approx \frac{WP_1P_{dh} + (i-W)P_0(1-P_{fh})}{WP_1(MP_{da} + HP_{dh}) + (i-W)P_0(N - MP_{fa} - HP_{fh})}\end{aligned} \tag{15.47}$$

and for an attacker as follows

$$\overline{P_{sa}}\Big|_{wcII} \approx \frac{WP_1P_{da} + (i-W)P_0(1-P_{fa})}{WP_1(MP_{da} + HP_{dh}) + (i-W)P_0(N - MP_{fa} - HP_{fh})} \tag{15.48}$$

Comparing (15.47) and (15.48), the reader can notice that the scheduling probability for an honest CU is larger than the scheduling probability for an attacker since $P_{dh} > P_{da}$ and $P_{fh} < P_{fa}$. Also, it can be noted that the difference increases with time.

15.6 Performance Evaluation and Simulation Results

This section provides a comprehensive evaluation of the two proposed polices. Particularly, we show the performance of the proposed attacker-identification policy compared to the proposed policy in [118]. Briefly, the proposed attacker-identification in [118] has the same procedure as ours except that the evaluation is based on the agreement with the global decision taken at the FC. Regarding the proposed attacker-punishment policy, as there is no similar policy in the literature, we explore the performance by comparing the individual energy efficiency between attackers and honest CUs.

A CRN of a fixed number of honest CUs ($H = 5$) is considered. The number of attackers is left variable in order to show its influence on the different system parameters and probabilities. The simulation parameters regarding the licensed spectrum occupancy, energy consumption, and local sensing performance are kept fixed as shown in Table 15.1. Other parameters which differ among figures are listed in the caption of the corresponding figure.

Table 15.1: Simulation Parameters

Parameter	Value	Parameter	Value
P_0	0.5	R	64 $Kbps$
P_{dh}	0.8	T_t	0.03 $secs$
P_{fh}	0.1	E_{css}	11 mJ
P_{da}	0.1	E_t	0.5 J
P_{fa}	0.8	FR	Majority

15.6.1 Attacker-Identification Policy

The probability of incrementing the B_n counter, λ_n, plays a key role in the proposed attacker-identification policy. Fig. 15.3 plots λ_n for honest CUs and attackers versus the total number of attackers present in the CRN. The large difference between λ_h and λ_a even for the whole range of M is due to the reliable evaluation base, i.e., the data delivery, by which the counters are updated. Notice that even in the case of large number of attackers, the honest CUs still have low probability of incrementing their counters compared to the attackers. The initial fluctuation in both curves is due to the FR and odd-even of the total number of CUs (N). For example, at $M = 2$ and $M = 3$, the total numbers of CUs are $N = 7$ and $N = 8$, respectively, while the FR in both cases is $K = 4$. However, the induced fluctuation diminishes as M increases. Another important note is on the range of $M \gg H$, where both λ_h and λ_a stay constant and to the values obtained in (15.28) and (15.29), respectively, which verifies the approximations we made in the worst-case scenario.

The ignoring probability of attackers and honest CUs versus the ignoring threshold for the proposed policy and [118] is shown in Fig. 15.4 at $M = 1$ and in Fig. 15.5 at $M = 10$. In both figures and for both types of CUs, the ignoring probability is a decreasing function of ζ. When the honest CUs represent the

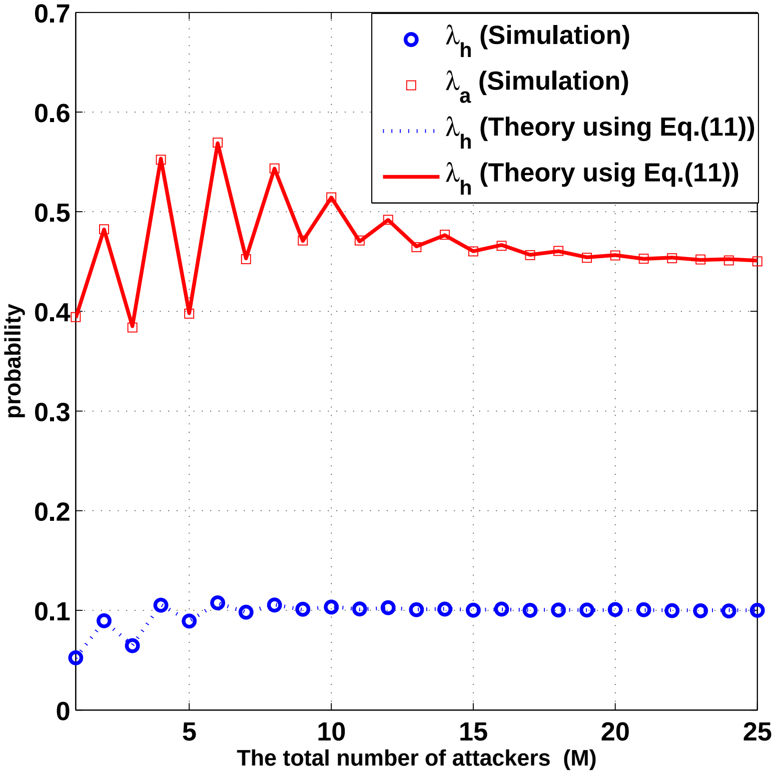


Figure 15.3: The counter's incrementing probability for honest CUs (λ_h) and attackers (λ_a) versus the total number of attackers (M). ($W = 30$)

majority, Fig. 15.4 both policies present a good performance and all attackers can be identified without ignoring any of the honest CUs when ζ is properly adjusted. However, when th attackers pose the majority of the CUs, Fig. 15.5, the ignoring probability of honest CUs is more than for the attackers in the policy proposed in [118], whereas our proposal is still able to provide $P_{igna} = 1$ and $P_{ignh} = 0$ with a proper choice of ζ. This is due to the fact that the global decision is used in [118] as evaluation base, which is mainly affected by the majority of CUs, while our proposal is approximately unaffected by the majority of CUs.

The difference between the ignoring probabilities for attackers and honest

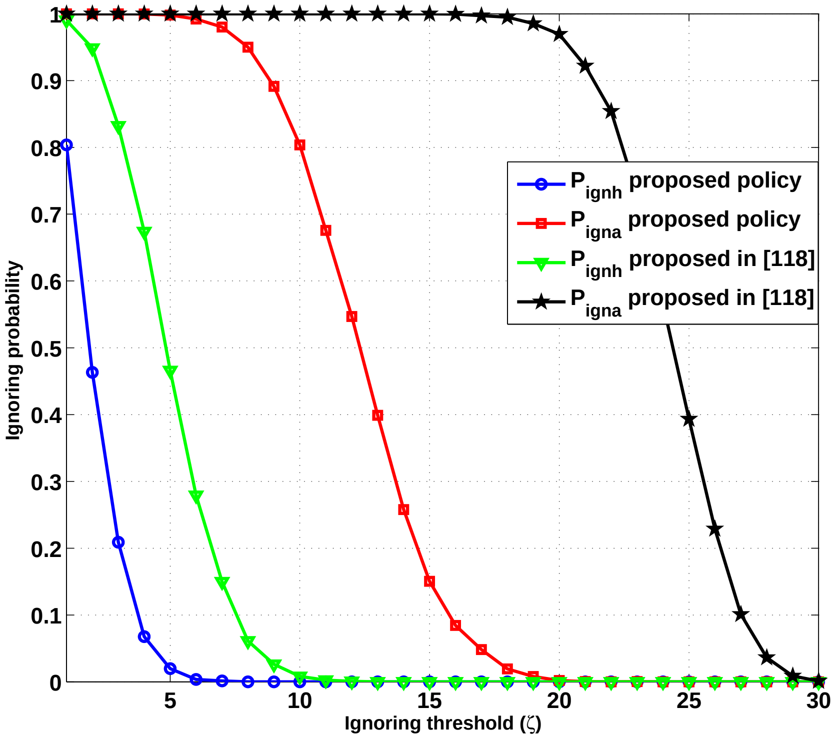


Figure 15.4: The ignoring probability for honest CUs and attackers versus the ignoring threshold (ζ). ($W = 30$, $M = 1$)

CUs, which is used as optimization objective, is shown versus ζ at different durations of the evaluation time window (W) in Fig. 15.6. The curve show a convex shape that achieves its maximum at the optimal ignoring threshold (ζ^*).

From Fig. 15.4, Fig. 15.5 and Fig. 15.6, the importance of optimizing ζ is clear. Thus, we use the optimal ζ that maximizes the difference between P_{igna} and P_{ignh} for the two policies to find the number of ignored attackers and honest CUs versus the total number of attackers, as shown in Fig. 15.7. Regarding our proposal, almost all attackers can be identified whatever their number, and, at the same time, none of the honest CUs will be incorrectly identified as attacker. On the other hand, the proposal of [118] works well only when the majority of

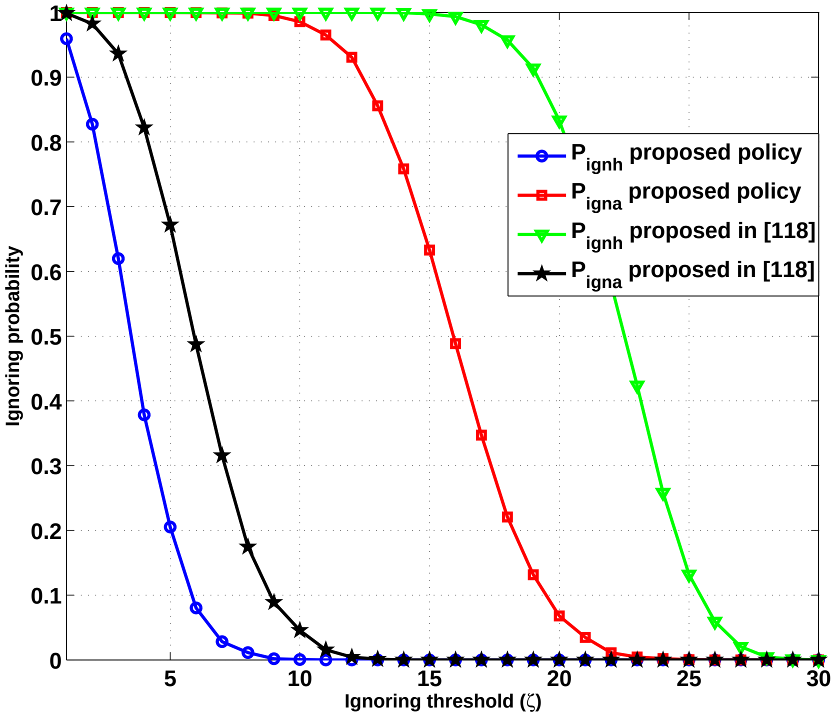


Figure 15.5: The ignoring probability for honest CUs and attackers versus the ignoring threshold (ζ). ($W = 30$, $M = 10$)

CUs are honest. In the case of the majority being attackers, the proposal either identifies all CUs as attackers or does not identify any of them as attackers.

15.6.2 Attacker-Punishment Policy

As we have shown the performance of the proposed attacker-identification policy in the previous results, we now investigate on the performance of the attacker-punishment policy. Particularly, the influence on the individual energy efficiency of attackers and honest CUs will be shown before and after removing the identified attackers from the fusion process. Notice that, as the energy effi-

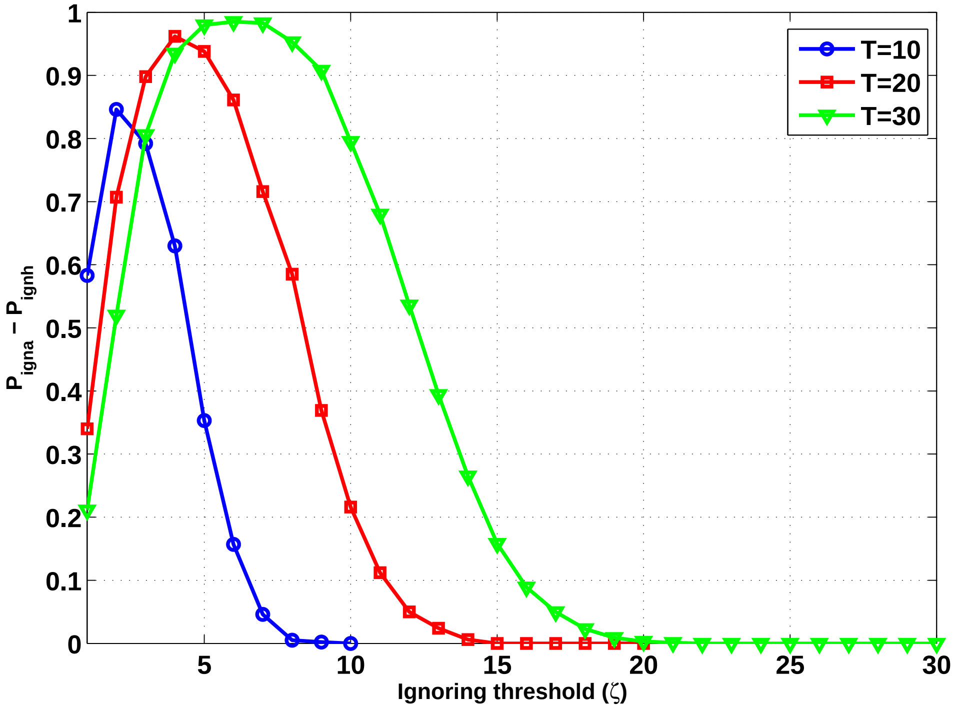


Figure 15.6: The difference between ignoring probability for attackers (P_{igna}) and honest CUs (P_{igna}) versus the ignoring threshold (ζ) for different values of W. ($M = 1$)

ciency combines both the throughput and energy consumption together, there is no need to show them individually.

Fig. 15.8 shows the individual energy efficiency of an attacker and honest CU versus the total number of attackers before removing the identified attackers, i.e. when $i \leq T$. The individual energy efficiency of honest CUs decreases as the number of attackers increases due to the increase in the false alarm and the missed detection rates. Increasing the false-alarm rate degrades the achievable throughput, while increasing the missed-detection rate wastes the energy consumption. The individual energy efficiency of an attacker initially increases and then starts decreasing as the number of attacker increases, as shown in Fig. 15.8.

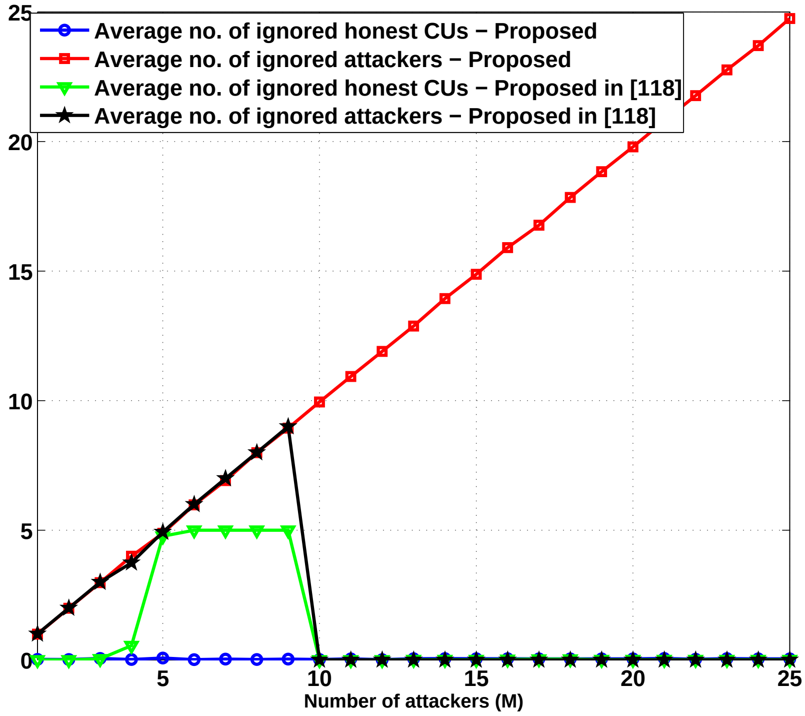


Figure 15.7: The average number of ignored honest CUs and attackers at the optimal ignoring threshold (ζ^*) versus the total number of attackers (M) for the proposed attacker-identification policy and the one proposed in [118]. ($W = 30$, $\zeta = \zeta^*$)

There are two reasons of the initial improvement. The first reason is that increasing the number of attackers will increase the false-alarm rate in the global decision taken at the FC, which increases their chances to exploit the unoccupied channel in an illegitimate transmission. The second reason is decreasing the false alarm rate in the decision made cooperatively by the attackers themselves. However, at large number of attackers, the individual energy efficiency degrades as they equally share the illegitimate transmission. An important note is that if we equally distribute the legitimate transmission opportunities among all CUs, i.e. without punishment, an attacker will legitimately achieve the same energy efficiency as an honest CUs, and due to the illegitimate transmission attackers will achieve higher energy efficiency than honest CUs.

From Fig. 15.8, the proposed attacker-punishment policy succeeds i reducing the energy efficiency of attackers at low number of attackers. However, in the presence of large number of attackers the proposed policy can not provide the desired performance unless the attackers are removed. Fig. 15.9 and Fig. 15.10 plot the individual energy efficiency of an attacker and an honest CU versus the ignoring threshold (ζ) after removing the identified attackers at $M = 1$ and $M = 10$, respectively. Apparently, ζ has a significant role in the performance of the attacker-punishment after removing the identified attackers ($i > W$). A proper choice of ζ can remove all attackers from the fusion process and leave only the honest CUs. Hence, the former effect of the attackers on the sensing performance (P_D and P_F) will be totally eliminated, which consequently, reduces the illegitimate throughput of attackers. Notice that at $\zeta = W$, none of the attackers nor the honest CUs will be removed and thus the obtained values will be exactly as in the case of $i \leq W$.

The optimization of ζ should be carried out in order to avoid punishing honest CUs rather than attackers. In Fig. 15.11, ζ is set to the optimal value, and the individual energy efficiency of an attacker and an honest CU are found versus the number of attackers. The high performance of the proposed attacker-punishment policy clearly appears in the difference in the energy efficiency even in the case of large number of attackers. The individual energy efficiency of an honest CU slightly decreases as the number of attackers increases due to the increase in the probability of not-detecting some of the attacker as their number increases. However, the energy efficiency of an honest CU is still more than twice the energy efficiency of an attacker.

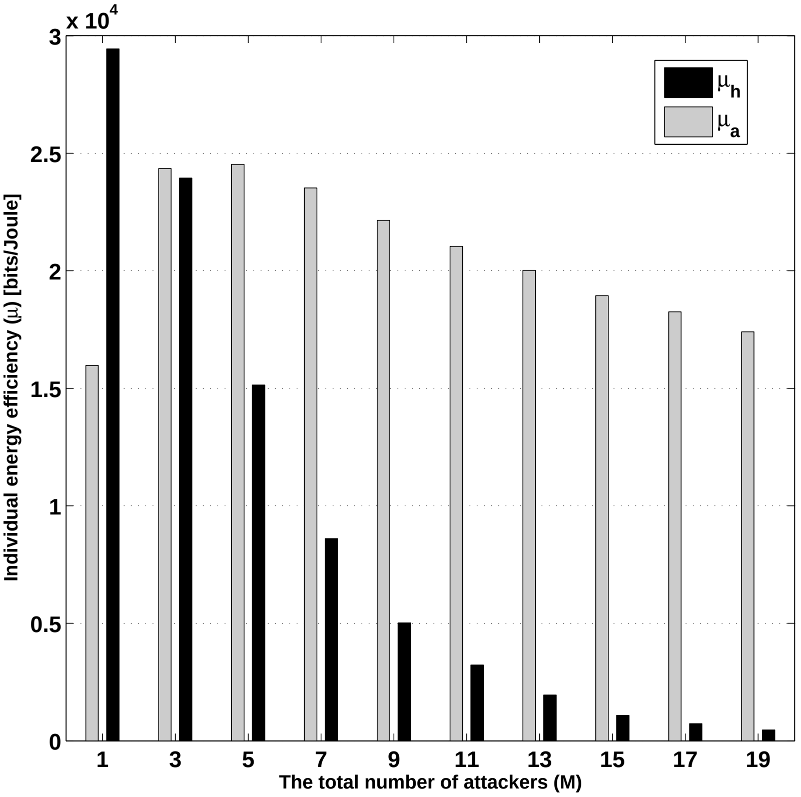


Figure 15.8: The individual energy efficiency of an honest CUs and an attacker versus the total number of attackers (M) before removing the identified attackers ($i \leq W$). ($W = 30$)

15.7 Summary

Two policies to combat spectrum sensing data falsification attackers in infrastructure-based cognitive radio networks have been proposed. The first policy is an attacker-identification policy that aims at detecting attackers and ignoring their reported sensing results. The second is an attacker-punishment policy that redistributes the transmission opportunities among users based on their local performance. Both policies are developed based on a novel approach for assessing the local performance according to the delivery of the

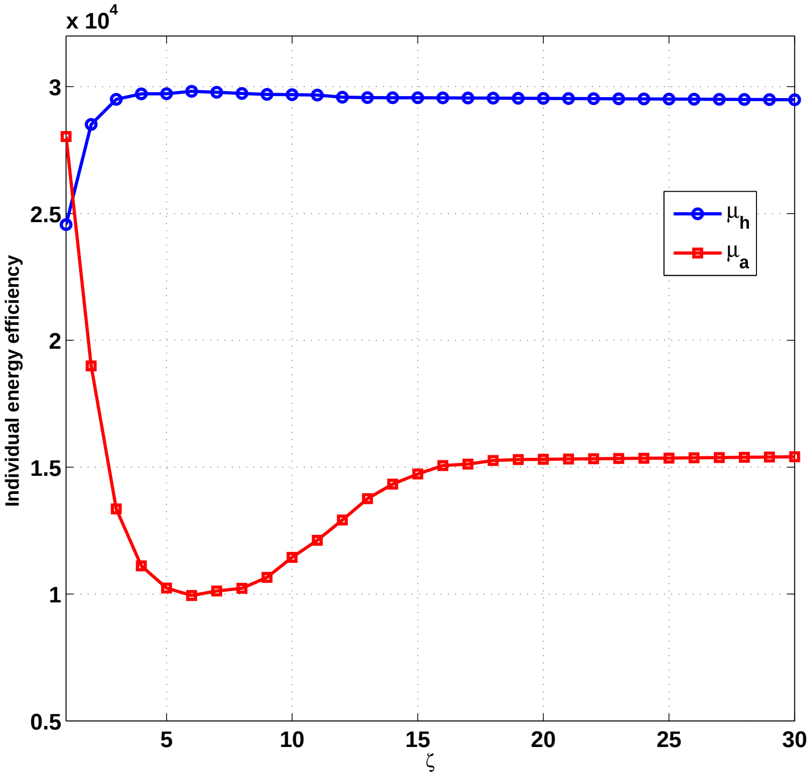


Figure 15.9: The individual energy efficiency of an honest CUs and an attacker versus the ignoring threshold (ζ) after removing the identified attackers ($i > W$). ($M = 1, W = 30$).

transmitted data. Analytical and simulation results have shown that the attacker -identification policy is able to identify attackers whatever their number in the network. Also, it has been shown through simulations that the proposed attacker-punishment policy is able to punish attackers by degrading their individual energy efficiency compared to the honest users.

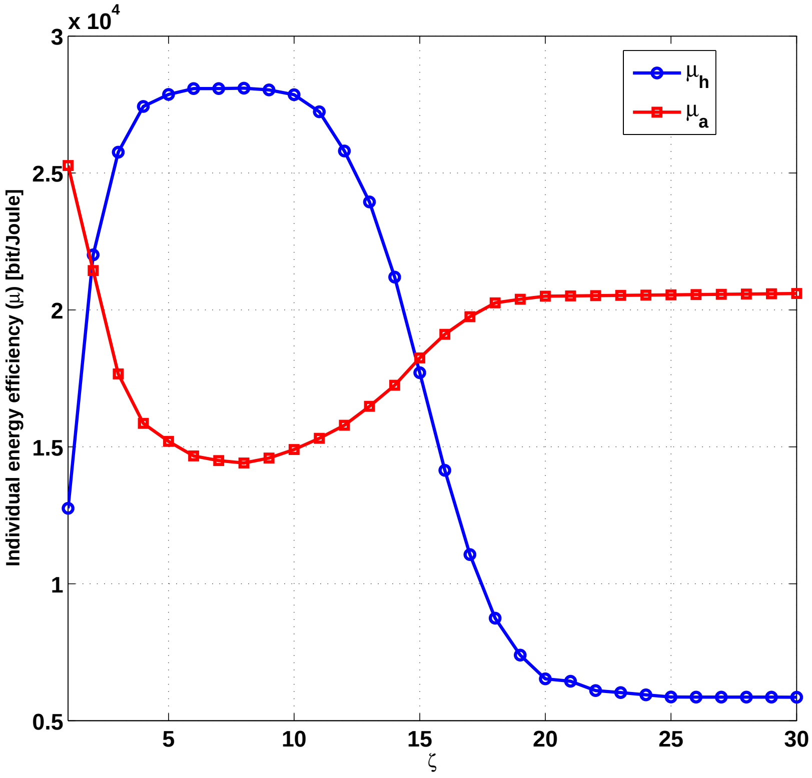


Figure 15.10: The individual energy efficiency of an honest CUs and an attacker versus the ignoring threshold (ζ) after removing the identified attackers ($i > W$). ($M = 10$, $W = 30$).

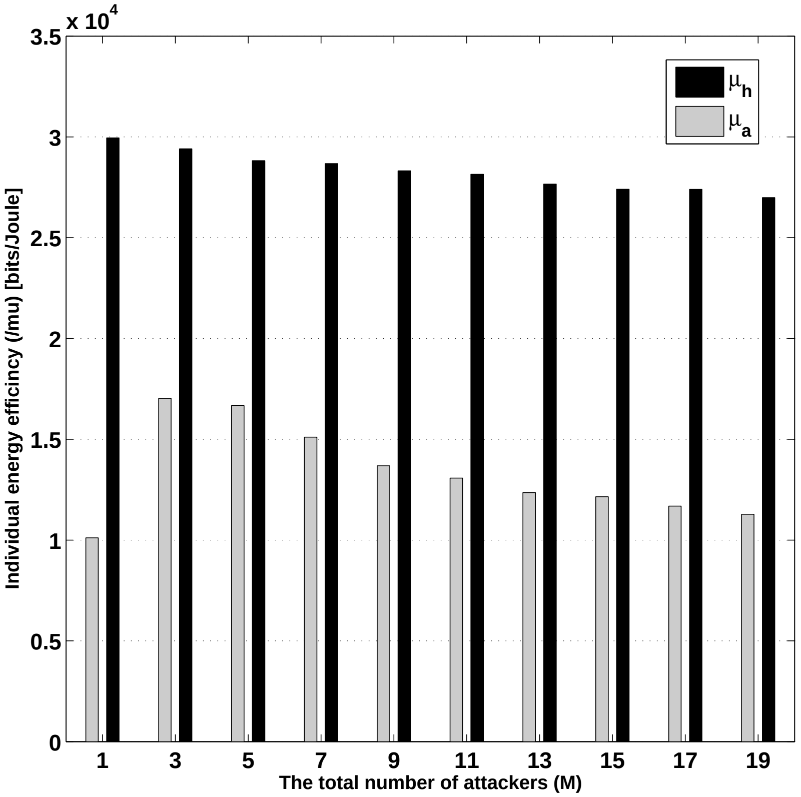


Figure 15.11: The individual energy efficiency pf an honest CUs and an attacker at the optimal ignoring threshold (ζ^*) versus the total number of attackers (M) after removing the identified attackers ($i > W$). ($W = 30$, $\zeta = \zeta^*$)

CHAPTER 16

A LOW-OVERHEAD SECURITY PROTOCOL FOR COOPERATIVE SPECTRUM SENSING IN COGNITIVE RADIO NETWORKS

16.1 Introduction

A possible approach to prevent SSDF outsider attack in CSS is to create a secure link between CUs and FC, implying that only the reported results from authenticated CUs are accepted and used to make the final decision. In a secure link, authentication and integrity are fundamental properties. The receiver of a data message is able to recognize that the conveyed information comes from the legitimate sender (authentication) and the information was not modified in transit (integrity). However, due to the overhead required in cryptographic mechanisms, previous works on this field are mainly based on intrusion detection techniques instead of using cryptographic operations.

In this chapter, we propose a low-overhead symmetric cryptographic mechanism that reduces the effects of the external attackers on the detection accuracy and the energy efficiency of the legitimate network. To the best of our knowledge, introducing authentication in the centralized CSS process has never been proposed previously in the literature.. The proposed mechanism implies that the FC and legitimate CUs share some data that are used to generate authentication code reported to the FC. The required data are updated by the FC and sent to the legitimate CUs. However, using a cryptographic mechanism generates long codes that should be reported to the FC, which results in extra energy consumption. For this reason, the generated code is truncated to a small number of bits that is further optimized to maximize detection accuracy and energy efficiency.

A related work can be found in [136], where authors also show the efficiency of introducing the authentication in non-centralized CSS based on ad-hoc CRN scenario. However, the considered scenario in [136] implies performing authentication and integrity between each two neighboring CUs. Hence, the requirements of this scenario are different and do not allow for the novelties proposed in our protocol. Namely, the protocol in [136] suggests unique keys per CU pair, user identities are mandatory and no variability on the security bits is proposed.

16.2 System Model

We consider a CRN consisting of L legitimate CUs that try to access a licensed spectrum whenever it is free. The probability that the spectrum is not being used by any licensed user is denoted by P_0. In order to avoid collision with licensed users, each CU is enforced to sense and make a local binary decision $u_i\{1, 0\}$ about the spectrum status. If $u_i = 1$, then the CU decides that the spectrum is used. Otherwise, the spectrum is identified as unused by the i^{th} CU. The reliability of the local decision u_i is evaluated by the local detection probability ($P_{d,i}$) and the local false-alarm probability ($P_{f,i}$).

In view of CSS, all local decisions have to be reported to the FC, where the *K-out-of-N* rule [45] is employed to process these received decisions in order to make a global decision about spectrum occupancy. However, due to the effects of the channel between CUs and FC, called reporting channel, the reported decisions may be received in error [23]. We adopt a symmetric noisy channel model for the reporting channel between the FC and each CU with a bit-error rate $P_{e,i}$.

However, in such an environment, it is possible to have some other CUs that try to invade the legitimate CRN, and consequently, degrade the overall performance. These CUs are usually called attackers or malicious users. The strategy of these attackers consists of reporting false data about the spectrum status in order to mislead the global decision of the CRN. There are several types of attacks based on the reported false data. In this work, we consider the worst case, where the attacker reports a decision that is the opposite of its actual spectrum sensing result. Without loss of generality, we assume that all legitimate CUs have equal local detection and false-alarm probabilities represented by P_d and P_f, respectively. Also, all attackers have local detection and false-alarm probabilities represented by q_d and q_f, respectively. The number of attackers is denoted by M so that the total number of CUs, legitimate and attackers, becomes $N = L + M$. Also, the quality of reporting channel is considered identical for all CUs, legitimate and attackers, with a bit-error probability P_e.

The overall detection accuracy of CSS process is assessed by computing two metrics regarding the global decision, namely, the overall detection probability (P_D) and the overall false alarm probability (P_F). Both probabilities are combined in one metric that indicates the false-decision probability, denoted by ϵ, given as follows:

$$\epsilon = P_0 P_F + P_1(1 - P_D) \tag{16.1}$$

where $P_1 = 1 - P_0$. The first term in (16.1) refers to the false alarm case, whereas the second term represents the missed detection case.

The overall performance of the cognitive transmission is measured by the obtainable energy efficiency (μ) of the considered CRN. Energy efficiency is given as follows

$$\mu = \frac{P_0(1 - P_F)R\,T_t}{E_{css} + P_{unused}E_t} \tag{16.2}$$

where R is the data rate in bps, T is the transmission time, E_t is the transmit energy by the scheduled CU, P_{unused} is the transmitting probability and E_{css} is the energy consumed by all legitimate CUs during CSS.

Since the reported decisions are submitted without any accompanied transmitter identification, the decisions reported by attackers will be considered and processed together with decisions from legitimate CUs. Thus, the resulting detection accuracy will be influenced, and consequently, the obtainable energy efficiency. The degradation in overall performance of the CRN depends on the number of attacks, their actual local performance, and the reporting channel quality. Next, we discuss the conventional insecure CSS in detail, and then we propose a novel secure CSS that can mitigate the impact of the malicious users.

16.3 Conventional (Insecure) Cooperative Spectrum Sensing

In conventional CSS, local decisions made by CUs are reported to the FC as they are, i.e., no security protocol is applied. This is due to the small amount of the reported data (a single bit), avoiding any transmission delay and saving the limited energy resources. Consequently, all reports from legitimate and attacker CUs are received at the FC and handled as honest reports, since the FC has no ability to distinguish between CUs. However, due to channel impairments, the transmitted local decision may be corrupted, and thus, inverted at the FC. Therefore, the local performance of each CU will appear at the FC differently from the actual values. Let us define P_x and P_y as the local detection and local false-alarm probabilities for a legitimate CU as they appear at the FC, respectively. P_x and P_y are expressed as follows

$$P_x = P_d(1 - P_e) + (1 - P_d)P_e \tag{16.3}$$

$$P_y = P_f(1 - P_e) + (1 - P_f)P_e \tag{16.4}$$

and similar quantities for an attack are defined as follows:

$$q_x = q_d(1 - P_e) + (1 - q_d)P_e \tag{16.5}$$

$$q_y = q_f(1 - P_e) + (1 - q_f)P_e \tag{16.6}$$

According to the *K-out-of-N* FR, the overall detection and false-alarm probabilities of conventional CSS can be expressed in mathematical forms for arbitrary values of K as follows:

$$P_D^{insec} = \sum_{k=K}^{N} \sum_{j=1}^{\binom{N}{k}} \prod_{i \in A_j^{(N,k)}} P_{x,i} \prod_{i \notin A_j^{(N,k)}} \left(1 - P_{x,i}\right) \tag{16.7}$$

$$P_F^{insec} = \sum_{k=K}^{N} \sum_{j=1}^{\binom{N}{k}} \prod_{i \in A_j^{(N,k)}} P_{y,i} \prod_{i \notin A_j^{(N,k)}} \left(1 - P_{y,i}\right) \tag{16.8}$$

where $A_1^{(N,k)}, A_2^{(N,k)}, ..., A_{\binom{N}{k}}^{(N,k)}$ represent all the possible combinations of k integers drawn from the interval $[1, N]$, where the number of these combinations is $\binom{N}{k}$. Notice that if the i^{th} CU is a legitimate (an attacker), $P_{x,i}$ and $P_{y,i}$ are replaced by P_x and P_y (q_x and q_y), respectively.

A popular FR that is derived from the *K-out-of-N* FR by setting $K = 1$ is called OR-Rule. In OR-Rule, if at least one local decision is received at the FC as 1, then the global decision will be 1. Otherwise, the global decision is 0. In this work we adopt OR-Rule as the employed FR since it is preferred as it limits the induced interference to the licensed users by reducing the missed detection probability. Both (16.7) and (16.8) can be rewritten for OR-Rule as follows, respectively

$$P_D^{insec} = 1 - \big(1 - P_x\big)^L \big(1 - q_x\big)^M \tag{16.9}$$

$$P_F^{insec} = 1 - \big(1 - P_y\big)^L \big(1 - q_y\big)^M \tag{16.10}$$

The achievable false-decision probability, ϵ^{insec}, transmission probability (P_t^{insec}) and energy efficiency (μ^{insec}) for conventional CSS can be easily computed by proper substitution of P_D^{insec}, P_F^{insec} and E_{css}^{insec} instead of P_D, P_F and E_{css} in (16.1), (5.2) and (16.2), respectively. E_{css}^{insec} denotes the energy consumption during sensing and reporting by all legitimate CUs in conventional CSS, which is defined as follows

$$E_{css}^{insec} = LE_s + LE_r \tag{16.11}$$

where E_s and E_r is the energy consumed in local sensing and result reporting for one CU, respectively.

In the view of OR-Rule, the effects of the performance of malicious users can be clearly seen in (16.9) and (16.10), where decreasing q_x decreases P_D^{insec} and increasing q_y increases P_F^{insec}. As previously mentioned, these effects are directly reflected on the achievable energy efficiency of the legitimate CRN.

16.4 Secure Cooperative Spectrum Sensing

This section introduces a security protocol to prevent CSS from spectrum sensing data falsification attacks under a trade-off between security and energy efficiency. This protocol consists of a low-overhead security mechanism based on symmetric cryptography with a tunable number of security bits. The objective of the security mechanism is to authenticate the spectrum sensing reports from legitimate CUs and reject reports from malicious users with a probability that is proportional to the number of security bits.

The proposed mechanism is based on the generation of unforgeable Message Authentication Codes (MAC) [137] that are computed and sent by legitimate CUs and validated by the FC. A MAC is a sequence of B bits generated with a Hash function $H(\cdot)$ [138]. A Hash function is a one-way function that always outputs a fixed length bit sequence for an input data of arbitrary length. Hash functions cannot be inverted, thus for a given output it is computably impossible to obtain the input data. Moreover, a secret key that is only known by legitimate CUs and the FC is used for MAC generation, depriving malicious users of the capability of MAC generation. These features make MACs very suitable for data authentication and integrity. The drawback is the MAC length; a hash function output is commonly between 128 and 256 bits (depending on the function), thus this technology may have a high cost in low debit systems (systems with small data transmissions). In the proposed mechanism the MAC is truncated to the first B bits, in order to achieve less security overhead and increased energy efficiency in a tread-off with security.

On the contrary with respect to digital signatures, where computation of intensive public key cryptography is used, MAC uses a pre-shared symmetric key (PSK) between the intended participants, the legitimate CUs and the FC. In the proposed approach, at initialization phase, the FC must agree on a Master Session Key to all legitimate CUs. The MSK can be obtained by encrypting the MSK with a long term PSK, by using extensible authentication protocol (EAP) [139] or by means of digital certificates (DC) [140]. After initialization phase, legitimate CUs and FC use the MSK to derive a Temporal Key (TK) that can be used to provide authentication, integrity and/or confidentiality. TK computations is performed with a Hash function and triggered by the FC that provides the extra information required: "TK = H(*Info* $||$ MSK)" (where the operator $||$ refers to concatenation of two bit sequences). The sequence *Info* is computed randomly by the FC and provided to all legitimate CUs. This information is periodically sent by the FC in order to renew the TK. The lifetime of a TK is related to a timer or the volume of secured traffic exchanged. Note that the MSK is only used for TK derivation, it has little exposure, so there is no need for its periodical renewal. It is worth noting that it is common practice to provide a unique MSK per CU, hence unique TK. In our protocol, however, all authenticated users share the same MSK and TK, hence there is no need to add the identities of the legitimate CUs in the reports for authentication purposes. The FC only needs to distinguish between legitimate CUs and malicious users, but there is no need to differentiate legitimate CUs.

In each spectrum sensing round, the legitimate CUs independently compute the same MAC using the TK and a new Nonce (random number used only once) sent by the FC and truncate this MAC to the first B bits:

$$MAC = \lceil H(TK||Nonce) \rceil^{B} \tag{16.12}$$

where the function $\lceil x \rceil^{y}$ denotes the truncation operation of x to the first y bits. Upon computing the MAC, each legitimate CU will produce the report that should be transmitted to the FC, as follows

$$Report = MAC \oplus u_i \tag{16.13}$$

where $\oplus$ denotes the 'XOR' operator. Function (16.13) implies that if the local decision identifies the channel as unused, i.e., $u_i = 0$, the transmitted report of the corresponding legitimate CU will be exactly as the MAC. On the other hand, if the channel is identified as used, i.e, $u_i = 1$, the transmitted report will be the inverse of the generated MAC.

At the FC side, the FC generates the same MAC and validates the received reports matching with the MAC or its inverse as '0' or '1', respectively. Any other reports will be neglected. Remember that all CUs compute the same MAC because they use the same TK and the same nonce. The Nonce is provided during the initialization phase (when the FC authenticates CUs and provides the MSK) and is renewed in every spectrum sensing round when the FC provides the decision on the channel availability. The Nonce prevents against replay-attacks [138] since the generated MACs in consecutive spectrum sensing rounds are different. Thus, an attacker cannot obtain a valid report from a legitimate CU and re-submit it in a different period. The replay attack that is able to submit a report at the same spectrum sensing period will be discussed later. Fig. 16.1 illustrates how the proposed security protocol works.

The difference between the proposed authentication mechanism and common security mechanisms is the truncation of the MAC, and the absence of of

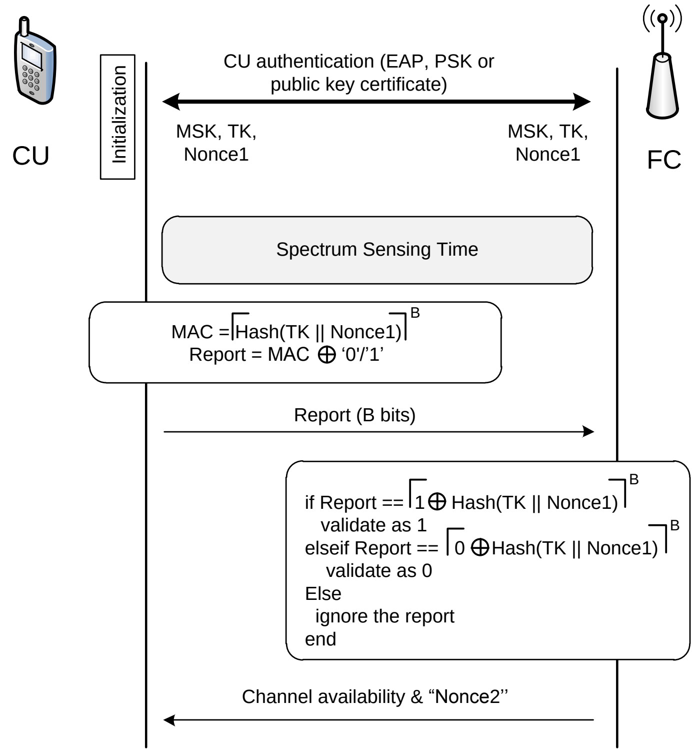

CU
Initialization
CU authentication (EAP, PSK or public key certificate)
MSK, TK, Nonce1
MSK, TK, Nonce1
FC
Spectrum Sensing Time
MAC = ⌈Hash(TK || Nonce1)⌉^B
Report = MAC ⊕ '0'/'1'
Report (B bits)
if Report == ⌈1 ⊕ Hash(TK || Nonce1)⌉^B
validate as 1
elseif Report == ⌈0 ⊕ Hash(TK || Nonce1)⌉^B
validate as 0
Else
ignore the report
end
Channel availability & "Nonce2"

Figure 16.1: Description of the security protocol proposed and message exchage. The symbol $\oplus$ refers to the arithmetic operation "xor".

any extra information transmitted with the report, i.e. CUs identities and the authenticated data (sensing information). This is possible due to the special characteristics of the CRN scenario, where there is no need to differentiate legitimate CUs and the transmitted sensing information is binary, i.e. 'busy' or 'available' channel.

The penalty for the MAC truncation is that the malicious users can now randomly pick a sequence of B bits and get its report validated by the FC if it matches the actual MAC or its inverse. As a consequence, our proposal presents a trade-off between the energy consumed in overhead for authentication purposes and the level of security achieved. However, the fact of truncating the MAC to a small sequence of bits has no further disadvantages in terms of security. Note that the decrease of the MAC length produces an increase in the probability of collision (probability of finding messages producing the same given MAC), thus it protects the TK against brute force search [138], providing TKs with longer lifetime. Moreover, the avalanche effect of hash functions (capability of significantly change the output when a minor change occurs in the input) maintains the effectiveness of the proposed protocol even when B is small.

16.4.1 Detection Accuracy and Energy Efficiency

Following the proposed secure protocol, a received report at the FC from a legitimate CU will be validated only if it matches the actual MAC or its inverse. However, considering the noisy reporting channel, the sent reports may suffer from probable error during transmission, and thus, arrive at the FC modified. At the FC, the received report will be regarded only in two cases: either all the

B bits remain unaffected or all of them have been inverted. In all other cases, the report will be neglected. Mathematically, the validation probability of a received report from legitimate CU (P_{val}^{leg}) is given as follows for legitimate CU,

$$P_{val}^{leg} = (1 - P_e)^B + P_e^B \tag{16.14}$$

while the neglecting probability of a received report from a legitimate CU (P_{neg}^{leg}) is given as follows

$$P_{neg}^{leg} = 1 - (1 - P_e)^B - P_e^B \tag{16.15}$$

Accordingly, P_x^{leg} and P_y^{leg} will be different from the case of conventional CSS due to the multiple-bit report, which can be respectively expressed as follows

$$P_x^{leg} = P_d(1 - P_e)^B + (1 - P_d)P_e^B \tag{16.16}$$

$$P_y^{leg} = P_f(1 - P_e)^B + (1 - P_f)P_e^B \tag{16.17}$$

Clearly, as report length increases, both P_x^{leg} and P_y^{leg} will be decreased. While the decrease in P_x^{leg} degrades the overall detection probability, the decrease in P_y^{leg} improves the overall false-alarm probability.

Regarding the performance of the attack according to secure CSS, we consider that a malicious users generates a random report of B bits and transmits it to the FC. Similar to the legitimate CUs, the attack report will be validated only if its identical to the MAC (validated as 0) or its inverse (validated as 1). In all other cases, the report will be neglected. Thus the validating and neglecting probability for an attack are respectively given as follows

$$P_{val}^{att} = \frac{2}{2^B} \tag{16.18}$$

$$P_{neg}^{att} = 1 - \frac{2}{2^B} \tag{16.19}$$

Compared to the conventional insecure CSS, the validation probability of attacker's report is reduced from 1 to $\frac{2}{2^B}$ that decreases as B increases, while the neglecting probability is increased from 0 to $1 - \frac{2}{2^B}$ that increases as B increases.

By the same way, the detection and false-alarm probabilities of an attacker as it appears at the FC can be evaluated as follows

$$q_x^{sec} = q_d \frac{1}{2^B} + (1 - q_d) \frac{1}{2^B} = \frac{1}{2^B} \tag{16.20}$$

$$q_y^{sec} = q_f \frac{1}{2^B} + (1 - q_f) \frac{1}{2^B} = \frac{1}{2^B} \tag{16.21}$$

It is worth noting that both q_x^{sec} and q_x^{sec} are independent of the actual local performance, i.e., q_d and q_f, and of the channel effects, i.e., P_e, representing the main benefit of the proposed security protocol. This independence is due to the random generation of the report.

Fig. 16.2 shows the sensing performance of the legitimate CUs and the attackers versus B and P_e. At a given P_e, as increasing B results in a decreasing the probability of receiving an error-free report, it decreases the detection probability of an honest CU. However, the false-alarm probability of both types of users is decreased as B increases. Notice that the degradation rate with respect to B on the performance of an attacker is much faster than it on the sensing performance of an honest CU.

The effects of P_e on the individual performance of users are shown in Fig. 16.2-b. As can be seen, both P_x^{leq} and P_y^{leg} start from their initial values, P_d and P_f respectively, and draw a convex curve as P_e increases with minimum values at $P_e = P_d$ and $P_e = P_f$, respectively. The cnvex shape is due to the contrasting effects of increasing P_e as they appear in the two terms of (16.16) or

(16.17). The constant value of the q_x^{sec} ($\equiv q_y^{sec}$) can be interpreted as a result of the random generation of the reports by the attackers accompanied by symmetric uniform noisy reporting channel.

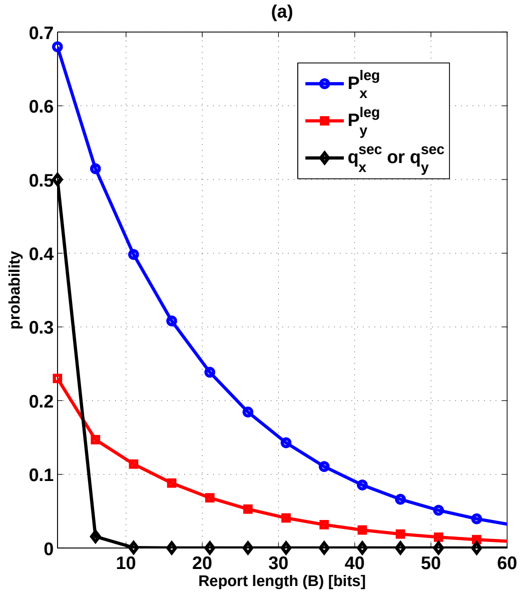


Figure 16.2: *The sensing performance for a legitimate CU and an attack versus (a) report length at $P_e = 0.05$ and (b) bit error probability at $B = 2$. In both curves $P_d = 0.7$, $P_f = 0.2$, $q_d = 0$ and $q_f = 1$.*

The overall detection accuracy of the proposed secure CSS, represented by the overall detection (P_D^{sec}) and false alarm probabilities (P_F^{sec}), can be easily obtained by replacement of the local performance of legitimate CUs and attackers in (16.9) and (16.10) by the values indicated in (16.16), (16.17), (16.20) and (16.21), as follows

$$P_D^{sec} = 1 - \big(1 - P_x^{leg}\big)^L \big(1 - \frac{1}{2^B}\big)^M \tag{16.22}$$

$$P_F^{sec} = 1 - \big(1 - P_y^{leg}\big)^L \big(1 - \frac{1}{2^B}\big)^M \tag{16.23}$$

The achievable false-decision probability for secure CSS, denoted by ϵ^{sec}, the achievable energy efficiency for secure CSS, denoted as μ^{sec}, and the transmission probability for secure CSS, denoted as P^{sec}_{unused}, can be easily obtained by replacing P_D and P_F in (16.1), (16.2) and (5.2) by P^{sec}_D and P^{sec}_F, given in (16.22) and (16.23), respectively. While the average total energy consumption during CSS E_{css} in (16.2) should be replaced by E^{sec}_{css} that is expressed as follows

$$E^{sec}_{css} = LE_s + LBE_r \tag{16.24}$$

16.4.2 Performance in Presence of Replay Attacks

The attack considered in our study consists of a random computation of B bits by the malicious user. The performance of this attack is formulated in previous section. However, in this scenario the special case of replay attacks must be carefully evaluated.

A replay attack in CSS is performed by a malicious user, and consists in the re-submission of a valid report from a legitimate user. In general, the effectiveness of a replay attack depends on two parameters, (i) the ability of the attacker to distinguish the legitimate CUs from other attackers, and (ii) the ability to perfectly hear the report. We must also assume that the security protocol is public and the attacker knows that the different sensing decisions are represented by inverted bit sequences. Now let us consider a worst-case scenario, where a malicious user first intercepts an error-free report from a legitimate CU and then inverts the bit sequence. The attacker can only use the inverted report in the current spectrum sensing session since the following session uses a unique nonce, leading to a different MAC. If the attacker uses the intercepted report in a different sensing period the effectiveness of such an attack is equivalent of computing randomly the B bits (the attack considered in previous section). In our study we make the reasonable assumption that there is no enough time window to efficiently perform a replay attack within only one spectrum session period. However, the implications of such an attack are derived in this section. If an attacker is able to intercept, invert and re-submit a valid report in the same spectrum sensing session, it will severely affect the performance of the CSS. The attacker will perform exactly opposite to the legitimate CU. Thus, its sensing performance at the FC is represented as follows:

$$q_x^{re} = (1 - P_d)(1 - P_e)^B + P_d P_e^B \tag{16.25}$$

$$q_y^{re} = (1 - P_f)(1 - P_e)^B + P_f P_e^B \tag{16.26}$$

Unlike the performance of the normal attack where the bit sequence is randomly obtained, described in (16.20) and (16.21), the performance of the replay attack depends on the sensing performance of the legitimate CUs and the reporting channel quality.

It is worth noting the importance of using random numbers (nonces) for MAC generation. No sequential numbers are valid, since the attacker could predict a future sequential number, then it could play the role of the FC and challenge an honest CU in order to obtain a valid Hash-MAC for the sensing period of the predicted sequence number.

16.5 Comparison and Performance Optimization

The report length, i.e., B, of the proposed secure CSS is a key parameter in the evaluation of the overall performance with respect to detection accuracy and energy efficiency. Generally, longer report increases the neglecting probability of an attacker (16.19). On the other hand, the probability of receiving an error-free report from a legitimate CU decreases, thus increasing the probability of neglecting a valid report from the legitimate CU (16.15). These two contrasting factors impact the overall detection accuracy and the energy efficiency. Thus, the report length should be optimized based on the above observations. We start this section by proving that a single-bit secure CSS can outperform the conventional insecure CSS under any circumstances in both detection accuracy and energy efficiency.

16.5.1 Secure CSS vs Insecure (Conventional) CSS

Let us denote the secure CSS when $B = 1$ by single-bit secure CSS. Notice that P_x^{leg}, P_y^{leg}, and E_{css}^{sec} for single-bit secure CSS are identical for the corresponding values in conventional CSS, and the differences are in the values of q_x and q_y, which affects P_D, P_F, ϵ and μ. In this subsection we prove the superiority of the single-bit secure CSS over conventional CSS in terms of ϵ and μ.

Regarding ϵ, the superiority of the single-bit secure CSS can be ensured if the following condition is satisfied

$$\epsilon^{sec} \leq \epsilon^{in} \tag{16.27}$$

which can be rewritten as follows

$$P_1(1 - P_D^{sec}) + P_0 P_F^{sec} \leq P_1(1 - P_D^{in}) + P_0 P_F^{in} \tag{16.28}$$

$$P_1(1-P_x^{leg})^L(\frac{1}{2})^M + P_0\Bigg(1-(1-P_y^{leg})^L(\frac{1}{2})^M\Bigg) \leq P_1(1-P_x)^L(1-q_x)^M + P_0\Bigg(1-(1-P_y)^L(1-q_y)^M\Bigg) \tag{16.29}$$

since $P_x^{leg} = P_x$ and $P_y^{leg} = P_y$ at $B = 1$, then the previous condition can be simplified as

$$P_1(1-P_x)^L\Bigg((\frac{1}{2})^M - (1-q_x)^M\Bigg) + P_0(1-P_y)^L\Bigg(((1-q_y)^M - (\frac{1}{2})^M\Bigg) \leq 0 \tag{16.30}$$

Based on the fact that $q_x \leq 0.5 \leq q_y$ for any attack[1], the two terms in (16.30) are negative, and thus the condition given in (16.27) is always satisfied. Therefore, the single-bit-secure CSS always provides less false-decision probability than the conventional CSS.

Similarly, the sufficient condition in energy efficiency is formulated as follows

$$\mu^{sec} \geq \mu^{in} \tag{16.31}$$

which can be rewritten as follows

$$\frac{P_0(1-P_F^{sec})R\,T_t}{E_{css}^{sec} + P_t^{sec}E_t} \geq \frac{P_0(1-P_F^{in})R\,T_t}{E_{css} + P_t^{in}E_t} \tag{16.32}$$

since $E_{css}^{sec} = E_{css}^{insec}$ when $B = 1$, and by performing cross product and some cancellation in both sides, the previous condition is rewritten as follows

$$(1 - P_F^{sec})(E_{css} + P_t^{in}E_t) \geq (1 - P_F^{in})(E_{css} + P_t^{sec}E_t) \tag{16.33}$$

[1] Notice that if an attack has $q_x > 0.5$ or $q_y < 0.5$, it no longer will be considered as an attack.

using (16.10) and (16.23), (16.33) can be rearranged into

$$E_{css}(1-P_y)^L\bigg((\frac{1}{2})^M-(1-q_y)^M\bigg)+E_t(1-P_y)^L\bigg((\frac{1}{2})^M P_t^{in}-(1-q_y)^M P_t^{sec}\bigg)\geq 0 \tag{16.34}$$

substituting the values of P_t^{in} and P_t^{insec}, the previous formula results in

$$E_{css}(1-P_y)^L\bigg((\frac{1}{2})^M-(1-q_y)^M\bigg)+E_t(1-P_y)^L(1-P_x)^L(\frac{1}{2})^M\bigg((1-q_x)^M-(1-q_y)^M\bigg)\geq 0 \tag{16.35}$$

Now, it is easy to note that both terms are positive and thus the condition in (16.31) always holds.

It is worth mentioning that the superiority of the single-bit secure CSS over the conventional CSS is satisfied regardless the number of the attackers, the performance of attackers, the performance of the legitimate CUs and the reporting channel quality.

16.5.2 Report Length Optimization

As we have proved the superiority of the proposed single-bit secure CSS over the conventional secure CSS, we now formulate optimization problems for the report length for different objectives. Minimizing the false-decision probability and maximizing the achievable energy efficiency represent the major interests of any system designer in the framework of cognitive radio networks.

The optimal report length, i.e., number of security bits, that minimizes false decision probability, denoted by $B^{min\epsilon}$ can be expressed as follows

$$B^{min\epsilon}=\arg\min_{B}\epsilon^{sec}=\arg\min_{B}P_1-P_1P_D^{sec}+P_0P_F^{sec} \tag{16.36}$$

by using Lagrange method, $B^{min\epsilon}$ can be found by solving the following equation

$$P_1 \frac{\partial P_D^{sec}}{\partial B} = P_0 \frac{\partial P_F^{sec}}{\partial B} \tag{16.37}$$

Let us consider $(1 - P_e)^B \approx 1 - P_e B$ and $P_e^B \approx 0$, then P_x^{leg} and P_y^{leg} can be rewritten respectively as follows

$$P_x^{leg} = P_d(1 - P_e B) \tag{16.38}$$

$$P_y^{leg} = P_f(1 - P_e B) \tag{16.39}$$

Accordingly, the first derivative of P_D^{sec} and P_F^{sec} are computed as follows

$$\frac{\partial P_D^{sec}}{\partial B} = -\frac{M(1 - P_x^{leg})^L \ln 2}{2^B - 1} - L(1 - P_x^{leg})^{L-1} P_d P_e \tag{16.40}$$

$$\frac{\partial P_F^{sec}}{\partial B} = -\frac{M(1 - P_y^{leg})^L \ln 2}{2^B - 1} - L(1 - P_y^{leg})^{L-1} P_f P_e \tag{16.41}$$

By substituting (16.40) and (16.41) into (16.37), and after some mathematical processes, the optimal number of bits that minimizes ϵ can be expressed as follows:

$$B^{min\epsilon} = \log_2 \left(\frac{M\big(P_0(1 - P_y^{leg})^L - P_1(1 - P_x^{leg})^L\big) \ln 2}{LP_e\big(P_0 P_f (1 - P_y^{leg})^{L-1} - P_1 P_d (1 - P_x^{leg})^{L-1}\big)} + 1 \right) \tag{16.42}$$

Another important objective is to maximize energy efficiency. The optimal report length that maximizes energy efficiency can be found by solving the following problem

$$B^{max\mu} = \arg\max_B \mu^{sec} = \arg\max_B \frac{P_0(1 - P_F^{sec}) R T_t}{E_{css}^{sec} + P_t^{sec} E_t} \tag{16.43}$$

Similar to (16.36), $B^{max\mu}$ can be found using Lagrange method

$$\frac{\partial \mu^{sec}}{\partial B} = 0 \tag{16.44}$$

which can be rewritten as follows

$$(E_{css}^{sec} + P_t^{sec} E_t)\frac{\partial P_F^{sec}}{\partial B} + (1 - P_F^{sec})(NE_r + E_t\frac{\partial P_t^{sec}}{\partial B}) = 0 \tag{16.45}$$

Clearly, obtaining a closed form for $B^{max\mu}$ is analytically intractable. However, a simple bisection search algorithm can be employed to find the optimal value of B that maximizes energy efficiency.

16.6 Performance Evaluation and Simulation Results

A number of CUs $N = 5$ is assumed, where L of them are legitimate CUs, while the rest $M = 5 - L$ are considered as attackers. All simulation parameters regarding local sensing performance for legitimate CUs and attackers, energy consumption and network specifications are summarized in Table 16.1.

Table 16.1: Simulation Parameters

Parameter	Value	Parameter	value
P_0	0.5	P_d	0.7
P_f	0.2	q_d	0
q_f	1	R	$64K\ bps$
T_t	$0.1\,s$	E_s	$2 \times 10^{-4}\ Joule$
E_r	$1 \times 10^{-3}\ Joule$	E_t	$1 \times 10^{-1}\ Joule$

Fig. 16.3 plots the overall detection and false-alarm probabilities of the proposed secure CSS versus report length, bit-error probability and number of attackers. The system performance increases when the probability of detection increases and the false-alarm probability decreases. As it can be appreciated in Fig. 16.3-a, longer reports decrease both P_D^{sec} and P_F^{sec} due to the fact that increasing B decreases the probability of receiving error-free reports, affecting the local

sensing performance of the legitimate CUs and attackers as well (this effect is indicated in Fig. 16.2). In Fig. 16.3-b, the false-alarm and detection probabilities are given for different values of bit-error probability due to different channel conditions. With the increase of bit-error probability P_D^{sec} is reduced and P_F^{sec} is magnified. This is because increasing the bit-error probability of reporting channel increases the probability of validating reports as inverted. Similarly, increasing the number of attackers (or decreasing the number of honest CUs) will negatively affect both, decreasing P_D^{sec} and increasing P_F^{sec}, as shown in Fig. 16.3-c.

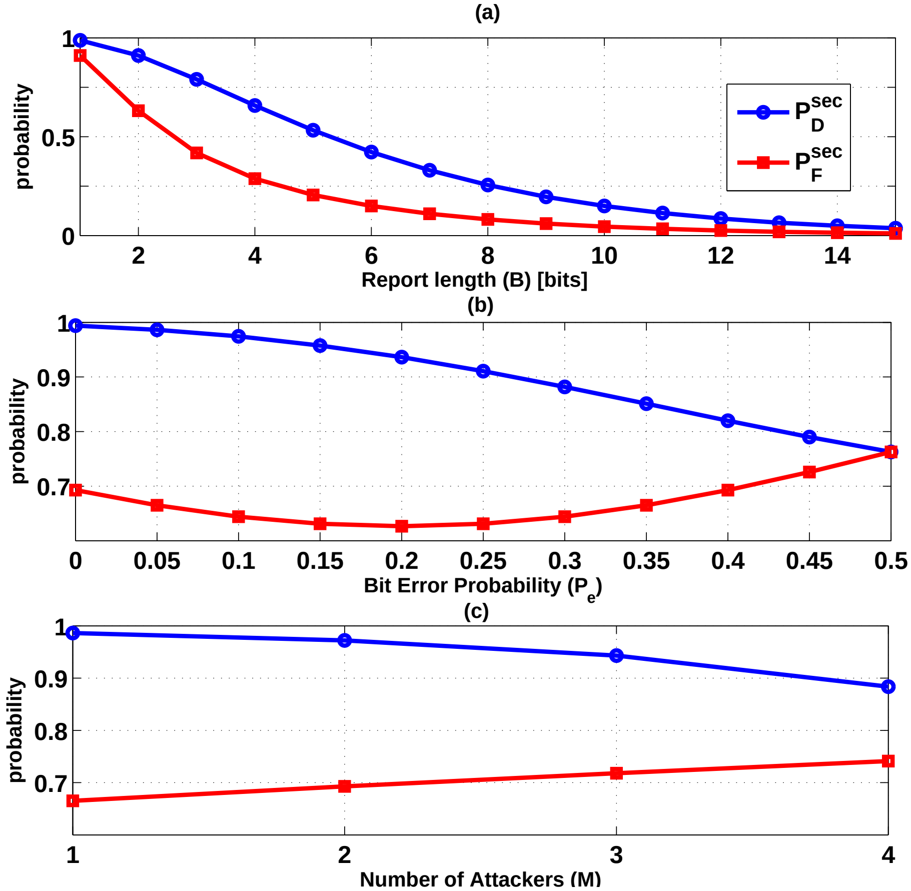


Figure 16.3: *The overall detection and false-alarm probabilities for the considered CRN using the proposed secure CSS versus (a) report length at $P_e = 0.05$ and $M = 1$, (b) bit error probability at $B = 2$ and $M = 1$, and (c) number of attacks at $B = 2$ and $P_e = 0.05$.*

In the following, we evaluate the performance of the proposed secure CSS in terms of false-decision probability and energy efficiency versus B, P_e and M. Moreover, in each figure we show the performance of the conventional insecure approaches in order to better show the superiority of our proposal.

Fig. 16.4, Fig. 16.5 and Fig. 16.6 compare between the two different approaches in terms of the false-decision probability. In Fig. 16.4, for $M = 1$ and $P_e = 0.15$, the proposed secure CSS outperforms the other approach as the report length increases. The conventional CSS shows a constant false-decision probability since it is independent of B. Regarding the secure approach, it presents a convex curve. This is because a small number of security bits B highly reduces the impact of malicious users. However when B increases more degradation appears on the sensing performance of the legitimate CUs.

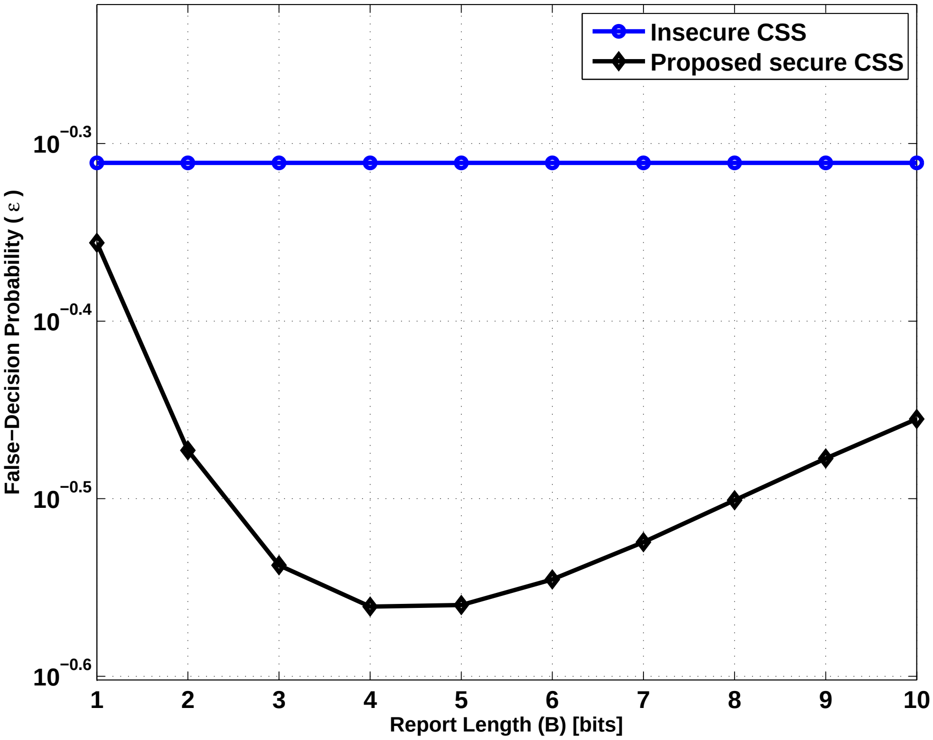


Figure 16.4: *The false-decision probability (ϵ) versus the report length (B) when $M = 1$ and $P_e = 0.15$.*

It is worth noting from Fig. 16.4 that the secure CSS protocol requires optimizing B to attain the minimum false-decision probability. In Fig. 16.5 and Fig. 16.6, the minimum false-decision probability, which is achieved by optimizing B, is plotted versus bit-error probability and the number of attackers, respectively. In both figures, the minimum false-decision probability increases for both approaches when the bit-error probability of the reporting channel increases, Fig. 16.5, or when the number of attackers increases, Fig. 16.6. This is because both effects degrade the overall detection accuracy as shown in Fig. 16.3. The secure CSS approach outperforms the conventional CSS.

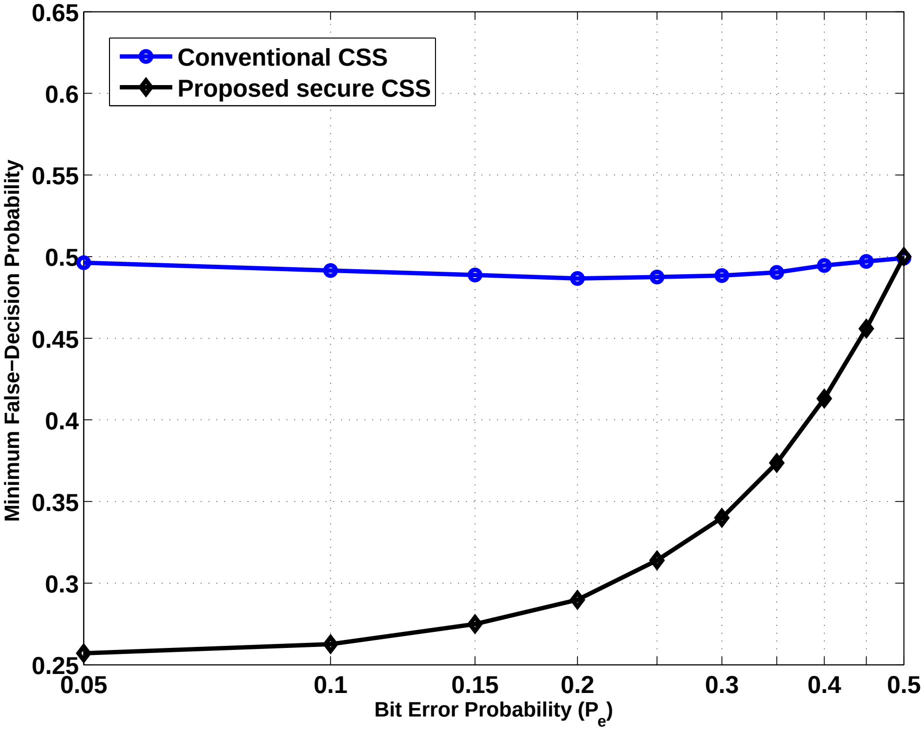


Figure 16.5: *The minimum false-decision probability versus the bit error probability (P_e) when $M = 1$.*

The comparison between the two different approaches in terms of the energy efficiency is addressed in Fig. 16.7, Fig. 16.8 and Fig. 16.9. In Fig. 16.7, for $M = 1$ and $P_e = 0.25$, the achievable energy efficiency for the the considered

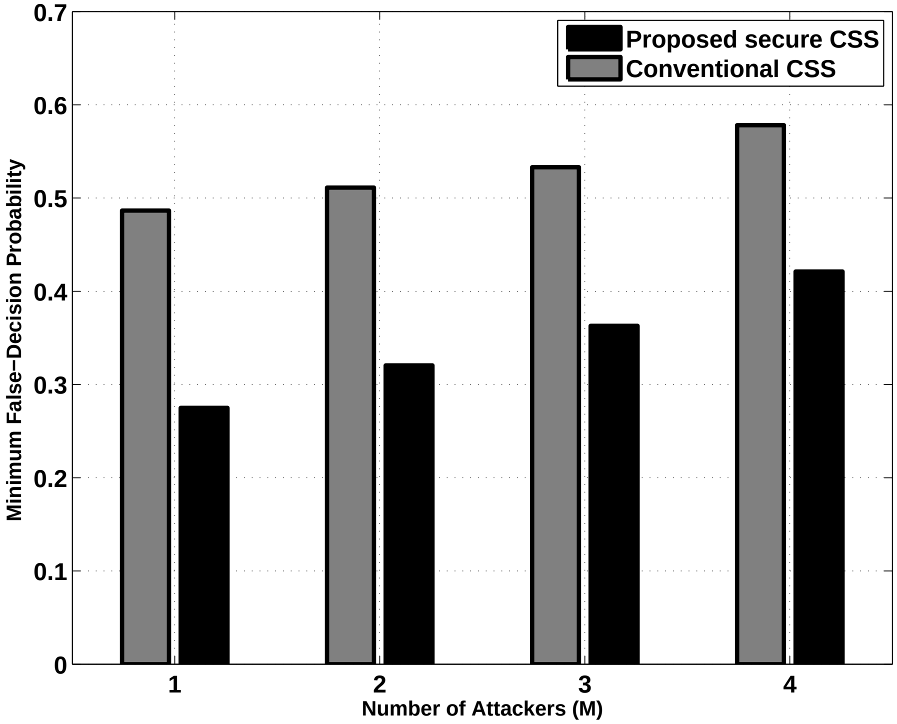


Figure 16.6: *The minimum false-decision probability versus the number if attackers (M) when* $P_e = 0.2$.

approaches versus the report length is shown. The conventional CSS presents the lowest energy efficiency which is independent of the report length. On the other hand, the secure CSS proposal draws a concave curve, which can be interpreted as a result of the effects on the detection accuracy which can be reflected on energy efficiency, see (16.2).

The optimal report length that maximizes energy efficiency is used to plot the maximum energy efficiency versus P_e and M in Fig. 16.8 and Fig. 16.9, respectively. In both figures, the proposed protocol keeps attaining higher energy efficiency than the conventional approach.

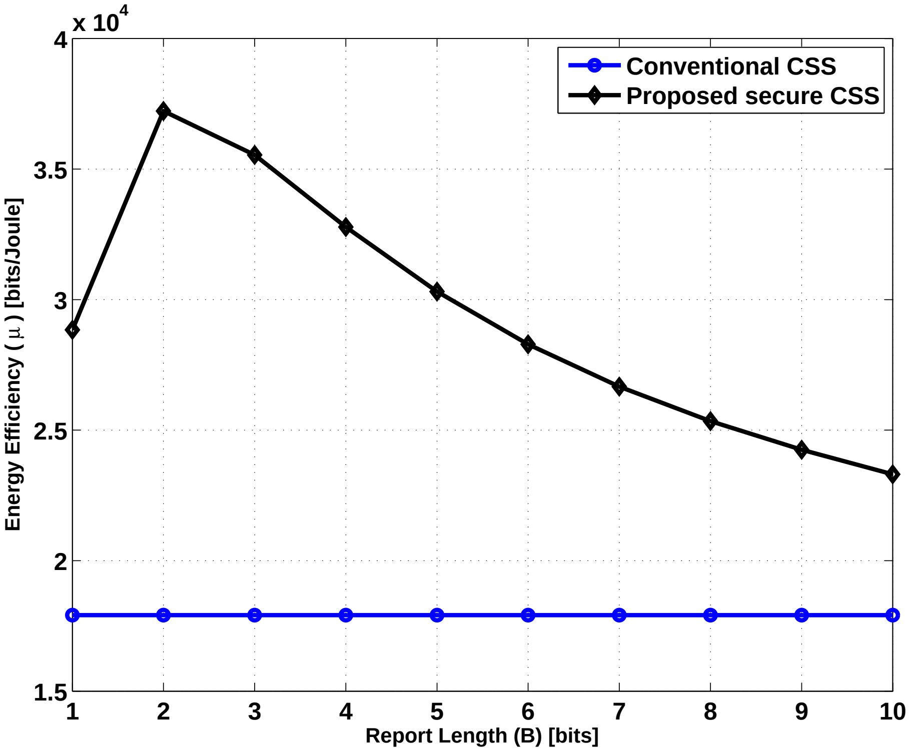


Figure 16.7: *The achievable energy efficiency versus the report length* (B) *when* $M = 1$ *and* $P_e = 0.25$.

16.7 Summary

A secure cooperative spectrum sensing in cognitive radio networks against spectrum sensing data falsification attacks has been presented in this chapter. The effects on the detection accuracy and energy efficiency is investigated considering the conventional conventional cooperative spectrum sensing. The first contribution of this chapter is proving the feasibility of introducing authentication in cooperative spectrum sensing by exploiting special characteristics of cognitive radio networks, which has never been investigated before. Conventional authentication mechanisms imply a heavy overhead, resulting in more bandwidth and energy consumption. In order to address this problem, this chapter has proposed a low-overhead energy-efficient security protocol that can

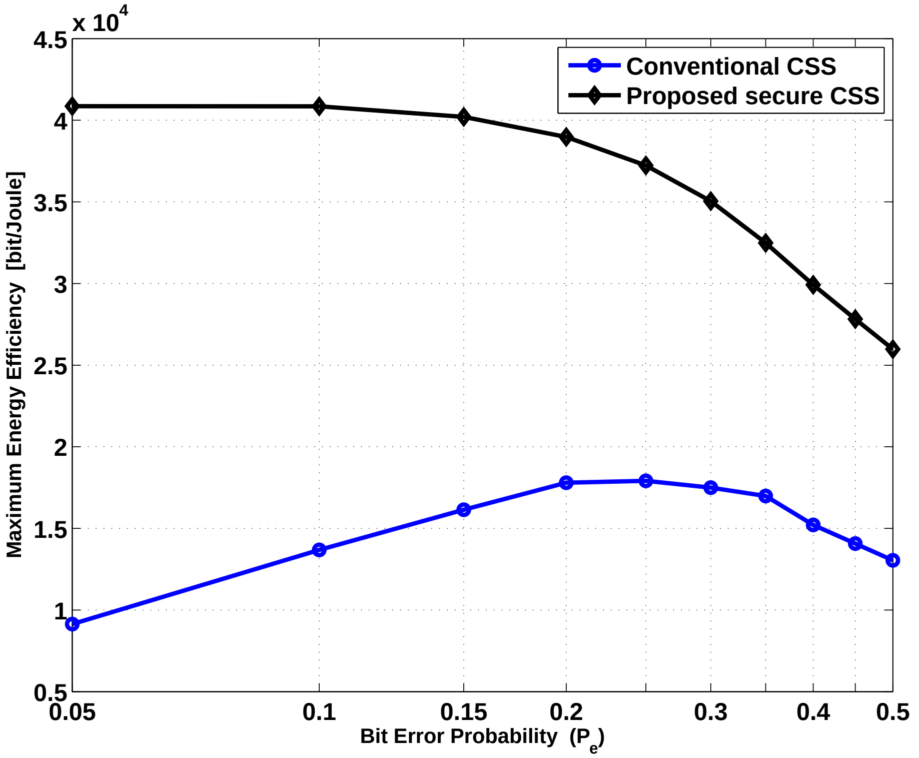


Figure 16.8: *The maximum energy efficiency versus the bit error probability (P_e) when* $M = 1$.

effectively combat the external malicious users. Moreover, the design of the proposed protocol alleviates the impact of the noisy reporting channels on the overall performance.

The superiority of the proposed secure cooperative spectrum sensing over the conventional (insecure) approach is proved analytically. The influence of the report length, reporting channel quality and the number of attackers are discussed. Accordingly, two optimization problems of the report length for minimizing false-decision probability and maximizing energy efficiency are formulated in the chapter. The overall performance of the legitimate network in terms of detection accuracy and energy efficiency is shown for the proposed approach, where it is proved that the proposed protocol can outperform the other approaches.

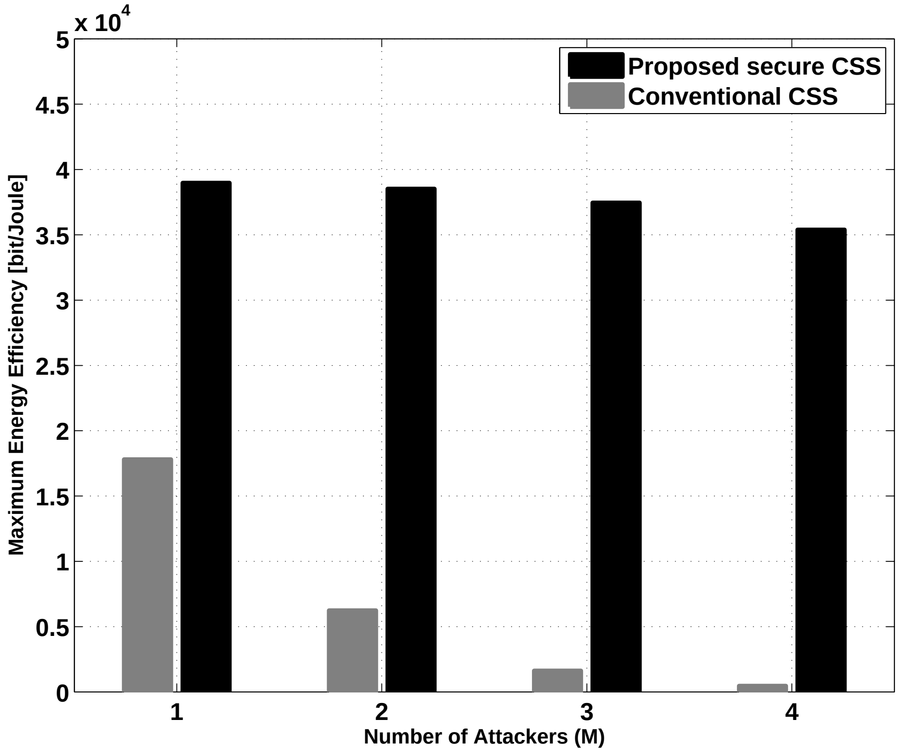


Figure 16.9: *The maximum energy efficiency versus the number of attackers (M) when $P_e = 0.2$.*

Part VI

Towards Energy Efficient Cooperative Spectrum Sensing, Comprehensive Solutions

CHAPTER 17

COMPREHENSIVE ENERGY-EFFICIENT SOLUTIONS FOR COOPERATIVE SPECTRUM SENSING

17.1 Introduction

In **Chapter 4** to **Chapter 16**, different algorithms, policies and protocols have been presented in order to improve energy efficiency and security in cooperative spectrum sensing in infrastructure-based CRNs. Each proposed work is dedicated for a single stage of the cooperative spectrum sensing stages. Aiming at maximizing the energy efficiency gain, in this chapter, we propose different combinations among those algorithms. In detail, for each stage in CSS, an energy-efficient algorithm for each stage is picked up among the works presented previously in this dissertation. The selected algorithms will be applied together as a united energy-efficient framework in order to maximize the energy efficiency in all CSS stages.

The main focus of this chapter is threefold: (i) proposing different approaches for a comprehensive energy-efficient framework for CSS, (ii) exploring the promising results by combining the proposed approaches in terms of energy efficiency, and (iii) proving the consistency of the proposed algorithms in this dissertation, where they can be seamlessly applied together.

17.2 The First Comprehensive Energy-Efficient Approach

In this section, the first approach of the possible combinations of three different algorithms for the three different stages of CSS. The first approach includes the following:

- **Local Sensing Stage**: the number of sensing users is optimized in order to maximize the achievable energy efficiency, as proposed in **Chapter 6**.
- **Results' Reporting Stage**: the hard-based CSS is used as it has been proved to be more energy-efficient than the soft-based CSS in **Chapter 7**. Also, the scheme presented in **Chapter 8** is followed in this approach, where the reporting process is terminated once the global decision can be made.
- **Decision-Making Stage**: the fusion threshold is optimized for energy efficiency maximization as proposed in **Chapter 12**.

It is worth noting here that all stages depend on each other. For example, the number of sensing users is optimized based on a given decision-making threshold and via versa. Thus, to build the framework, we first consider the optimal fusion rule is the majority rule in order to obtain the optimal number of sensing users. Then, the reporting scheme proposed in **Chapter 8** is employed based on the optimal number of sensing users and the optimal fusion rule. The first approach is compared to four different scenarios. Each scenario implies applying only one energy-efficient algorithm for a single stage. The considered scenarios aims at showing the accumulated gain of energy efficiency in case of using a comprehensive energy efficient approach for all stages. The considered scenarios are summarized as follows:

- **Conventional CSS**: where all the users sense the spectrum and report their results to the FC. At the FC, the AND rule is employed to issue the global decision.
- **EE sensing only**: in this scenario, the optimal number of sensing users that maximize energy efficiency is used as in **Chapter 6**. In th following CSS stages, this scenario follows the conventional CSS scheme, where all sensing CUs report their results, and the AND rule is employed at the FC.
- **EE reporting only**: in this scenario, the reporting process follows the scheme proposed in **Chapter 8**. In sensing stage, all available CUs sense the spectrum, while the FR adopted is AND rule.
- **Optimal EE fusion rule only**:in this scenario, all available CUs sense the spectrum and report their local results based on the hard-based scheme as in the conventional CSS. At the FC, Optimal FR that maximizes energy efficiency is employed as derived in **Chapter 12**.

The parameters listed in Table 17.1 are used to generate Fig 17.1. Fig 17.1 plots the energy efficiency versus the total number of the CUs in the considered CRN for all the considered scenarios above and the first comprehensive approach. An initial note on the results is that the first comprehensive energy efficient approach achieves the highest energy efficiency among all the other considered approaches. This is because that the first comprehensive energy efficient approach combines the three different energy-efficient schemes for all the stages, while each scenario of the others targets only a single stage. Also, it can be noticed that optimizing the number of sensing users for energy efficiency maximization the largest contributer to the overall gain in the first comprehensive approach. On the other hand, the energy efficient reporting scheme has the lowest improvement, compared to the conventional CSS scheme.

Considering the energy efficiency of the conventional CSS scheme, applying only the energy efficient sensing yields in an energy efficiency gain ranges from 1.5 to 1.8, while applying only the energy efficient reporting yields in $1.01 - 1.1$ energy efficiency gain. Using only the optimal fusion rule achieves $1.0 - 1.45$ energy efficiency gain. However, the energy efficiency gain over the conventional CSS, which is achieved by the first comprehensive approach, ranges from 1.63 to 2.13. These results clearly indicate that importance of combining different energy efficient approaches in a comprehensive energy efficient solution in order to maximize the energy efficiency gain.

Table 17.1: Simulation Parameters for Fig. 17.1 and Fig. 17.2

Parameter	Value	Parameter	value
P_0	0.5	$\frac{\sigma_x^2}{\sigma_w^2}$	$-20\,dB$
f_s	$1\,MHz$	ρ_t	$1\,W$
ρ_s	$0.1\,W$	ρ_r	$1\,W$
τ	$0.05\,ms$	R	$100\,Kbps$
T	$50\,ms$	T_t	$45\,ms$
P_d^{th}	0.85	ρ_{bc}	$1.8\,W$

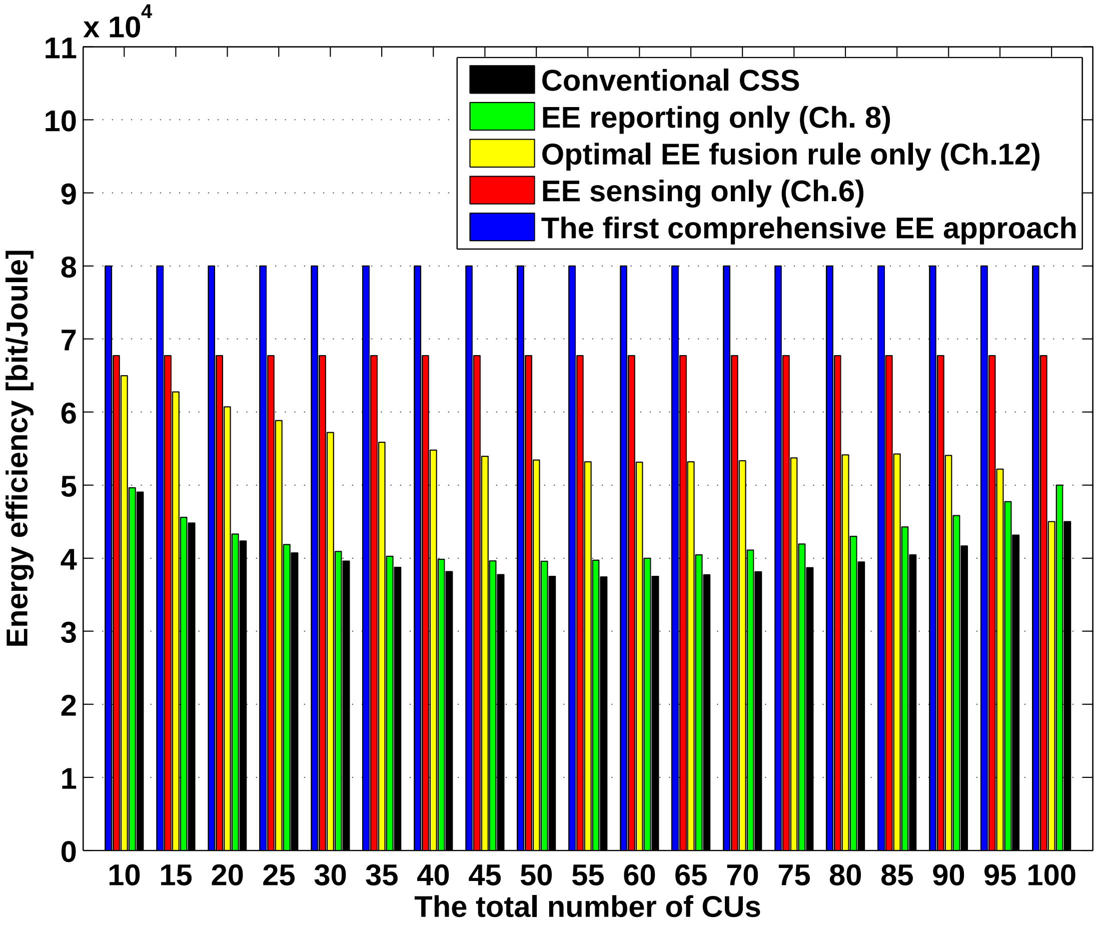


Figure 17.1: The energy efficiency versus the total number of CUs for different proposed EE schemes individually and the first comprehensive energy efficient approach.

17.3 The Second Comprehensive Energy-Efficient Approach

In this section, the second approach of the possible combinations of three different algorithms for the three different stages of CSS. The second approach includes the following:

- **Local Sensing Stage**: the number of sensing users is optimized in order to maximize the achievable energy efficiency, as proposed in **Chapter 6**.
- **Results' Reporting Stage**: the hard-based CSS is used as it has been proved to be more energy-efficient than the soft-based CSS in **Chapter 7**. Also, the objection-based reporting scheme presented in **Chapter 9** is followed in this approach.
- **Decision-Making Stage**: the fusion threshold used to make the global decision is optimized for energy efficiency maximization as proposed in **Chapter 12**.

Compared the the first approach, in the second approach, only the reporting scheme proposed in **Chapter 8** is replaced by the objection-based reporting scheme proposed in **Chapter 9**. As in the previous section, four different scenarios are considered for comparison, as follows

- **Conventional CSS**: as described before in the previous section.
- **EE sensing only**: as described before in the previous section.
- **EE Objection-based reporting only**: in this scenario, the reporting process follows the objection-based reporting scheme proposed in **Chapter 9**. In sensing stage, all available CUs sense the spectrum, while the FR adopted is AND rule.
- **Optimal EE fusion rule only** as described in the previous section.

The same simulation parameters listed in Table 17.1 are used to simulate the second comprehensive approach. Similar to Fig. 17.1, in Fig. 17.2, almost the same gains can be achieved by the considered scenario due to the small difference in energy efficiency between the objection-based reporting scheme and the scheme proposed in **Chapter** 8.

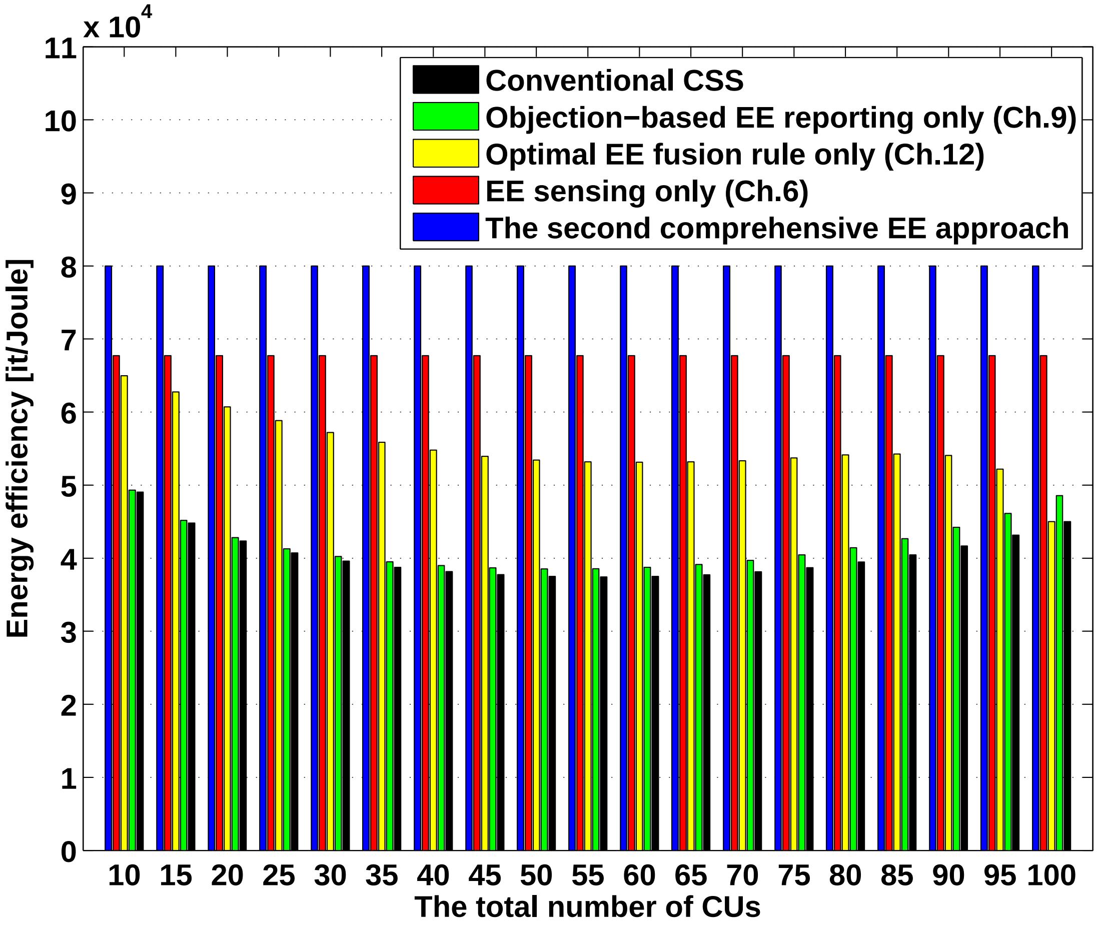


Figure 17.2: The energy efficiency versus the total number of CUs for different proposed EE schemes individually and the second comprehensive energy efficient approach.

17.4 The Third Comprehensive Energy-Efficient Approach

Another third approach can be built from three different energy efficient schemes, as follows

- **Local Sensing Stage**: the minimum number of sensing users that achieves predefined threshold on detection accuracy is used, as proposed in **Chapter 4**.
- **Results' Reporting Stage**: the hard-based CSS is used as it has been proved to be more energy-efficient than the soft-based CSS in **Chapter 7**. Also, the objection-based reporting scheme presented in **Chapter 9** is followed in this approach.
- **Decision-Making Stage**: the fusion threshold used to make the global decision is optimized for energy efficiency maximization as proposed in **Chapter 12**.

The third comprehensive approach is compared to four different scenarios described as follows

- **Conventional CSS**: as described in Section 17.2.
- **EE sensing only**: where the minimum number of sensing users that achieves th thresholds on detection accuracy is used as in **Chapter 4**. In th following CSS stages, this scenario follows the conventional CSS scheme, where all sensing CUs report their results, and the AND rule is employed at the FC.
- **EE objection-based reporting only**: in this scenario, the reporting process follows the objection-based reporting scheme proposed in **Chapter 9**. In sensing stage, all available CUs sense the spectrum, while the FR adopted is AND rule.
- **Optimal EE fusion rule only**:as described in Section 17.2.

Table 17.2 lists the simulation parameters used in this section. Fig. 17.3 shows the energy efficiency versus the total number of CUs for the third comprehensive approach and the other individual schemes.

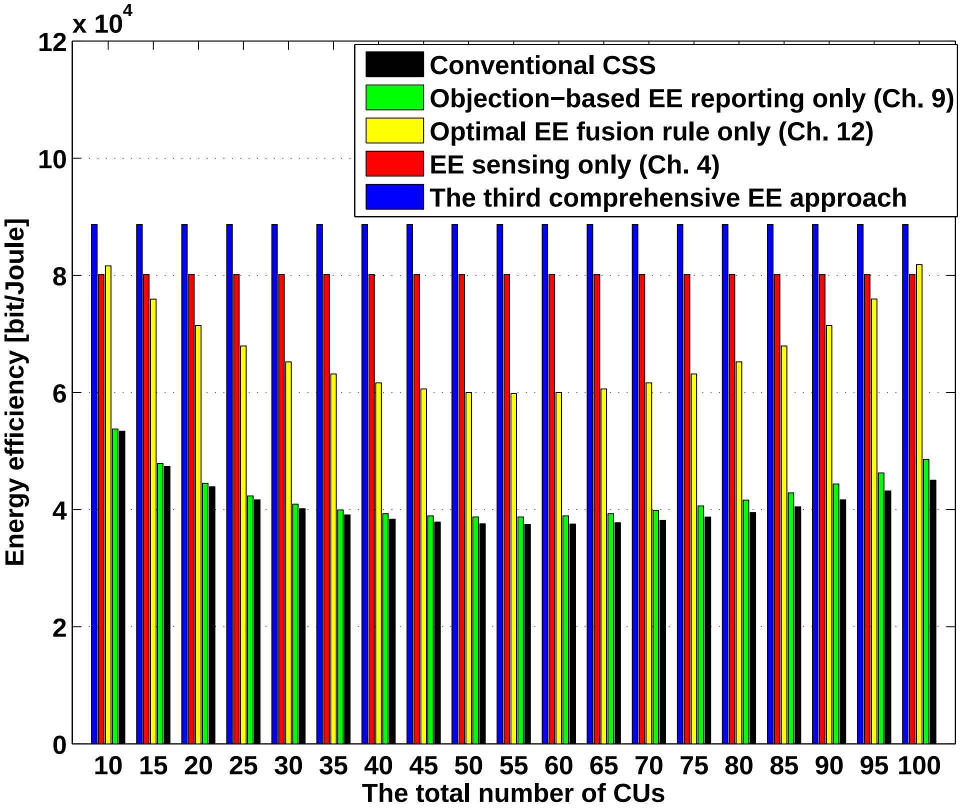


Figure 17.3: The energy efficiency versus the total number of CUs for different proposed EE schemes individually and the third comprehensive energy efficient approach.

Table 17.2: Simulation Parameters for Fig. 17.3

Parameter	Value	Parameter	value
P_0	0.5	P_D^{th}	0.8
P_F^{th}	0.1	ρ_t	$1\,W$
ρ_s	$0.1\,W$	ρ_r	$1\,W$
τ	$0.05\,ms$	R	$100\,Kbps$
T	$50\,ms$	T_t	$45\,ms$
ρ_{bc}	$1.8\,W$	P_d	0.9
P_f	0.2		

As shown in Fig. 17.3, applying only the energy efficient algorithm proposed in **Chapter 4** achieves an energy efficiency gain $1.5 - 2.13$ over the conventional CSS scheme. On the other hand, applying only the objection-based reporting scheme provides $1.01 - 1.1$ energy efficiency gain. In the case of using only the optimal fusion rule, the energy efficiency gain ranges from 1.53 to 2.18. However, applying the third comprehensive energy efficient approach, which combines the three scenarios, results in $1.66 - 2.37$ energy efficiency gain compared to the conventional CSS scheme.

17.5 Remarks

The presented results in this chapter have shown that the proposed algorithms/schemes in the previous chapter can be combined in different approaches in order to build a comprehensive energy efficient framework for CSS process. The built framework has proven the consistency of the proposed algorithms to each other. Most importantly, the results have shown that any of the proposed approaches in this chapter can at lest double the energy efficiency of the conventional CSS scheme. Also, it has been shown that the comprehensive approaches improve the energy efficiency gain compared to the separated energy efficient algorithms.

It is worth mentioning here that other possible comprehensive energy efficient approaches can be suggested other than the presented in this chapter. However, the presented approaches in this chapter have been selected since they represent the most efficient approaches.

Part VII

Conclusions

CHAPTER 18

CONCLUSIONS

This dissertation has investigated the high energy consumption problem in cooperative spectrum sensing for cognitive radio networks. Firstly, a deep review of the state of the art has been presented, where all the proposed energy efficient approaches for cooperative spectrum sensing have been discussed. The available works in the literature have been classified into three different approaches, namely, energy-efficient local sensing stage, energy-efficient reporting stage, and energy-efficient decision-making stage. Thus, the classification depends on the running stage of each work.

Following the classification of the previous works, we have presented several energy-efficient algorithms/schemes for the different stages of the cooperative spectrum sensing. Specifically, three different algorithms have been presented in **Part II** in order to improve energy efficiency in the local sensing stage by reducing the number of the participating users in cooperative spectrum sensing process. In **Part III**, four different approaches aiming at reducing energy consumption in reporting stage have been presented. The works presented in **Part III** focus on: optimizing the report form, reducing the number of reporting users, and limiting the reported data. In **Part IV**, optimization problems for the employed fusion rule have been presented and solved for energy efficiency maximization in cooperative spectrum sensing scheme.

Moreover, the energy efficiency problem has been investigated in presence of malicious users in cooperative spectrum sensing in **Part V**. Specifically, a low-overhead authentication protocol for outsider attackers, a energy-efficient weighted cooperative spectrum sensing scheme , and a punishment policy for malicious attackers are all presented in **Part V**. The main aim of the proposed works is to eliminate the negative effects of malicious attackers on the energy efficiency of cognitive radio networks, and to achieve the balance of the trade-off between security and energy efficiency in cooperative spectrum sensing.

However, as the main aim of this work is design comprehensive energy-efficient cooperative spectrum sensing, three different comprehensive energy-efficient approaches have been presented in **Part VI**. Each comprehensive approach combines three different energy-efficient algorithms/schemes of the proposed in this dissertation, one for each stage of the stages of cooperative spectrum sensing. The evaluation results of the proposed comprehensive approaches have shown: (i) a significant improvement of the energy efficiency of cooperative spectrum sensing, (ii) the consistency between the proposed algorithms/schemes in this dissertation, and (iii) the importance of the designing a comprehensive energy-efficient framework for cooperative spectrum sensing instead of the the proposed algorithms for individual stages.

BIBLIOGRAPHY

[1] FCC, “Spectrum Policy Task Force Report (ET Docket no.02-135), Nov. 2002.

[2] J. Mitola and G.Q. Maguire, “Cognitive radio: Making software radios more personal, IEEE Personal Communications, vol. 6, no. 4, pp. 13-18, August 1999.

[3] Radiocommunication Study Groups, “WORKING DOCUMENT TOWARDS A PRELIMINARY DRAFT NEW REPORT: SOFTWARE DEFINED RADIO IN LAND MOBILE SERVICES (Question 230-1/8),” International Telecommunications Union Document 8A/121-E, 15 September 2004.

[4] FCC: ET Docket No 03-108 Notice of proposed rule making and order: Facilitating opportunities for flexible, efficient, and reliable spectrum use employing cognitive radio technologies. Federal Communications Commission (FCC) (2005)

[5] S. Haykin, “Cognitive radio: brain-empowered wireless communications, *IEEE Transactions on Communications,* vol. 23, no. 2, pp. 201220, 2005.

[6] M. Sherman, et al., “IEEE standards supporting cognitive radio and networks, dynamic spectrum access, and coexistence” *IEEE Communications Magazine,* vol. 46, no. 7, pp. 72-79.

[7] M. Mueck, et al., “ETSI reconfigurable radio systems: status and future directions on software defined radio and cognitive radio standards”, *IEEE Communications Magazine,* vol. 48, no. 9, pp. 78-86.

[8] H. Yoshino, “ITU-R standardization activities on cognitive radio”, *IEICE transactions on communications,* vol. 95, no. 4, pp. 1036-1043.

[9] F. Granelli, et al., “Standardization and research in cognitive and dynamic spectrum access networks: IEEE SCC41 efforts and other activities” *IEEE Communications Magazine,* vol. 48, no.1, 2010, pp. 71-79.

[10] S. Filin et al., “ITU-R standardization activities on Cognitive Radio Systems”, *IEEE Sixth International ICST Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM),* June 2011, pp. 116-120.

[11] Y. Zeng et al., "Worldwide regulatory and standardization activities on cognitive radio", *IEEE symposium on New Frontiers in Dynamic Spectrum,* 2010.

[12] A. Goldsmith et al., "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective", *Proceedings of the IEEE,* 97(5), 894-914, 2009.

[13] S. Srinivasa and S.A. Jafar, "Cognitive radios for dynamic spectrum access-the throughput potential of cognitive radio: A theoretical perspective", *IEEE Communications Magazine,* 45.5 (2007): 73-79.

[14] G. Scutari et al., "Cognitive MIMO radio", *IEEE Signal Processing Magazine,* 25.6 (2008): 46-59.

[15] J. Mitola, "Cognitive radio for flexible mobile multimedia communications", *999 IEEE International Workshop on Mobile Multimedia Communications (MoMuC'99)*, 1999.

[16] OFCOM, "Digital dividend: clearing the 800 MHz band, in http://www.ofcom.org.uk/consult/condocs/cognitive/.

[17] Report ITU-R SM.2152, "Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS), September 200

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

[19] D. Cabric et al., "Implementation issues in spectrum sensing for cognitive radios." Signals, systems and computers, 2004. Conference record of the thirty-eighth Asilomar conference on. Vol. 1. IEEE, 2004.

[20] I.F. Akyildiz et al., "Cooperative spectrum sensing in cognitive radio networks: A survey" *Physical Communication,* vol. 4, no. 1, 2011, pp. 40-62.

[21] M. Di Renzo et al., "Cooperative spectrum sensing in cognitive radio networks over correlated log-normal shadowing." *IEEE 69th Vehicular Technology Conference VTC Spring 2009*, 2009.

[22] K.B. Letaief et al., "Cooperative spectrum sensing." Cognitive Wireless Communication Networks. Springer US, 2007. 115-138.

[23] M. Di Renzo et al., "Cooperative Spectrum Sensing over Correlated Log Normal Sensing and Reporting Channels," *IEEE Global Communications Conference*, November 30 - December 4, 2009, Honolulu, Hawaii, USA.

[24] C. Cordeiro et al., "Cognitive PHY and MAC layers for dynamic spectrum access and sharing of TV bands, *in Proc. first international workshop on Technology and policy for accessing spectrum (TAPAS06),* Boston, MA, USA, August 2006.

[25] W. Hu et al., "COGNITIVE RADIOS FOR DYNAMIC SPECTRUM ACCESS - Dynamic Frequency Hopping Communities for Efficient IEEE 802.22 Operation, *IEEE Communications Magazine,* vol. 45, no. 5, pp. 8087, May 2007.

[26] I. Akyildiz et al., "CRAHNs: Cognitive radio ad hoc networks," *Ad Hoc Networks,* 7.5 (2009): 810-836.

[27] W. Xia et al., "Optimization of cooperative spectrum sensing in ad-hoc cognitive radio networks." Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE. IEEE, 2010.

[28] F. Adelantado et al., "Sensing Users Selection with Overhead Reduction for Cognitive Wireless Ad-Hoc Networks." GLOBECOM. 2010.

[29] K.R. Chowdhury and I.F. Akyildiz, "Cognitive wireless mesh networks with dynamic spectrum access", *IEEE Journal of Selected Areas in Communications,* 26 (1) (2008) 168181.

[30] I. Pefkianakis et al., "SAMER: Spectrum-aware mesh routing in cognitive radio networks, *in Proc. 3rd IEEE Int. Symp. DySPAN,* Chicago, IL, Oct. 2008, pp. 15.

[31] F.F. Digham, M.-S. Alouini, M.K. Simon, "On the energy detection of unknown signals over fading channels," *IEEE Transactions on Communications,* 55 (1) (2007) 2124.

[32] J. G. Proakis, Digital Communications, 4th ed. McGraw-Hill, 2001.

[33] M. Oner and F. Jondral, "Cyclostationarity based air interface recognition for software radio systems, in Proc. *IEEE Radio and Wireless Conference*, Atlanta, Georgia, USA, Sept. 2004, pp. 263266.

[34] H. Tang, "Some physical layer issues of wide-band cognitive radio systems,

in Proc. *IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks,* Baltimore, Maryland, USA, Nov. 2005, pp. 151159.

[35] T. Yucek, H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications", *Communications Surveys Tutorials, IEEE*, 11 (1) (2009) 116130.

[36] J. Ma et al., "Signal processing in cognitive radio", Proceedings of the*IEEE,* vol. 97, no. 5, 2009, pp. 805-823.

[37] S. M. Mishra et al., "Cooperative sensing among cognitive radios, in Proc. *IEEE International Conference in Communication,* Jun. 2006, pp. 16581663.

[38] A. H. Nuttall, "Some integrals involving the Q_M function", *IEEE Transactions on Information Theory*, vol. 21, no. 1, pp. 9596, January 1975.

[39] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 5th ed. Academic Press, 1994.

[40] A. Ghasemi and E.S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks DySPAN*, 2005

[41] S. Maleki, et al., "Energy-efficient distributed spectrum sensing for cognitive sensor networks," *IEEE Sensors Journal,* vol. 11, no. 3, 2011, pp. 565-573.

[42] H. Li et al., "Collaborative quickest spectrum sensing via random broadcast in cognitive radio systems, *IEEE Transactions on Wireless Communications,* vol. 9, no. 7, pp. 23382348, Jul. 2010.

[43] J. Ma et al., "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks" , *IEEE Transactions on Wireless Communications,* vol. 7, no. 11, 2008, pp. 4502-4507.

[44] E. Visotsky et al., "On collaborative detection of TV transmissions in support of dynamic spectrum sharing, in Proc. *1st IEEE International Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN),* 2005, pp. 338345.

[45] E.C.Y. Peh et al., "Optimization of cooperative sensing in cognitive radio networks: a sensing-throughput tradeoff view", *IEEE Transactions on Vehicular Technology,* vol. 58, no. 9, pp. 5294 - 5299, 2009.

[46] Ch. Sun et al., "Cooperative spectrum sensing for cognitive radios under bandwidth constraints," *IEEE Wireless Communications and Networking Conference WCNC,* 2007.

[47] P. Qihang et al., "A distributed spectrum sensing scheme based on credibility and evidence theory in cognitive radio context, in Proc. *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications,* Helsinki, Finland, Sept. 2006, pp. 15.

[48] J. Unnikrishnan, and V. Veeravalli, "Cooperative sensing for primary detection in cognitive radio," *IEEE Journal of Selected Topics in Signal Processing,* vol. 2, no. 1, 2008, pp. 18-27.

[49] M. Di Renzo, "Energy Efficiency Metrics and Performance Tradeoffs of GREEN Wireless Networks", book chapter in "Green Communications: Principles, Concepts and Practice," Wiley-Blackwell, ISBN-13: 978-1118759264.

[50] S. Wang et al. "Energy-efficient spectrum sensing and access for cognitive radio networks," *IEEE Transactions on Vehicular Technology,* vol. 61, no. 2, 2012, pp. 906-912.

[51] R. Chen et al. "Toward secure distributed spectrum sensing in cognitive radio networks" *IEEE Communications Magazine,* vol. 46, no. 4, 2008, pp. 50-55.

[52] S. Maleki et al., "Energy and throughput efficient strategies for cooperative spectrum sensing in cognitive radios", *IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC),* 2011.

[53] H.N. Pham et al. "Energy minimization approach for optimal cooperative spectrum sensing in sensor-aided cognitive radio networks," *The 5th Annual ICST Wireless Internet Conference (WICON),* 2010.

[54] P. Cheng et al., "Energy-efficient cooperative spectrum sensing in sensor-aided cognitive radio networks" *IEEE Wireless Communications,* vol. 19, no. 6, 2012, pp. 100-105.

[55] Najimi, M., Ebrahimzadeh, A., Andargoli, S., Hosseini, M., & Fallahi, A. (2013). A novel sensing nodes and decision node selection method for energy efficiency of cooperative spectrum sensing in cognitive sensor networks. IEEE Sensors Journal, 13(5), 1610-1621.

[56] Ergul, O., & Akan, O. B. (2013, July). Energy-efficient cooperative spectrum sensing for cognitive radio sensor networks. In Computers and Communications (ISCC), 2013 IEEE Symposium on (pp. 000465-000469). IEEE.

[57] Monemian, M., & Mahdavi, M. (2014, September). Analysis of a New Energy-Based Sensor Selection Method for Cooperative Spectrum Sensing in Cognitive Radio Networks. *Sensors Journal,* IEEE , vol.14, no.9, pp.3021-3032.

[58] Wang, G., Guo, C., Feng, S., Feng, C., & Wang, S. (2013, September). A two-stage cooperative spectrum sensing method for energy efficiency improvement in cognitive radio. In Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on (pp. 876-880). IEEE.

[59] Eryigit, S., Bayhan, S., & Tugcu, T. (2013). Energy-efficient multichannel cooperative sensing scheduling with heterogeneous channel conditions for cognitive radio networks. Vehicular Technology, IEEE Transactions on, 62(6), 2690-2699.

[60] Su, H. & Zhang X. (2010). Energy-Efficient Spectrum Sensing for Cognitive Radio Networks. *International Conference on Communications (ICC),* IEEE , vol., no., pp.1,5, 23-27.

[61] Wang, B., Feng, Z., Huang, D., & Zhang, P. (2013). Discontinuous spectrum sensing scheme for energy-constrained cognitive radio networks. Electronics letters, 49(6), 429-430.

[62] Wu, Y., & Tsang, D. H. (2011). Energy-efficient spectrum sensing and transmission for cognitive radio system. IEEE Communications Letters, 15(5), 545-547.

[63] Zhao, N., Yu, F.R., Sun, H., Nallanathan, A. (2012). An energy-efficient cooperative spectrum sensing scheme for cognitive radio networks, *Global Communications Conference (GLOBECOM),* IEEE, pp.3600-3604.

[64] Feng, X., Gan, X., & Wang, X. (2011, December). Energy-constrained cooperative spectrum sensing in cognitive radio networks. In Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE (pp. 1-5). IEEE.

[65] Gao, Y., Xu, W., Yang, K., Niu, K., & Lin, J. (2013, April). Energy-efficient transmission with cooperative spectrum sensing in cognitive radio net-

works. In Wireless Communications and Networking Conference (WCNC), 2013 IEEE (pp. 7-12). IEEE.

[66] Jun, Y., & Qi, Z. (2013, January). Optimization of cooperative sensing based on energy consume in cognitive radio networks. In Conference Anthology, IEEE (pp. 1-5). IEEE.

[67] Li, X., Cao, J., Ji, Q., & Hei, Y. (2013, April). Energy efficient techniques with sensing time optimization in cognitive radio networks. In Wireless Communications and Networking Conference (WCNC), 2013 IEEE (pp. 25-28). IEEE.

[68] Xu, M., Li, H., & Gan, X. (2011, June). Energy efficient sequential sensing for wideband multi-channel cognitive network. In Communications (ICC), 2011 IEEE International Conference on (pp. 1-5). IEEE.

[69] Mishra, S. M., Sahai, A., & Brodersen, R. W. (2006, June). Cooperative sensing among cognitive radios. In Communications, 2006. ICC'06. IEEE International Conference on (Vol. 4, pp. 1658-1663). IEEE.

[70] Chaudhari, S., Lunden, J., Koivunen, V., & Poor, H. V. (2012). Cooperative sensing with imperfect reporting channels: Hard decisions or soft decisions?. Signal Processing, IEEE Transactions on, 60(1), 18-28.

[71] Sakran, H., & Shokair, M. (2013). Hard and softened combination for cooperative spectrum sensing over imperfect channels in cognitive radio networks. Telecommunication Systems, 52(1), 61-71.

[72] Shen, J., Liu, S., Zhang, R., & Liu, Y. (2008, August). Soft versus hard cooperative energy detection under low SNR. In Communications and Networking in China, 2008. ChinaCom 2008. Third International Conference on (pp. 128-131). IEEE.

[73] Lundn, J., Koivunen, V., Huttunen, A., & Poor, H. V. (2009). Collaborative cyclostationary spectrum sensing for cognitive radio systems. Signal Processing, IEEE Transactions on, 57(11), 4182-4195.

[74] Appadwedula, S., Veeravalli, V. V., & Jones, D. L. (2008). Decentralized detection with censoring sensors. Signal Processing, IEEE Transactions on, 56(4), 1362-1373.

[75] Maleki, S., & Leus, G. (2013). Censored truncated sequential spectrum sens-

ing for cognitive radio networks. Selected Areas in Communications, IEEE Journal on, 31(3), 364-378.

[76] Lee, C. H., & Wolf, W. (2008, January). Energy efficient techniques for cooperative spectrum sensing in cognitive radios. In Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE (pp. 968-972). IEEE.

[77] Yang, H., Zhao, Z., & Zhang, H. (2013, December). Hard Combining Based Energy Efficient Spectrum Sensing in Cognitive Radio Network. In 2013 IEEE Global Communications Conference (Globecom2013) (pp. 1060-1065).). 2013.

[78] Sun, C., Zhang, W., & Ben, K. (2007, June). Cluster-based cooperative spectrum sensing in cognitive radio systems. In Communications, 2007. ICC'07. IEEE International Conference on (pp. 2511-2515). IEEE.

[79] Xia, W., Wang, S., Liu, W., & Chen, W. (2009, September). Cluster-based energy efficient cooperative spectrum sensing in cognitive radios. In Wireless Communications, Networking and Mobile Computing, 2009. WiCom'09. 5th International Conference on (pp. 1-4). IEEE.

[80] Wei, J., & Zhang, X. (2010, March). Energy-efficient distributed spectrum sensing for wireless cognitive radio networks. In INFOCOM IEEE Conference on Computer Communications Workshops, 2010 (pp. 1-6). IEEE.

[81] Khasawneh, M., Agarwal, A., Goel, N., Zaman, M., & Alrabaee, S. (2012, July). Sureness efficient energy technique for cooperative spectrum sensing in cognitive radios. In Telecommunications and Multimedia (TEMU), 2012 International Conference on (pp. 25-30). IEEE.

[82] Kozal, A. S., Merabti, M., & Bouhafs, F. (2014, April). Spectrum sensing-energy tradeoff in multi-hop cluster based cooperative cognitive radio networks. In Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on (pp. 765-770). IEEE.

[83] Peh, E.C.Y., Y.C Liang, Y.L. Guan, & Y. Pei (2011, December). Energy-Efficient Cooperative Spectrum Sensing in Cognitive Radio Networks," *IEEE Global communications Conference*, pp.1-5.

[84] Maleki, S., Chepuri, S. P., & Leus, G. (2013). Optimization of hard fusion based spectrum sensing for energy-constrained cognitive radio networks. Physical Communication, 9, 193-198.

.

[85] E. Hossain and V. K. Bhargava, ”Cognitive Wireless Communication Networks”, NewYork , Springer Science Business Media, LCC, 2007.

[86] J. Shen, S. Liu, R. Zhang and Y. Liu, ”Soft versus Hard Cooperative Energy Detection under Low SNR”, *CHINACOM*, 2008.

[87] A. Ghasemi and S. Sousa, ”Opportunistic Spectrum Access in Fading Channels Through Collaborative Sensing”, *Journal of Communications*, vol. 2, no. 2, pp. 71-82, March 2007.

[88] S. Cui, A. Goldsmith, and A. Bahai, ”Energy-efficiency of MIMO and Cooperative MIMO Techniques in Sensor Networks”, *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 6, pp. 1089-1098, 2004.

[89] Y. Chen, Optimum Number of Secondary Users in Collaborative Spectrum Sensing Considering Resources Usage Efficiency, IEEE Communication Letters, vol.12 (12), December 2012.

[90] S. Wu, M. Zhao and J. Zhu, Optimal Number of Secondary Users through Maximizing Utility in Cooperative Spectrum Sensing, IEEE VTC-Fall 2009, September 2009.

[91] Y.C. Liang, Y. Zeng, E. Peh, and A.T. Hoang, Sensing-Throughput Tradeoff for Cognitive Radio Networks, IEEE ICC, June 2007.

[92] G. J. Foschini, Private conversation, AT&T Labs-Research, May 2007.

[93] P.C. Pinto and M.Z. Win, Communication in a Poisson Field of InterferersPart I: Interference Distribution and Error Probability, IEEE Transactions on Wireless Communications, vol. 9 (7), July 2010, pp. 2176-2186.

[94] W. Zhang, and Ch.K. Yeo, Joint iterative algorithm for optimal cooperative spectrum sensing in cognitive radio networks, Computer Communications 36 (2012) 80-89.

[95] T.J. Osler, Leibniz rule for fractional derivatives generalized and an application to infinite series, SIAM Journal on Applied Mathematics, 18.3 (1970): 658-674.

[96] L.R. Burden and J.D. Faires. Numerical analysis PWS. (1989).

[97] B. Chen, R. Jiang, T. Kasetkasem, and P.K. Varshney, "Channel aware decision fusion in wireless sensor networks," *IEEE Transactions on Signal Processing,* vol. 52, no.12, pp.3454-3458, 2004.

[98] P. K. Varshney, *Distributed detection and data fusion*, New York: Springer-Verlag, 1997.

[99] Y. Wang, C. Feng, Z. Zeng and C. Guo,"A Robust and Energy Efficient Cooperative Spectrum Sensing Scheme in Cognitive Radio Networks", *IEEE 11th International Conference on Advanced Communication Technology ICACT*, Gangwon-Do Korea, February 2009.

[100] S. Maleki, A. Pandharipande and G. Leus,"Energy-efficient spectrum sensing for cognitive sensor networks", *IEEE 35th Annual Conference of Industrial Electronics IECON,* Porto Portugal, November 2009.

[101] R. Deng, J. Chen, C. Yuen, P. Cheng and Y. Sun, "Energy-Efficient Cooperative Spectrum Sensing by Optimal Scheduling in Sensor-Aided Cognitive Radio Networks", *IEEE Transactions on Vehicular Technology,* vol. 61, no. 2, February 2012.

[102] R.M. Gray and D.L. Neuhoff, "Quantization, *IEEE Transactions on Information Theory* , vol. 44, no. 6, pp. 2325-2383, October 1998.

[103] J. Buhmann, H. Kuhnel, "Vector quantization with complexity costs", *IEEE Transactions on Information Theory,* vol.39, no.4, pp.1133,1145, Jul 1993.

[104] R. Viswanathan and P. K. Varshney, "Distributed detection with multiple sensors I. Fundamentals", *Proceedings of the IEEE*, vol. 85, no. 1, pp. 54-63, January 1997.

[105] W. Zhang, R. K. Mallik, and K. B. Letaief, "Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks, *IEEE Trans. on Wireless Comm.*, vol. 8, no. 8, pp. 5761-5766, December 2009.

[106] S. Maleki, A. Pandharipande, G. Leus, "Optimal Hard Fusion Strategies for Cognitive Radio Networks", *IEEE WCNC*, Cancum-Mexico, 2011.

[107] C. You, J. Lee, J. Kim, and J. Heo, "Efficient Cooperative Spectrum Sensing for Wi-Fi on TV Spectrum", *IEEE ICCE*, Las Vegas-USA, January 2011.

[108] M Di Renzo, L Imbriglio, F Graziosi, F Santucci, "Distributed data fusion

over correlated log-normal sensing and reporting channels: Application to cognitive radio networks", *IEEE Trans, on Wireless Comm.*, vol. 8, no. 12, pp. 5813-5821.

[109] W. Feller, An Introduction to Probability Theory and its Application. vol. 1, New York: Willey, 1950.

[110] R. Chen, J.M. Park, Y.T. Hou and J.H. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks", *IEEE Communications Magazine*, vol. 46, no. 4, pp. 50-55, April 2008.

[111] A.G. Fragkiadakis, E.Z. Tragos, I.G. Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks", *IEEE Comm. Surveys and Tutorials*, vol. 15, no.1, 2013.

[112] Penna, F.; Yifan Sun; Dolecek, L.; Cabric, D., "Detecting and Counteracting Statistical Attacks in Cooperative Spectrum Sensing," Signal Processing, IEEE Transactions on , vol.60, no.4, pp.1806,1822, April 2012.

[113] Wassim El-Hajj, Haidar Safa, Mohsen Guizani, " Survey of Security issues in Cognitive Radio Networks",

[114] A. Sethi, and T.X. Brown. "Hammer model threat assessment of cognitive radio denial of service attacks." *New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on. IEEE*, 2008.

[115] Vartiainen, Johanna. "Always one/zero malicious user detection in cooperative sensing using the FCME method." Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM), 2012 7th International ICST Conference on. IEEE, 2012.

[116] Linjun Lu, Soo-Young Chang et al., Technology Proposal Clarifications for IEEE 802.22 WRAN Systems, IEEE 802.22 WG on WRANs, March, 2006.

[117] Joerg Hillenbrand, Timo Weiss and Friedrich K. Jondral, Calculation of Detection and False Alarm Probabilities in Spectrum Pooling Systems, IEEE Communication Letters, Vol.9, No.4, 2005, pp.349-351.

[118] A.S. Rawat, P. Anand, C. Hao and P.K. Varshney, "Collaborative Spectrum Sensing in the Presence of Byzantine Attacks in Cognitive Radio Networks," *IEEE Transactions on Signal Processing,* vol.59, no.2, pp.774,786, Feb. 2011.

[119] W. Wang, H. Li, Y. Sun and Z. Han, “Attack-proof collaborative spectrum sensing in cognitive radio networks”, *Annual Conference on Information Sciences and Systems*, March-2009.

[120] A.W. Min, K.G. Shin, and X. Hu, “Secure Cooperative Sensing in IEEE 802.22 WRANs Using Shadow Fading Correlation” *IEEE Transactions on Mobile Computing*, vol. 10, no. 10, pp. 1434-1447, October-2011.

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

[122] W. Wang, H. Li, Y. Sun and Z. Han, “Attack-proof collaborative spectrum sensing in cognitive radio networks”, *43rd Annual CISS*, March-2009. pp. 130-134.

[123] Lingjie Duan; Min, A.W.; Jianwei Huang; Shin, K.G., “Attack Prevention for Collaborative Spectrum Sensing in Cognitive Radio Networks,” Selected Areas in Communications, IEEE Journal on , vol.30, no.9, pp.1658,1665, October 2012

[124] Rui Zhang; Ying-Chang Liang; Shuguang Cui, ”Dynamic Resource Allocation in Cognitive Radio Networks,” Signal Processing Magazine, IEEE , vol.27, no.3, pp.102,114, May 2010

[125] Attar, Alireza, et al. ”A survey of security challenges in cognitive radio networks: Solutions and future research directions.” Proceedings of the IEEE 100.12 (2012): 3172-3186.

[126] Stevenson, C.; Chouinard, G.; Zhongding Lei; Wendong Hu; Shellhammer, S.J.; Caldwell, W., ”IEEE 802.22: The first cognitive radio wireless regional area network standard,” Communications Magazine, IEEE , vol.47, no.1, pp.130,138, January 2009.

[127] Praveen Kaligineedi, Majid Khabbazian and Vijay K. Bhargava, “Secure Cooperative Sensing Techniques for Cognitive Radio Systems, IEEE International Conference on Communications 2008 (ICC 08), Beijing, China, May, 2008, pp.3406-3410.

[128] L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem, ACM Transactions on Programming Languages and Systems, vol. 4, no. 3, p. 382401, July 1982.

[129] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks, in IEEE INFOCOM, Apr. 2008, pp. 1876 1884.

[130] Akyildiz, I.F.; Won-Yeol Lee; Vuran, Mehmet C.; Mohanty, S., "A survey on spectrum management in cognitive radio networks," Communications Magazine, IEEE , vol.46, no.4, pp.40,48, April 2008

[131] Weijia Han; Jiandong Li; Zhi Tian; Yan Zhang, "Efficient Cooperative Spectrum Sensing with Minimum Overhead in Cognitive Radio," Wireless Communications, IEEE Transactions on , vol.9, no.10, pp.3006,3011, October 2010

[132] Peh, E.; Ying-Chang Liang, "Optimization for Cooperative Sensing in Cognitive Radio Networks," Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE , vol., no., pp.27,32, 11-15 March 2007.

[133] Saad, W.; Zhu Han; Rong Zheng; Hjorungnes, A.; Basar, T.; Poor, H.V., "Coalitional Games in Partition Form for Joint Spectrum Sensing and Access in Cognitive Radio Networks," Selected Topics in Signal Processing, IEEE Journal of , vol.6, no.2, pp.195,209, April 2012.

[134] Gelabert, X.; Sallent, O.; Perez-Romero, J.; Agusti, R., "Flexible Spectrum Access for Opportunistic Secondary Operation in Cognitive Radio Networks," Communications, IEEE Transactions on , vol.59, no.10, pp.2659,2664, October 2011

[135] J.J. Schiller, R.A. Srinivasan and M.R. Spiegel, Schaum's Outline of Probability and Statistics. New York, NY: McGraw-Hill, 2008.

[136] Yan, Qiben, et al. "Vulnerability and protection for distributed consensus-based spectrum sensing in cognitive radio networks." *IEE INFOCOM,* 2012.

[137] CFRG Working Group, "VMAC: Message Authentication Code using Universal Hashing", Retrieved 16 March 2010.

[138] C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010.

[139] Blunk L.l, "RFC 2284: PPP Extensible Authentication Protocol (EAP)", 1998.

[140] , Li Zhu and Huaqing Mao, "Research on Authentication Mechanism

of Cognitive Radio Networks Based on Certification Authority”, *International Conference on Computational Intelligence and Software Engineering (CiSE)*, December-2010.