

Robust Distributed Spectrum Sensing in Cognitive Radio Networks

Ruiliang Chen, Jung-Min Park, and Kaigui Bian
Bradley Department of Electrical and Computer Engineering
Virginia Polytechnic Institute and State University
Blacksburg, VA, USA
{rlchen, jungmin, kgbian}@vt.edu

Abstract—Cognitive radio is an enabling technology for efficient utilization of radio spectrum. A key function of cognitive radios is spectrum sensing, which enables secondary users to identify vacant spectrum not used by primary users (a.k.a. spectrum “white spaces”). Although spectrum sensing is one of the essential functionalities of cognitive radios, its security-related problems have not been studied. In this paper, we consider a cognitive radio network that employs a distributed spectrum sensing framework. Under this framework, we associate a secondary user terminal reporting false spectrum sensing information with a terminal experiencing Byzantine failure. To enhance the robustness of distributed spectrum sensing against such terminals, we propose a scheme called weighted sequential probability ratio test (WSPRT). Analysis and simulation results show that WSPRT can guarantee the accuracy of sensing results even when a considerable number of secondary users are reporting false sensing information.

Index Terms—Byzantine failure, cognitive radio, spectrum sensing, weighted sequential probability ratio test.

I. INTRODUCTION

The tremendous success and growth of wireless applications operating in unlicensed bands have led to the overcrowding of these bands. Meanwhile, studies have shown that licensed spectrum is underutilized. For instance, one study has shown that only 5.2% of the radio spectrum below 3GHz is in use at any given time on average. Even in populous areas such as Washington DC, where both government and commercial spectrum usage is intensive, less than 35% of the radio spectrum below 3GHz was found to be used [2].

The need to meet the spectrum demands of emerging wireless applications and the need to better utilize spectrum has led the Federal Communication Commission (FCC) to revisit the problem of spectrum management. In the conventional spectrum management paradigm, most of the spectrum is allocated to licensed users for exclusive use. It has been proposed to allow unlicensed radios to operate in licensed spectrum,

provided no harmful interference is experienced by incumbent services. In this way, a licensed user (a.k.a. primary user) can share its spectrum with unlicensed users (a.k.a. secondary users), thereby increasing the efficiency of spectrum utilization. This method of sharing is often called Opportunistic Spectrum Sharing (OSS).

Cognitive Radios (CRs) [5] are seen as the enabling technology for OSS. A CR should be able to scan through the spectrum bands and find vacant bands to operate in. To avoid interfering with primary users, a CR needs to carry out accurate spectrum sensing.

Recently, the problem of spectrum sensing has attracted a lot of attention from the research community. In [1, 7], the authors discuss physical-layer power measurement issues in the context of spectrum sensing. Other works [3, 6, 11, 14] investigate techniques for cooperative spectrum sensing to overcome the problems caused by multipath fading and shadow loss. In [4, 9, 15], MAC protocols for CR networks are proposed. Although there is a significant body of research on spectrum sensing, there is very little, if any, research that addresses the security problems related to spectrum sensing.

In this paper, we are primarily interested in the security problems related to spectrum sensing. Specifically, we focus on robust spectrum sensing. Considering the limitation of collocated architecture for spectrum sensing [11], we adopt a distributed spectrum sensing architecture. Under this architecture, we associate a secondary user terminal reporting false spectrum sensing information as a terminal experiencing Byzantine failure. We propose a scheme that uses the weighted sequential probability ratio test (WSPRT) to make a relatively accurate sensing decision in spite of such Byzantine failure. We compared our approach with other distributed spectrum sensing schemes. Our simulation results show that WSPRT outperforms the other schemes that were considered. In our particular simulation environment, WSPRT can achieve a correct sensing ratio of over 95% when 20%

of the users are misbehaving (i.e., reporting false sensing information).

The rest of the paper is arranged as follows. Section II describes the problem model. Our proposed solution, WSPRT, is detailed in Section III. We provide simulation results in Section IV. An overview of related research is given in Section V and we conclude the paper in Section VI.

II. PROBLEM MODELING

The primary user network may be a TV broadcast network, a cellular network, or some other licensed user network that is open to OSS. The secondary users are mobile devices communicating with each other in a multi-hop manner, composing a mobile ad hoc network, which we refer to as a *CR network*. A mobile device typically has a maximum transmitter output power on the order of a few hundred milliwatts, which corresponds to a transmission range of a few hundred meters.

In a multi-hop CR network, correct spectrum sensing is crucial. Inaccurate sensing may cause either interference to primary user communications or spectrum under-utilization. It has been shown that because of the hidden terminal problem and signal fading in a wireless environment, it is difficult for a secondary user to acquire accurate spectrum measurements on its own. Instead, it should learn sensing information from other secondary users in the neighborhood and integrate all data to make a correct decision [11]. The sensing information can be exchanged in a common control channel shared by all users—although there is no established standard yet, the existence of a common control channel is a characteristic shared by most of the MAC protocols proposed for CR networks [4, 9, 15].

However, due to Byzantine failures, such as device malfunction or attacks, a neighboring secondary user may send wrong sensing information. This might severely obstruct correct spectrum sensing. For example, a conservative method is to decide a spectrum to be busy whenever there is at least one neighboring user reporting that the spectrum is in use. If there is an attacker who constantly reports the spectrum being in use, then a spectrum opportunity will never be identified, causing severe under-utilization. For alternative methods, there are other failures that might cause miss detection of primary user, resulting in interference with its communication. It is therefore a practical but challenging problem to make a correct decision in spite of such Byzantine failures.

As the first step toward the solution to the problem, we model it into a parallel fusion network as Fig. 1

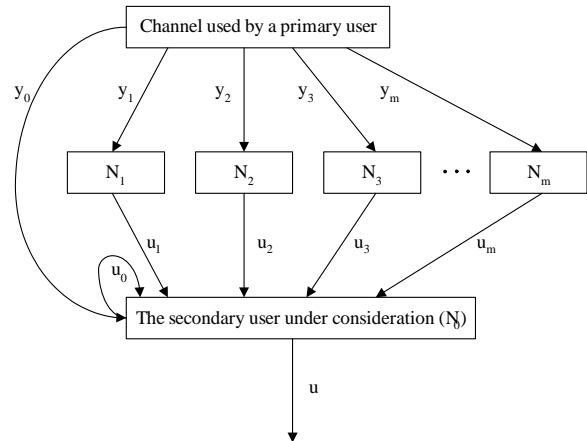


Fig. 1. A parallel fusion network model for spectrum sensing.

shows. (For more information about parallel fusion network, please refer to [12].) In this figure, N_i denotes a neighbor of a secondary user under consideration (denoted as N_0), y_i represents the channel usage information received at N_i , and u_i is the sensing information N_i updates to N_0 ($i = 0, 1, 2, \dots, m$, where m is the number of neighboring secondary users of N_0). In practice, both y_i and u_i represent the power level received at the considered channel, but y_i is an observed analog value while u_i is quantized from y_i . It depends on actual application how many bits are used to quantize the value. For example, if the communication overhead between N_i and N_0 is a major concern, u_i might only have one bit. User N_0 executes a data fusion process to make a final decision u , which is a binary variable meaning that a primary user is detected when it is one and that there is no primary user when it is zero. In the model, N_0 is both a sensor and a fusion center. We assume that not only y_i can differ from y_j ($0 \leq i, j \leq m, i \neq j$), but also u_i may not be consistent with y_i . The former is due to signal fading or noise in wireless networks, and the latter results from malfunction or misbehavior of a neighboring secondary user.

In such a model, there are several candidate techniques that can potentially be used to make a quality decision on u . These are:

- Decision fusion [8]: Taking u_i as a binary variable (i.e., a local decision made by N_i), this technique calculates u as the result of a logical operation on u_i 's. The logical operation, a.k.a. fusion rule, can be “AND”, “OR” or “Majority”. More details about these rules are discussed in Section IV.
- Bayesian Detection [12]: This technique requires the knowledge of a priori probabilities of u_i 's when u is zero or one. It associates a cost with each decision situation, i.e., any of the four situations when u is

decided as 1/0 when u is actually 1/0. The total cost can be minimized using Bayesian Detection.

- Neyman-Pearson Test [12]: This technique does not rely on the knowledge of any cost associated with each decision situation. It requires that the maximum acceptable probability of false alarm (i.e., u is decided as one when it is actually zero) be defined. Neyman-Pearson Test guarantees that the probability of miss detection (i.e., u is decided as zero when it is actually one) is minimized while the false alarm probability remains acceptable.
- Sequential Test [12]: All previously mentioned techniques are based on a fixed number of observation samples. Sequential Test, or Sequential Probability Ratio Test (SPRT), however, takes variable number of observation samples as inputs based on need. Given the knowledge of a priori probabilities of u_i 's when u is zero or one and given the maximum acceptable false alarm probability and miss detection probability, SPRT minimizes the number of observations.

Among these options, we prefer the Sequential Test for two reasons. First, the value of m and the number of observations can vary in our problem, which is only supported by Sequential Test. Second, SPRT has the preferred property of both bounded false alarm probability and bounded miss detection probability. However, two factors hinder a direct application of SPRT to our specific problem. Firstly, we need somehow obtain the required a priori probability of u_i 's, which is not readily known. Secondly, SPRT assumes identical probability distribution for all observations. Nevertheless, in our problem the neighboring secondary users that are undergoing Byzantine failures may behave differently. In the next section, we describe our solution, WSPRT, which addresses both problems.

III. WEIGHTED SEQUENTIAL PROBABILITY RATIO TEST (WSPRT)

We begin with the representation of a priori probabilities of u_i 's. Because u_i is a quantized value, u_i has a discrete probability mass function (pmf). If we use "0" to denote the event that a sensing result is clear and "1" to show that a primary user in the considered channel is sensed, then when the primary user is indeed active, we denote u_i 's pmf as f_{1i} , and when it is not, its pmf is assumed to be f_{0i} . Whether a primary user is indeed active in a channel can be decided by utilizing the result of WSPRT, whose detail will be described later in this section.

Assume that f_{0i} and f_{1i} are given, and that N_0 assigns a weight, w_i , to each u_i . The weight is calculated as

follows. Assume $f_{0i}(j) = a_j$ and $f_{1i}(j) = b_j$, where

$$j = 0, \dots, t-1, \sum_{j=1}^t a_j = 1, \sum_{j=1}^t b_j = 1, \text{ and } t \text{ is the}$$

maximum number of quantized power levels that any u_i may contain. User N_0 assigns the same values of a_j 's and b_j 's for all u_i 's. How to get the values of a_j 's and b_j 's will be discussed later. Initially, every w_i is set to 1. After each decision process is finished (i.e., a WSPRT produces a result u), N_0 updates w_i in two steps:

$$1) \ w_i \Leftarrow \begin{cases} w_i / C_{00} & \text{if } (u = 0, f_{0i}(u_i) \geq 1/t) \\ C_{01} w_i & \text{if } (u = 0, f_{0i}(u_i) < 1/t) \\ C_{10} w_i & \text{if } (u = 1, f_{1i}(u_i) < 1/t) \\ w_i / C_{11} & \text{if } (u = 1, f_{1i}(u_i) \geq 1/t) \end{cases}, \text{ and}$$

$$2) \ w_i \Leftarrow w_i / \max_i w_i.$$

Here C_{xy} ($x = 0, 1; y = 0, 1$) is a non-zero scaling factor used to update w_i when u is x while N_i 's report favors y . The values of C_{xy} are calculated as follows. If we define E_{xy} as:

$$\begin{cases} E_{00} = E\{a_j : a_j \geq 1/t\} \\ E_{01} = E\{a_j : a_j < 1/t\} \\ E_{10} = E\{b_j : b_j < 1/t\} \\ E_{11} = E\{b_j : b_j \geq 1/t\} \end{cases},$$

where E represents the mathematical expectation of a set, then we calculate C_{xy} as:

$$\begin{cases} C_{00} = E_{00} / (E_{00} + E_{01}) \\ C_{01} = E_{01} / (E_{00} + E_{01}) \\ C_{10} = E_{10} / (E_{10} + E_{11}) \\ C_{11} = E_{11} / (E_{10} + E_{11}) \end{cases}.$$

We calculate w_i in this way because we require it to have two properties. First, w_i is kept within the range from zero to one, which is guaranteed by the normalization operation in step 2). Second, we want to increase the weight of N_i when its report is consistent with u while decreasing its weight otherwise. In addition, because $C_{00} \geq C_{01}$ and $C_{11} \geq C_{10}$ (which is obvious since $E_{00} \geq E_{01}$ and $E_{11} \geq E_{10}$), the weight increase is expected to be slower than the weight decrease. This implies that to avoid the value of w_i from getting smaller, user N_i must send correct information

¹ Note in the extreme case when $\{a_j : a_j < 1/t\}$ or $\{b_j : b_j < 1/t\}$ is an empty set, we set $E_{01} = E_{00}$ or $E_{10} = E_{11}$.

(i.e., $f_{u_i}(u_i) \geq 1/t$) more often than send false information (i.e., $f_{u_i}(u_i) < 1/t$).

Maintaining the weight has two purposes. First, if N_i is subject to certain Byzantine failure and frequently sends its report inconsistent with the final decision, its weight is likely to decrease. Then if w_i is lower than a specific threshold, we can identify N_i as a malfunctioning user. Second, the weight decides how much a report may contribute to the final decision. This is reasonable since if the report from a neighboring secondary user tends to be incorrect, it should be counted less in a final decision. This logic is reflected by our WSPRT process. A conventional SPRT method uses the likelihood ratio as the decision variable [12]:

$$S_n = \frac{f_1(u_1, \dots, u_n)}{f_0(u_1, \dots, u_n)} = \prod_{i=1}^n \frac{f_1(u_i)}{f_0(u_i)}$$

where f_u ($u = 0, 1$) is the probability density function (pdf) of random variable u under hypothesis H_u and all observations u_1, \dots, u_n are with the same pdfs. The variable n refers to the number of observations.

In our WSPRT, we modify the decision variable into:

$$S_n = \prod_{i=0}^{n-1} \left(\frac{f_{1i}(u_i)}{f_{0i}(u_i)} \right)^{w_i}$$

In this context, H_0 denotes the hypothesis that a channel is clear and H_1 means the hypothesis that a channel is in use. Here n is not necessarily no greater than m . When n is greater than m , it means that some N_i 's may report multiple independent sensing results. In that case, the variable i in " f_{1i} ", " f_{0i} ", and " w_i " actually means $(i \bmod (m+1))$, and u_i means $(\lfloor i/(m+1) \rfloor + 1)$ -th report that N_0

takes from N_i . It can be easily seen that when $w_i = 1$, WSPRT degenerates to conventional SPRT. It can also be seen that when w_i approaches to 0,

$(f_{1i}(u_i)/f_{0i}(u_i))^{w_i}$ approaches 1, in which case u_i

barely changes S_n . The decision is taken based on the criteria:

$$\begin{cases} S_n \geq \eta_1 \Rightarrow \text{accept } H_1, \\ S_n \leq \eta_0 \Rightarrow \text{accept } H_0, \\ \eta_1 < S_n < \eta_0 \Rightarrow \text{take another observation.} \end{cases}$$

It can be proved that the values of η_1 and η_0 are decided by

$$\eta_1 = \frac{1-P_{10}}{P_{01}} \text{ and } \eta_0 = \frac{P_{10}}{1-P_{01}},$$

where P_{01} and P_{10} are the tolerated false alarm

probability and the tolerated miss detection probability, respectively.

We can also calculate that the expected values of n 's to accept hypothesis H_1 and H_0 are

$$E[n | H_1] = \frac{(1-P_{10}) \log \eta_1 + P_{10} \log \eta_0}{E[w_i] E[\log \frac{f_{1i}(u_i)}{f_{0i}(u_i)} | H_1]} \quad (3)$$

and

$$E[n | H_0] = \frac{P_{01} \log \eta_1 + (1-P_{01}) \log \eta_0}{E[w_i] E[\log \frac{f_{1i}(u_i)}{f_{0i}(u_i)} | H_0]} \quad (4)$$

Due to the space limit, we do not present the derivation details of the above equations.

- Now, we need to determine the values for a_j 's and b_j 's. (1) Our strategy is to first predefine their values by approximate estimations. Then we use the result of WSPRT to feedback to the values so that they can be updated based on practical observations. To detail this approach, we define two arrays R_0 and R_1 , each of size t . Because u_i is a value representing a signal power level, it is reasonable to assume that the greater the value of u_i is, the stronger it supports H_1 ; in contrast, a smaller value of u_i tends to indicate H_0 . Based this assumption, (2) we initialize arrays R_0 and R_1 as $R_0(j) = t - j$ and $R_1(j) = j + 1$ ². The values of a_j and b_j are computed as

$$a_j = R_0(j) / \sum_{j=1}^t R_0(j) \text{ and } b_j = R_1(j) / \sum_{j=1}^t R_1(j).$$

After a WSPRT is finished and the result u is obtained, array R_u should be updated correspondingly. Specifically, for each u_i that is used for WSPRT, $R_u(u_i)$ is increased by one. In this way, past experience is used for future decisions.

IV. SIMULATIONS

We carried out initial simulations to test the effectiveness of WSPRT. In the simulation, 500 secondary users are randomly located in a 2000m \times 2000m square, each with a transmission range of 250m. There are two TV towers. Each TV tower has one TV channel, which is used to broadcast TV signals at a probability of 0.2. The locations of the two towers are shown in Fig. 2. The tower that is further away from the square has a transmission radius of 9000m and the other tower has a transmission radius of 6000m. Out of all 500 secondary users, we vary the number of attackers from 1 to 100. A normal user can correctly report 70% of spectrum sensing results to its neighbors, while an

² If there is experience data to load into R_0 and R_1 , then this initialization process is not necessary.

attacker always reports the opposite results and thus has 30% correctness. Each secondary user moves with a random waypoint model, which repeats the following four steps:

- 1) It randomly chooses a destination in the area with a uniform distribution;
- 2) It chooses a velocity v that is uniformly distributed over $[0, v_{max}]$;
- 3) It moves along the straight line from its current position to the destination with the velocity v until it arrives; and
- 4) It pauses in the destination for a random period that is uniformly distributed over $[0, tp_{max}]$.

We adopt $v_{max} = 10\text{m/s}$ and the $tp_{max} = 60\text{s}$. Every node periodically carries out spectrum sensing for each channel every 30 seconds. The simulation spans a one-hour period.

To demonstrate the effectiveness of WSPRT, we compared it with several other schemes. We use $t = 2$ in the simulation to facilitate the comparison, because decision fusion schemes do not support $t > 2$. The schemes to be compared include:

- Decision fusion with “OR rule”:

$$u = u_0 \vee u_1 \vee \dots \vee u_m.$$

- Decision fusion with “AND rule”:

$$u = u_0 \wedge u_1 \wedge \dots \wedge u_m.$$

- Decision fusion with “Majority rule”:

$$u = \begin{cases} 0 & \text{if } \sum_{i=0}^m u_i < (m+1)/2 \\ 1 & \text{if } \sum_{i=0}^m u_i > (m+1)/2 \\ u_0 & \text{if } \sum_{i=0}^m u_i = (m+1)/2 \end{cases}.$$

- SPRT: The same procedure is used as WSPRT (including the way to get a priori probabilities) except that the value of all w_i 's are set to one for the entire simulation duration.

In the simulation, we use $P_{10} = 0.001$ and $P_{01} = 0.01$ for both SPRT and WSPRT. Figs. 3–5 show the simulation results of miss detection ratio, false alarm ratio, and correct sensing ratio respectively. The three ratios add up to one. A correct sensing instance occurs when the result of spectrum sensing is true. As the figures show, the “OR rule” scheme has the least miss detection ratio since it senses spectrum most conservatively and causes the largest false alarm ratio. The “AND rule” sacrifices miss detection ratio in order to minimize false alarm ratio. Among the schemes compared, WSPRT achieves the best balance between both factors, thereby leading to the maximum overall correct sensing ratio, which is over 95% when 100 attackers are in place. The weight values play a key role

in sensing performance. This is evident when we compare WSPRT with SPRT—in the 100-attacker case, incorrect sensing ratio is reduced from 20% to 5%.

The better performance of WSPRT comes at the expense of more spectrum sensing attempts. In our simulations, we observed that SPRT requires the collection of 0.68 to 1.15 independent sensing results from each neighboring user and WSPRT requires the collection of 3.26 to 5.72 results. This cost may be considered reasonable when reliability of spectrum sensing is a primary concern.

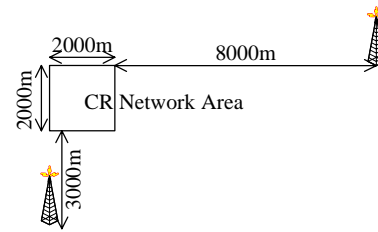


Fig. 2. Simulation layout.

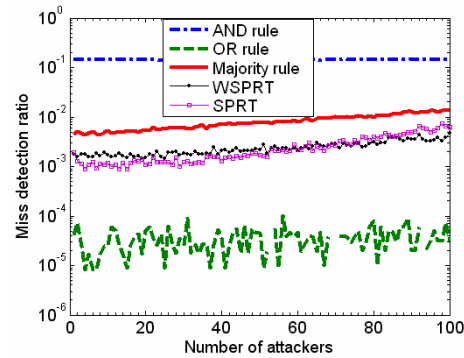


Fig. 3. Miss detection ratio of five schemes.

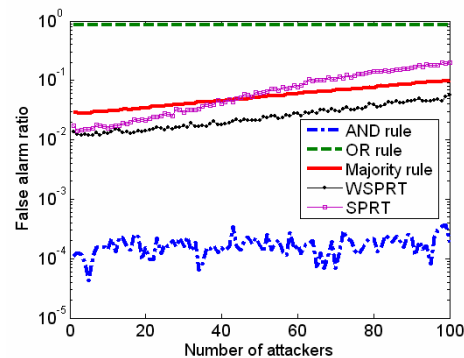


Fig. 4. False alarm ratio of five schemes.

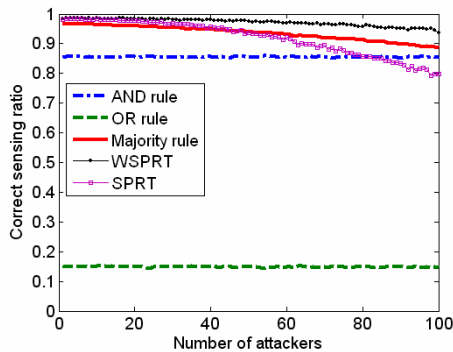


Fig. 5. Correct sensing ratio of five schemes.

V. RELATED RESEARCH

CR related research has received great attention recently. Because its dynamic spectrum access is fundamentally different from conventional wireless systems, there is a need to design different components in the protocol stack.

The physical layer requires most fundamental change. A major research problem is how to correctly detect the existence of primary users and spectrum opportunities. In [1], Challapali et. al proposes to use Hough Transform and autocorrelation function to detect spectrum opportunities. A more direct approach was presented in [7] to observe primary user's signal-to-noise ratio (SNR) and entropy for seeking spectrum opportunities. A spectrum opportunity is recognized only when a spectrum has both low SNR and low entropy. According to [11], these schemes belong to collocated sensing architectures, since a single secondary user device carries on the spectrum sensing task and makes an independent decision to access a spectrum. However, due to the hidden-terminal problem, such a scheme may show poor performance in terms of miss detection and false alarm probabilities. To address this problem, techniques for cooperative spectrum sensing was investigated in [3, 6, 11, 14]. In [3], the authors utilize the fact that noise is independent at different users while signals are correlated, so adding up the received signals at two secondary users can increase SNR and improve detection accuracy. A similar approach is used in [6] to increase detection sensitivity. The authors of [11, 14] employ sensors for distributed spectrum sensing. In [14], some sensors are placed close to primary receivers to detect their local oscillator leakage power, and then these sensors relay the detection information to secondary users. In [11], an independent sensor network is proposed to be deployed specially for spectrum sensing. All secondary users query the sensor network to learn the information about

spectrum opportunities.

In the link layer, CR related research mainly investigates new media access control (MAC) protocols to adapt to the dynamic change of spectrum opportunities. These protocols are more or less derived from conventional wireless MAC protocols. For example, DC-MAC [15] is a slotted MAC protocol similar to ALOHA but with an enhanced mechanism to optimize per-slot throughput; DOSS protocol [4] was derived from MAC protocols based on busy tone; and CR MAC protocol [9] generalizes 802.11 into supporting multiple channels.

There is less research on the network layer or layers above since the lower layers are still not well-defined for CR networks. However, there has been research that takes cross-layer approaches to optimize network or above layer objectives by defining MAC or physical layer behaviors [10, 13]. Although security is an important aspect of spectrum sensing, to the best of our knowledge, there is virtually no previous work that addresses this issue. In [6], the authors discuss the impact of malicious users on the required sensing sensitivity of individual terminals when cooperative spectrum sensing is performed. However, methods to ensure the robustness of spectrum sensing were not discussed.

VII. CONCLUSION

Although spectrum sensing is an essential functionality of cognitive radios, its security-related problems have not been studied previously. In this paper, we considered a cognitive radio network in a hostile environment that employs a distributed spectrum sensing framework. We formulated the problem of spectrum sensing as a parallel fusion network model that utilizes a weighted sequential probability ratio test (WSPRT). Our analysis and simulation results showed that our spectrum sensing framework can achieve a high level of performance even in a hostile environment. To the best of our knowledge, our work is the first to directly address the security issues of spectrum sensing in CR networks.

REFERENCES

- [1] K. Challapali, S. Mangold and Z. Zhong, "Spectrum agile radio: Detecting spectrum opportunities", *Proc. 6th Annual Int'l Symposium on Advanced Radio Technologies*, March 2004.
- [2] Federal Communications Commission, "Facilitating opportunities for flexible, efficient, and reliable spectrum use employing spectrum agile radio technologies," *ET Docket No. 03-108*, Dec. 2003.
- [3] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio networks," *Proc. DySPAN*, Nov. 2005, pp. 137-143.
- [4] L. Ma, X. Han, and C.-C. Shen, "Dynamic open spectrum

- sharing MAC protocol for wireless ad hoc networks," *Proc. DySPAN*, Nov. 2005, pp. 203–213.
- [5] J. Mitola, "Cognitive radio: an integrated agent architecture for software defined radio," *PhD Dissertation*, Royal Institute of Technology (KTH), Stockholm, Sweden, June 2000.
- [6] S. M. Mishra, A. Sahai, and R. Brodersen, "Cooperative sensing among cognitive radios," *unpublished paper*, available at: http://www.eecs.berkeley.edu/~sahai/Papers/ICC06_final.pdf.
- [7] M. P. Olivieri, G. Barnett, A. Lackpour, A. Davis, and P. Ngo, "A scalable dynamic spectrum allocation system with interference mitigation for teams of spectrally agile software defined radios," *Proc. DySPAN*, Nov. 2005, pp. 170–179.
- [8] A. Pandharipande, J.-M. Kim, D. Mazzaresse, and B. Ji, "IEEE P802.22 Wireless RANs: Technology Proposal Package for IEEE 802.22," Jan. 2006, available at: http://www.ieee802.org/22/Meeting_documents/2005_Nov/22-05-0099-00-0000_Samsung_Proposal_Outline.doc.
- [9] P. Pawelczak, R. V. Prasad, X. Liang Xia, and I. G. M. M. Niemegeers, "Cognitive radio emergency networks - requirements and design," *Proc. DySPAN*, Nov. 2005, pp. 601–606.
- [10] C. Peng, H. Zheng, and B.Y. Zhao, "Utilization and Fairness in Spectrum Assignment for Opportunistic Spectrum Access," *ACM Monet*, to appear.
- [11] S. Shankar N; C. Cordeiro, K. Challapali, "Spectrum agile radios: utilization and sensing architectures," *Proc. DySPAN*, Nov. 2005, pp. 160–169.
- [12] P. K. Varshney, *Distributed Detection and Data Fusion*, Springer-Verlag New York, 1997.
- [13] Q. Wang and H. Zheng, "Route and spectrum selection in dynamic spectrum networks," *Proc. CCNC*, Jan. 2006, pp. 625–629.
- [14] B. Wild, K. Ramchandran, "Detecting primary receivers for cognitive radio applications," *Proc. DySPAN*, Nov. 2005, pp. 124–130.
- [15] Q. Zhao, L. Tong, and A. Swami, "Decentralized cognitive mac for dynamic spectrum access," *Proc. DySPAN*, Nov. 2005, pp. 224–232.